¿Crees que tu información está segura? Seguridad de la información de los servicios web en las Entidades de Salud

Mauricio Agudelo Zapata, Institución Universitaria Salazar y Herrera, Octubre de 2016.

RESUMEN:

En este artículo se presenta un modelo enfocado en la formalización del contexto en las políticas de acceso, para el caso particular de las funcionalidades que apoyan los procesos eHealth publicadas como servicios. Dicho modelo tiene como objetivo indicar bajo qué condiciones un usuario puede acceder a datos sensibles asociados al historial médico de un paciente, considerando no solo su rol sino también meta-información almacenada en un log. La principal motivación para la formulación de dicho modelo es brindar mayor información que apoye la toma de decisión sobre el acceso a un recurso, permitiendo mejorar la seguridad, minimizando el riesgo de que sea usada para propósitos que se desvían de su uso inicial y mitigar el posible acceso de malware a los sistemas de información.

Palabras clave: políticas de acceso, modelo, información contextual, log, servicios Web.

ABSTRACT

This article presents a model focused on the formalization of context access policies, for the particular case of the functionalities that support processes eHealth services published as presented. This model is designed to show under what conditions a user can access sensitive data associated with the medical history of a patient, considering not only his role but also meta-information stored in a log. The main motivation for the development of this model is to provide more information to support decision making on access to a resource, allowing improving safety and minimizing the risk of being used for purposes that deviate from its initial use.

Keywords: access policies, model, contextual information, log, web services.

1. Introducción

Actualmente, los servicios web han cambiado la forma no solo de acceder a aplicaciones y funcionalidades sino también la forma como las organizaciones y las personas interactúan. Dicho cambio, se hace evidente al ver como actividades que eran anteriormente realizadas bajo paradigmas de interacción de persona-a-persona, son actualmente reemplazadas (parcial o totalmente) por servicios ofrecidos en Internet, bajo paradigmas de comunicación persona-máquina o máquina-máquina. Ejemplos de este fenómeno se encuentran en situaciones como el e-Shopping, las apuestas en línea, los servicios ofrecidos en la nube o incluso la creación de bancos virtuales. Esta mediación de la tecnología en la realización de actividades, ha generado nuevos modelos económicos como el consumo y la economía colaborativa (Sharing Economy).

Desde una aproximación tecnológica, los servicios web son simples aplicaciones informáticas similares a las tradicionales, pero basadas en principios de colaboración, distribución y reutilización. Por tanto, las soluciones informáticas (servicios) son concebidas desde su diseño y arquitectura para que puedan ser integradas a otras aplicaciones y ser (re)utilizadas por varios usuarios a través de Internet. Dichos principios de desarrollo pueden ser soportados por la arquitectura orientada a servicios SOA (Service Oriented Architecture). SOA, es un paradigma arquitectónico que se enfoca en la interoperabilidad de los sistemas de información a través de un principio de acoplamiento mínimo (loose coupling), es decir, esta arquitectura está basada en una definición de servicio que no incluye información de las dependencias entre el servicio y otros componentes. Como consecuencia, los servicios pueden ser integrados a otras aplicaciones de manera automática independientemente del lenguaje en el que ambos sean desarrollados o los sistemas operativos utilizados.

Particularmente, las entidades de salud (ES) están en una persistente búsqueda de integración de la información y comunicación unificada, dada la constante necesidad de renovar sus procesos debido a que se busca lograr mejores resultados en materia de equidad, eficiencia y calidad, por lo cual, utilizan las arquitecturas orientadas a los servicios web para optimizar recursos y procesos con fines de obtener información más ágil y segura, entre estos se encuentran actividades como el registro y lectura de la Historia Clínica Electrónica (HCE).

En este escenario, en lo que respecta a la información almacenada en la HCE, es de aclarar que dicha información es privada y de vital importancia para el paciente, por lo cual es necesario proteger y velar por la seguridad de todo lo que allí se registra con el fin de que ésta no sea usada para propósitos que se desvíen de su uso inicial, de hecho, para este fin existen varias regulaciones en Colombia tales como la ley 1581 de 2012 (COLOMBIA, Secretaría General de la Alcaldía Mayor de Bogotá D.C., 2012), la ley 1438 de 2011 (COLOMBIA, 2011), el decreto 1377 DE 2013 (COLOMBIA E. P., 2013), las cuales soportan y recalcan que la información personal es confidencial y debe ser manejada de forma privada y segura. No obstante, la falencia en los controles de seguridad de la información se hace más evidente en los servicios web, aunque estén basados en estándares, las técnicas de seguridad en los servicios web presentan retos adicionales, pues se trata de ambientes dinámicos, colaborativos y distribuidos.

