

MÓDULO DE ADMINISTRACIÓN SIRIO MOBILE ADMIN

D. Rodríguez¹, R. Pérez²

¹ Universidad Ciencias Informáticas, Centro Telemática drrodriguez@uci.cu

² Universidad Ciencias Informáticas, Centro Telemática rrajadel@cfg.ecc.cu

RESUMEN / ABSTRACT

El presente artículo presenta el uso de teléfonos celulares para monitorear y administrar diferentes procesos en entornos empresariales. Recoge los resultados del desarrollo de SIRIO Mobile Admin, módulo de administración dirigido a teléfonos móviles e incorporado a la plataforma SIRIO, encargada de la gestión de juegos multiusuario para celulares. Este módulo facilita el control del servidor y proporciona las herramientas necesarias para su constante monitoreo, asegurando interoperabilidad con la incorporación de Servicios Web como intermediarios entre las aplicaciones clientes y el servidor de la plataforma. Incorpora además elementos de seguridad con el establecimiento de un canal seguro para la comunicación.

Palabras claves: Administración, Seguridad, Servicio Web, Teléfonos Celulares.

SIRIO MOBILE ADMIN ADMINISTRATION MODULE

The great development achieved by mobile telephony has enabled an indisputable increase in the software production of applications designed to them, constituting one of the fastest worldwide growing industries. Our paper presents the use of cellular phones in the monitoring and management processes in enterprise environments, as well as security-related topics in the establishment of communications. To cover a wide range of devices, two applications were developed client platforms at two of the most currently used in the software world for mobile phones.

Key words: Administration, Security, Web Service, Cell Phones.

INTRODUCCIÓN

La telefonía celular brinda ubicuidad e inmediatez, convirtiéndose en una de las tecnologías más utilizadas a nivel mundial. En el período 2005-2010 se prevé un crecimiento medio anual del 11,9% alcanzando para el año 2010, 3.9 mil millones de clientes celulares de una población mundial estimada en 7 mil millones de habitantes según estudios realizados por el Observatorio Europeo de Tecnologías de la Comunicación.

Los celulares actuales, incluyen funciones cada vez más versátiles, convirtiéndose prácticamente en una pequeña computadora de bolsillo. Puesto que son impulsados por procesadores cada vez más potentes, memorias con mayor capacidad y poseen compatibilidad con estándares abiertos, se están convirtiendo en sólidas plataformas de aplicaciones para usos empresariales. Su conectividad, comodidad y su capacidad de comunicación prometen nuevos aumentos de productividad dentro de estos entornos.

En Procyon, entidad que se encuentra enmarcada dentro de la infraestructura productiva (IP) de la Universidad de las Ciencias Informáticas (UCI), se fomenta el uso de las nuevas tecnologías de comunicación en función de la producción de aplicaciones para móviles. Producto al alto crecimiento en la demanda de los juegos en red se desarrolló la plataforma SIRIO, para la gestión de éstos, que tiene como característica fundamental el soporte para múltiples juegos.

La plataforma está conformada por tres módulos, el Servidor Web, el API de Conexión y el Módulo de Administración Web, éste último presenta gran importancia ya que permite el monitoreo del estado del servidor [1], a continuación se abunda en algunas de sus características.

Para su uso se necesita una computadora con acceso a la plataforma SIRIO. No posee flexibilidad para migraciones futuras a otro tipo de aplicaciones o diferentes dispositivos.

El tráfico de información, entre el navegador y el servidor es inseguro ya que los datos transferidos viajan como texto

plano por la red, estando propensos a ser interceptados o modificados por intrusos, esto puede causar inestabilidad en el sistema, insatisfacción y pérdida de clientes, lo que reportaría disminución en los ingresos.

Como parte del proceso de mejoras de la primera versión de la plataforma SIRIO, fueron identificadas funcionalidades necesarias a incluir en el Módulo de Administración.

Se necesita una mayor capacidad de uso del módulo de administración, de forma tal que sea accesible desde casi cualquier lugar a través de teléfonos celulares.

Requiere mayor flexibilidad para la adaptación del módulo a nuevos dispositivos y plataformas.

