En cuanto al acceso de la información se ha determinado usar el Control de Acceso Basado en Roles (en inglés Role–Based Access Control, RBAC); un modelo introducido por David Ferraiolo y Richard Kuhn [5] que desde el año 2001 ha incrementado su empleo por investigadores académicos [6]. Este mecanismo de acceso provee una forma más general de control de acceso mandatario que el modelo Bell–LaPadula [16], donde las decisiones de acceso no dependen de los nombres de los usuarios sino de las funciones que ellos están desempeñando actualmente dentro de la organización. El modelo RBAC trata con asuntos de integridad, así como de confidencialidad, permitiendo que los roles de los miembros (así como sus derechos) sean revisados cuando ciertos programas son invocados; adicionalmente, este diseño ha sido utilizado para el control de acceso sobre servidores Web, los cuales en su mayoría, utilizan las entidades individuales de los usuarios [7].

Para el servicio de no repudiación se incluyó en el modelo el uso de elementos de la infraestructura de clave pública (PKI), específicamente de la utilización de la autoridad certificadora.
En el diseño del modelo se empleó el método de desarrollo de software "Rational Unified Process" (RUP), el cual asegura la producción de un software de alta calidad [8] por ser iterativo e incremental. Este método permitió definir los requerimientos funcionales, los atributos y los casos de uso que proporcionaron el fundamento para los procesos de análisis y diseño. También se elaboró el modelo conceptual, los diagramas de secuencia y de colaboración [18]. En este artículo se discuten los casos de usos del servicio de publicación, la arquitectura del sistema y se especifican los procesos de dominio.

3. MODELO DE CASOS DE USO

En este parte del artículo se presenta el diagrama de casos de uso asociado al servicio de publicación, para ello, se provee una vista global de cómo trabajará el sistema que ayuda a entender su funcionamiento por completo [9]. Adicionalmente, se describen los procesos asociados al caso de uso y se explican los atributos identificados.
Los actores identificados que tendrán interacción con el sistema son: profesor, empleado y estudiante. Todos ellos se denominarán con el nombre de *usuario* y estarán en contacto con el sistema de seguridad, cuando quieran realizar operaciones de: Agregar, modificar, eliminar o consultar una página web. La Figura 1 muestra el diagrama de casos de uso correspondiente.

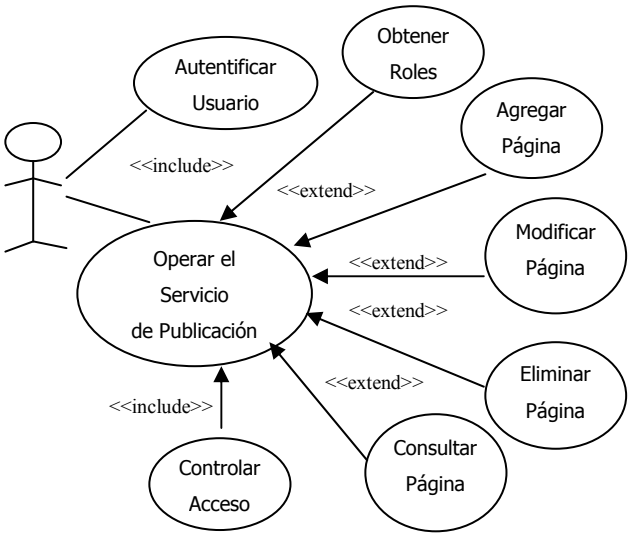

Figura 1. Diagrama de casos de uso

Descripción de los procesos

A continuación se describirán los procesos que constituyen el diagrama de caso de uso.

Autentificar usuario: Un usuario desea acceder al servicio de publicación, para ello el sistema a través de una secuencia de operaciones deberá verificar que el usuario es realmente quien señala ser.

Obtener Roles: Cuando un usuario desea ejecutar alguna de las operaciones del servicio de publicación, debe solicitar se le asigne el rol que le corresponde de acuerdo a sus funciones dentro de la institución.