Por lo cual, en este artículo se propone un modelo que representa la información contextual que ayude a la evaluación sobre si un recurso (en particular la HCE de los pacientes) puede ser accedido o no, basado en un registro (Log) de actividades, compuesto por historial de atención, registro de atención y registro de ingreso. En la sección 2 se presenta la revisión de literatura, en la cual se analizan diferentes enfoques propuestos en la literatura para dar solución a la problemática de la seguridad de la información; en la sección 3 se presenta la descripción y explicación del modelo, en la sección 4 se ilustra la validación del modelo propuesto y para finalizar una sección de conclusiones y trabajos futuros sobre la posible expansión de la solución propuesta.

2. Revisión de literatura

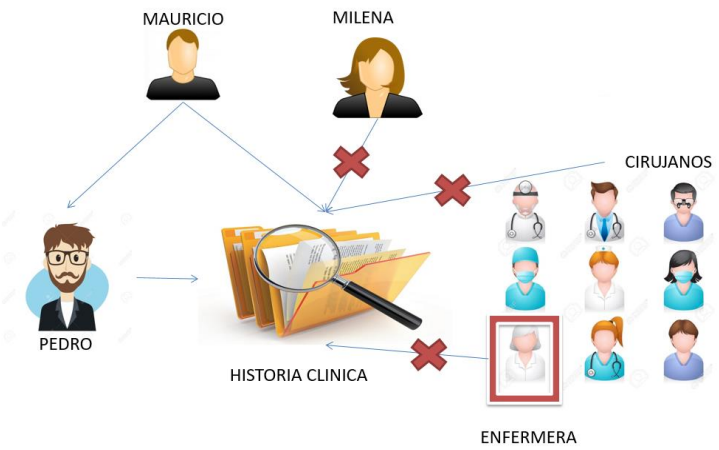
Para abordar la problemática de la seguridad de la información hay soluciones tanto desde el modelo como desde la implementación. El modelo RBAC (Role-based access control – Control de acceso basado en roles) (Habib, 2014), permite asignar privilegios de acceso mediante distribución por roles, es decir, para cada recurso, se especifican roles que pueden acceder a éste y a su vez a cada

persona se le asigna un rol, esto permite una simplificación en la definición de la política de seguridad ya que el acceso no es asignado individualmente a cada sujeto sino a un grupo de sujetos representado por un rol. De igual forma, OrBAC (OrBAC, 2013), se basa en tres entidades, a saber: sujeto, acción y objeto, para definir políticas de seguridad; dicho modelo es similar a RBAC dado a que también trabaja con entidades abstractas, pero incluye el modelo basado en Organización y contexto, el cual permite describir en que condición se aplicarán las reglas que autorizan el acceso a un recurso. Variaciones de OrBAC como MultiOrBAC, TorBAC, MultiTrusOrBAC incluyen aspectos como definición de políticas de seguridad inter-organizacionales, nivel de confianza y penalidad.

Actualmente, a pesar de que sistemas de seguridad basados en modelos como RBAC, OrBAC, entre otros, están bien estructurados al interior de la mayoría de las ES, no son suficientes para prevenir que la información de los pacientes y su HCE esté segura, debido a que aún hay una limitación, la cual es que los modelos mencionados trabajan con información contextual estática, la información contextual es aquella que está relacionada con las circunstancias de un evento en particular, es decir, a manera de ejemplo:

Mauricio es Cirujano, Milena es Cirujano, Pedro es operado por Mauricio, por lo tanto, dado a que ambos tienen el mismo rol, Milena podrá acceder a la información de Pedro aunque no tenga ningún tipo de relación con el paciente. Si en una ES hay aproximadamente 30 cirujanos, todos podrán acceder a la información de Pedro, anexo a este ejemplo, en el caso de tener una política basada en contexto, si se cuenta con una política que permita el acceso a la información, la cual se aplica para el rol de Enfermera, siempre y cuando el paciente entre en un estado de emergencia, el rol de Enfermera también podrá acceder a la información de Pedro; lo cual aumenta el riesgo de que la información sea usada para propósitos que se desvían de su uso inicial e incrementa el posible acceso de malware a los sistemas de información, generando así consecuencias graves como fraude, extorsión, suplantación, entre otros. Estos casos no son aislados y se han visto en otros escenarios como bancos donde los propios empleados de la organización han utilizado de manera incorrecta información sensible de sus clientes (Ernst & Young, 2011).

