

SLD199 COMPONENTE DE SEGURIDAD Y ADMINISTRACIÓN DEL REGISTRO INFORMATIZADO DE SALUD.

SLD199 COMPONENT AND SAFETY MANAGEMENT HEALTH COMPUTERIZED REGISTER

Mirna Cabrera Hernández¹, Ariel Delgado Ramos², Denis Derivet Thaureaux³,
Alfredo Sánchez Rodríguez⁴, Laura González Cabrera⁵, María Antonia Tardío López⁶

1 MINSAP, Cuba, mirna@infomed.sld.cu Barrera 23A e/. Masip y José Miguel Gómez. Regla, La Habana

2 MINSAP, Cuba, ariel.delgado@infomed.sld.cu

3 MINSAP, Cuba, derivet@infomed.sld.cu

4 SOFTEL, Cuba, alfredo@softel.cu

5 ISPJAE, Cuba, laurag@udio.cujae.edu.cu

6 COPEXTEL, Cuba, matota@copextel.com.cu

RESUMEN: El Sistema de salud cubano es un sistema complejo que se caracteriza por la presencia de un número elevado de elementos, relaciones, propiedades, jerarquías y fronteras que tienen numerosas formas de combinarse y recombinarse y que están sometidos a una dinámica muy elevada. La infraestructura tecnológica y los servicios que soporta, permite garantizar el adecuado funcionamiento de los sistemas de información utilizados en el proceso de intercambio, análisis y toma de decisiones sectoriales e intersectoriales sobre los problemas de salud. El surgimiento de los Servicios Web basados en XML, implicó la aparición de variantes mucho más factibles para la integración. Se realizó una investigación tecnológica con el objetivo de obtener los componentes de administración y seguridad de la Plataforma informática para el Sistema Nacional de Salud. Se implementó en el Sistema Nacional de Salud una solución tecnológica utilizando XML Web Services y elevados estándares de seguridad, fue implementado con éxito el servicio de Certificación Digital para el sector de la salud, se garantizó la confidencialidad e integridad de los datos y su manipulación por medio de usuarios con diferentes privilegios, roles y contraseñas.

Palabras Clave: Seguridad Informática, Certificación Digital, XML Web Services

ABSTRACT: The Cuban health system is a complex system which is characterized by the presence of a large number of elements, relationships, properties, hierarchies and boundaries that have numerous ways to combine and recombine and are subjected to a very high dynamic. The technology infrastructure and support services, ensures the proper functioning of information systems used in the process of exchange, analysis and decision making on sectoral and intersectoral health problems. The emergence of XML-based Web Services, led to the emergence of variants much more feasible for integration. Technological research was conducted in order to obtain the management and security components of the platform for the National Health System. We implemented a solution using XML Web Services technology and high safety standards, was successfully implemented digital certification service for the health sector, ensured the confidentiality and integrity of the data and its manipulation by users with different privileges, roles and passwords.

KeyWords: Computer Security, Digital Certification, XML Web Services

1. INTRODUCCIÓN

El sistema de salud cubano es un sistema complejo que se caracteriza por la presencia de un número elevado de elementos, relaciones, propiedades, jerarquías y fronteras que tienen numerosas formas de combinarse y recombinarse y que están sometidos a una dinámica muy elevada. Está constituido por un conjunto de Instituciones de salud, coordinadas, integradas y regionalizadas con funciones de promoción, prevención, atención, recuperación y rehabilitación de la salud, estructurado en tres niveles de atención, donde se realizan acciones de salud con el objetivo de incrementar los niveles de salud y la calidad de vida de la población. [1]

La informatización del sistema nacional de salud implica mejoras en los procesos de salud y en su conjunto a mejorar la calidad de la asistencia médica. Contar con un sistema robusto de seguridad es un aspecto importante para la protección de la información producto a que la información contenida dentro del sistema es vital y por lo tanto tiene que ser protegida.