Operar el Servicio de Publicación: En este proceso se requiere que al usuario se le haya asignado su rol correspondiente, lo cual le permitirá realizar algunas de las siguientes operaciones sobre la página web: agregar, modificar, eliminar o consultar. El sistema proporcionará al usuario una interfaz con las distintas opciones que le permitirá escoger una de las operaciones y posteriormente, ejecutar la acción deseada de acuerdo con el permiso correspondiente, que fue suministrado por el proceso de control de acceso que seguidamente se describe.

Controlar Acceso: Una vez que el rol haya seleccionado la opción deseada, el sistema deberá chequear el tipo de operación que ejecutará sobre la página web, de acuerdo a los permisos establecidos.

Agregar Página: El rol debidamente autentificado y autorizado podrá almacenar una página web en el dispositivo donde tiene acceso, luego, se indicará el resultado de la operación.

Modificar Página: El rol debidamente autentificado y autorizado podrá con esta opción, reemplazar la página web existente. Posteriormente el sistema le notificará el resultado de la operación.

Eliminar Página: El rol debidamente autentificado y autorizado podrá eliminar una página web en el dispositivo donde tiene acceso. Posteriormente el sistema le notificará el resultado de la operación.

Consultar Página: El rol debidamente autentificado y autorizado podrá consultar una página web del dispositivo

donde tiene acceso. Luego el sistema le notificará el resultado de la operación.

Atributos del Sistema

Los atributos del sistema especifican las características o dimensiones del mismo [9]. En este modelo se han identificado los atributos integridad, confidencialidad y no repudiación, los cuales representan tres de los requerimientos de seguridad que deben ser satisfechos. No obstante es importante mencionar que el resto de los requerimientos de seguridad que deben satisfacer el modelo están contemplados en el diagrama de casos de uso, como son el control de acceso y la autentificación. A continuación se explican los atributos:

Integridad: Garantiza que la información contenida en la página web no sea modificada por un rol no autorizado. Este requerimiento se garantizará cada vez que el usuario intente realizar una operación de agregar o modificar o durante el tránsito de la información a través de las facilidades de comunicación.

Confidencialidad: Garantiza que sólo usuarios debidamente autorizados podrán tener acceso a consultar una página web. Un rol sólo podrá tener acceso a una página web si a través del sistema se le ha otorgado el permiso correspondiente. Este requerimiento se garantizará cada vez que el usuario intente realizar una operación de consulta o cuando la información sea transferida por las facilidades de comunicación.

No repudiación: Garantiza que el rol que realice las operaciones de agregar o modificar sobre una página web no pueda negar haber ejecutado tal operación. Este requerimiento se alcanza a través de un esquema de registro de las operaciones.

4. OPERATIVIDAD POTENCIAL DEL MODELO INSTRUMENTADO

El modelo de seguridad propuesto para el servicio de publicación deberá ser instrumentado al final del desarrollo y ello obliga a que el diseñador conciba, en forma abstracta, una primera instrumentación del producto final que, sin encasillar la metodología de desarrollo, permita evidenciar las pautas de viabilidad operativa que ese producto tendrá. Una aproximación mental a una potencial instrumentación del desarrollo se muestra a través de la Figura 2 que seguidamente se presenta.

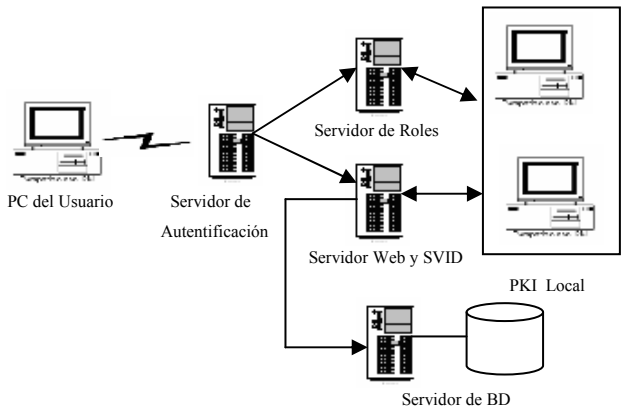

Figura 2. Elementos de la viabilidad instrumental de la concepción inicial del servicio de publicación