Garantizar la confidencialidad en el intercambio de información.

Por lo que se dio inicio a una nueva investigación con el fin de resolver el siguiente problema:

¿Cómo desarrollar un nuevo módulo de administración de la plataforma SIRIO, destinada a dispositivos móviles, que brinde mayor interoperabilidad y provea seguridad en la transferencia de datos?

El objeto de estudio de la investigación se enmarca en la telefonía móvil, las comunicaciones inalámbricas, el paradigma Cliente – Servidor, la tecnología de Servicios Web y la seguridad a través del protocolo de comunicación HTTPS (del inglés Hypertext Transfer Protocol Secure). Siendo su campo de acción, la interoperabilidad, seguridad y movilidad en sistemas de administración de plataformas de juegos para móviles que se comuniquen vía GPRS (del inglés General Packet Radio Service).

Con el fin de obtener una solución de alta calidad se plantean los siguientes objetivos.

Objetivo General:

Definir una solución para un nuevo módulo de administración de la plataforma SIRIO, que incorpore elementos claves como la ubicuidad, la interoperabilidad con diferentes aplicaciones y la seguridad en la transferencia de información.

Objetivos Específicos:

Obtener una aplicación orientada a dispositivos que presenten Windows Mobile¹ como sistema operativo, para el monitoreo y administración de la plataforma SIRIO.

Obtener una aplicación orientada a dispositivos J2ME (del inglés Java 2 Micro Edition), para el monitoreo y administración de la plataforma SIRIO.

Crear un Servicio Web para la interacción con la plataforma SIRIO, que brinde las funcionalidades necesarias para su administración y garantice una mayor interoperabilidad.

¹ Sistema operativo compacto destinado a dispositivos móviles.

Garantizar la confidencialidad de la información en el proceso de comunicación.

Metodología

El desarrollo de software es un proceso muy complejo requiriendo de una metodología eficiente y sistemática. Su misión fundamental es brindarnos un entorno de trabajo bien definido y estandarizado, que facilite la obtención de productos que aseguren los requerimientos de calidad, que cubran las exigencias de los clientes y cumpla con el tiempo estimado de desarrollo. Para la realización de la plataforma se decidió el uso de RUP (del inglés Rational Unified Process).

El Proceso Unificado de Desarrollo de Software (RUP), es la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. Constituye una forma disciplinada de asignar tareas y responsabilidades en una empresa de desarrollo y tiene como objetivo asegurar la producción de software de calidad dentro de plazos y presupuestos predecibles.

Se caracteriza por ser iterativo e incremental, estar centrado en la arquitectura y guiado por los casos de uso. Incluye artefactos (que son los productos tangibles del proceso como por ejemplo, el modelo de casos de uso, el código fuente, etc.) y roles (papel que desempeña una persona en un determinado momento, una persona puede desempeñar distintos roles a lo largo del proceso). [2]

Plataformas para el soporte de juegos

A nivel mundial empresas informáticas han realizado plataformas y servidores que dan soportes a juegos en red desde teléfonos móviles, entre ellas encontramos:

Neutrón, plataforma para el desarrollo de aplicaciones multiusuario producida por Exit Games, en San Francisco, Estados Unidos, actualmente se encuentra desplegada y brinda servicios a nivel global, sirviendo de alojamiento a una gran cantidad de juegos multiusuario para teléfonos celulares. [3]

Deus, plataforma producida y puesta en marcha en el 2003 por Exmachina, que radica en Ámsterdam, Holanda. Basada en la arquitectura empresarial de Java. Es capaz de manejar miles de jugadores de forma simultánea en un servidor, es escalable a cualquier capacidad necesaria. [4]

La plataforma Gex desarrollada por GameFederation, de Estocolmo, Suecia, funciona como un intermediario que provee una solución estandarizada para proveedores de servicios, operadores de telecomunicación y desarrolladores. Gex provee importantes beneficios al cliente permitiéndole a los proveedores distribuir los juegos multiusuario en sus teléfonos y habilitando los juegos multi-jugadores en línea. La plataforma Gex posibilita registrarse en los juegos, obtener nombres de usuarios, subir sus puntuaciones, participar en torneos y recibir estadísticas [5].