Para el logro de estos objetivos convoca y actúa conjuntamente con otros sectores económicos y sociales a través de actividades intersectoriales, que se ven mediadas por un fuerte intercambio de información que permite la concertación de objetivos y acciones, que se establecen a través de las relaciones de trabajo entre los actores y representantes de las instituciones y organizaciones que integran una red que actúa en función de resolver las situaciones que propicien el alcance de los objetivos encaminados a lograr la salud y calidad de vida de los habitantes en la comunidad.

El uso de las tecnologías para la salud garantiza a través de la informatización, el intercambio de información, la concertación de actividades, la rapidez y el dinamismo necesarios para una mayor efectividad de las acciones intersectoriales. Permite universalizar estas acciones y facilita la toma de decisiones. [2] Es por ello que el Ministerio de Salud Pública ha desarrollado varias etapas estratégicas para la informatización del Sector de la Salud. [3,4]

La infraestructura tecnológica y los servicios que soporta, permite garantizar el adecuado funcionamiento de los sistemas de información utilizados en el proceso de intercambio, análisis y toma de decisiones sectoriales e intersectoriales sobre los problemas de salud.

De igual forma, las políticas definidas para la informatización del sector plantean que todos los productos y servicios se integrarán a la ciberinfraestructura del sector: uso de sistemas abiertos, arquitectura orientada a los servicios y basadas en componentes, utilizando software libre y deben constituirse en componentes modulares y estables, que compartan normas y cooperen entre sí.

El surgimiento de los Servicios Web basados en XML, implicó la aparición de variantes mucho más factibles para la integración, ya que tienen el objetivo de desarrollar aplicaciones distribuidas altamente integradas que interactúen por XML entre los servicios Web y múltiples servicios WEB.

El Registro Informatizado de Salud (RIS) constituyó la aplicación pionera en la utilización de esta tecnología de avanzada, que además permitiría la reutilización, la no duplicación de esfuerzos y el logro de la confiabilidad e integridad de la información clínica que se gestionaría; garantizando la seguridad informática y de contingencia como requisito imprescindible y responsabilidad ineludible de los productores, prestadores y usuarios que participan en este proceso de informatización.

2. CONTENIDO

2.1 MÉTODO

Se realizó una investigación tecnológica con el objetivo de obtener los componentes de administración y seguridad de la Plataforma informática para el Sistema Nacional de Salud. El desarrollo se basó en:

1. Desarrollo integral de las soluciones informáticas para el Sistema Nacional de Salud.
2. Acompañar los proyectos de las soluciones de sostenibilidad y mantenimiento de los mismos.
3. Desarrollo de los Recursos Humanos en informática necesarios para la explotación de los sistemas.

Para desarrollar los componentes de administración y seguridad se tuvieron en cuenta los siguientes criterios:

- Administrador del Sistema Operativo, Administrador del Sistema de Gestión de Base de Datos (DBA) y Administrador de los demás servidores.
- Desarrolladores de la aplicación.

- Mantenedores de la aplicación (Gestor Producto).
- Administrador de LAN y proveedores de Conectividad.
- Gestor de datos del usuario. Administración aplicación usuario.
- Usuarios finales.

Se implementaron los siguientes aspectos relacionados con el filtraje Ip y TCP.

- Filtrado capa 3 y 4 OSI-ISO con IPTables.
- Filtrado capa 7 OSI-ISO (5 modelo híbrido) con virtualhosts.
- Filtrado capa 3 y 4 OSI-ISO con ACL en los conmutadores capa 3, enrutadores y cortafuegos de Infomed.
- Política de denegación por defecto.
- En profundidad o multi-defensa y variado en tecnologías.
- Gestionado por múltiples autoridades.

Se tuvo en cuenta además la Gestión de contingencias desencadenada por:

- Monitoreo automático.
- Revisión manual frecuente.
- Reportes / solicitudes de gestores.
- Reportes / solicitudes de usuarios.

Se implementó el monitoreo, no sólo de los servicios sino también de otros parámetros críticos o no, tales como:

- Servicios de otros proveedores (DNS, parches de seguridad, etc.).
- Visibilidad intra-servidores.
- Salvas automáticas.