Los elementos que constituyen esta concepción se fundamentan en el uso de un computador personal que le permitirá al usuario acceder al servicio de publicación. El servicio de autentificación, que será ejecutado a través de un *servidor de autentificación*, el cual usará el mecanismo reto-respuesta. En este caso se requerirá de un elemento denominado "token", que estará representado inicialmente por un disco flexible –a modo de abaratar costes-, pero que podría terminar siendo una tarjeta inteligente. Ese elemento le será entregado a todo usuario de la intranet académica en el momento de incorporarlo a la misma y quedará bajo su supervisión personal. En ese disco, se almacenarán tanto la clave simétrica que permitirá al usuario ser autentificado, como su clave secreta que será utilizada en combinación con su clave pública. Si el proceso de autentificación fue exitoso el usuario deberá acceder al *servidor de roles*, para solicitar el rol que le corresponde. Una vez almacenado el rol del usuario en su computador personal, este podrá solicitar ejecutar una operación sobre el *servidor web*, el cual estará en comunicación con el servidor de base de datos donde se encuentran registradas la información de control de las páginas web, así como los permisos y regulaciones correspondientes. Otro elemento del modelo es parte de una *infraestructura de clave pública (PKI*), tradicional. Estas serán utilizadas para el manejo de certificados digitales.

5. DESCRIPCIÓN DEL MODELO DE SEGURIDAD

En esta sección se describirá el modelo de seguridad propuesto para el servicio de publicación, a través de la arquitectura del sistema y de la descripción de los procesos del servicio de publicación.

Arquitectura del Sistema

La arquitectura del sistema consta fundamentalmente de tres capas [10]: la capa de presentación representado por el módulo de control de interfaz, la capa de dominio representada por los módulos de control de seguridad, control de roles y operaciones del servicio de publicación y la capa de almacenamiento que incluye al sistema manejador de base de datos.

La capa de presentación involucra todo lo referente a las interfaces que permiten la interacción del usuario con el sistema, esto es la interfaz gráfica de usuario que en este caso se propone la construcción de un "browser" propio de la institución, para ser usado exclusivamente en los servicios de la intranet, específicamente en el servicio de publicación.

La capa de almacenamiento se refiere a todas las operaciones que pueden ejecutarse sobre la base de datos.

En cuanto a la capa de dominio se describen sus procesos, haciendo especial énfasis en la solución a los requerimientos de seguridad planteados. Esta explicación se hace a través del tratamiento de los módulos de control de la seguridad, de control de los roles y el de operaciones.

El módulo de control de seguridad se encargará de garantizar la autentificación del usuario ante la intranet; también aplica en la integridad y en la confidencialidad de la información en tránsito o una vez almacenada en disco. Regula también el control acceso sobre las páginas web, el servicio de no repudiación y finalmente incluye todos los chequeos de seguridad entre las

entidades de software que así lo requieran. *El módulo de control de roles* se encargará de que a cada usuario en la intranet le sea asignado el rol correspondiente de acuerdo a la función que desempeña en la institución. *El módulo de operaciones* del servicio de publicación se encargará de que se ejecuten las operaciones sobre las páginas ubicadas en los servidores web.

La Figura 3 describe en forma genérica la estructura y vinculación de cada componente principal de la arquitectura del sistema.

