Mecanismos lógicos de seguridad en la gestión de datos geológicos

Autor: Rocny Morales Delgado - 24-08-2009
https://vinculando.org/documentos/mecanismos_logicos_de_seguridad_sistema_de_administracion_de_datos.html

Introducción

Con el decursar de los siglos el hombre ha buscado incansablemente la manera de desarrollarse y así hacer su vida más cómoda y llevadera. Siempre ha estado intentado cambiar el medio ambiente que lo rodea, esto lo ha logrado creando, descubriendo y estudiando diferentes eventos que ocurren a su alrededor. De esta forma han transcurridos diferentes etapas en la historia de la humanidad. La actualidad se encuentra enmarcada en la época de la información, donde la mayoría de los procesos están controlados por microprocesadores, y la información está almacenada en servidores informáticos.

Cuba no está ajena al desarrollo mundial alcanzado en los últimos años referido a las Tecnología de la Información y las Comunicaciones (TIC) y conoce la importancia que tiene mantenerse al día en este sentido. De ahí que ha tomado la inteligente estrategia de informatizar los procesos referentes a la industria, la producción y la sociedad en general. Como parte de esta tarea se encuentra el Programa Nacional de Informatización del Conocimiento Geológico, mediante el cual se pretende realizar la informatización de los procesos llevados a cabo en la Oficina Nacional de Recursos Minerales (ONRM).

La Oficina Nacional de Recursos Minerales fue creada en 1995 con la promulgación de la Ley de Minas la cual la inviste como la Autoridad Minera del país. Hereda y acrecienta las funciones del Centro Nacional del Fondo Geológico, su precursor, el cual realizaba esta tarea desde su fundación en 1960. Pertenece al Ministerio de la Industria Básica pero su esfera de influencia y acción se extiende a todos los órganos y organismos de la administración central del Estado. Es la entidad que vela por el aprovechamiento racional de los recursos minerales del país y constituye el órgano que controla el proceso concesionario, ordenando y fiscalizando la actividad geológica, minera y petrolera de la República de Cuba. La Oficina Nacional de Recursos Minerales cuenta en la actualidad con un sistema para gestionar la información que se encuentra en forma digital, aún así tiene la necesidad de mejorar dicho sistema ya que la información no se encuentra almacenada de forma persistente, además no cuenta con un sistema de consulta en línea de la información lo cual provoca que esta sea poco accesible suscitando un proceso tedioso que genera pérdida de tiempo a la hora de gestionar y consultar la misma. (1)

El Programa Nacional de Informatización del Conocimiento Geológico es desarrollado por un equipo de trabajo de la Facultad 9 de la Universidad de la Ciencias Informáticas (UCI). Dada la gran envergadura del proyecto se ha dividido en ocho módulos (Balance Agua, Balance Minerales, Balance Petróleo, Base de Datos Referativa, Concesionario Minerales, Concesionario Petróleo, Metadatos y Nomencladores) que serán los encargados de informatizar la mayoría de los procesos que en la actualidad se realizan de forma tradicional como son el registro y almacenamiento de la información referente a la actividad minera, así como su consulta fundamentalmente para la toma de decisiones.

Con la unión de los módulos anteriormente mencionados se conformará el Sistema de Gestión de Datos Geológicos, el cual almacenará y gestionará toda la información referente a la actividad minera en el país. Como parte principal de la información a proteger se encuentra el conocimiento adquirido sobre el níquel y el petróleo, el primero ya es parte importante de nuestra economía y el segundo puede llegar a convertirse también en un renglón importante de la misma. Dada la sensibilidad de la información anteriormente mencionada, por solo mencionar dos ejemplos, y su importancia para la economía se hace necesario implementar los mecanismos de seguridad que garanticen la integridad de la misma. Más aún si se tiene en cuenta que dos de los módulos mencionados estarán de cara a Internet (Base de Datos Referativa, Metadatos).

La seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico. Por ejemplo, cuando se guardan cosas en una caja fuerte en un banco real, no se piensa que cualquier persona del mundo puede llegar a ésta de una forma inmediata como si se tratara, en lugar de un banco, de una estación de autobuses. En el mundo intangible de la informática, tan cerca de un servidor están sus usuarios legítimos como los usuarios que hacen uso de la misma red de comunicaciones. Es más, estos usuarios, en el caso de una red global, se cuentan por millones. Algunos serán “buenos vecinos” pero otros serán agentes hostiles. De ahí que la seguridad de un sistema informático sea de gran importancia ya que permite preservar la confidencialidad e integridad de la información que se gestiona.

Desarrollo

Mecanismos Lógicos de Seguridad Informática (15)

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y la disponibilidad de un sistema informático. Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

Los mecanismos de seguridad informática se clasifican según su función:

> Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
> Detectivos: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.
> Correctivos: Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

Mecanismos de seguridad en la actualidad existen muchos. Es de vital importancia el conocimiento y aplicación de los mismos, para lograr crear un sistema informático seguro. Siempre tener en cuenta que la seguridad de un sistema informático nunca es a un 100% de ahí que siempre debamos estar alertas. Entre los mecanismos más utilizados y recomendados de la actualidad están:

> Encriptación o cifrado de datos: Es el proceso que se sigue para enmascarar los datos, con el objetivo de que sean incomprensibles para cualquier agente no autorizado. Los datos se enmascaran usando una clave especial y siguiendo una secuencia de pasos pre-establecidos, conocida como algoritmo de cifrado. El proceso cifrado inverso se conoce como descifrado, usa la misma clave y devuelve los datos a su estado original.
> Mecanismos de autenticación e identificación: Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto. Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios. Existen dos grados en el mecanismo de autenticación.
> 1. Autentificación simple. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.
> 2. Autentificación fuerte. Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que

obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado. Un certificado es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario.