En relación con las salvas de la información quedaron implementadas de la siguiente forma:

- Automáticas:
 - Periodicidad.
 - Multiplicidad y expiración temporal (diaria, semanal, mensual).
 - Monitoreo automático de éxito de las salvas.

- Cruzadas y geográficamente distantes:
 - Locales
 - Desde otros servidores en housing en Infomed.
 - Desde Softel.
 - Propuesta de salvas desde Cedisap.
 - Canal encriptado para TxD.
 - Manuales offline (por administradores).
 - Salvas por los gestores de producto.
 - Protección de acceso a las salvas.

Se definió el servicio de parches de seguridad que garantizó la continua actualización de los sistemas utilizados implementando la actualización:

1. Diaria (madrugada) y automática contra repositorio de seguridad de Infomed (actualización c/ 1/2 hora).
2. Binaria automática (las que no son de seguridad). Se hacen manualmente, de forma ocasional y cuidadosamente probadas antes.

En el caso de los accesos de actualización se tuvieron en cuenta los siguientes aspectos:

- Actualización de código: solo un gestor de producto por cada sistema.
- Actualización de BsDs: solo el mismo gestor de producto por cada sistema.
- Aislamiento total de privilegios de acceso. Mínimos privilegios necesarios (Código y BsDs).
- Autenticación doble (local y remota). Además filtrado por direcciones IP.
- Se ha regularizando el proceso con los profesores jefes de los desarrollos en la UCI.
- Administradores no tocan código ni datos. Un solo responsable: el gestor de producto.

Para el caso de la recuperación de contingencia se implementaron las siguientes medidas:

- Identificación del problema, diagnóstico de la causa, decisión de acciones a tomar.
- Escalamiento a proveedores (conectividad,

housing y reparación de hardware).

- Re-montaje del S.O. y servidores.
- Restaura de la configuración salvada.
- Restaura del código. (Gestor producto)
- Restaura de las BsDs. (Gestor producto)

La administración de contraseñas se realizó en tres niveles, las administrativas, las de los gestores de productos y de los administradores.

- Administrativas.
 - Fichero encriptado.
 - Generación aleatoria y automática.
 - 32 caracteres (ASCII de 7 bits c/u) mixtos
 - Uso de Gestores de passwords (Kepass 1.x)
 - Clientes SSH en fichero encriptado
 - Todas diferentes.
- De gestores de producto.
 - Entregan y se cambian.
 - Todas diferentes aunque sea un mismo objeto de administración (usuarios diferentes).
- De administradores.
 - Login como usuarios individuales y escalamiento de privilegios SUDO.

Finalmente quedó implementado el proceso de contabilidad y auditoría a través del registro en papel de accesos desde las cabinas de acceso, registro en Softel de las actualizaciones, contabilidad de acceso de los administradores y traza en los logs de los servidores de las incidencias y accesos.

Todas fueron desarrolladas con el empleo de las tecnologías informáticas de "Software libre" o plataformas de código abierto, XML Web Services y el uso de estándares para el desarrollo de aplicaciones informáticas en el sector de la salud.

2.2 RESULTADOS Y DISCUSIÓN

SISalud es el Portal de aplicaciones para la Informatización del sector; es la plataforma para la administración, procesamiento y transmisión de la información en el Sistema Nacional de Salud, que

permite la gestión de la información a todos los niveles para la toma de decisiones a partir de la integración de los componentes que se encuentran actualmente desplegados en servidores centrales, ubicados en Infomed, y destinados a estos fines.

Concretamente, como parte de SISalud, se encuentra en funcionamiento el Registro Informatizado de Salud (RIS), el cual contiene un grupo de registros primarios que persiguen como objetivo que se codifique de manera uniforme, de forma tal que el resto de las aplicaciones en desarrollo y otras que serán abordadas a corto, mediano y largo plazo puedan enviar información a los niveles superiores de manera única y la misma pueda ser procesada adecuadamente.

Desarrollo de la infraestructura.