En este tipo de soluciones informáticas siempre es necesario contar con herramientas que permitan a los administradores tener control sobre los servidores donde se encuentran alojados los juegos. El hecho de que a los usuarios finales les sea indiferente todo lo concerniente a la administración de los servidores, hace que no se divulgue mucho sobre estas aplicaciones en las plataformas mencionadas.

A pesar de esto, se pudo constatar algunas características administrativas, por ejemplo, la plataforma Neutrón posee aplicaciones que monitorean las conexiones con el servidor, controlando las cuentas de usuarios y cada tipo de juego a los que provee soporte, por otro lado Gex brinda la posibilidad de darle seguimiento a las actividades que realicen sus usuarios, ya sea procesos de descarga, de búsqueda o pago a través de la plataforma, de igual forma tienen un control de los torneos establecidos, que pueden servir para atraer la actividad de los suscriptores.

SIRIO GPRS

SIRIO GPRS es la plataforma servidora desarrollada entre el año 2006 y 2007 en la entidad Procyon, su principal función es gestionar, de forma eficiente, las peticiones de los clientes, organizando de forma interna los usuarios conectados por canales correspondientes al juego desde el cual se encuentran autenticados en el sistema. [1]

La plataforma cuenta actualmente con tres módulos fundamentales:

Cliente API: Para el desarrollo de las aplicaciones cliente.

Servidor Web: Es la aplicación encargada de gestionar las peticiones de las aplicaciones y de generar la respuesta correcta a cada acción enviada.

Módulo de Administración Web: Brinda la posibilidad de administrar el servidor a través de una interfaz Web, desde la que se pueden acceder a una serie de funcionalidades, tales como registrar usuario, listar canales, listar usuarios y puntuaciones. Permite al administrador del sistema enviar mensajes de avisos, a todos los usuarios que se encuentren conectados. Facilita la interacción con el servidor y proporciona datos referentes al estado del mismo. [1]

Es importante destacar que el propósito de la entidad es entrar en el mercado y competir con las plataformas descritas anteriormente. Una mayor facilidad de uso y movilidad al utilizar el Módulo de Administración, se traduciría en un producto mejorado, con un incremento de la capacidad de control y monitoreo del servidor. Para lograrlo, se pretende desarrollar aplicaciones para los teléfonos móviles que presenten Windows Mobile como sistema operativo y para los que soporten aplicaciones J2ME, una en cada caso. Éstas ofrecerán nuevas funcionalidades, además de las ya brindadas por el Módulo de Administración Web, incorporarán elementos de seguridad y potenciarán la interoperabilidad con diferentes aplicaciones.

Plataformas de Desarrollo

Aunque hoy, los teléfonos celulares cuentan con capacidades y prestaciones que hace algunos años eran impensables, aun resultan insuficientes principalmente para los desarrolladores que siempre intentan lograr con estos escasos recursos, aplicaciones que cumplan las expectativas del cliente. Debido a esto se utilizan lenguajes que facilitan un grupo de bibliotecas o paquetes de clases reducidos, que sean capaces de ejecutarse en dichos dispositivos.

El desarrollo de dos aplicaciones similares, en plataformas diferentes, es parte de los requisitos del cliente, para así cubrir una gama más alta de teléfonos. Teniendo en cuenta esto, fueron escogidas dos de las plataformas más empleadas actualmente en el desarrollo de software para móviles, J2ME y .Net Compact Framework.

Para el desarrollo de las aplicaciones, se decidió el uso de los lenguajes Java y C#. Además utilizaremos la plataforma J2EE (del inglés Java 2 Enterprise Edition) para la incorporación de un Servicio Web que brinde las funcionalidades de administración del servidor de la plataforma SIRIO.