Mecanismos de control de acceso: Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema. Dentro de Unix, el control de acceso más habitual es el discrecional (DAC, Discretionary Access Control), implementado por los bits rwx y las listas de control de acceso para cada fichero del sistema; sin embargo, también se permiten especificar controles de acceso obligatorio (MAC).
Mecanismos de separación: Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre

objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso. Los mecanismos de separación se dividen en cinco grandes grupos, en función de cómo separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación. Dentro de Unix, el mecanismo de separación más habitual es el de separación lógica o aislamiento, implementado en algunos sistemas mediante una Base Segura de Cómputo (TCB).
Mecanismos de seguridad en las comunicaciones: Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, hemos de utilizar ciertos mecanismos, la mayoría de los cuales se basan en la Criptografía: cifrado de clave pública, de clave privada, firmas digitales...Aunque cada vez se utilizan más los protocolos seguros (como SSH o Kerberos, en el caso de sistemas Unix en red), aún es frecuente encontrar conexiones en texto claro ya no sólo entre máquinas de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red.
Anti-virus: Ejercen control preventivo, detectivo y correctivo sobre ataques de virus al sistema.
Firewall: Ejercen control preventivo y detectivo sobre intrusiones no deseadas a los sistemas.
Software para sincronizar transacciones: Ejercen transacciones control sobre las transacciones que se aplican a los datos.
Planes de recuperación o planes de contingencia: Es un esquema que específica los pasos a seguir en caso de que se interrumpa la actividad del sistema, con el objetivo de recuperar la funcionalidad. Dependiendo del tipo de contingencia, esos pasos pueden ejecutarlos personas entrenadas, sistemas informáticos especialmente programados o una combinación de ambos elementos.
Respaldo de los datos: Es el proceso de copiar los elementos de información recibidos, transmitidos, almacenados, procesados o generados por el sistema. Existen muchos mecanismos para tomar respaldo, dependiendo de lo que se quiera asegurar. Algunos ejemplos son: Copias de la información en dispositivos de almacenamiento secundario, computadores paralelos ejecutando las mismas transacciones.
Punto de choque: Esta estrategia consiste en depender de un único punto de acceso al sistema. Ya que no existe otro camino, los esfuerzos de control y mecanismos de seguridad se centran y simplifican en monitorear un solo sitio de la red. Este punto debe estar fuertemente defendido contra todo tipo de ataques y estar listo para responder si los detecta. Hay muchos ejemplos de puntos de choque en la vida cotidiana: los pasos fronterizos, las cajas registradoras de un supermercado, la taquilla de un cine.

Esta estrategia se considera como una solución todo en uno. Como consecuencia, uno de los problemas que presenta es que si un atacante es capaz de traspasar la seguridad de este único punto del acceso tendrá

acceso a todos los recursos del sistema. Esta situación puede ser tratada utilizando mecanismos de protección redundantes (defensa a fondo) y así reforzar la seguridad de dicho punto. Otro de los inconvenientes que puede

provocar esta estrategia, es que pueden producirse bajas en el desempeño si se ve superada la capacidad del punto de acceso de registrar los sucesos y controlar todo el tráfico de entrada y salida.

La estrategia del punto de choque no es útil si existe una forma alternativa de acceder a la red, por lo que estos caminos deben ser cuidadosamente localizados y restringidos del acceso exterior.

> El eslabón más débil: Se basa en la idea de que una cadena es tan fuerte como su eslabón más débil. Se deben conocer los puntos débiles de las defensas para, si es posible, eliminarlos o monitorizarlos. Aunque no por esto debe restarse importancia a la seguridad de otros aspectos del sistema.

Siempre habrá algún punto que será el más débil de todos, la idea es que ese enlace debe ser lo suficientemente seguro en proporción al riesgo que implica que sea vulnerado. Algunos afirman que el eslabón más débil en la cadena de la seguridad informática es el usuario.

Además, diversos sistemas configurados por la misma persona (o el mismo grupo de personas) pueden compartir problemas comunes, por ejemplo, si el problema es un malentendido sobre cómo funciona un protocolo específico, todos sus sistemas pueden estar configurados incorrectamente siguiendo ese malentendido. Por eso, adicionalmente estos sistemas pueden ser configurados por distintos administradores de seguridad para evitar que algún error conceptual por parte de los mismos afecte a la protección completa. Aunque se reconoce que utilizar múltiples tipos de Sistemas de Seguridad pueden potencialmente incrementar la seguridad, con frecuencia se concluye que la diversificación de defensas requiere más trabajo de lo que vale, y que las ganancias y mejoras no compensan el costo.

> Simplicidad: La simplicidad es una estrategia de seguridad que se basa en dos principios:
> 1. Mantener las cosas sencillas las hace más fáciles de comprender. Si algo no se entiende, no se puede saber si es seguro o no.
> 2. Lo complejo proporciona muchos escondites para que se oculten toda clase de cosas.

Se sabe que cuanto más grande y complejo es un sistema, más errores tendrá, será más difícil de utilizar y más costoso de testear. Además, probablemente posea agujeros de seguridad no conocidos que un atacante puede explotar, por más complejos que sean.

La simplicidad de los sistemas de seguridad es un factor importante de una sólida defensa de red. Particularmente los sistemas de seguridad de red a nivel de aplicación no deberían tener funcionalidades desconocidas y deberían mantenerse lo más simples posible.

> Falla segura: Como ya se dijo anteriormente la seguridad absoluta no existe, por tanto, en la medida de lo posible los sistemas deben tener una falla segura, es decir, si van a fallar deben hacerlo de tal forma que nieguen el acceso a un atacante en lugar de dejarlo entrar, o dejen de funcionar si detectan alguna anomalía.

La estrategia de falla segura es ampliamente aplicada en la vida diaria. Los dispositivos eléctricos están diseñados para apagarse cuando fallan de alguna forma.