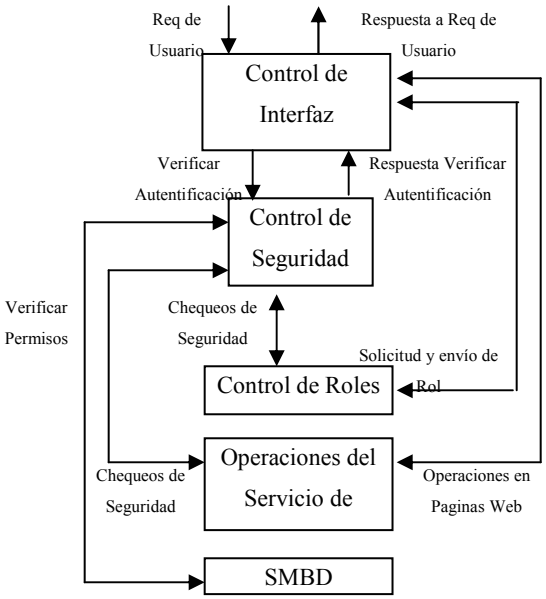

Figura 3. Arquitectura del sistema

Descripción de los Procesos del Servicio de Publicación

A continuación se describen cada uno de los procesos que están involucrados durante la utilización del servicio de publicación.

Proceso de autentificación

1.- El usuario inicia una solicitud de requerimiento al servidor de autentificación, a través del "browser" de la intranet académica. Cada "browser" instalado en el PC del usuario posee un código que está asociado unívocamente a dicho computador, a través de la dirección MAC de la tarjeta de red. Una vez establecida la sesión toda la comunicación será cifrada.

2.- El servidor de autentificación envía al computador del usuario una información solicitando que el mismo introduzca su número de identificación personal (PIN).

3.- El usuario introduce el PIN y posteriormente es enviado como respuesta al servidor de autentificación.

4.- En el servidor de autentificación se ejecuta un proceso que permitirá generar un número pseudo aleatorio (denominado "challenge") que será enviado al computador local del usuario y presentado a través de la interfaz gráfica.

5.- Posteriormente se le solicita al usuario que introduzca el "diskette" que contiene la clave personal simétrica que identifica al usuario y adicionalmente aparecerá otro "prompt" donde se le solicita al usuario que escriba la contraseña correspondiente a la clave personal simétrica y luego se le pedirá que introduzca el valor del "challenge" visualizado, con el objeto de que este sea cifrado. El producto resultante del cifrado es enviado por el "browser" al servidor de autentificación, quien en forma paralela ha estado ocupado extrayendo de la base de datos la clave personal simétrica asociada al PIN que recibió al inicio del proceso. Con esta clave el servidor ejecuta la misma operación de cifrado sobre la copia del "challenge" enviado al computador local del usuario.

6.- El servidor de autentificación al recibir la respuesta enviada por el "browser" en el paso anterior, procede a comparar el cifrado calculado en el computador local del usuario con el resultado de su propio cálculo. Si la comparación es falsa, entonces el servidor envía un mensaje de error al computador local del usuario, indicando que su autentificación no procede. Por el contrario si la comparación es exitosa se da entrada al usuario a la intranet. La Figura 4 muestra el flujo de comunicación entre el cliente y el servidor para el proceso de autentificación