La infraestructura se organiza a partir de la estrategia diseñada en el Programa de Informatización, de acuerdo al sistema de aplicaciones a implantar, comportándose de la siguiente manera hasta el momento:

- Equipamiento y distribución: Se ha distribuido equipamiento profesional para los nodos de 41 hospitales incluidos 116 servidores. Más de 40 000 computadoras, de ellas 19 236 (48 %) dedicadas a la docencia, de igual modo se han cubierto todas las bibliotecas de la Atención Primaria de Salud, las redes de Bancos de Sangre, Nefrología, Anatomía Patológica, Imágenes médicas y Electromedicina y otras redes nacionales.
- Infraestructura de Conectividad: Mejoramiento de la conectividad, si en el año 2009 contábamos con 1 125 instituciones de salud con enlaces dedicados, hoy tenemos 1 450 unidades de salud conectadas a la Red Telemática INFOMED, que constituye la intranet de la Salud Pública Cubana, entre ellas se destacan 376 Policlínicos, 110 hospitales, 180 Direcciones de Salud Municipales y Provinciales.

Desarrollo integral de las soluciones informáticas para el Sistema Nacional de Salud.

En el último decenio se han enfatizado los siguientes desarrollos:

- Registros del Sistema de Información para la Salud (SISalud).
- Atención Primaria de Salud.
- Sistema de Información Hospitalario.

- Red Nacional de Imágenes Médicas.
- Red Nacional de Bancos de Sangre.
- Proyecto Galenomedia.
- Sistema de Estadística.
- Sistema de Nefrología.
- Sistema de Farmacias.
- Sistema de Genética Médica.
- Sistema de Colaboración Médica.
- Sistema de Control Sanitario Internacional.

Requerimientos de Seguridad

Los Requerimientos de Seguridad forman parte de los Requisitos No Funcionales (RFN) y constituyen la base que debe sustentar la arquitectura de cualquier proyecto de informatización en el sector de la salud, ya que responden a las políticas de informatización definidas y que son de estricto cumplimiento por las entidades involucradas en el desarrollo de un producto informático para el Sistema Nacional de Salud. Entre otros, se pueden mencionar:

RFN de Seguridad: Disponer de un mecanismo de seguridad basado en el modelo de Autenticación, Autorización y Auditoría (AAA).

RFN de Confianza: La información manejada por el sistema está protegida de acceso no autorizado. El sistema debe prevenir posibles fallos y/o errores y presentar facilidades para una rápida recuperación en dichos casos.

RFN de Integridad: Que la información sea modificada (incluyendo su creación y borrado) sólo por personal autorizado. Se implementarán políticas de resguardo de información, así como la realización de copias periódicas de seguridad.

RFN de Disponibilidad: Los usuarios autorizados tendrán acceso a la información en todo momento.

Estos RFN están avalados por más de 15 sistemas que integran hoy SISalud y la reutilización de esta arquitectura garantizará el aprovechamiento de los recursos tecnológicos con los que se cuenta.

Un aspecto importante para el desarrollo e implantación de estas aplicaciones es el componente de seguridad y administración, claves para el adecuado funcionamiento del resto de los componentes y esenciales para garantizar y certificar la protección y eficiencia del resto.

Modulo Administración:

Es el módulo que utilizan los administradores del SISalud en los diferentes niveles del SNS para crear y configurar los usuarios.

El registro de un nuevo usuario en SISalud (ver Figura 1) se realiza con la previa presentación de la planilla con sus datos, aprobada debidamente por el máximo responsable de la unidad de salud, donde se constatan los datos generales y los permisos aprobados según el módulo al que deba acceder.

Figura 1: Registrar usuarios en SISalud

Para registrar usuarios se realiza la búsqueda en el Registro de Ciudadanos (RC) donde debe aparecer la persona para crearle su usuario, de lo contrario se inserta en el RC antes de crearlo como usuario en SISalud. (ver Figura 2).

Usuario	Nombre y Apellidos	Nivel	Ubicación
<input type="radio"/> Lopez	Ismary López Noa	Nacional	Nivel Nacional
<input type="radio"/> yaso	JOSE PEDRO VAZQUEZ VIZOZO	Nacional	Nivel Nacional
<input type="radio"/> nortis	Olivia Caballero Martinez	Nacional	Nivel Nacional

Figura 2: Listado general de usuarios en SISalud

Posteriormente se procede a asignar el (o los) accesos al módulo según le corresponda y según el rol que realizará en el mismo (ver Figura 3).