> Menor privilegio: Este es uno de los principios más fundamentales de seguridad. La estrategia consiste en conceder a cada objeto (usuario, programa, sistema, etc.) solo aquellos permisos o privilegios que son necesarios para realizar las tareas que se programó para ellos. El tipo de objeto al cual se apliquen los permisos determinará la granularidad el grado de detalle de la seguridad obtenida. Esta estrategia permite limitar la exposición a ataques y limitar el daño causado por ataques particulares. Se basa en el razonamiento de que todos los servicios ofrecidos por una red están pensados para ser utilizados por algún perfil de usuario en particular, y no que todos los usuarios pueden utilizar todos los servicios de la red. De

esta forma es posible reducir los privilegios requeridos para varias operaciones sin afectar al servicio prestado a los usuarios del sistema.
Estado a prueba de fallos: Uno de los principios fundamentales en la seguridad es que si un mecanismo de seguridad fallara, debería negarse el acceso a todo usuario, inclusive aquellos usuarios permitidos ya que no se puede determinar si lo son si la función de autenticación no está funcionando, es decir debe fallar en un estado seguro. Este principio debe ser considerado al diseñar firewalls de Internet. Los filtros de paquetes, deben fallar en tal forma que el tráfico desde y hacia Internet sea detenido. La mayoría de las aplicaciones y dispositivos utilizados en una solución firewall, como routers de filtrado de paquetes y servidores proxy, dejan de retransmitir información si fallan.

Esta estrategia está apoyada por la implementación de una posición específica con respecto a decisiones de seguridad y políticas. Existen dos posibles posiciones:

1. Rechazar por defecto, estableciendo cuales son los servicios que serán permitidos, cualquier otro será rechazado.
2. Aceptar por defecto, estableciendo cuales son los servicios que no son permitidos, cualquier otro será aceptado.

Es claro que la posición de rechazar por defecto es una estrategia a prueba de fallos ya que si el mecanismo falla no habrá comunicación se que sea aceptada. Por otro lado, la posición de Aceptar por defecto, asume que todo es permitido a menos que se conozca que es inseguro, en cuyo caso se prohíbe su acceso. Esta posición no es en absoluto una implementación de una estrategia de estado a prueba de fallos.

Participación universal: Más que una estrategia, es un principio que debería cumplir toda solución de seguridad. Se plantea que todo individuo en la organización que posee la red privada debe colaborar en mantener y cumplir las Medidas de Seguridad que permitan ofrecer una protección efectiva sus sistemas. De otra forma, un atacante podría aprovechar la debilidad de aquellos sistemas a cargo de estas personas para poder llegar al resto de los recursos de la red. Un ejemplo claro de esto sería el caso de alguien que desde su equipo decidiera establecer una conexión telefónica a Internet utilizando un modem, sin ningún tipo de protección. Estaría abriendo una puerta trasera a posibles atacantes. Esta colaboración es necesaria ya que al administrador de seguridad de la red no puede estar en todos lados; al menos no debería convertirse en una batalla entre éste y los individuos de la organización.
Seguridad a través de oscuridad: La idea de esta estrategia está basada en mantener oculta la verdadera naturaleza del sistema de seguridad, de esta forma, un atacante lo pasará por alto como una posible víctima. Pero esta suposición es algo ingenua ya que varios estudios han demostrado que el interés de un atacante por un determinado sitio no solo está determinado por el interés que éste tenga sobre la información del sistema.

Esta estrategia, aunque puede ser útil en el comienzo de la vida de un sitio, y una buena precaución, es una base pobre para una solución de seguridad a largo plazo ya que la información tiende a filtrarse y los atacantes son habilidosos para obtener información relevante del sitio

Seguridad basada en Hosts: En este modelo, los esfuerzos de protección están enfocados en los sistemas finales de una red privada, es decir que los mecanismos de seguridad son implementados en estos sistemas, y son ellos mismos quienes deciden si aceptar o no los paquetes de una comunicación. Probablemente sea el modelo de seguridad para computadoras más comúnmente usado en la actualidad, aunque el mayor problema con este modelo es que no es escalable si no se considera un esquema de administración apropiado, por lo que solo es usado en ambientes muy pequeños o donde no existe una red configurada que pueda ofrecer tal tipo de protección.

El mayor impedimento para hacer efectiva la seguridad de estos sistemas en ambientes de redes de computadoras actuales es la complejidad y heterogeneidad de esos ambientes. Inclusive si todos los hosts fueran idénticos o si tal heterogeneidad fuera superada, un sitio con un gran número de hosts hace que sea difícil asegurar de forma efectiva a cada uno. Mantener e implementar efectivamente la protección a este nivel requiere una importante cantidad de tiempo y esfuerzo, y es una tarea compleja. En pocas palabras, puede no ser rentable implementar un nivel de seguridad a nivel de hosts para sitios grandes ya que requieran muchas restricciones, y mucho personal de seguridad. Adicionalmente, este modelo presenta un problema importante en cuanto a puntos de ahogo y enlaces débiles: no existe un único punto de acceso

ya que existen múltiples conexiones, una para cada host, muchas de las cuales pueden estar débilmente protegidas.

> Seguridad basada en la Red: El modelo de seguridad de red se enfoca en controlar el acceso a la red, y no en asegurar los hosts en sí mismos. Este modelo está diseñado para tratar los problemas identificados en el ambiente de seguridad de hosts, aplicando los mecanismos de protección en un lugar en común por el cual circula todo el tráfico desde y hacia los hosts: los puntos de acceso a la red. Un enfoque de seguridad de red involucra la construcción de firewalls para proteger redes confiadas de redes no confiables, utilizando sólidas técnicas de autenticación, y usando encriptación para proteger la confidencialidad e integridad de los datos a medida que atraviesan la red.

La ventaja sobre el modelo de seguridad de hosts es una considerable reducción del costo para proveer la misma o mejor protección, ya que solo se necesita proteger unos pocos puntos de acceso (en muchos casos, uno) lo que permite concentrar todos los esfuerzos en una solución perimetral. Este modelo es escalable en la medida de que la solución perimetral pueda soportar los cambios sin afectar su desempeño. Una desventaja de este modelo es que es muy dependiente de algunos pocos puntos de acceso por lo que pueden producirse reducciones en el desempeño del tráfico de entrada y salida de la red; por otro lado, la protección lograda no es flexible y posee un bajo grado de granularidad, es decir, no es posible especializar la protección necesaria para cada host y sistema final de la red privada.