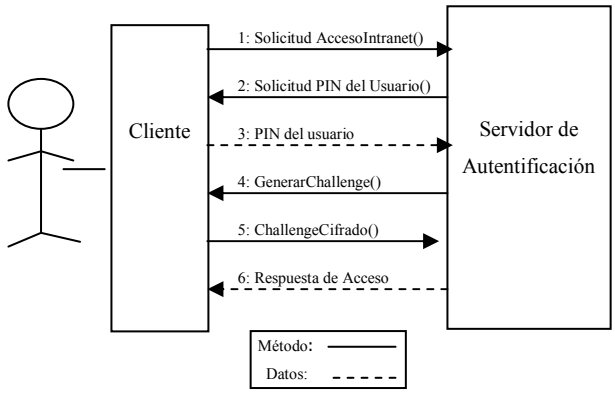

Figura 4. Autentificación del usuario

Proceso de acceso al servidor de roles

El usuario a través del "browser" solicita una conexión con el servidor de roles, con la finalidad de que su rol sea almacenado temporalmente en el disco duro de su computador personal.
Esta conexión se hace utilizando el protocolo Secure Sockets Layer (SSL) que permitirá ejecutar una autentificación mutua entre el "browser" y el servidor de roles; el cual se llevará a cabo a través de la verificación de los certificados de cada uno, que estarán disponibles en la autoridad certificadora (CA) dentro del sistema PKI local a la intranet. Si la autentificación falla en alguno de los dos extremos, se emite un mensaje de error indicando que la comunicación no puede establecerse por medidas de seguridad. Si por el contrario la autentificación resulta exitosa, el usuario oprimirá un botón del "browser" que le permitirá solicitar el rol correspondiente y así dar inicio a las operaciones que desea ejecutar.

Cuando el servidor de roles recibe el requerimiento envía un mensaje al computador local del usuario solicitando que introduzca su PIN, posteriormente el servidor lo busca en su base de datos y obtiene el rol correspondiente. Inmediatamente

se inicia un procedimiento de construcción de un "cookie" seguro que contendrá el nombre del usuario, el rol que le corresponde, la dirección IP de la PC donde se conecta y la firma digital del servidor de roles. Una vez construido el "cookie" se envía al PC del usuario para que sea almacenado en el disco duro. La Figura 5 muestra el flujo de comunicación.

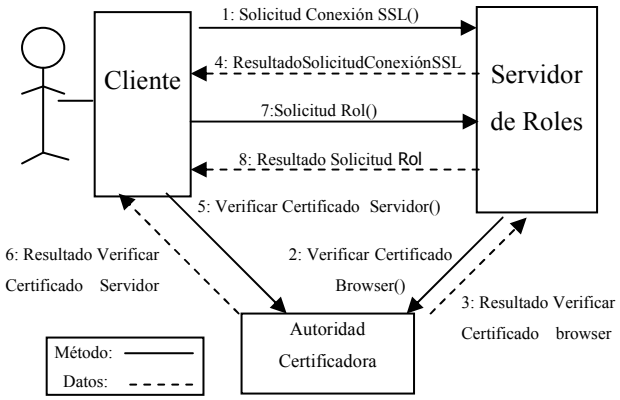

Figura 5. Acceso al servidor de roles

Proceso de acceso al servidor web

Cuando el usuario desea ejecutar alguna operación en cualquier servidor Web, oprime un botón en el "browser" que indica acceso a servidores Web; posteriormente el "browser" buscará el rol del usuario en el "cookie", y procede a consultar la base de datos para verificar sobre cuáles servidores web tiene acceso el rol del usuario solicitante. Luego se mostrará una interfase que indicará un listado de todos los servidores web.
Una vez seleccionado el servidor se realizará un procedimiento de autentificación mutua entre el cliente y el servidor web a través de SSL, con lo cual cada uno deberá acceder a los certificados del otro utilizando el sistema PKI.

Si la autentificación fue exitosa el cliente web envía el "cookie" al servidor, quien posteriormente autentificará que la dirección IP que contiene el "cookie" se corresponde con la computadora que está haciendo la solicitud. Luego el servidor web chequeará la integridad del "cookie" verificando la firma digital del servidor de roles que está contenida en el mismo, para ello utilizará el sistema PKI para acceder a la clave pública del servidor de roles. Si el "cookie" asociado a cada usuario es validado y verificado exitosamente el servidor web confiará en el rol del usuario y usará a este para el control de acceso sobre las páginas web o directorios.

Para realizar una operación sobre una página web en el computador que contiene el servidor, se mostrará una interfase que indicará las opciones que pueden ejecutarse sobre las páginas web, específicamente: agregar, modificar, eliminar o consultar. La Figura 6 ilustra la explicación.

