# Diseño Básico de la Seguridad para un Servicio Nacional de Salud Pública en Venezuela

Mireya Morales[1] y Emilio Hernández[1]

[1] Universidad Simón Bolívar, Departamento de Computación,
Apartado Postal 89.000, Caracas 1080, Teléfono: +58 (212) 9063261,
Fax: +58 (212) 9063243, Venezuela
{mprimera, emilio}@usb.ve

**Resumen.** En este artículo se propone una infraestructura de seguridad que permite el almacenamiento de los datos de un Sistema Nacional de Salud bajo un esquema de jerarquía de memoria de tres niveles. Esto implica que las funciones de seguridad se deben tomar en cuenta en todos los repositorios distribuidos y en todos los niveles. Para ello se consideran los requerimientos de autenticación, confidencialidad y control de acceso y se describen los mecanismos de seguridad soportados con técnicas de cifrado de clave privada y clave pública, certificados, y un mecanismo de control de acceso basado en roles.

**Palabras claves:** Seguridad de datos, *Grids* de salud, Sistemas de información de salud.

## 1 Introducción

En Venezuela se ha planteado la necesidad de usar tecnologías de información y de cómputo de alto rendimiento para el acceso a datos relacionados con salud, a nivel nacional. Este planteamiento ha dado origen a un proyecto, actualmente en progreso, que propone el diseño y despliegue de un sistema nacional de información de salud. En la primera fase de este proyecto, se planteó un modelo de referencia llamado SINAPSIS (Sistema de Información Nacional Público de Salud para la Inclusión Social), el cual servirá de soporte para el Sistema de Información de Salud Nacional [1]. Actualmente este proyecto se encuentra en la fase de despliegue de un prototipo en 16 centros de salud remotos, con un servidor centralizado. No obstante se espera que en el futuro el sistema completo tenga miles de puntos de acceso y esté organizado en tres niveles, que incluyen en el nivel superior una plataforma de servicios *grid* en la que estarán replicados todos los datos del sistema nacional de salud. En el desarrollo del diseño intervinieron instituciones como el Ministerio de Salud, el Ministerio de Telecomunicaciones e Informática, el Ministerio de Ciencia y Tecnología y la Universidad Simón Bolívar, entre otras instituciones venezolanas.

Hasta este momento en Venezuela no se había abordado el desarrollo de un sistema de información nacional de salud que preste su servicio a toda la población, de modo

que esta iniciativa corresponde a un hecho sin precedentes. Con la puesta en marcha del satélite venezolano VENESAT-1 se espera tener un avance significativo en la ejecución del proyecto. Frente a este panorama se hace necesaria la adecuada protección de los datos médicos de los pacientes, por lo tanto el balance entre el servicio que ofrecerá el sistema y la protección de los datos adquiere un carácter estratégico. El diseño de la seguridad ya no puede ser un asunto de implantación sino que la seguridad es un elemento de primer nivel cuyos requisitos deben ser considerados durante todo el proceso de desarrollo del sistema [2].

En algunos países de Europa el despliegue de nodos *grid* en centros de salud, tales como hospitales, laboratorios de investigaciones médicas, administraciones de salud pública, entre otros, es aún muy restringido [3]. Esto se debe principalmente a las limitaciones presentes en el *middleware* de los ambientes *grid*, que no ofrecen las funcionalidades necesarias para asegurar la manipulación confidencial de los datos médicos. En cuanto a la estandarización, se requiere la adopción de estándares internacionales y de mecanismos de interoperabilidad para el almacenamiento de información médica, lo que implica aspectos relacionados con asegurar consentimientos y anonimización.

En este artículo se plantea un análisis en términos de los requerimientos de seguridad: autenticación de usuarios, confidencialidad de los datos y control de acceso para el sistema planteado que soportará el servicio nacional de salud. También se propone el diseño de los mecanismos de seguridad para resolver tanto la autenticación como la confidencialidad y se plantea además la conveniencia de usar control de acceso basado en roles (RBAC o *Role-Based Access Control*) como un esquema en el manejo de la autorización y gestión en el control de acceso. Esto se debe a que RBAC ha sido uno de los métodos de control de acceso más usados en numerosas aplicaciones de base de datos, incluyendo las médicas [15]. Pero aparte de esta realidad, también se ha propuesto el uso de la variante de RBAC conocida como TRBAC (*Temporal Role-Based Access Control*) [6], con la finalidad de dar soporte a aquellas operaciones relacionadas con eventos dependientes del tiempo.