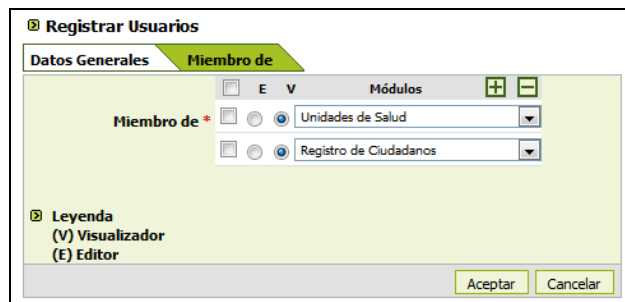


Figura 3: Asignación de privilegios y permisos

Algunas consideraciones generales para los usuarios del SISalud:

- Cada usuario puede pertenecer únicamente a un nivel del SNS.
- Un usuario, que no sea administrador, puede ser “Editor” o “Visualizador” de un módulo del SISalud.
- Un usuario, en el nivel que fue creado, puede tener acceso a varios módulos del SISalud, definiendo para cada módulo si es Editor o Visualizador, o sea, el mismo usuario puede ser Editor Nacional del módulo “Registro de Unidades de Salud” y Visualizador Nacional del módulo “Registro de Ubicación”.
- El nombre de un usuario no se repite, puede un ciudadano, (es decir una persona) tener otro usuario para otro nivel, pero no con el mismo nombre de usuario.
- Los usuarios pueden ser de tres tipos:
 - Los **administradores** que sólo realizan tareas de administración en los diferentes niveles, según corresponda con la estructura del SNS, sin tener acceso a otra información del sistema.
 - Los **editores** son responsables de la inserción y modificación de la información.
 - Los **visualizadores** que sólo tienen derecho a consultar y evaluar la información.

El proceso de administración del SISalud tiene carácter jerárquico (ver Figura 4), ya que el administrador nacional crea los editores y visualizadores para su propio nivel, así como los administradores para el nivel inmediato inferior.

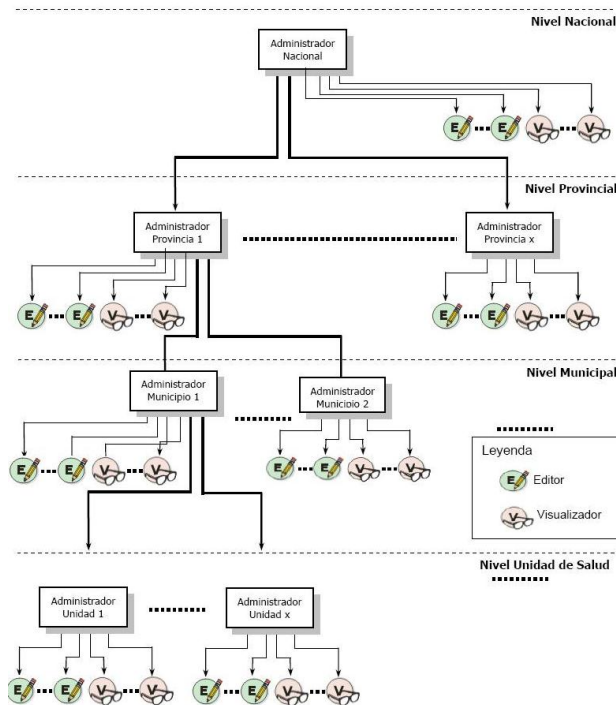


Figura 4: RIS. Árbol Jerárquico de Administración

Componente de Seguridad (SAAA).

Está basado en el modelo de Autenticación, Autorización y Auditoría (SAAA-Single Authentication Authorization and Account) donde la autenticación debe ser la primera acción del usuario en el sistema y consistirá en suministrar un nombre de usuario único y una contraseña que debe ser de conocimiento exclusivo de la persona que se autentica. Si el usuario autenticado no se encuentra registrado se reporta un error de acceso. En caso contrario, se autoriza su acceso y se crea un certificado digital y se retornan todos los datos y permisos del usuario, desglosado por módulos. Cada Petición de usuario, autorizada o no, es registrada, así como el día, mes, año, hora, minuto, segundo en que se registra y si fue o no autorizada.