Dada esta limitación, un modelo enfocado en el historial de atención, registro de atención y de ingreso realizado diariamente por los usuarios, logrará establecer una política de acceso mucho más certera dado a que se tendrá información contextual constantemente actualizada y se dará acceso a dicha información el personal interno y externo que tenga algún tipo de relación con el paciente, es decir, basados en el ejemplo planteado anteriormente:



A pesar de que Mauricio y Milena tienen el mismo rol, Milena no podrá acceder a la información de Pedro dado a que no tiene ningún tipo de relación con el paciente, permitiendo así el acceso a la información solamente a las personas que pertenezcan al proceso de atención del paciente.

La insuficiencia en la seguridad de la información se evidencia aún más en las cifras presentadas por entes nacionales e internacionales. En cuanto a los entes nacionales, la superintendencia de industria y comercio de Colombia revela cifras para el primer semestre 2014, con 19 sanciones en materia de protección de datos personales a diferentes compañías del país por un valor de $ 686.224.000 millones de pesos (comercio, 2014). Y en cuanto a entes internacionales, la compañía a nivel mundial Cisco, reportando en el informe anual de seguridad del año 2015 (CISCO, 2015), que el 25% de las vulnerabilidades son generadas por fraudes y además a modo de conclusión respecto a la visión sobre la ciberseguridad, informan que es más importante que "*comprendan que la seguridad es un problema relacionado con las personas, que la vulnerabilidad es inevitable y que ha llegado el momento de adoptar un nuevo planteamiento de seguridad.*"

3. **Modelo ES.**

Las ES son empresas especializadas en la prestación de servicios de salud, servicios como consultas médicas, hospitalización, urgencias y cirugía, dichos servicios son trabajados en conjunto por todos los colaboradores que hacen parte de las ES, los cuales están clasificados y categorizados en: personal administrativo, personal asistencial y personal externo. La prestación de servicios de las ES está ligada a procesos estándares debido a que se busca lograr mejores resultados en materia de equidad, eficiencia y calidad. Es de aclarar que en Colombia las ES y sus procesos están bajo la supervisión de la Superintendencia Nacional de Salud (SuperSalud, s.f.).

Uno de los procesos estandarizados es el de registros de atención (Historia Clínica Electrónica - HCE) el cual es alimentado por el personal asistencial de las ES, en éste se encuentra que a los pacientes se les asigna un médico específico y/o en caso de ser hospitalizado, una enfermera, dichas personas son las encargadas de registrar la atención de los pacientes a través de "notas". En las notas se especifica el diagnóstico realizado por el médico y las actividades realizadas por las enfermeras a los pacientes.

Con el fin de lograr que el registro y lectura de la HCE sea de fácil acceso para los usuarios que lo requieran, incluyendo auditores externos, las ES tienden a utilizar los servicios web con fines de integración y comunicación unificada generando obtener ventajas competitivas desde el punto de vista organizacional y tecnológico para así lograr un servicio de alta disponibilidad y calidad.

De igual forma y en lo que respecta a la información almacenada en las notas de la HCE, es privada y de vital importancia para el paciente, por lo cual es necesario proteger y velar por la seguridad de todo lo que allí se registra, con el fin de que esta no sea usada para propósitos que se desvíen de su uso inicial.

Teniendo en cuenta lo anterior, es importante tener presente que hay casos en los cuales la información de los pacientes en las ES ha sido usada para propósitos que se desvían de su uso inicial, incluyendo información personal (ej. nombre, dirección, etc.) e historia clínica. Por lo cual, se logra inferir que los métodos actuales de seguridad no son suficientes para que dicha información se encuentre segura, en consecuencia, las ES ven la necesidad de permitir el acceso a la información de los pacientes, netamente a las personas que participen en su proceso de atención, debido a que en este momento no se tiene un control detallado de quien puede acceder a esta información y así dar cumplimiento a la normatividad vigente.

Para dar solución a la problemática que se presenta en la seguridad de la información del paciente, se tendrá en cuenta que para dar acceso a dicha información el personal interno y externo deberá tener algún tipo de relación con el paciente, es decir, basados en un historial de atención, registro de ingreso y registro de atención, se planteara la política de acceso a la información del paciente, como se menciona en el ejemplo anterior: Mauricio es Cirujano, Milena es Cirujano, Pedro es operado por Mauricio, por lo tanto y a pesar de que ambos médicos tienen el mismo rol, Milena no podrá acceder a la información de Pedro dado a que no tiene ningún tipo de relación con el paciente.