El resto de este artículo se estructura de este modo: en la sección 2 se discuten algunos trabajos relacionados con soluciones a los requerimientos planteados en este artículo; en la sección 3 se describe la plataforma que dará soporte al sistema nacional de salud y se discuten los requerimientos de seguridad, así como los mecanismos que se proponen para dar la solución; en la sección 4 se presentan los mecanismos de seguridad, se identifican los actores, y se describen los procesos de autenticación que son parte del funcionamiento del sistema; en la sección 5 se describen trabajos futuros y finalmente en la sección 6 las conclusiones.

## 2 Trabajos Previos Relacionados

Existen propuestas relacionadas con el uso de mecanismos de seguridad para la protección de los datos en sistemas de salud. Hembroff y Cai [16] introducen la seguridad relativa a la autenticación y a la autorización en un sistema de redes de salud. Ellos proponen un repositorio centralizado para almacenar datos con un formato HL7 [17], transferidos desde varias organizaciones de salud afiliadas a una

red común. La información de los pacientes contenida en los registros médicos electrónicos puede ser accedida en forma segura utilizando una interfaz *web* a través de la red por el personal debidamente autenticado y autorizado. Kiyomoto et al. [4] propone el desarrollo de una plataforma distribuida de información médica, utilizando un esquema P2P. Cada par (hospital) comparte la información entre ellos y se provee de un sistema de alta velocidad para compartir la información a bajo costo. En ese artículo se propone una combinación de técnicas existentes, tales como cifrado simétrico y asimétrico, certificados de atributos y gestión de claves. El mecanismo de seguridad es validado asumiendo una carga típica de procesamiento de las operaciones reales.

Park y Gyu [18] han propuesto un servicio de información inteligente y seguro para pacientes basado en el modelo CC-RBAC (*Content and Context based RBAC*), que considera un contexto temporal y espacial para hospitales de próxima generación con ambientes de computación ubicua. El modelo RBAC no puede reflejar varios elementos dinámicos de ambientes ubicuos; para resolver este asunto es necesario analizar los modelos TRBAC y GTRBAC (Generalized Temporal Role-Based Access Control)[7] y aplicarlos al esquema planteado. En ese trabajo también se presentan definiciones del tipo de contexto, de las restricciones de contexto y de las políticas de control de acceso. Además se presenta una definición formal de CC-RBAC y su arquitectura. En [15] se reporta la experiencia de la implementación de RBAC dentro de una base de datos médicos existentes. El propósito de este trabajo es evaluar la conveniencia de RBAC a nivel de implementación y no a nivel de aplicación. También se demuestra que las implementaciones RBAC son factibles en aplicaciones de base de datos para un sistema de salud nacional con jerarquía de roles. Franco et al. en [19] estudian el uso del sistema SELinux en sistemas de información de salud. La propuesta se centra en la gestión de las políticas de SELinux, lo que se considera como el principal factor que limita la adopción de SELinux. También se selecciona RBAC como la opción más adecuada, dado que el acceso a los recursos debe estar basado en la función del usuario dentro de la organización.

## 3 Requerimientos de Seguridad para SINAPSIS

Esta sección describe los mecanismos de seguridad propuestos, así como también los requerimientos de seguridad necesarios en SINAPSIS.

### 3.1 Descripción del Modelo de Referencia SINAPSIS

SINAPSIS es un modelo de referencia que define el desarrollo y el despliegue progresivo del sistema de información de salud nacional [1]. El diseño de SINAPSIS tiene dos aspectos ortogonales: su definición como una jerarquía de memoria y su definición como un conjunto de módulos de software que coleccionan datos y eventualmente mueven esos datos ascendentemente en la jerarquía de memoria, con el objeto de mantener una base de datos global actualizada.