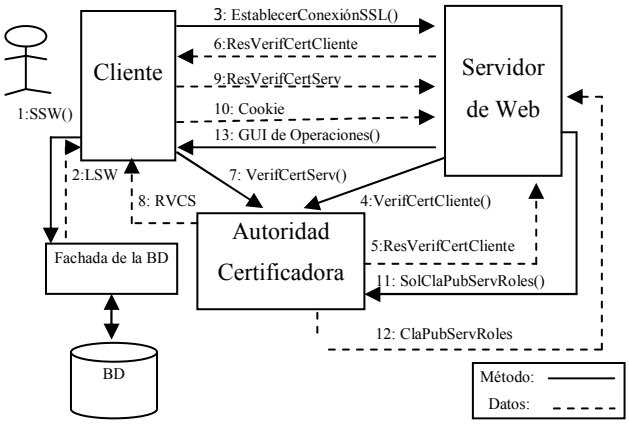

Figura 6. Acceso al servidor web

Proceso de agregar o modificar una página web

Si el usuario selecciona la opción agregar, el "browser" usa el rol para solicitar al servidor web una consulta sobre la base de datos de permisos, que arrojará como resultado un listado en pantalla de todos los directorios sobre los cuales tiene acceso el rol. Cuando el usuario seleccione el directorio, se mostrará automáticamente una caja de diálogo que le permitirá hacer la transferencia de la página web hacia el servidor web, pero antes de la transferencia el "browser" solicitará al usuario su firma digital, la cual será un archivo adicional producto de aplicar una función "hash" al contenido de la página que se va ha transferir. Para obtener la firma digital es necesario cifrar la salida de la función hash con la clave privada del rol que se encuentra almacenado en el "diskette", finalmente se adjuntará a la página web y será enviada. Posteriormente será almacenada y se debe registrar en la base de datos la operación ejecutada por el rol, así como la fecha y hora de la operación y el rol que la ejecutó.

En el servidor Web se encuentra el *Sistema de Verificación de Integridad de Datos* (SVID); este sistema se encargará de conectarse a la autoridad certificadora dentro de la estructura PKI para acceder a la clave pública del rol. Una vez obtenida la clave, el SVID procede a desencriptar la firma digital obteniendo la salida de la función hash aplicada sobre la página web, luego el SVID cifra esta salida con la clave privada del servidor web y se procede entonces a almacenar la página web con la firma digital del rol y la firma digital del servidor web en la base de datos.

Si durante el proceso de almacenamiento se encuentra que existe una página web con el mismo nombre, se emite un mensaje al usuario preguntando si desea reemplazar la página web actual, de ser negativa la respuesta se emite un mensaje indicando que la operación no se ejecutó, en caso contrario y al igual que cuando la página web no existe se almacenan todos los archivos y posteriormente se asignan los permisos de lectura y escritura asociados a este rol. Adicionalmente se registra en la base de datos, el tipo de operación ejecutada, la fecha, la hora, el rol que efectuó la operación y el nombre de la página que se agregó. Si la operación es culminada exitosamente se emite un mensaje indicando que la operación se ejecutó sin problemas y luego se retorna a la interfase que contiene las operaciones que puede seguir ejecutando el rol.

Proceso de eliminar una página web

Si el usuario selecciona la opción de eliminar, el cliente web usará el rol para solicitarle al servidor web una consulta a la base de datos de permisos sobre las páginas web que pueden ser eliminadas por este rol. El resultado de la consulta es un listado con todas las páginas web. Una vez seleccionadas las páginas que el rol desea eliminar, se oprime un botón en el "browser" que permitirá ejecutar la operación. Posteriormente se activa un proceso que comunicará esta información al servidor web; luego este último accede a la base de datos donde modifica un campo lógico asociado a cada página que se desea eliminar; esto indica que estas páginas han sido desactivadas temporalmente; es decir han sido eliminadas en forma lógica. Una vez aplicada esta operación se deben eliminar todos los permisos de la base de datos asociados a cada una de las páginas. Finalmente se debe registrar en la base de datos la operación ejecutada por el rol, así como la fecha y hora de la operación y el rol que la ejecutó.
Posteriormente y de acuerdo con la política de seguridad se establecerán procedimientos de mantenimiento que activará un proceso que eliminará aquellos registros físicos de la base de datos cuya fecha de desactivados haya alcanzado el tiempo máximo, conforme lo indique la política.