Servidor Web

Un servidor web podría definirse como un proceso capaz de interpretar peticiones que le llegan mediante el Protocolo de Transferencia de Hipertexto HTTP (del inglés Hypertext Transfer Protocol), procesar dichas peticiones y emitir una respuesta HTTP. Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas Web o páginas HTML: textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música. El uso más habitual de éstos es devolvernos páginas web que los usuarios piden introduciendo una dirección URL (del inglés Uniform Resource Locator) a través de un navegador.

Otro uso posible para los servidores web es devolver el resultado de la ejecución de un método que se ha dado de alta en el servidor web y al que ha pedido su ejecución un programa cliente remoto. Las peticiones y respuestas se realizan mediante el protocolo HTTP, pero aquí en vez de que personas pidan páginas web, son los programas los que piden la ejecución de métodos a la máquina servidora.

Para la publicación y alojamiento de los Servicios Web se usará el servidor Web Apache -Tomcat el cual constituye el proyecto de software libre más famoso escrito en Java, puede integrarse fácilmente a muchos sistemas y servidores de forma eficiente, además de ser utilizado por la plataforma SIRIO. [6]

Servicios Web

A grandes rasgos, un Servicio Web es un conjunto de métodos que realizan una funcionalidad que se exponen al resto de las aplicaciones, XML es el formato estándar para el intercambio de información.

Permiten la comunicación entre aplicaciones o componentes de aplicaciones de forma estándar a través de protocolos comunes (como HTTP) y de manera independiente al lenguaje de programación, plataforma de implantación, formato de presentación o sistema operativo. Presentan independencia del protocolo de transporte.

Los cambios en los métodos de los Servicios Web son transparentes para el programador. El almacenamiento y ejecución de los programas no recae en una sola máquina sino que está repartida por todas las máquinas de la red de las que se hace uso. Fomentan los estándares y protocolos basados en texto, que hacen más fácil acceder a su contenido y entender su funcionamiento. [7]

Protocolo de Comunicación

SOAP (del inglés Simple Object Access Protocol) es el protocolo utilizado por los Servicios Web en el intercambio de información. Es un protocolo de comunicación basado en XML, considerado como la columna vertebral de una nueva generación de aplicaciones de computación distribuida, sin tener la dependencia de plataformas, modelos de desarrollo y lenguajes de programación usados, denominada Servicios Web.

No está asociado con ningún lenguaje, los desarrolladores involucrados en nuevos proyectos pueden elegir desarrollar con el último y mejor lenguaje de programación que exista. No se encuentra fuertemente asociado a ningún protocolo de transporte. No está atado a ninguna infraestructura de objeto distribuido. Aprovecha los estándares existentes en la industria, los principales contribuyentes a la especificación SOAP evitaron, intencionadamente, reinventar las cosas, optaron por extender los estándares existentes para que coincidieran con sus necesidades. Por ejemplo, el uso de XML para la codificación de los mensajes.

Permite la interoperabilidad entre múltiples entornos, se desarrolló sobre los estándares existentes de la industria, por lo que las aplicaciones que se ejecuten en plataformas con dichos estándares pueden comunicarse mediante mensaje SOAP con aplicaciones que se ejecuten en otras plataformas. [8]

Protocolo Seguro de Transferencia de Hipertexto (HTTPS)

Versión segura del protocolo HTTP. HTTPS utiliza un cifrado basado en Secure Socket Layers (SSL) para crear un canal más apropiado para el tráfico de información sensible.

Funciona gracias a la criptografía, que permite asegurar mediante una serie de funciones matemáticas el origen y la ocultación de los datos.

Cada servidor que quiera implementar HTTPS debe disponer de un certificado, una especie de identidad digital,

que indica todos sus datos y la clave que permite cifrar todo lo que enviamos y recibimos del servidor. Estos certificados son emitidos por una serie de compañías a nivel mundial, que garantizan la identidad del propietario del certificado.

Certificados Digitales

Existen tres tipos principales de certificados digitales: certificados autofirmados, certificados generados por infraestructura de llave pública (PKI) de Windows y certificados de terceros.