Por lo anterior, se construye un modelo el cual logrará detectar información contextual de manera constante la cual nos permitirá tomar una decisión más certera sobre bajo qué condiciones un usuario puede acceder a la información sensible, a diferencia de los demás modelos que cuenta con información contextual estática, y así la información de las personas estará más segura ya que se minimizará el riesgo de que sea usada para propósitos que se desvíen de su uso inicial.

El modelo estará compuesto por:

Entidad de salud: Se tendrá registro de los datos básicos de la ES.
Personal Interno: El personal interno es todo el personal que trabaja su jornada laboral completa en la ES, dicho personal está dividido en Administrativo, de atención y atención médica.
Personal Externo: En el personal externo encontramos todos los terceros que se asocian con la ES, como por ejemplo, seguro obligatorio, servicios de anestesiología, Auditores externos, organizaciones externas, etc.
Paciente: Se tendrá un registro de todos los servicios que ha solicitado un usuario de la ES y además tendrá relación con el almacenamiento de historia clínica electrónica.
Servicios: Es de aclarar que esta entidad es referente a los servicios prestados por las ES, es decir, servicio de rayos x, urgencias, etc.
Historial de atención: El personal de atención Médica llevará un registro de cada una de las acciones que realice en su proceso de atención con el fin de tener almacenados la sucesión de eventos (episodios) y así generar la historia clínica del paciente.
Registro de atención: El personal de atención (Médica y administrativo) llevara un registro de todos los pacientes que ha atendido, con el fin de dar acceso netamente a los datos de los pacientes

con los que se ha tenido contacto.

Registro de Ingreso: El personal interno y externo de las ES llevaran un registro de ingreso al sistema, el cual estará compuesto por, hora, salida y ubicación de ingreso del usuario.

Cada una de las entidades descritas son necesarias para definir un registro detallada y constante de cada actividad que se realiza en la entidad de salud, más específicamente con la información conjunta del historial de atención, el registro de atención y registro de ingreso se logrará tener un criterio más sólido para definir la política de acceso a la información.