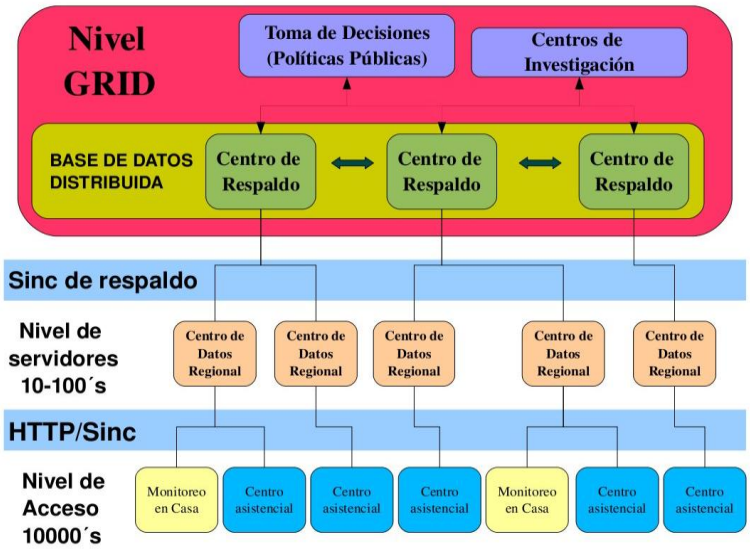


**Fig. 1.** Jerarquía de memoria y protocolos de sincronización.

La Fig. 1 muestra a Sinapsis como una jerarquía de memoria de tres niveles:

1. **Nivel de Acceso**. Este nivel está compuesto por los sistemas de usuario final, que permiten al personal médico interactuar con el sistema, así como también el monitoreo de sistemas que envían información de pacientes desde el hogar o desde dispositivos móviles.
2. **Nivel de Servidor Regional**. En este nivel se encuentran los centros de datos regionales, donde los datos son realmente almacenados. Este nivel en combinación con el nivel de acceso se asimila básicamente a un modelo cliente-servidor con características de tolerancia a fallos. Los servidores regionales pueden ser localizados dentro de los centros de salud, si tienen la capacidad de administrar un centro de datos pequeño. Para la mayoría de los centros de salud, el Ministerio de Salud proveerá conexiones de red para acceder al servidor regional más cercano. Los formatos de datos o el software cliente-servidor usados en los diferentes servidores regionales, puede variar de un sitio a otro.
3. **Nivel *Grid* de Respaldo**. En este nivel se encuentra una única base de datos, posiblemente distribuida, con la información de todos los usuarios del servicio de salud nacional, en un formato unificado. Los servidores regionales deben periódicamente sincronizar sus bases de datos con el nivel grid de respaldo, usando un protocolo de sincronización que ejecute transformaciones de formatos de datos si es necesario. En este nivel se deben proveer dos tipos de servicio a los servidores regionales:
    - **Servicio de sincronización**: para sincronizar los datos del servidor regional con el *grid* de respaldo
    - **Servicio de consulta**: es posible que un usuario vaya a un centro de salud lejano a su lugar de residencia, por ejemplo que tenga que ir

por una emergencia a un hospital en otra región. La historia médica de ese paciente se recupera desde el nivel de *grid* de respaldo, no desde el servidor regional donde están sus datos.

**Niveles de Sincronización.** Los niveles de comunicación deben tomar en cuenta la funcionalidad y la tolerancia a fallos. El flujo de datos entre el nivel de acceso y el nivel de servidor regional ocurrirá normalmente a través de una aplicación *web*. Sin embargo en algunos lugares en Venezuela, la comunicación debe ser vía enlace satelital, en cuyo caso la transmisión de la información se puede ver afectada por razones atmosféricas. En este sentido el sistema debe tener la posibilidad de trabajar en un modo independiente de la red, para lo que la aplicación *web* debe ser capaz de conectarse a una base de datos local y almacenar los datos temporalmente. Posteriormente, cuando se restablezca la conexión, se hará la transferencia de la información hacia el servidor regional. Eventualmente, el nivel de acceso también podría incluir sistemas relacionados con el monitoreo desde el hogar de los datos de los pacientes.