Por otra parte la seguridad física es la encargada de proteger todos los dispositivos que componen el hardware: Procesador, memoria principal, dispositivos de entrada y de salida, dispositivos de almacenamiento y los respaldos. Esto se puede lograr restringir el acceso a las áreas de computadoras, restringir el acceso a las impresoras, instalar detectores de humo y extintores, colocar los dispositivos lejos del piso, colocar los dispositivos lejos de las ventanas, colocar pararrayos y proteger las antenas externas.

Módulos que conforman el Sistema Gestión de Datos Geológicos (SGDG)

Inventario Nacional de Reservas de Aguas Minerales.

Este módulo se encarga de la gestión y consulta de las estadísticas de los recursos y reservas naturales que existen en el país. A partir de esta información es que se realiza anualmente el Balance Nacional de Recursos y Reservas de los recursos naturales disponibles para controlar y garantizar su uso racional.

Este proceso es llevado a cabo en la Oficina Nacional de Recursos Minerales por los especialistas. El mismo se realiza anualmente con la colaboración de los concesionarios que son las entidades que trabajan con los yacimientos, en este caso yacimientos de agua mineral. Estos especialista deberán entregar además los recursos en explotación por cada yacimiento así como la materia prima que este posea, para junto a los recursos disponibles y recursos de explotación conformar el Balance para la Administración Central del Estado cada año.

En el caso de la explotación de Aguas Minerales Naturales se tiene que entregar anualmente el Proyecto de Explotación y Procesamiento al igual que el Balance o Estado Anual de los Recursos Disponibles y de Explotación

de las Aguas Minerales de la nación a la Dirección Técnica.

Inventario Nacional de Recursos y Reservas de Minerales Sólidos.

Este módulo se encarga de la gestión y consulta de las estadísticas de los recursos y reservas minerales que existen en el país. A partir de esta información es que se realiza anualmente el Balance Nacional de Recursos y Reservas de los Minerales Sólidos para controlar y garantizar su uso racional.

Las estadísticas de los recursos y reservas son actualizadas a través de informes geológicos o del balance, entregadas por los concesionarios que estén explorando o explotando un área determinada. Los informes son entregados al departamento de Documentación de la ONRM. Este departamento entrega el informe a la Dirección Técnica, encargada de revisar el informe y si lo aprueba, emite un modelo de aprobación y le entrega los dos documentos al administrador del balance para que los archive.

Los depósitos de minerales sólidos están compuestos por sectores y estos, a su vez, por bancos o bloques, que son las unidades que poseen los recursos y reservas. Los recursos y reservas que pertenecen a estas unidades pueden estar concesionados o no, de acuerdo al área del depósito que esté concesionada.

Todos los años el concesionario debe entregar un informe con la información de la zona explotada para actualizar el balance de los recursos y reservas. El balance también es actualizado a través de los informes geológicos entregados que brindan información de nuevos descubrimientos de recursos y minerales no concesionados hasta el momento ó la actualización de los mismos.

Inventario Nacional de Recursos de Petróleo y gas.

El Balance Nacional de Recursos y Reservas de Petróleo y Gas se refiere al conjunto de actividades que se realizan sobre los datos de los recursos y reservas de petróleo y gas que existen en todo el territorio nacional y en la zona económica de Cuba. Estas actividades son fundamentalmente de inserción, eliminación, actualización y reportes, tienen además una amplia repercusión en la vida económica y social del país.

A partir de la información referida a la investigación, descubrimiento, exploración y explotación del petróleo y el gas derivado, se realizan los respectivos balances, de manera tal que el país conoce en todo momento el petróleo comprobado del que dispone, el que supone que dispone, el que posiblemente podría suponer y el petróleo y gas que posee pero que por las condiciones tecnológicas o por la factibilidad económica es imposible extraer. Una vez introducidos y actualizados, estos datos, son usados por diferentes organismos nacionales e internacionales en sus procesos habituales, tales son los casos de CUPET, el Centro de Investigaciones del Petróleo (CEINPET), la Administración Central del Estado e Instituciones Petroleras Internacionales, los cuales se nutren de la información contenida en el Balance para tomar decisiones que luego inciden económica, política y socialmente sobre todo el país.

Cada entidad debe de entregar un informe a la ONRM en el cual esté recogida toda la información referente a la explotación o exploración según el contrato realizado por esta. Las acciones de Inserción y/o modificación de los datos solo pueden ser realizadas por los trabajadores del balance, que está conformado por el grupo del balance que son los encargados de actualizar la información del Balance Nacional de Recursos y Reservas del Petróleo y Gas.

Búsqueda Referativa.

El módulo Búsqueda Referativa se encarga de la gestión y consulta de la información geológica almacenada en el archivo técnico de la Oficina Nacional de Recursos Minerales, esta información es necesario que se vea desde

cualquier lugar con una conexión a internet para poder brindar estos servicios a todo aquel que necesite información sobre el suelo cubano a lo largo de la Isla y el mundo.

Cuando un concesionario desarrolla una investigación en una zona perteneciente al suelo cubano realiza un informe de su investigación, un documento que tiene una serie de datos particulares de esa investigación, incluye la fecha, los autores, los minerales existentes, las coordenadas. Este documento es guardado en el archivo técnico y registrado en una base de datos. El encargado de administrar la aplicación es un trabajador de la oficina que además es quien registra la información de los nuevos documentos en la base de datos y tiene el derecho de eliminar o actualizar la información en la misma.

Como ya se planteaba anteriormente este modulo va a estar de cara a Internet de hay que la información que en el se gestiona es de carácter publico, en el caso de que alguna información sea restringida esta no será publicada. Por las razones anteriormente expuestas el modulo contara con dos niveles de usuarios los cuales son administrador e invitados. El administrador será uno o varios trabajadores de la entidad y los invitados todas aquellas personas que consulten la información publicada. Este modulo debe tener un correcto manejo de la gestión de usuarios y una protección eficaz de la información ya que se puede convertir en una puerta de acceso para los atacantes de todo el mundo.