Certificados autofirmados:

Un certificado autofirmado lo firma el propio emisor. Éstos se deben copiar manualmente al almacén de certificados de raíz de confianza en el equipo cliente o el dispositivo móvil. Cuando un cliente se conecta a un servidor por SSL y el servidor presenta un certificado autofirmado, el mismo lo comprueba en su almacén de certificados de confianza. Si el certificado del servidor está dentro de los que el cliente tiene registrados, éste debe confiar explícitamente en la entidad emisora. [9]

Certificados de infraestructura de llave pública de Windows:

El segundo tipo de certificado es un certificado generado por la PKI de Windows. Una PKI es un sistema de certificados digitales, entidades de certificación y entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica, mediante el uso de criptografía con claves públicas. Todo esto, sin embargo, conlleva un coste asociado al tener que implementar servidores e infraestructuras adicionales para crear y administrar los certificados generados por la PKI de Windows. [9]

Certificados de confianza de terceros:

Los certificados comerciales o de terceros son generados por una entidad certificadora externa o comercial, adquiridos para usarlos en sus servidores de red. La mayoría de los certificados de entidad certificadora comerciales son de confianza porque el certificado ya reside en el almacén de certificados raíz de confianza. Dado que el emisor es de confianza, el certificado también lo es. El uso de certificados de terceros simplifica notablemente la implementación. [8]

Para las organizaciones de mayor tamaño o las que deben implementar certificados de forma pública, el uso de certificados comerciales o de terceros es la mejor solución, a pesar del coste que llevan asociados. Los certificados comerciales pueden no ser la mejor solución para las organizaciones de pequeño o mediano tamaño, para las que puede preferir usar alguna de las otras opciones de certificados disponibles.

En el caso que se está tratando, no se cuenta con la posibilidad de acceder a una entidad certificadora reconocida para obtener un certificado digital, que sería la solución más idónea, ya que la mayoría de los dispositivos móviles tienen varios certificados comerciales de confianza

de terceros preinstalado y en algunos casos los fabricantes y operadores móviles deshabilitan el acceso al almacén de certificados de raíz de confianza. Esto provoca que no se puedan instalar certificados autofirmados, ni certificados de una PKI de Windows en el dispositivo móvil.

Después de una investigación, se arribó a la conclusión de que el más apropiado para la solución necesaria es el certificado autofirmado ya que éste cuenta con un coste mínimo y una configuración sencilla, lo que se ajusta a las condiciones de escasez de presupuesto y falta de experiencia del equipo de desarrollo. Independientemente de esto, presenta como desventaja la dificultad al establecer una infraestructura para la administración del ciclo de vida y la renovación de certificados.

Resultados y Discusión

En la entidad Procyon con el desarrollo de la plataforma SIRIO se avanzó un escalón más en el desarrollo de juegos multiusuario, permitiendo conectarse desde largas distancias a través de la red GPRS. Para hacer uso del Módulo de Administración Web que propone esta plataforma, es necesario contar con la presencia física de una computadora, de esta forma se limita sus capacidades de uso, con el objetivo de facilitar el monitoreo constante del servidor, se decidió el desarrollo de un sistema orientado a teléfonos celulares que brinde las funcionalidades de dicho módulo, que provea seguridad en las transferencias de datos e interoperabilidad con diferentes aplicaciones.

Propuesta del Sistema

Descripción general.

Módulo de Administración Móvil: Brinda la posibilidad de administrar el servidor a través de un teléfono celular, se pueden acceder a una serie de funcionalidades, tales como, listar canales, listar juegos y usuarios. Permite al administrador del sistema enviar mensajes de avisos, a todos los usuarios que se encuentren conectados. Posibilita además la visualización de estadísticas de un juego determinado y funciones para la gestión de cuentas de usuarios con permisos de administración. Facilita la interacción con el servidor y proporciona a los administradores todos los datos referentes al estado del servidor.

Con el objetivo de cubrir el mayor número posible de teléfonos se decidió el desarrollo de dos aplicaciones, una para los dispositivos que soporten Java y otra para los que presenten Windows Mobile como sistema operativo.

Se desarrolló además, un Servicio Web que brinda la información referente al estado del servidor que presenta relevancia para la aplicación cliente.