El flujo de datos entre los servidores regionales y el nivel *grid* de respaldo fluirá a través de protocolos de sincronización de las estructuras de datos usadas en ambos lados. El protocolo de intercambio y de formato de datos podría ser HL7 o una adaptación de este. Un aspecto importante es que en este diseño no se está considerando la definición de protocolos de comunicación entre los servidores regionales (no es una red P2P), lo que implica que si un paciente requiere ser atendido en un centro de salud lejos de su casa, el servidor regional asignado debe recuperar el registro médico del paciente desde el nivel de *grid* de respaldo.

### 3.2 Requerimientos de Seguridad

En esta sección se discuten los requerimientos que permitirán determinar los mecanismos de seguridad que deberán ser aplicados dentro de SINAPIS. Básicamente, las políticas y mecanismos de seguridad para el acceso a los datos médicos deben proveerse con mucho detalle en el nivel de servidores regionales (segundo nivel). En el nivel de *grid* de respaldo el acceso a la base de datos unificada será muchísimo más restringido, en esencia sólo los administradores de seguridad y administradores de bases de datos podrán hacerlo. Los servidores regionales podrán sincronizar sus datos con este nivel de *grid* de respaldo, pero casi ninguno de los roles de usuarios podrán acceder a los datos en el nivel de respaldo.

Los mecanismos de seguridad son en general combinaciones de funciones que sirven para mantener satisfactoriamente la seguridad de la información [4], por lo tanto la implementación del sistema nacional de salud pública propuesto requiere de la inclusión de los aspectos de seguridad necesarios para garantizar en lo posible la autenticación y el control de acceso a los datos de los pacientes. En la infraestructura planteada existe también la amenaza de que la comunicación entre los elementos de los niveles descritos pueda ser interceptada por algún usuario no autorizado, así como también que la información almacenada pueda ser adquirida ilegalmente por un intruso. En este caso debe haber una función que mantenga la seguridad de la información en forma adecuada.

En resumen, los requerimientos a ser considerados para esta infraestructura son:

1. La información transmitida por los medios de comunicación entre los diferentes niveles debe ser protegida, así como también la información que se encuentra almacenada en los repositorios de datos.
2. Se debe garantizar la autenticación de los usuarios; es decir verificar que un usuario es quien dice ser.
3. Las operaciones que el usuario ejecute sobre los datos de los pacientes deberán ser establecidas de acuerdo a los permisos asignados al rol que tiene el usuario, determinados en la política de seguridad.
4. Que las operaciones realizadas sobre los datos sean registradas para su posterior auditoria.

Para satisfacer el primer requerimiento es necesario utilizar técnicas de cifrado de la información, no sólo para la transmisión de los datos sino también para el almacenamiento [8]. Sin embargo, un aspecto crucial en la creación de un sistema seguro es la selección del método de gestión de claves que se usará en el cifrado [9].

El segundo requerimiento puede ser satisfecho a través del uso de un sistema de autenticación, en este caso se puede hacer uso de certificados de clave pública, ya que está planteado utilizar una Infraestructura de Clave Pública (Public Key Infrastructure, PKI). Con este esquema, se espera que se realice una autenticación mutua entre el solicitante y el servidor de autenticación.

Una vez autenticado el usuario, el tercer requerimiento será satisfecho a través de la implementación de RBAC, para permitir asignar la autorización correspondiente a un usuario, de acuerdo al rol que desempeñe dentro del sistema de salud y por lo tanto podrá ejecutar las operaciones sobre los datos médicos, de acuerdo a los permisos otorgados. Con el uso de RBAC, los roles representan funciones dentro de las organizaciones. Las autorizaciones son otorgadas a los roles y no a los usuarios [5], por lo tanto una vez que un usuario es autenticado y entra al sistema, puede activar un subconjunto de roles que le han sido otorgados, de acuerdo a la política de seguridad implementada.