Cualquier componente que se integre al Sistema de Información para la Salud debe:⁵

1. Registrarse con la información que se solicita según los documentos de integración existentes.
2. Solicitar el registro de todos sus métodos en este componente para garantizar la seguridad de su aplicación.
3. Entregar los niveles de acceso que permitirá a su componente para ser registrados en SAAA.

4. Antes de invocar a cualquier método, deberá preguntar a la SAAA si el usuario tiene acceso al método invocado para garantizar una mayor seguridad.

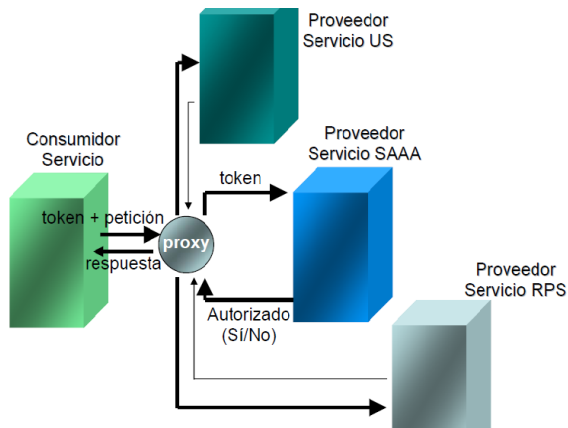


Figura 5: Consumo de peticiones al servidor

A través de estos componentes se puede realizar un monitoreo sistemático del uso de la aplicación lo cual permite corregir deficiencias en los usuarios y garantizar el adecuado uso del mismo.

De esta manera, hasta diciembre del 2011 el sistema contaba con 346 usuarios registrados y se habían realizado 6 mil 027 autentificaciones con un total de 364 mil 137 accesos al sistema. La Tabla I muestra un ejemplo de cómo se ha comportado el acceso por alguno de los componentes disponibles y en uso en la actualidad y en la Tabla II se muestra el acceso al sistema por años.

Tabla I. Accesos al sistema por componente

Componente	Cantidad de Accesos
Registro del Ciudadano	855
Registro de Trabajadores de Salud	5194
Registro de Unidades de Salud	77949

Tabla II. Cantidad de Accesos por año

Años	Cantidad de Accesos
2009	94878
2010	145914
2011	116809

En la Tabla III se muestra el acceso al sistema por años y para algunos componentes: RC: Registro

Ciudadano, RTS: Registro Trabajadores de la Salud, RUS: Registro Unidades de Salud.

Tabla III. Cantidad de accesos por año y por componente

Años/ Componente	RC	RTS	RUS
2009	18	167	19093
2010	477	3173	31087
2011	337	1628	26355

Nota: Cada acceso se corresponde con la ejecución de un método de un componente.

En las figuras 6 y 7 se muestra cómo se ha comportado el acceso al sistema según los días de la semana y el horario del día, de tal manera los días laborables como era de esperar son los de mayor utilización, aunque llama la atención que el sábado y el domingo se mantiene el mismo, en el caso de las horas del día de mayor empleo predomina sobre todo entre las 9 y 11 de la mañana descendiendo progresivamente en la tarde.