Para garantizar la seguridad en la comunicación entre el Servicio Web y las aplicaciones que lo van a consumir se decidió el uso del protocolo HTTPS. En la figura 1 se muestra una representación gráfica de la propuesta de solución.

Análisis comparativo.

Anteriormente las aplicaciones administrativas de la plataforma SIRIO intercambiaban información directamente con el servidor de juegos a través de Servlets (código en Java que se ejecuta en un servidor web), éstos contienen la lógica de programación y aunque mantienen asegurado el código, éste no es independiente de la interfaz. No definía métodos para el aseguramiento de las transferencias de datos en la red, provocando falta de seguridad y confianza.

La nueva propuesta está basada en una idea novedosa, la creación de un Servicio Web para servir de intermediario entre las aplicaciones y el servidor. Proporcionará las funcionalidades anteriormente implementadas, además provee un sistema que brinda interoperabilidad, permitiendo a cualquier tipo de aplicación utilizar el servicio, convirtiéndolo en una solución más madura y adaptable a las necesidades del mundo actual, en este tipo de aplicaciones. El nuevo Módulo de Administración constará de dos aplicaciones orientadas a teléfonos móviles para el monitoreo del estado del servidor, de esta forma se incrementa la ubicuidad del sistema, al poder hacer uso del mismo en todo lugar donde el celular tenga cobertura. Se propone además, la utilización de un protocolo seguro, como HTTPS, para asegurar la integridad y la confidencialidad de los datos en el intercambio información entre el Servicio Web y las aplicaciones que lo consumen.

El sistema propuesto subsana aspectos que quedaron inconclusos en la primera versión del Módulo de Administración, ganando en interoperabilidad, ubicuidad y seguridad. Convirtiéndolo en un producto superior y mejorado, con más atractivo para los posibles clientes y de este modo con mayores posibilidades de generar ingresos.

Cuando se utilizan Servicios Web la seguridad es algo primordial, debido a que los mensajes SOAP son transmitidos en texto plano por la red, éstos pueden ser interceptados, poniendo en peligro la confidencialidad de la información. Para evitar esto, fueron creadas una serie de acciones que fortalecen todos los mecanismos de seguridad definidos en la plataforma SIRIO.

Para mitigar este problema surgió la idea de utilizar HTTPS para asegurar la transferencia de información. El proceso de establecimiento de una comunicación segura utilizando SSL se describe a continuación.

Se utilizó la opción de certificado autofirmado, una vez creado se le incluye en la raíz de certificados de confianza de los teléfonos móviles. Al crear un certificado, se genera un par de claves en el servidor: una pública y una privada. La clave privada se instala en su servidor y es de crucial importancia que nadie más tenga acceso a la misma. La clave pública concordante se instala en el servidor web como parte del certificado digital. Ambas claves, públicas y privadas, se relacionan matemáticamente, pero no son idénticas. [10]

Cuando el cliente envíe una petición al servidor, éste responderá con el certificado digital, en ese momento el

cliente chequea en su lista de certificados de confianza, una vez comprobada la identidad digital del servidor, se procede a enviar una clave de sesión encriptada con la llave pública del servidor, la cual solo podrá ser descifrada con la llave privada que posee el mismo. En cada petición al HTTPS se generan nuevas claves de sesión y se repite el proceso. Una vez establecida una clave de sesión se iniciarán las comunicaciones seguras entre el cliente y el servidor. [10]

Otro aspecto importante es el trabajo con las sesiones de usuarios, éstas son asignadas en el momento de la autenticación y cuentan con un tiempo de expiración, que está marcado por la inactividad del usuario, este parámetro es configurable. El sistema periódicamente chequea las sesiones y cierra aquellas cuyo tiempo inactivo es igual al de expiración. Con esto se prevé que una aplicación que accidentalmente haya quedado abierta, pueda ser utilizada por personas no autorizadas.

Además se comprueba la identidad del usuario antes de realizar cualquier acción en el servidor. Para evitar que datos sensibles como el usuario y la contraseña viajen con frecuencia por el canal de comunicación, se le otorga al usuario durante su autenticación, un identificador de sesión único compuesto por 28 caracteres, el mismo se genera automáticamente y tiene una vigencia igual al tiempo que se esté conectado, es decir, cada usuario contará con un identificador de sesión diferente cada vez que se autentique, después de esto, solo se comprobará su identidad a través de su identificador de sesión.