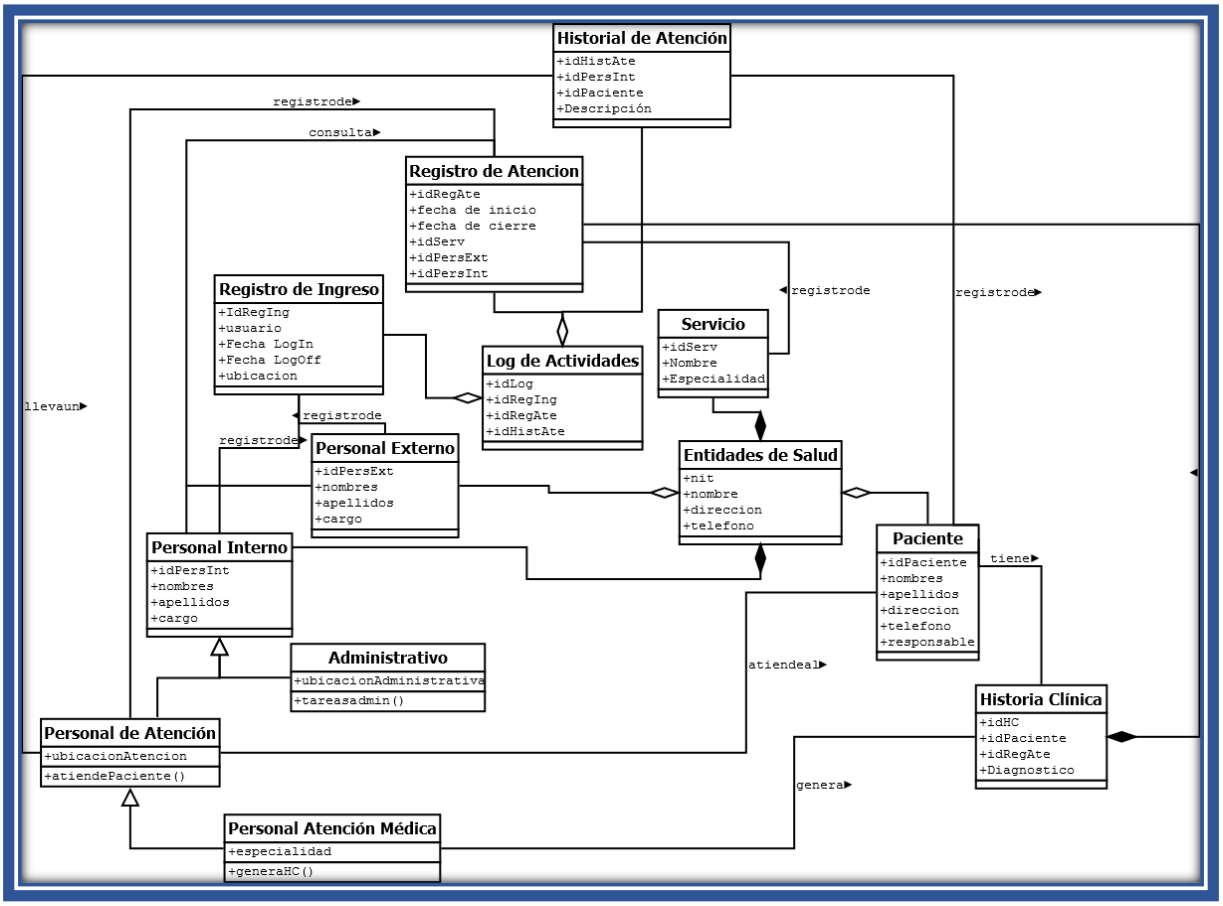


Ilustración 1 Modelo ES.

En la ilustración 1 Modelo ES, se grafica el modelo, su **principal funcionamiento** radica en la entidad **Log de Actividades**, el cual está compuesto por Registro de Ingreso, Registro de Atención e Historial de Atención, como se mencionaba anteriormente, es allí de donde se obtiene la información contextual actualizada, que nos permitirá tomar decisiones sobre los privilegios de acceso a la información del paciente, además, en la gráfica se incluye la interacción de cada uno de los participantes del proceso (los pacientes y su historia clínica, personal externo e interno).

4. **Validación**

4.1. Implementación del Modelo en XML

La implementación se realizó sobre la plataforma ECLIPSE, se utilizó Java, se construyó un archivo .XSD con la estructura del modelo representado en XML, debido a que este tipo representación apoya la interoperabilidad requerida por SOA y además los mensajes SOAP permiten añadir meta-información en el header del mensaje.

4.1.1. Archivo .xsd.

En la ilustración 2 se observa un esquema .xsd con los elementos que componen el log de actividades (registro de ingreso, registro de atención e historial de atención). Se plantea una propuesta inicial con el fin de dar a conocer su funcionamiento, por lo cual, se aclara que este puede extenderse hacia un modelo genérico.

```
<?xml version="1.0" encoding="utf-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:mauro="http://localhost:8080/axis2/pruebas/ModeloES.xsd"
            targetNamespace="http://localhost:8080/axis2/pruebas/"
            elementFormDefault="qualified">

      <element name='logdeactividades'>
        <complexType>
          <sequence>
              <element name='registrodeingreso'>
                <complexType>
                  <sequence>
                <element name='idreging' type='string'/>
                    <element name='usuario' type='string'/>
                    <element name='fechalogin' type='string'/>
                    <element name='fechaloff' type='string'/>
                    <element name='ubicacion' type='string'/>
                  </sequence>
                </complexType>
              </element>

              <element name='registrodeatencion'>
                <complexType>
                  <sequence>
                    <element name='idPaciente' type='string'/>
                    <element name='fechainicio' type='string'/>
                    <element name='fechacierre' type='string'/>
                    <element name='idserv' type='string'/>
                    <element name='idpersext' type='string'/>
                <element name='idpersint' type='string'/>
                  </sequence>
                </complexType>
              </element>

            <element name='historialdeatencion'>
              <complexType>
                <sequence>
                  <element name='idhistAte' type='string'/>
                  <element name='idpersint' type='string'/>
                  <element name='idPaciente' type='string'/>
                  <element name='descripcion' type='string'/>
                </sequence>
              </complexType>
            </element>
          </sequence>
        </complexType>
      </element>
</xsd:schema>
```