Registros Petroleros.

El módulo de Registros Petroleros trabaja directamente con el Departamento de la Dirección de Registro, Control y Asesoría Legal, que se encuentra en la Oficina Nacional de Recursos Minerales; en el cual se llevan a cabo cuatro trámites fundamentales referentes a la actividad petrolera, estos son:

Solicitar Calificación
Solicitar Permiso de Perforación
Solicitar Prorroga
Inscribir Contrato

Muchas compañías extranjeras se interesan por establecer contratos con CUPET que es la empresa cubana que posee el monopolio de los recursos del petróleo, para realizar disímiles operaciones petroleras en Cuba; pero no es

posible que esto ocurra sin antes haber sido calificada por la Oficina Nacional de Recursos Minerales. En esta calificación se evalúa si la compañía tiene capacidad tanto técnica como financiera. Es importante mencionar que no es posible explotar pozos una vez establecido el contrato con CUPET sin haber inscrito dicho contrato en la oficina y además haber recibido un permiso para perforar, esto evidencia la importancia que poseen estos procesos.

La solicitud de calificación para las compañías extranjeras interesadas en realizar actividades de exploración y producción de petróleo y/o gas en Cuba, se inicia cuando un cliente se dirige a la ONRM a solicitar ser calificado por la misma, especificando si desea calificarse para operar o no, o si lo hace por nuevo contrato o para uno ya vigente. En cualquier caso el cliente debe entregar al Grupo Documental los documentos que fundamentan su capacidad legal, técnica y financiera.

En caso de que la compañía haya sido calificada el abogado la inscribe en el libro de Registros Petroleros, lo que faculta a la compañía extranjera a negociar contratos de asociación con CUPET. Esto debe hacerlo antes de dos años, de lo contrario queda invalidada la calificación obtenida y debe iniciar el proceso de calificación nuevamente en caso de querer hacer un nuevo contrato.

Una vez que una compañía haga un contrato con CUPET está obligado a inscribirlo en el libro de contratos, este es otro de los trámites o procesos que se llevan a cabo en la oficina, y al igual que para ser calificado el cliente debe

presentar al Grupo Documental los documentos legales establecidos y efectuar el pago de la tarifa dispuesta, siguiendo la misma ruta crítica ya descrita entre el Grupo Documental, la Dirección de Control Económico y la Dirección de Registro, Control y Asesoría Legal, que igualmente conforma un expediente por cada contrato y procede a su inscripción de presentarse toda la documentación exigida y con las formalidades establecidas.

El otorgamiento del permiso de perforación es otro de los trámites que se realizan en la ONRM. El proceso culmina con la inscripción en los Libros correspondientes del Registro o con la devolución o rechazo de las solicitudes recibidas.

El otro trámite que se ejecuta en la ONRM referente a los registros petroleros es el otorgamiento de una prórroga, sólo pueden realizar este tipo de solicitud aquellas compañías que tengan un permiso para perforar.

En cualquiera de los procesos, si al ser revisada la documentación que la compañía entrega se encuentran errores o falta alguna información se le notifica lo ocurrido a la compañía y debe presentarse en la oficina con todo en orden para iniciar nuevamente el proceso.

Un cliente pueden ser Empresas Nacionales Estatales y Extranjeras. Un Contratista es un cliente que firma como parte el contrato de conjunto con la empresa petrolera estatal. Un Contratista Operador es un contratista que lleva a cabo la ejecución de las operaciones petroleras por cuenta del Contratista.

Un Contratista No Operador es un contratista que no ejecuta por si mismo las operaciones petroleras.

Registro Minero

El módulo de Registro Minero se encarga de llevar a cabo un programa para lograr la informatización de los trámites que se realizan en la ONRM en cuanto a los recursos mineros.

Solicitar Permiso de Reconocimiento
Solicitar derecho minero de Investigación Geológica (Prospección o Exploración)
Solicitar derecho minero de Procesamiento
Solicitar derecho minero de Explotación y Procesamiento
Solicitar derecho minero de Explotación.

La presentación de la solicitud debe cumplir toda una serie de requisitos reflejados en la Ley de Minas y su Reglamento, los cuales deben estar correctamente redactados, certificados en los casos que así lo requieran, así como cumplimentando lo relacionado con el pago de tributos correspondientes. Entre otras cuestiones debe presentarse los datos relativos al solicitante con su capacidad financiera y técnica, se debe delimitar bien el área a solicitar (que debe ser una poligonal cerrada representada por cuatro o más puntos en el terreno).

Cuando el usuario presenta toda la documentación requerida en la ONRM, cumplimentando el pago de las tarifas correspondientes, los especialistas del Registro Minero lo revisan y si todo está en condiciones perfectas entonces se abre un expediente al cual se le asigna un número de 9 dígitos y que no se repite para ningún expediente, se confecciona una ficha de la solicitud a partir de los datos que se introducen en el módulo de concesiones y se envía a consulta con otros organismos que deben dar sus criterios de la conveniencia de realizar la actividad minera en esa área o no.

Dependiendo del tipo de solicitud que se presente se circula a determinadas entidades consultadas que emiten sus criterios; si es un permiso de reconocimiento se le consulta a 3 entidades Ministerio de la Fuerzas Armadas(MINFAR), Ministerio de Ciencia, Tecnología y Medio Ambiente (CITMA), Ministerio de la Agricultura (MINAGRI), si son de los otros cuatro tipos de solicitudes, serán estas mismas entidades más 7 que darán sus

criterios, en donde pueden proponer excluir determinada área que se desea para operar en cualquiera de las cinco variantes debido a que las entidades consultadas pueden tener intereses que les pudieran afectar o simplemente no aprobar la solicitud.