Proceso de consultar una página web

Si el usuario selecciona la opción consultar, el cliente web usa el rol para solicitar al servidor web una consulta a la base de datos de permisos de las páginas web que pueden ser consultadas por este rol. El resultado de la consulta es un listado con todos los URL´s de las páginas web que pueden ser consultadas. El usuario en su rol seleccionará la página deseada y podrá visualizar la información. Posteriormente se registrará en la base de datos el rol, la operación ejecutada, la fecha y la hora.

6. JUSTIFICACIÓN DE LAS TECNOLOGÍAS EMPLEADAS EN EL MODELO

Una cantidad de tecnologías de la seguridad ya existentes en el mercado se han incorporado en el desarrollo, con el objeto de reutilizar productos y herramientas ya comprobadas e instrumentadas. Se incrementa así la viabilidad técnica del desarrollo final.

El esquema de autentificación reto-respuesta instrumentado a través de un disco provee mejor confiabilidad que el clásico esquema de nombre y clave, a la vez que minimiza costes frente a los sistemas ya disponibles que resultan ser más sofisticados y en consecuencia de mayor valor. Adicionalmente con este mecanismo se garantiza una mayor seguridad frente a la posible pérdida de uno de los elementos de este proceso, por lo tanto, representa una alternativa viable y factible dentro de una intranet académica.

El protocolo Secure Socket Layer (SSL) se ha convertido en un protocolo de uso muy extendido en los "browsers" conocidos [13], actualmente existen códigos en forma gratuita que permiten incorporarlos en otros desarrollos y hay renombrada literatura y productos que tratan el tema.

El control de acceso basado en roles (RBAC) usada por académicos [6] tiene un potencial para reducir la complejidad y el costo en la administración de la autorización en grandes sistemas [14]. Además debido a que los roles representan funciones y responsabilidades, pueden soportar directamente políticas de seguridad específicas de una organización. RBAC También puede incluir los modelos de control de acceso obligatorio y discrecional y aún específicos de un usuario. En el caso de la administración de la seguridad, ésta se simplifica enormemente, dado que el uso de roles para organizar privilegios de accesos en una organización, disminuye considerablemente la cantidad de recursos computacionales que deban asociarse con dicha tarea [2]. Finalmente el uso RBAC representa una meta altamente deseable para dirigir requerimientos de seguridad de aplicaciones soportadas en el Web [2].

La Infraestructura de Clave Pública (PKI) es útil ya que el requerimiento de la no repudiación únicamente puede ser satisfecho a través de esta tecnología. A esta conclusión se llega porque esta tecnología es un desarrollo iterativo común, a nivel mundial, que incorpora colaboraciones, académicas, privadas y gubernamentales. Se pretende con la misma organizar y estructurar una infraestructura que permita desarrollar confiablemente áreas como el comercio y la banca electrónica. Hasta que otro desarrollo mejore lo presente, PKI sigue siendo el acuerdo común de nuestro mundo que mayor respaldo posee.

Otro punto importante en la solución planteada, es que se propone el uso de un "browser" propio que sería desarrollado por los programadores del servicio de publicación. Como ya es conocido los "browsers" comerciales poseen una cantidad significativa de vulnerabilidades que constituirían una constante amenaza al buen funcionamiento de servicio de publicación.

Un componente más que interviene en la solución propuesta es el uso de "cookies". La idea que sustentó originalmente su desarrollo, por la corporación Netscape®, fue la de proveer al protocolo "HTTP" de un mecanismo que brindara el registro del "estado de sus operaciones" [15]. Por lo tanto, nuestra necesidad de mantener un registro de las operaciones ejecutadas por cada usuario puede ser plenamente satisfecha con esta tecnología Este modelo alterará el contenido tradicional de "cookie" de acuerdo a lo que Joon Park ya en el año 2001 demostró [15].