Ilustración 2 Esquema XSD

4.1.2. Validación del modelo en el archivo de configuración .wsdl.

En la ilustración 3, se evidencia la configuración en el archivo .wsdl del esquema creado y evidenciado en la ilustración 2.

```
<wsdl:types>
  <xsd:schema targetNamespace="http://ttdev.com/ss" xmlns:xsi="http://localhost:8080/axis2/pruebas/ModeloES.xsd">

         <xsd:element name='logdeactividades'>
             <xsd:complexType>
               <xsd:sequence>
                   <xsd:element name='registrodeingreso'>
                     <xsd:complexType>
                       <xsd:sequence>
                         <xsd:element name='idreging' type="xsd:string" />
                         <xsd:element name='usuario' type="xsd:string"/>
                         <xsd:element name='fechalogin' type="xsd:string"/>
                         <xsd:element name='fechaloff' type="xsd:string"/>
                         <xsd:element name='ubicacion' type="xsd:string"/>
                       </xsd:sequence>
                     </xsd:complexType>
                   </xsd:element>

                   <xsd:element name='registrodeatencion'>
                     <xsd:complexType>
                       <xsd:sequence>
                         <xsd:element name='idPaciente' type="xsd:string"/>
                         <xsd:element name='fechainicio' type="xsd:string"/>
                         <xsd:element name='fechacierre' type="xsd:string"/>
                         <xsd:element name='idserv' type="xsd:string"/>
                         <xsd:element name='idpersext' type="xsd:string"/>
                         <xsd:element name='idpersint' type="xsd:string"/>
                       </xsd:sequence>
                     </xsd:complexType>
                   </xsd:element>

                  <xsd:element name='historialdeatencion'>
                    <xsd:complexType>
                      <xsd:sequence>
                        <xsd:element name='idhistAte' type="xsd:string"/>
                        <xsd:element name='idpersint' type="xsd:string"/>
                        <xsd:element name='idPaciente' type="xsd:string"/>
                        <xsd:element name='descripcion' type="xsd:string"/>
                      </xsd:sequence>
                    </xsd:complexType>
                  </xsd:element>
               </xsd:sequence>
             </xsd:complexType>
           </xsd:element>
```