A pesar de que RBAC ha alcanzado un buen nivel de madurez, existen algunos requerimientos no soportados por este modelo [6]. Uno de ellos está relacionado con la dimensión temporal de los roles, por ejemplo el caso de un médico que trabaje a tiempo parcial en un hospital, digamos en el horario comprendido entre las 9 a.m. y las 2 p.m. Si este médico está representado por un rol, entonces ese rol debería ser activado sólo en ese intervalo de tiempo. Para cumplir con ese tipo de requerimientos Bertino et al. [6] ha propuesto una extensión del modelo RBAC denominado Temporal-RBAC (TRBAC) que soporta restricciones para habilitar y deshabilitar roles periódicos, así como también dependencias temporales entre tales acciones. Estas dependencias son expresadas por medio de accionadores (*triggers*) de roles, es decir roles activados que son automáticamente ejecutados cuando ocurre una acción específica. También puede ser usado para restringir el conjunto de roles que un usuario particular puede activar en un instante de tiempo dado. El disparo de un *trigger* puede causar que un rol sea habilitado/deshabilitado inmediatamente o después de una cantidad de tiempo especificada explícitamente. Otro aspecto importante es que este mecanismo le permite al administrador de seguridad reaccionar frente a situaciones de emergencia, es decir, que podrá cambiar dinámicamente el estado de un rol y también el conjunto de usuarios asignados para activar ese rol

particular a través de la emisión de un requerimiento dinámico, tal es el caso de la activación del rol que corresponde al médico de emergencia. Lo más importante de TRBAC es que se pueden habilitar roles en períodos de tiempo y dependencias temporales entre roles que pueden ser expresadas a través de *triggers*. Por ejemplo un caso de uso de un *trigger* se visualiza con el hecho de que habilitar/deshabilitar el rol del médico nocturno implica con alta prioridad habilitar/deshabilitar el rol de enfermera nocturna. En conclusión, el tercer requerimiento será satisfecho utilizando un mecanismo de control de acceso soportado en RBAC y TRBAC.

El cuarto requerimiento debe ser satisfecho escribiendo un registro de todas las operaciones que se ejecuten sobre el sistema de salud. Es decir, a partir del momento de la autenticación de usuarios, asignación de roles y de las modificaciones de los datos de los pacientes. También deben registrarse las operaciones de los administradores de seguridad.

## 4 Diseño de los Mecanismos de Seguridad para la autenticación y la confidencialidad de los datos

Con base en los requerimientos discutidos en la sección anterior, los mecanismos de seguridad se han diseñado de la siguiente manera:

1. Los canales de comunicación en cada nivel serán cifrados utilizando una Infraestructura de Clave Pública (PKI) [10].
2. En la sección 3.1 se plantea que SINAPSIS define una jerarquía de memoria de tres niveles, esto implica que en el nivel de acceso es factible llevar a cabo un almacenamiento de los datos, esto depende de la capacidad tecnológica que haya en el centro asistencial, en el nivel de servidor regional seguro se hará almacenamiento de los datos y en el nivel *grid* de respaldo, es donde estarán los datos a nivel nacional de todos los centros regionales, lo que indica claramente que se requiere de la protección de los datos en los tres niveles. Por lo tanto, se propone el uso de un esquema de cifrado simétrico que se aplicará en el sitio donde se encuentran almacenados los datos. La ejecución de este esquema será a través de los mecanismos de cifrado que ofrezca el servidor de bases de datos que opere en cada nivel.
3. La autenticación de los usuarios se hará a través de la criptografía de clave pública, con el soporte de la infraestructura de clave pública. Este esquema de autenticación funcionará en los tres niveles de SINAPSIS.
4. El control de acceso a los datos médicos estará sujeto a la política de seguridad que se defina para el servicio nacional de salud pública; esta política deberá estar soportada legalmente en el marco de las leyes venezolanas, fundamentalmente en la Constitución de la República Bolivariana de Venezuela, en su articulo 28, Titulo III [11], en la Ley Especial Contra Delitos Informáticos artículos 20, 21 y 22 [12], capítulo III, , en la Ley de Mensajes de Datos y Firmas Electrónicas [13], en la Ley de Protección de Datos y Habeas Data, que en este momento se encuentra bajo la condición de anteproyecto. No obstante, se sugiere la creación de una Ley sobre Información de Salud cuyo contenido sea específico y pueda ser la

plataforma legal para la definición de las políticas de seguridad en el área de salud. Adicionalmente se espera que estas políticas estén soportadas bajo un estándar internacional, como por ejemplo ISO 27799 [20]. Otro aspecto importante a mencionar es que en el nivel de *grid* el acceso estará restringido al administrador de seguridad, o al grupo de administración de seguridad.