7. CONCLUSIÓN Y TRABAJOS FUTUROS

Este trabajo expone una estrategia metódica y estructurada para desarrollar una herramienta que realice labores de protección de la publicación de contenidos, por parte de cualquier usuario, en los sistemas web de las intranets académicas venezolanas. Esas directrices hacen énfasis en que el desarrollo contemple aspectos que permitan ejecutar la operación deseada en una forma confiable para todos los actores involucrados. Eso significa, que se ha expuesto un enfoque y una serie de pasos que permiten realizar el desarrollo de un mecanismo de protección de modo que integra conceptos propios del desarrollo de software, con fundamentos y requerimientos de la seguridad.

El modelo desarrollado debe ser puesto en práctica con la elaboración de un producto tangible del mismo. Ese resultado será un sistema de software cuya ejecución deberá ser realizada dentro de un marco de regulación que aborde el área de la administración corporativa de la seguridad de la intranet académica.

8. REFERENCIAS

[1] Morales Mireya, Viloria Orlando, Torrealba Miguel & Isern Germinal. *Intranet Service Security System Design: Venezuelan Public Universities, a Case Study*. 4th World Multiconference on Systemics, Cybernetics and Informatics (SCI 2000) Proceeding Comunications Systems and Networks, volumen IV. Pp 510-514.

[2] J.B.D. Joshi, W.G. Aref, A. Ghafoor y E.H. Spafford. *Security Models for Web-Based Applications*. Communications of the ACM. Vol. 44, Nº2, Febrero 2001, Pp. 38-34.

[3] Halevi Shai, Krawczyk. *Public-Key Cryptography and Password Protocols*.ACM Transactions on Information and System Security, Vol. 2, No. 3. Agosto 1999. Pp 230-268.

[4] Denning Dorothy, Denning Peter. *Internet Besieged, Countering Cyberspace Scofflaws*. Addison–Wesley, ACM Press. Nueva Tork. 1998. Pp 414 .

[5] R. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. *Role Based Access Control Models*. IEEE Computer. Febrero 1996. Pp 38-47.

[6] Anderson Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc. Nueva York. 2001.

[7] Park Joon, Sandhu Ravi y Ahn Gail–Joon. *Role–Based Acces Control on the Web*. ACM Transactions on Information and System Security, Vol. 4, No. 1. Febrero 2001. Pp 37–71.

[8] Gornik Davor. *IBM Rational Unified Process. Best Practices for Software. Development Teams*. IBM Corporation. Noviembre 2001.

[9] Jacobson Ivar, Booch Grady y Rumbaugh James. *El Proceso Unificado de Desarrollo de Software*. Addison Wesley. España 2000.

[10] Larman Craig. *Uml y Patrones. Introducción al Anális y Diseño Orientado a Objetos*. Prentice may. México. 1999.

[11] Halevi Shai, Krawczyk. *Public-Key Cryptography and Password Protocols*. ACM Transactions on Information and System Security, Vol. 2, N º 3. Agosto 1999.

[13] Schneier Bruce. *Secrets & Lies. Digital Security in a Networked World*. John Wiley and Sons Inc., 2000.

[14] Ferraiolo David and Barkley John. *Specifying and Managing Role-Based Access Control within a Corporate Intranet*. Proceedings Second ACM Workshop on Role-Based Access Control. November 1997. Pp 77-82.

[15] Park Joon, Sandhu Ravi and Ahn Gail-Joon. Role-Based Access Control on the Web. ACM Transactions on Information and System security, Vol. 4, Nº 1, February 2001, Pp 37-71.

[16] Amoroso, E. *Fundamentals of Computer Security Technology*. Prentice Hall PTR, Upper Saddle River, New Jersey, 1994.

[17] Stallings, W. *Cryptography and network security. Principles and practice*. Prentice Hall PTR, Upper Saddle River, New Jersey, 1999.

[18] Morales, M. *Intranet Académica: Modelo del sistema de seguridad para un servicio de publicaciones*. Documento interno del postgrado en ciencias de la computación, Universidad Central de Venezuela, 2004.