CONCLUSIONES

Al finalizar la investigación se cumple con el objetivo planteado de definir una solución para un nuevo módulo de administración de la plataforma SIRIO, que incorpore elementos claves como la ubicuidad, la interoperabilidad con diferentes aplicaciones y la seguridad en la transferencia de información.

Para su cumplimiento se desarrolló un Servicio Web que fue incorporado en el servidor de la plataforma, éste brinda las funcionalidades necesarias para su administración y garantiza flexibilidad a la hora de realizar nuevas aplicaciones en diferentes plataformas de desarrollo o dispositivos. Fueron implementadas además, dos aplicaciones que consumirán este servicio, una destinada a los teléfonos celulares que soporten J2ME y otra a los que presenten Windows Mobile como sistema operativo, de esta forma se aprovechan las capacidades de movilidad y uso de los móviles. Se llevaron a cabo mecanismos para asegurar la confidencialidad en el envío de información con el uso del Protocolo Seguro de Transferencia de Hipertexto (HTTPS).

Para arribar a una solución que cumpliera con el objetivo se realizó un análisis de la Telefonía Móvil y las Comunicaciones Inalámbricas, se investigó sobre el uso de los teléfonos celulares en entornos empresariales para la administración de procesos, ubicando a SIRIO Mobile Admin en las tendencias más actuales. También se hizo un

análisis de la seguridad en este tipo de aplicaciones y particularmente el uso de HTTPS en los dispositivos móviles de poca capacidad de procesamiento. Se empleó RUP como metodología para organizar el proceso de desarrollo del software. Fueron realizadas las pruebas suficientes para hacer entrega a la entidad Procyon de un producto confiable y robusto.

Toda la documentación del módulo de administración SIRIO Mobile Admin está acompañada de una bibliografía actual y variada, se hizo uso de varias publicaciones confiables de internet y de otras en formato duro.

Como resultado de los estudios realizados y el desarrollo de la solución expuesta se puede concluir que fueron cumplidos cabalmente los objetivos planteados y se recomiendan para futuras versiones algunos aspectos que mejorarán e incrementarán las funcionalidades de administración en la Plataforma SIRIO Mobile.

REFERENCIAS

1. **BUEDO IDALGO, DENNYS, VIEIRA, YUNISEL.** Plataforma Sirio Mobile. 2007. Tesis de Pregrado.
2. **PRESSMAN, ROGER S.** Ingeniería de software un enfoque práctico. 2005.
3. **EXITGAMES.** ExitGames. [En línea] 2006. <http://www.exitgames.com/>.
4. **BV EX MACHINA.** Ex Machina. [En línea] 2005. <http://www.exmachina.nl/sp.html>.
5. **GAMEFEDERATION.** Gamefederation. [En línea] 2005. [Citado el: 5 de 11 de 2007.] <http://www.gamefederation.com/?pageID=14>.
6. **FOUNDATION APACHE SOFTWARE.** tomcat.apache.org. [En línea] 2007. [Citado el: 15 de 12 de 2007.] <http://tomcat.apache.org/>.
7. **BAILEY, THOMAS.** Getting started with web services. s.l.: Sony Ericsson, 2006. EN/LZT 108 8985 R1B.
8. **GONZÁLEZ, BENJAMÍN.** DesarrolloWeb. [En línea] 2004. <http://www.desarrolloweb.com/articulos/1557.php>.
9. **MICROSOFT CORPORATION.** MicrosoftTechNet. [En línea] 06 de 04 de 2007. [Citado el: 23 de febrero de 2008.] [http://technet.microsoft.com/es-es/library/bb430767\(EXCHG.80\).aspx](http://technet.microsoft.com/es-es/library/bb430767(EXCHG.80).aspx).
10. **THAWTE.** Transferencia Segura de Datos en Línea con SSL. [En línea] 2010. <http://www.thawte.com/resources/ssl-information-center/get-started-with-ssl/index.html>.