Si estos organismos no presentan objeción para la realización de las actividades mineras es decir compatibilizan de manera positiva, para lo cual tienen un término de 30 días hábiles para emitir sus criterios, se confecciona un dictamen técnico por los especialistas de la Dirección de Técnica y que posteriormente los abogados lo utilizan junto al expediente para confeccionar una propuesta de Resolución a la firma de la ministra otorgando o no el derecho minero.

Todo derecho minero al ser otorgado, tiene un término para cumplir con los objetivos que se propuso (ya sean de investigación o de explotación y procesamiento). Antes de la fecha de su vencimiento, si el concesionario necesita

otro período de tiempo para continuar sus actividades, la ley le da derecho de solicitar una prórroga, por un término que está de acuerdo con el tipo de derecho minero otorgado. La solicitud de esta prórroga debe cumplir así mismo con los requisitos establecidos en la legislación vigente, y que su recibo correctamente se elabora un dictamen técnico procediéndose a partir de aquí como si fuera una nueva solicitud para su aprobación o no.

Un concesionario puede, además, solicitar ampliar el mineral a investigar, explotar o hacer el uso del mismo. Existe la posibilidad de que un titular no posea la capacidad técnica y financiera suficiente para darle seguimiento a su derecho otorgado y puede traspasar o ceder el derecho a otra entidad o a otra persona que posea las características necesarias para continuar con el derecho otorgado. También un concesionario puede devolver un área parcial o totalmente, en dependencia del interés de la parte del derecho minero que tenga el concesionario.

Metadatos

El módulo de Metadatos se encarga de gestionar los metadatos geológicos en la ONRM para proveer una estructura bien organizada que permita documentar fácilmente los datos geológicos. En este se llevan a cabo 3 actividades fundamentales:

Gestionar metadatos.
Gestionar archivos XML.
Realizar consultas de metadatos.

Se puede definir como Metadato que estos son datos altamente estructurados que describen información, el contenido, la calidad, la condición y otras características de los datos. Es "Información sobre información" o "datos sobre los datos". Entre los principales usos de los Metadatos están: Organizar y mantener el acervo del conjunto de datos de una organización. Proveer información necesaria para interpretar y procesar datos transferidos por otra organización. Los Metadatos están estructurados por un mínimo de elementos tales como: título, autor, fecha de creación, etc. Típicamente, los elementos que conforman un Metadato están definidos por algún estándar, donde los usuarios que deseen compartir Metadatos están de acuerdo con un significado preciso de cada elemento. (Instituto Nacional de Estadística, G. e. I. d. M., 2003)

Específicamente un metadato geológico es un conjunto de información que identifica diferentes aspectos relacionados a grupos de datos o a datos específicos y permite conocer características de estos, que los particularizan dentro de un conjunto. Describe aspectos de los datos geoespaciales como son: calidad, actualización, referencia geoespacial, autor, entre otras. Constituyen información sobre la forma y el contenido de los recursos informativos. (Rafael Oliva Santos, 2006)

Los metadatos geológicos son documentados basados en el estándar internacional ISO 19115.TC 211 desarrollado

en el año 2003 por el comité 211 de la ISO. El objetivo de este estándar internacional es proporcionar una estructura para describir datos geográficos digitales. Este estándar está pensado para ser utilizado por analistas, programadores y desarrolladores de sistemas de información geográfica, así como todos aquellos que quieran

entender los principios básicos y los requerimientos de la estandarización de la información geográfica. Además define los elementos de los metadatos, proporciona un esquema y establece un conjunto común de terminología de metadatos y definiciones.

Nomencladores

Todos los procesos que se desarrollan en el Sistema de Gestión de Datos Geológicos utilizan información geológica organizada en nomencladores. Existen Listas Códigos para las cuales se han declarado como oficiales mediante algún instrumento legal un determinado subconjunto de palabras que forman parte de ellas, ese subconjunto de términos oficialmente asumidos constituye un nomenclador. Un ejemplo ilustrativo de esto es la lista código de provincias, donde aparecen los nombres de las antiguas provincias y las vigentes, las cuales constituyen el nomenclador provincias de la división política administrativa vigente.

Estas Listas código actualmente son gestionadas por la Geominera de Oriente. Una vez que esta institución realiza algún cambio en las Listas códigos comparte un fichero con las actualizaciones realizadas, para que las demás empresas interesadas accedan a este y puedan mantener actualizados los nomencladores en sus respectivas bases de datos.

Solo la Geominera de Oriente puede realizar cambios en las listas de código, sin embargo las demás empresas que utilizan los nomencladores, entre ellas la Oficina Nacional de Recursos Minerales, pueden crear listas configurables. Estas últmas son conformadas a partir de elementos pertenecientes a listas Código oficiales, generalmente son un subconjunto de las primeras.

La información contenida en las Listas es de gran importancia para la Oficina Nacional de Recursos Minerales y puede ser consultada por cualquier trabajador de esta empresa o de otra entidad relacionada a la actividad geominera.

Atendiendo a lo expuesto anteriormente para este módulo se evidencian tres roles de usuarios los cuales son enumerados a continuación:

> Administradores: especialista aprobado por la Geominera de Oriente con los permisos necesarios para gestionar las Listas de Código Oficiales.
> Usuarios Avanzados: especialista aprobado por la Oficina Nacional de Recursos Minerales para gestionar las Listas Configurables (solo las Listas Configurables, no las Listas Código Oficiales).
> Consultores: solo tendrán derecho a consultar la información referente a los nomencladores. Pueden ser cualquier trabajador de la Oficina Nacional de Recursos Minerales o de otra entidad vinculada a la actividad geominera.

Mecanismos Lógicos de Seguridad

Mecanismo de Autenticación e Identificación

Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las

entidades que acceden a un objeto. Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios. Existen dos grados en el mecanismo de autenticación.

> Autentificación simple. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.
> Autentificación fuerte. Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado. Un certificado es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario.

Mecanismo de seguridad implementado

La investigación realizada en capítulos anteriores permitió una correcta elección de los mecanismos lógicos de seguridad, así como de las mejores prácticas a utilizar a la hora de llevar a cabo una correcta implementación de los mismos. A raíz de todo este estudio se concluyó que los mecanismos fundamentales a utilizar para garantizar la seguridad del SGDG serían la Autenticación de Usuario, Falla Segura y Encriptación o Cifrado de los Datos.