5. Los usuarios cuyos roles estén definidos y relacionados con funciones de Investigador y de Gestor de Datos Estadísticos para la definición de políticas públicas en salud (estos últimos serán en general empleados adscritos al Ministerio de Salud) deben tener acceso a datos consolidados, no individuales. Para los roles de Investigador y de Gestor de Datos Estadísticos, la información solicitada deberá ser sometida a un proceso de aprobación por parte de una autoridad superior que debe pertenecer al Ministerio de Salud. Posteriormente el administrador de seguridad deberá tener la competencia, establecida en un procedimiento de la política de seguridad, para garantizar la anonimización de los datos que no deben darse a conocer. Los datos autorizados deben ser extraídos de la base de datos y copiados en un medio físico diferente que será entregado a los solicitantes, nunca como una vista que acceda a la base de datos original, para evitar posibles rupturas de la protección de los datos.

### 4.1 Identificación de Actores

En esta sección se definen un conjunto inicial de los actores que tendrán acceso al sistema. Cada uno de estos actores tendrá privilegios bien definidos para el acceso a los datos, establecidos en la política de seguridad que soportará el sistema de salud. Los actores que en principio, tendrán interacción con el sistema nacional de salud pública son:

1. Pacientes y familiares. Normalmente acceden al sistema de salud para solicitar citas y eventualmente extraer información relacionadas con sus propios datos.
2. Personal médico, técnico y administrativo del sistema de salud: médico tratante, médico interconsultado, enfermera, personal administrativo, técnico de laboratorio, técnicos de imagenología (radiologías, tomografías, entre otras) otro profesional médico. Ellos tendrán contacto con el sistema, cuando quieran realizar operaciones de: agregar, modificar, eliminar o consultar datos vinculados con la historia médica de los de pacientes.
3. Personal técnico informático: administradores de seguridad (AS), administradores de redes y administradores de bases de datos. Tienen acceso a los datos por razones técnicas, pero deben firmar compromisos muy firmes relativos a mantener la confidencialidad de los datos. Los administradores de seguridad podrán realizar operaciones de crear usuarios, asignar roles a usuarios, asignar permisos a roles, establecer jerarquía de roles, crear restricciones, entre otras operaciones.
4. Funcionarios para toma de decisiones de políticas públicas: técnicos en estadística, personal de epidemiología, funcionarios del Ministerio de Salud, etc. No necesitan tener acceso a los datos directamente, se les pueden

suministrar conjuntos de datos consolidados por región, incidencia de enfermedades, uso de recursos hospitalarios, etc.

5. Investigadores: Tampoco necesitan tener acceso a los datos directamente, se les pueden suministrar conjuntos de datos consolidados similares a los que se entregan para tomas de decisiones en políticas públicas y adicionalmente conjuntos de datos no cuantificables, como por ejemplo imágenes médicas debidamente anonimizadas.

**Metas del sistemas.** Garantizar en lo posible, los requerimientos de seguridad: autenticación, confidencialidad, control de acceso, y auditoria de datos.

### 4.2 Procesos de autenticación

En esta sección se describen los procesos de autenticación para cada uno de los tres niveles de SINAPSIS.