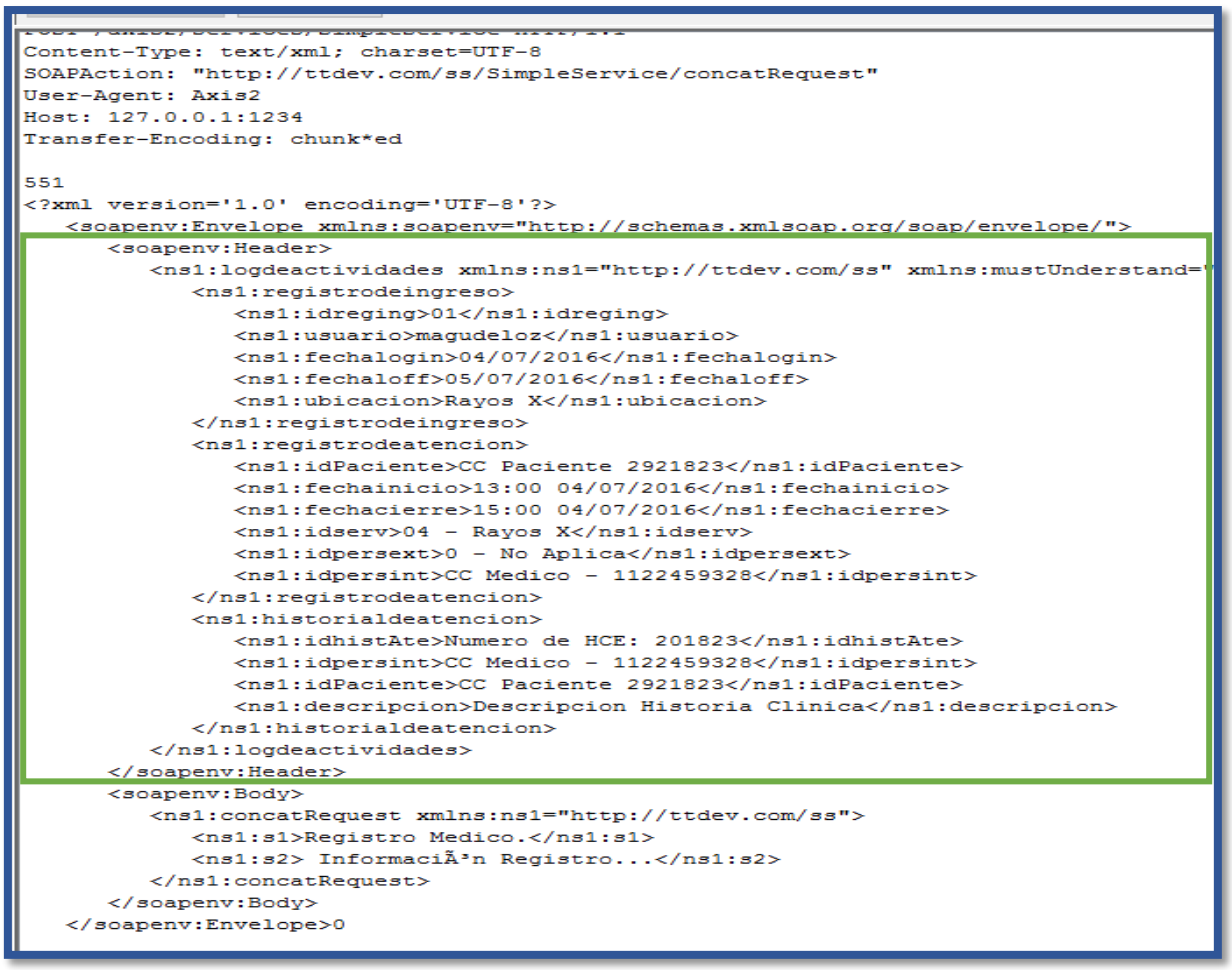
Ilustración 3 Validación en .WSDL

4.1.3. Añadiendo el modelo mediante un ejemplo al header del mensaje SOAP.

En la ilustración 4 se evidencian las pruebas de funcionamiento del log de actividades y se verifica que la información que seleccionamos (esquema xsd) sea enviada en el head del mensaje SOAP.

Ilustración 4 Prueba Funcionamiento

En la ilustración 5 se evidencia el resultado de la información que elegimos (esquema .xsd) transportada en el head del mensaje SOAP.



```
Content-Type: text/xml; charset=UTF-8
SOAPAction: "http://ttdev.com/ss/SimpleService/concatRequest"
User-Agent: Axis2
Host: 127.0.0.1:1234
Transfer-Encoding: chunk*ed

551
<?xml version='1.0' encoding='UTF-8'?>
   <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
      <soapenv:Header>
         <ns1:logdeactividades xmlns:ns1="http://ttdev.com/ss" xmlns:mustUnderstand="
            <ns1:registrodeingreso>
               <ns1:idreging>01</ns1:idreging>
               <ns1:usuario>magudeloz</ns1:usuario>
               <ns1:fechalogin>04/07/2016</ns1:fechalogin>
               <ns1:fechaloff>05/07/2016</ns1:fechaloff>
               <ns1:ubicacion>Rayos X</ns1:ubicacion>
            </ns1:registrodeingreso>
            <ns1:registrodeatencion>
               <ns1:idPaciente>CC Paciente 2921823</ns1:idPaciente>
               <ns1:fechainicio>13:00 04/07/2016</ns1:fechainicio>
               <ns1:fechacierre>15:00 04/07/2016</ns1:fechacierre>
               <ns1:idserv>04 - Rayos X</ns1:idserv>
               <ns1:idpersext>0 - No Aplica</ns1:idpersext>
               <ns1:idpersint>CC Medico - 1122459328</ns1:idpersint>
            </ns1:registrodeatencion>
            <ns1:historialdeatencion>
               <ns1:idhistAte>Numero de HCE: 201823</ns1:idhistAte>
               <ns1:idpersint>CC Medico - 1122459328</ns1:idpersint>
               <ns1:idPaciente>CC Paciente 2921823</ns1:idPaciente>
               <ns1:descripcion>Descripcion Historia Clinica</ns1:descripcion>
            </ns1:historialdeatencion>
         </ns1:logdeactividades>
      </soapenv:Header>
      <soapenv:Body>
         <ns1:concatRequest xmlns:ns1="http://ttdev.com/ss">
            <ns1:s1>Registro Medico.</ns1:s1>
            <ns1:s2> InformaciÃ³n Registro...</ns1:s2>
         </ns1:concatRequest>
      </soapenv:Body>
   </soapenv:Envelope>0
```

Ilustración 5 Mensaje SOAP

Cabe recordar, que la información que se encuentra en el header del mensaje SOAP es meta-información, es decir, no es visible ante el usuario final que usa el servicio, por lo cual, se alcanza un nivel de seguridad mayor si se trabaja en conjunto con las políticas de acceso a la información.

Algunos ejemplos de aplicación y/o lectura de reglas de accesos mediante la información suministrada en el header del mensaje SOAP:

- Con los elementos de la entidad historial de atención, se tomará la decisión de otorgar los permisos al médico que realizó la atención para acceder a la información del paciente que se registra con el número de HCE asignado.

- Con los elementos de la entidad registro de ingreso se podría comparar con la información que hay en la reglas de acceso al sistema según su hora y/o fecha.