AUTORES

David Rodríguez Rodríguez, Ingeniero en Ciencias Informáticas, Instructor, UCI, Carretera de San Antonio KM 2 y ½, Boyeros, 8358873, drrodriguez@uci.cu. Actualmente se desempeña como Subdirector de Formación del Centro de Telemática de la Facultad 2 de la UCI, además como profesor de las asignaturas de Sistema Operativo y Seguridad Informática. Pertenece al grupo

investigativo sobre redes TETRA y al proyecto productivo Serwap con la empresa española TELTRONIC.

Rigoberto Pérez Rajadel, Ingeniero en Ciencias Informáticas, Correo Postal, Provincia Cienfuegos, rrajadel@uci.cu. Miembro del equipo de desarrollo de software de la empresa. Ha desarrollado algunos sistemas para la empresa tales como:

-Sistema para la gestión de bultos postales.

-Sistema para la venta de especies
-Sistema para la gestión de ventas de postales.
Administra red provincial en la empresa, servidores de clientes ligeros, correo y jabber.

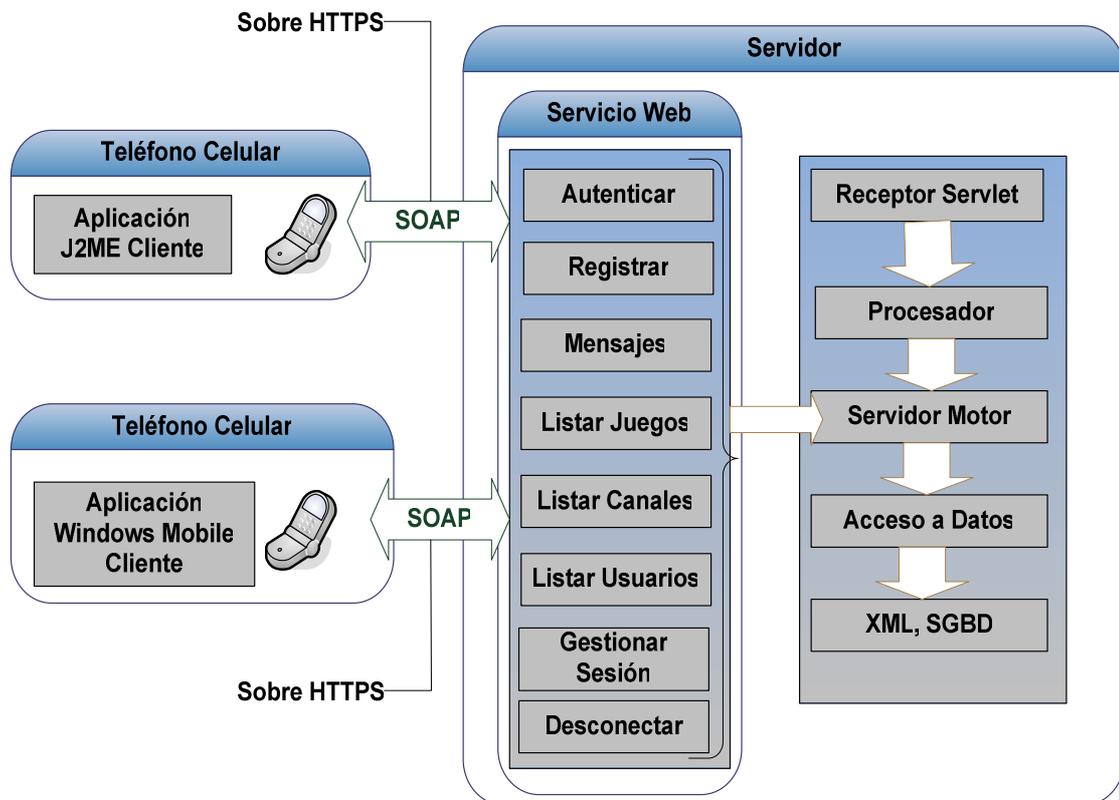


Figura 1. Propuesta del Sistema.