**Autenticación al nivel de acceso.** En este nivel básicamente accede personal médico, técnico y administrativo del sistema de salud. Debe haber un mecanismo básico de autenticación, principalmente basado en los mecanismos de acceso (*login*) que tienen los equipos basados en Linux. No obstante, también se está estudiando la posibilidad del uso de una tarjeta inteligente que permita el acceso a las computadoras. En estos equipos puede haber datos temporales de pacientes que no han sido enviados al servidor regional debido a problemas de sincronización. Una vez que se subsanan las restricciones de comunicación, los datos recabados localmente se envían y se borran. Mientras esos datos estén almacenados localmente, una persona no autorizada podría acceder a ellos. Aunque este riesgo es limitado, circunscrito a un ámbito local, y con pocos datos en riesgo de estar comprometidos, debe proveerse el mecanismo básico de seguridad de acceso a los equipos.

**Autenticación al nivel de servidor regional**. El verdadero acceso a los datos no se realiza accediendo al equipo local, sino accediendo al servidor regional a través de alguna de las aplicaciones cliente-servidor que sean parte de SINAPSIS. En este nivel se ha planteado el uso de un esquema de autenticación mutua entre un usuario del sistema de salud y el servidor de autenticación, de modo que un usuario que ingrese al sistema de salud debe solicitar la creación de su par de claves pública y privada ante la autoridad de registro de la infraestructura de clave pública. Posteriormente le será otorgada la información, que contiene el par de claves, los datos personales del usuario y el rol que asumirá, de acuerdo al cargo que desempeña. También se emitirá un certificado de clave pública X.509, que será gestionado por la autoridad de certificación.

La red que implementa a SINAPSIS debe tener entre otros elementos una infraestructura de clave pública, es decir una autoridad de registro, una autoridad certificadora y un servidor de directorios ubicados en el nivel de servidor regional, un servidor de autenticación y un servidor de roles que estarán colocados también a este nivel.

**Autenticación en los equipos de acceso al *grid* de respaldo**. El *grid* de respaldo, que corresponde con el tercer nivel de SINAPSIS, debe ofrecer al menos los servicios de sincronización y de consulta, como se explica en la sección 3.1. En ambos casos, la conexión debe provenir de un servidor regional. Los servidores de sincronización y consulta del nivel de grid de respaldo sólo saben permitir conexiones desde los servidores regionales, y en los protocolos especificados, que en ningún caso es http, sino un protocolo basado en HL7 sobre un canal seguro. Las conexiones sobre ese canal seguro deben estar protegidas con certificados digitales y la autentificación debe ser mutua.

**Autenticación dentro del grid de respaldo.** La autenticación dentro del *grid* de respaldo será la usual dentro de un *grid* estándar: hay una doble verificación, una basada en certificados digitales asociadas a los equipos y otra basada en certificados digitales de los usuarios. Los roles de Investigador y Gestor de Datos Estadísticos pueden tener acceso a recursos del *grid*, pero no un acceso directo a la base de datos médicos. Los datos consolidados que serán usados por usuarios con estos roles deben extraerse de la base de datos y estar debidamente anonimizados.

## 5 Trabajos Futuros

Esta investigación debe continuar con la implementación de los mecanismos de seguridad propuestos, con la finalidad de proveer la protección de los datos médicos de pacientes en el sistema. En este momento se está trabajando en hacer una implementación del requerimiento de control de acceso a través de SELinux, debido a que este módulo incorpora RBAC. Se implementará alguna versión adaptada de TRBAC.

Se espera seguir desarrollando el resto de los requerimientos, como son: integridad, anonimización de datos, auditoria, no repudio, entre otros. Otro aspecto es el desarrollo del requerimiento de control de acceso aplicado al equipo de administradores de la red y administradores de la seguridad que estarán a cargo del servicio técnico de la plataforma del sistema de salud. Se aspira también que la gestión de los administradores del sistema de salud se haga con RBAC.

## 6 Conclusiones

En este trabajo se presenta un análisis de los mecanismos de seguridad para dar soporte a los requerimientos de: autenticación, confidencialidad y control de acceso en una infraestructura propuesta para un Sistema de Información Nacional de Salud (SINAPSIS). Cabe destacar que un aspecto importante es el hecho de que la seguridad ha sido tomada en cuenta como un elemento clave en el desarrollo de la infraestructura de la red que soportará el servicio de salud.