Los mecanismos de Autenticación de Usuario y el de Falla Segura son la columna vertebral del módulo de Seguridad del SGDG ya que los mismos brindan las funcionalidades que permiten realizar el tratamiento de usuarios, el otorgamiento de los diferentes permisos a los usuarios y además garantizan en caso de que el sistema falle deniegue todos los permisos. El de cifrado de los datos no es utilizado con profundidad ya que por petición del cliente solo se utiliza en el almacenamiento de la clave de los usuarios.

Módulos de Seguridad

Además de lo anteriormente mencionado se debe añadir que cada módulo del SGDG es reconocido por Symfony como una aplicación, y dichas aplicaciones están formadas por módulos los cuales contienen la vista y el controlador (success y actions). Estos módulos están estrechamente relacionados con el modelo. También se debe

acotar que los módulos están divididos por las operaciones que realizan o mayormente por la información que manejan. Además cada aplicación contiene clases que son las encargadas de cargar los Java script (.js) y los ccs, también están las clases que se encargan del direccionamiento y la seguridad, estas clases se encuentran en la carpeta config del proyecto. La aplicación de seguridad por su parte está conformada por 7 módulos (Usuario, Área, Permisos, Asignar, Login, Principal, Seguridad).

El módulo principal es el encargado de cargar el layout principal del SGDG, el cual brinda la posibilidad de acceder a los diferentes módulos del sistema. Dicho layout se encuentra en la aplicación de seguridad ya que esto garantiza que una vez el usuario accede al sistema, se encuentra en la aplicación encargada de la autenticación de los usuarios.

Figura 1 Layout principal del SGDG

El módulo seguridad por su parte es el encargado de cargar su layout principal. El mismo brinda a los usuarios la posibilidad de acceder a las funcionalidades de gestión que brinda la aplicación de seguridad. Este layout es solo

visible para las personas que ocupen el rol de Administrador en la aplicación de seguridad.

Figura 2 Layout principal del módulo de Seguridad

El módulo login se encarga de la autentificación de los usuarios que forman parte del grupo de trabajo del SGDG ya que los usuarios invitados no tendrán que autenticarse. Este módulo puede ser accedido desde cualquier aplicación del SGDG. El mismo pide al usuario que desea autenticarse o que debe hacerlo para acceder a una información determinada, un usuario y clave, dicha información es comprobada a través de una consulta a la base de datos, y brinda una respuesta la cual puede ser permitir el acceso a dicha información o denegar el acceso a la misma, debido a que el usuario y clave no se corresponde con ninguno de los existentes en la BD.

Figura 3 Success del módulo login

El módulo Usuario es el encargado de mostrar la información y funcionalidades que hacen posible la gestión de los usuarios que forman parte del grupo de trabajo del SGDG. Este módulo permite conocer los datos de los usuarios que se encuentran en la BD, ya que cuando el administrador accede a este módulo se muestra una tabla con los datos de los usuarios (nombre, usuario, teléfono y e-mail). Este módulo además brinda la posibilidad de adicionar un nuevo usuario, así como modificar o eliminar los datos de uno ya existente. Es importante señalar que estas operaciones solo podrán ser realizadas por los administradores de la aplicación de seguridad.

Figura 4 Success módulo usuario

El módulo Permisos es el encargado de mostrar la información y funcionalidades que hacen posible la gestión de los permisos que se podrán otorgar a los usuarios que forman parte del grupo de trabajo del SGDG. Este módulo permite conocer los datos de los permisos que podrán tener los usuarios del SGDG, ya que desde que el administrador accede a este módulo se muestra una tabla con los datos de dichos permisos (nombre y descripción). Además brinda la posibilidad de adicionar nuevos permisos así como modificar y eliminar los ya existentes. Las operaciones para modificar y eliminar podrán ser accedidas en la columna de la tabla que cuyo encabezado es Acciones. Es importante señalar que estas operaciones solo podrán ser realizadas por los administradores de la aplicación de seguridad.

Figura 5 Success del módulo permiso

El módulo Área es el encargado de mostrar la información y funcionalidades que hacen posible la gestión de las áreas que forman el SGDG. Una vez que el administrador accede a este módulo se muestra una tabla con los datos de dichas áreas (nombre, descripción y etiqueta). Además brinda la posibilidad de adicionar nuevas áreas, así como modificar y eliminar las ya existentes. Las operaciones para modificar y eliminar un Área podrán ser accedidas en la columna de la tabla que cuyo encabezado es Acciones. Es importante señalar que estas operaciones solo podrán ser realizadas por los administradores de la aplicación de seguridad.

Figura 6 Success del módulo área

El módulo Asignar permiso permite asignarle los permisos correspondientes a los usuarios en cada una de las áreas del SGDG. El mismo comienza brindándole al administrador del sistema la posibilidad de seleccionar el usuario al cual desea gestionarle los permisos.

Figura 7 Success asignar permisos

Después de seleccionar el usuario al cual se le desea gestionar los permisos se muestra una tabla en la cual se encuentran los permisos del usuario por área. Esta tabla permite la gestión de los permisos de los usuarios por cada

área de la aplicación, los campos que se encuentran marcados son los permisos con los que cuenta el usuario por área. Si quieres asignar un nuevo permiso marcas el campo que coincide con la intercepción del área con el permiso en la tabla. Para eliminar un permiso se sigue este mismo proceso, pero esta vez desmarcando dicho campo. Esta página fue realizada utilizando la técnica de programación AJAX siglas de Asynchronous JavaScript and XML. Esto brinda como ventaja que solo se actualice en la success el elemento modificado. Este módulo al igual que el resto solo puede ser accedido por los administradores de la aplicación de Seguridad.