- Con la información de la entidad de registro de atención se tomará la decisión de dar acceso a la información del paciente al personal externo que se registra en la atención.

5. **Conclusiones y trabajo futuro.**

Este trabajo de investigación es de vital importancia tanto para los profesionales en ingeniería informática como para la sociedad en general, ya que este será un incentivo para que las compañías adopten medidas de seguridad de la información día a día, mediante el modelo basado en un log de actividades, ayudará a las compañías a definir una política de seguridad sólida que permitirá el acceso a la información adecuadamente y a su vez este logrará incrementar el nivel de seguridad de la información en los servicios web, en esta ocasión, en las entidades de salud, con la finalidad de que la información de las personas este más segura y logre minimizar el riesgo de que sea usada para propósitos que se desvían de su uso inicial y mitigar el posible acceso de malware a los sistemas de información.

Se pretende extender el modelo para que este sea genérico y así lograr que cualquier tipo de compañía lo pueda implementar, para esto, se tomara como base y equivalencias con otros modelos como OrBAC (OrBAC, 2013), dado a que trabaja con roles y además incluye el modelo basado en Organización y contexto, el cual permite describir en que condición se aplicarán las reglas que autorizan el acceso a un recurso.

6. **Referencias.**

[1] CAMP, C. (2 de MAR de 2015). welivesecurity. Obtenido de http://www.welivesecurity.com/la-es/2015/03/02/robo-de-registros-datos-salud-informacion-medica/

[2] Christoph, R., & Steffen, S. (2007). Logging in Distributed Workflows. Busan, Korea: PEAS 2007.

[3] CISCO. (2015). Obtenido de http://www.cisco.com/c/dam/global/es_es/assets/pdf/asr_final_os_ah_es.pdf

[4] COLOMBIA, E. C. (19 de Enero de 2011). Secretaría General de la Alcaldía. Obtenido de Ley 1438 de 2011 Nivel Nacional: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[5] COLOMBIA, E. C. (17 de Octubre de 2012). Secretaría General de la Alcaldía Mayor de Bogotá D.C. Obtenido de Ley 1581 de 2012: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[6] COLOMBIA, E. P. (27 de Junio de 2013). Secretaría General de la Alcaldía Mayor de Bogotá D.C. Obtenido de Decreto 1377 de 2013 : http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0

[7] comercio, S. d. (2014). Obtenido de http://www.sic.gov.co/drupal/sites/default/files/files/informe_consolidado_sanciones_1_2014_VERSION_SIC.pdf

[8] Damiani, E., Coviello, V., Frati, F., & Santacesaria, C. (2014). The Problem of Handling Multiple Headers in WSSecurity. Computer Software and Applications Conference Workshops (COMPSACW) (págs. 396-400). IEEE 38th International.

[9] M. A. Habib, N. Mahmood, M. Shahid, M. U. Aftab, U. Ahmad and C. M. N. Faisal, "Permission based implementation of Dynamic Separation of Duty (DSD) in Role based Access Control (RBAC)," *Signal Processing and Communication Systems (ICSPCS), 2014 8th International Conference on*, Gold Coast, QLD, 2014, pp. 1-10.

[10] Kent, T. K. (2010). Developing Web Services with Apache CXF and Axis2 (3rd ed.).

[11] OrBAC. (2013). *OrBAC: Organization Based Access Control*. Obtenido de http://orbac.org/

[12] SuperSalud. (s.f.). SuperSalud. Obtenido de https://www.supersalud.gov.co/es-co

[13] Web Services Reliable Messaging TC WSReliability 1.1. (15 de Noviembre de 2004). Obtenido de OASIS Standard.: http://docs.oasisopen.org/wsrm/wsreliability/v1.1

[14] WSCoordination 1.2. (02 de Febrero de 2009). Obtenido de OASIS Standard incorporating Approved Errata.: http://docs.oasisopen.org/wstx/wstxwscoor1.2spec.html

[15] WSS: SOAP Message Security WSSecurity. (1 de Febrero de 2006). Obtenido de OASIS Standard.: https://www.oasisopen.org/committees/download.php/16790/wssv1.1specosSOAPMessage Security.pdf

[16] WSTrust 1.4. (25 de April de 2012). Obtenido de OASIS Standard incorporating Approved Errata.: http://docs.oasisopen.org/wssx/wstrust/v1.4/errata01/os/wstrust1.4errata01osc

[17] Ernst & Young. (2011). Data loss prevention Keeping your sensitive data out of the public domain. Reino Unido.