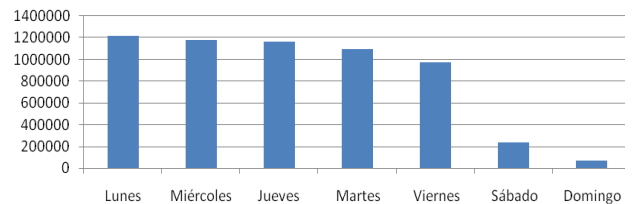


Figura 6: Acceso al sistema según día de la semana

Fuente: componente de seguridad

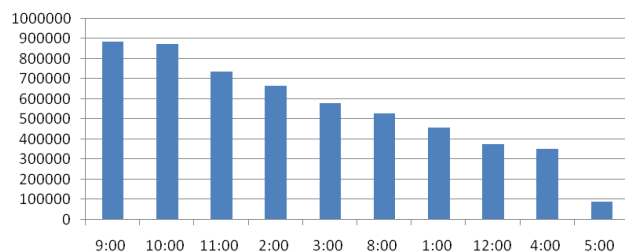


Figura 7: Accesos al sistema según horario del día

Fuente: componente de seguridad

3. CONCLUSIONES

1. Se implementó en el Sistema Nacional de Salud una solución tecnológica utilizando XML Web Services y elevados estándares de seguridad.

2. Fue implementado con éxito el servicio de Certificación Digital para el sector de la salud.
3. Se garantiza la confidencialidad e integridad de los datos y su manipulación por medio de usuarios con diferentes privilegios, roles y contraseñas.
4. El sistema utiliza una seguridad interna que asegura la defensa ante a los diferentes riesgos o ataques.
5. Se describe los principales procesos que deben tenerse en cuenta con el sistema de autenticación, auditoría, traza de los usuarios, sus permisos según nivel de acceso a la información según corresponda.

4. REFERENCIAS BIBLIOGRÁFICAS

1. Vidal Ledo, M., Obregón Martín, M., Gálvez González, A., Morales Valera, A., Gómez de Haz, H. et col. *Sistema de información en Salud: Herramienta para la toma de decisiones*. Rev. INFODIR. No. 13, 2011. [Consultado: 10/06/2012]. <http://bvs.sld.cu/revistas/infdir/n1311/infdir0313.htm>
2. Vidal Ledo, M., Castell-Florit Serrate, P. *La intersectorialidad y el uso de las tecnologías para la salud* [En: Intersectorialidad en salud. Fundamentos y aplicaciones]. La Habana, Editorial de Ciencias Médicas. ECIMED. 2010, [Consultado: 10/06/2012]. http://www.bvs.sld.cu/libros/intersectorialidad_salud_fundamentos/indice_p.htm
3. Vidal Ledo, M. *Primera estrategia para la informatización del sector de la Salud Pública*

Cubana. La Habana, Editorial de Ciencias Médicas. ECIMED. 2007, [Consultado: 10/06/2012]. http://www.bvs.sld.cu/libros/prim_estrategia_inform/index.htm

4. Delgado A., Cabrera, M., Rodríguez, A. *Estrategia de informatización del sistema nacional de salud*. [Ponencia: VIII Congreso Internacional de Informática en la Salud]. La Habana. [Consultado: 17/11/2009]. http://informatica2009.sld.cu/Members/mirnacabrera/estrategia-de-informatizacion-del-sistema-nacional-de-salud/at_download/trabajo

5. Delgado A., Rodríguez A., Cabrera M. *Solución informática integral para el Sistema Nacional de Salud. El Registro Informatizado de Salud (RIS)*, INFOLAC, 2008.

5. SÍNTESIS CURRICULAR DEL AUTOR PRINCIPAL

Mirna Cabrera Hernández, nacida 13 de enero de 1963, en La Habana, Cuba. Funcionaria de la Dirección de Informática y Comunicaciones. MINSAP. Graduada en ISPJAE de Ingeniería en Sistemas Automatizados de Dirección (SAD) en 1986. Máster en Ciencias Técnicas en Gestión de Proyectos Informáticos. Profesor Auxiliar de la Universidad de las Ciencias Informáticas, miembro de Tribunal de otorgamiento de Categoría Docente de Instructor y Asistente y miembro de las Sociedades Científicas de Salud Pública de Informática Médica. Más de 20 años activos con experiencia en el desarrollo de software y gestión de proyectos informáticos, desempeñando los roles de Jefe de Proyecto, Analista y Diseñador, Programador, Especialista de Calidad y Ejecutiva de ventas. Miembro de Tribunal de Tesis de Grado y Maestrías como Presidente, Tutor y Oponente. Más de 15 cursos recibidos, más de 20 eventos de salud y varias publicaciones en revistas (nacionales e internacionales).