Figura 8 Success asignar permiso

Se debe tener presente que en el desarrollo de la aplicación de seguridad se tuvo en cuenta que se maneja información que puede ser de vital importancia para la economía del país, además esta información no se encontrará en un módulo en específico. También se tuvo presente que en muchos de los casos los administradores de un módulo pueden ser invitados en otro módulo de la aplicación. De ahí que tomando esto en cuenta se creó una variable sesión que desde el momento en que el usuario se autentica se guardan los datos del mismo, incluyendo sus credenciales. Las credenciales son comprobadas cada vez que el usuario cambia de aplicación y también dentro de la misma aplicación.

Conclusiones

El presente trabajo, surgido a raíz del problema planteado de garantizar la seguridad del SGDG, no pretende buscar soluciones simples y rápidas, sino que cada mecanismo implementado sea el más conveniente dada las condiciones y necesidades del proyecto. Para lograr esto primeramente se realizó un estudio detallado sobre los mecanismos lógicos de seguridad en aplicaciones informáticas, lo cual constituye el objeto de estudio de la

investigación realizada. Se hizo un estudio comparativo de cada uno de ellos atendiendo a sus principales ventajas y desventajas seleccionando en cada caso los más convenientes. También se investigó a fondo la situación problémica para comprender de forma clara las necesidades a las cuales debía dar respuesta el trabajo. Todo este estudio y documentación contribuyó:

- A una correcta determinación de los estándares de seguridad adecuados para el SGDG teniendo en cuenta el grado de sensibilidad de la información que se gestionara por el sistema.
- A una correcta implementación de los mecanismos que garantizaran la seguridad del SGDG.
- También al entendimiento y posterior elección de las herramientas de seguridad informática a utilizar por la ONRM para garantizar la seguridad de la información que manejara el SGDG.

Notas

(1)Universidad de las Ciencias Informáticas, rmdelgado@estudiantes.uci.cu
(2)Universidad de las Ciencias Informáticas, jcrojas@uci.cu
(3)Universidad de las Ciencias Informáticas, ehernandezl@uci.cu

Trabajos citados

1. ONRM. ONRM. [En línea] [Citado el: 5 de Octubre de 2008.] .
2. mailxmail. Mailxmail. [En línea] [Citado el: 5 de Octubre de 2008.] .
3. daforos. Daforos. [En línea] [Citado el: 5 de Octubre de 2008.] .
4. mailxmai. Mailxmai. [En línea] [Citado el: 5 de Octubre de 2008.] .
5. antivirus. Antivirus-Interbusca. [En línea] [Citado el: 5 de Octubre de 2008.] .
6. firewall. Firewall-Blogcindario. [En línea] [Citado el: 5 de Octubre de 2008.] .

7. pergaminovirtual. Pergaminovirtual. [En línea] [Citado el: 5 de Octubre de 2008.] .
8. dotnetclubs. Dotnetclubs. [En línea] [Citado el: 5 de Octubre de 2008.] .
9. 1wikipedia. Wikipedia. [En línea] [Citado el: 29 de Enero de 2009.] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica.
10. maqui. Maqui. [En línea] [Citado el: 13 de Marzo de 2009.] .
11. carolinagomezc. Carolinagomezc. [En línea] [Citado el: 7 de Noviembre de 2008.] http://carolinagomezc.blogspot. com/2007/08/la-seguridad-informatica.html.
12. rediris. Rediris. [En línea] [Citado el: 24 de Noviembre de 2008.] http://www.rediris.es/cert/doc/unixsec/node5.html.
13. xombra. Xombra. [En línea] [Citado el: 10 de Enero de 2009.] \.
14. mundodescargas. Mundodescargas. [En línea] [Citado el: 3 de Febrero de 2009.] .
15. nod32. Nod32. [En línea] [Citado el: 17 de Febrero de 2009.] .
16. citltda. Citltda. [En línea] [Citado el: 18 de Febrero de 2009.] .
17. mcafee. Mcafee. [En línea] [Citado el: 20 de Febrero de 2009.] .
18. kaspersky. Kaspersky. [En línea] [Citado el: 9 de Marzo de 2009.] .
19. - Kaspersky. [En línea] [Citado el: 10 de Marzo de 2009.] .
20. genbeta. Genbeta. [En línea] [Citado el: 21 de Febrero de 2009.] http://www.genbeta.com/windows/kaspersky-ofrece-una-prueba-de-su-antivirus-para-windows-7.
21. wikipedia. Wikipedia. [En línea] [Citado el: 5 de Octubre de 2008.] http://es.wikipedia.org/wiki/Framework.
22. kioskea. Kioskea. [En línea] [Citado el: 4 de Marzo de 2009.] http://es.kioskea.net/contents/protect/firewall.php3.
23. comodo. Comodo. [En línea] [Citado el: 8 de Marzo de 2009.] http://comodo-firewall-pro.uptodown.com/.
24. hispazone. Hispazone. [En línea] [Citado el: 8 de Marzo de 2009.] http://www.hispazone.com/Descargar/487/Comodo-Firewall-Pro.html.
25. brothersoft. Brothersoft. [En línea] [Citado el: 9 de Marzo de 2009.] .
26. utilidades. Utilidades. [En línea] [Citado el: 9 de Marzo de 2009.] .
27. kaspersky. Kaspersky. [En línea] [Citado el: 21 de Febrero de 2009.] .
28. - Kaspersky. [En línea] [Citado el: 21 de Febrero de 2009.] .
29. techmixer. Techmixer. [En línea] [Citado el: 22 de Marzo de 2009.] .
30. jordisan. Jordisan. [En línea] [Citado el: 25 de Marzo de 2009.] .
31. Potencier, Fabien y Zaninotto, Francois. Symfony la guía definitiva. 2008.
32. Utria Pérez, Dianet y Santiesteban Rojas, José Carlos. Subsistema de consulta de la información referente a los pozos de petróleo en la Oficina Nacional de Recursos Minerales.

Título original: Mecanismos lógicos de seguridad para el sistema de gestión de datos geológicos en la Oficina Nacional de Recursos Minerales