La arquitectura propuesta tiene requerimientos bien específicos desde el punto de vista de seguridad. Los esquemas de seguridad propuestos serán implementados en una infraestructura de sistema que está soportada en un diseño particular, como lo es

la jerarquía de memorias de tres niveles. Los niveles tienen diferentes requisitos de seguridad y el diseño de seguridad debe contemplar este hecho. En este trabajo se plantea una solución adaptada a cada nivel.

Se propone el uso del modelo TRBAC para implementar el control de acceso de los datos de los pacientes y se espera que esta implementación sea útil en general, no solamente para el caso específico del sistema de información de salud que se está diseñando en Venezuela.

## Referencias


1. Hernández, E., Figueira, C.: Realistic Role of Grid Technologies in a National Health Service for Venezuela. First EELA-2 Conference, Bogotá, Colombia (2009)
2. Sanz, D., Aedo, I., Díaz, P.: Un Servicio Web de Políticas de Acceso Basadas en Roles para Hipermedia. IEEE Latin America Transactions, Vol. 4, No. 2, pp. 77--84 (2006)
3. SHARE Technology and Security Roadmap I., http://wiki.healthgrid.org/SHARE_Technology_and_Security_Roadmap_I
4. Kiyomoto, S., Tanaka, T., Miyake, Y., Mitamura, Y.: Development of Security Functions for a Medical Information Sharing Platform. System and Computers in Japan, Vol. 38, No. 11, pp. 49--62. Wiley Periodicals, Inc. (2007)
5. Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D., Chandramousli, R.: Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security, Vol. 4, No. 3, pp. 224--274 (2001)
6. Bertino, E., Andrea P., Ferrari, E.: TRBAC: A Temporal Role-Based Access Control Model. ACM Transactions on Information and System Security, Vol. 4, No. 3, pp. 191--223 (2001)
7. Joshi, J., Bertino, E., Latif, U., Ghafoor, A.: A Generalized Temporal Role-Based Access Control Model. IEEE Transactions on Knowledge and Data Engineering, Vol. 17, No. 1, pp. 4--23 (2005)
8. Blaze, M.: A Cryptographic File System for Unix. Proc. 1st ACM Conference on Communications and Computing Security, pp. 9--16 (1993)
9. Blaze, M.: Key Management in Encrypting File System. ISENIX Technical Conference, pp. 2--35, Boston (1994)
10. Nash, A., Duane, W., Joseph, C., Brink, D.: PKI Infraestructura de Claves Públicas. McGraw-Hill Interamericana, S.A. Colombia (2002)
11. Constitución de la República Bolivariana de Venezuela.: Gaceta Oficial No. 36.860. Oficio No. 0034-00 de la Asamblea Nacional Constituyente (2000)
12. Ley Especial Contra Delitos Informáticos. Gaceta Oficial No. 37.313 (2001)
13. Ley de Mensajes de Datos y Firmas Electrónicas. Gaceta Oficial No.37.148 (2001)
14. Joon, P., Ravi, S., Gail-Joon A.: Role-Based Access Control on the Web. ACM Transactions on Information and System Security, Vol. 4, No. 1, pp. 37--1 (2001)
15. Roled Based Access Control for a Medical Database, http://www.wmin.ac.uk/cscs/pdf/IASTED SEA 2007 RBAC Slevin Macfie.pdf
16. Hembroff, G., Cai, Y.: Secure Authentication and Authorization Design for Rural-Based Healthcare Institutions. Security and Communication Networks. Published online in Wiley InterScience, pp. 407--415 (2008)
17. HL7 Electronic Health Record Technical Committee, http://www.hl7.org/EHR/ [2/1/2008]
18. Park, J., Gyu, D.: PIS-CC RBAC: Patient Information Service based on CC-RBAC in Next Generation Hospital considering Ubiquitous Intelligent Environment. International Conference on Multimedia and Ubiquitus Engineering. IEEE Computer Society (2007)

19. Franco, L., Sahama, T., Croll, P.: Security Enhanced Linux to Enforce Mandatory Access Control in Health Information System. In: Warren, J., Yu, P., Yearwood, J., (Eds) HDKM 2008, Vol. 80, Australia (2008)
20. Area Normas, http://iso27000.wik.is/Area_Normas