Universidad de las Ciencias Informáticas.
Facultad 3 Turismo y Negocios.

Título:

Subsistema para la gestión de la seguridad en sistemas distribuidos

Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas

Autor: Yanay Hernández Sosa.

Tutor: Ing. Donel Vázquez Zambrano.

Ciudad de la Habana
16/06/2009

Datos de Contacto.

Tutor Ing. Donel Vázquez Zambrano.

Graduado de Ingeniero en Ciencias Informáticas en la UCI en 2008. En su trabajo de diploma presentó SIVEMA, un sistema para la realización de ventas de productos a precios mayoristas con soporte para el manejo de multimoneda.

Desde principios de 2008 ha trabajado en sistemas de gestión de entidades, particularmente en la gestión de contabilidad, finanzas y costos asociada al producto CEDRUX: Sistema Integral de Gestión. Actualmente trabaja en la línea de investigación de sobre comercio y negocio electrónico realizando una extensión de las funcionalidades de SIVEMA para la realización de todo tipo de ventas.

Agradecimientos.

A mi madre:

Por darme la vida y enseñarme a vivirla con la cabeza en alto. Por demostrarme que una mujer sí vale y que el conocimiento la hace respetable. Por ser mi fiel amiga, mi confidente, mi apoyo. Por siempre indicarme el camino correcto y darme fuerzas para separarme del nido aun cuando te doliera mi ausencia. Por enseñarme a respetar y convivir con las diferencias de todos. Por tus sacrificios y enseñanzas…mami con este trabajo las dos nos graduamos.

A mi padre:

Por tu consejo oportuno, tu sacrificio para sacar adelante los tuyos, tu dedicación, esfuerzo y valentía. Por respetar mis opiniones aunque no sean las mismas que las tuyas. Por quererme y brindarme tu amor de padre en la forma más pura y desinteresada. Por poner a tu hijas por delante de todo sin importar las consecuencias. Por enseñarme el valor de la familia. Por ser un ejemplo de revolucionario firme, honesto, solidario y humilde.

A mi hermana:

Por tu cariño, complicidad, ternura y comprensión eres una parte inseparable de mi vida. Aunque tienes menos años que yo, ya me has proporcionado muchas enseñanzas y me has salvado, defendido y apoyado en miles de ocasiones. Eres el mejor regalo que me han hecho mami y papi.

A mi novio:

Por darme fuerzas cuando pensaba que no era posible. Por las horas sin dormir, por tu cariño, interés, discreción y respeto. Por estar siempre a mi lado. Por tu valentía para defender lo que crees justo, por no doblegarte…simplemente, por ser tú.

A mis amigos:

Porque me acompañaron cuando estaba sola, porque me hicieron reír cuando estaba triste, porque cuidaron de mí cuando estaba enferma. En especial a Marín, Abel y Tania.

Dedicatoria.

A María Elena Sosa Mayo, ejemplo de madre, mujer y amiga.

A Nelson Hernández Rubio, padre preocupado y apoyo necesario.

A Yanary Hernández Sosa, hermana maravillosa de corazón puro y actos desinteresados.

A Donel Vázquez Zambrano, compañero especial de mis días y mis noches, resguardo de mi corazón y ejemplo de perseverancia.

A la Revolución Cubana, especialmente a su líder: Fidel Castro Ruz.

Resumen.

El presente trabajo de diploma expone una propuesta de Subsistema para la gestión de la seguridad en sistemas distribuidos. Tiene como objetivo resolver el problema de la gestión desordenada y dispersa de la seguridad en los sistemas distribuidos que influye negativamente en la garantía de la autenticación, confidencialidad, integridad y el no-repudio.

Para el desarrollo se utiliza la metodología ágil de construcción de software Scrum y se hace un estudio de los sistemas existentes y de las herramientas adecuadas para la construcción del subsistema.

Palabras Claves.

Seguridad, Sistemas distribuidos, Certificado digital, Infraestructura de clave Pública.

Tabla de Contenidos.

Tabla de ilustraciones.

Introducción.

El advenimiento de la nueva era computacional ha marcado un antes y un después en la historia de las empresas del mundo. Estas han revolucionado sus métodos y formas de producción enfocados en brindar mejores servicios a sus clientes y facilitar el desempeño de sus trabajadores.

Surgieron definiciones que ya son parte de la vida diaria de miles de personas pudiendo destacar: tienda virtual, teletrabajo, correo y comercio electrónico; que tienen como factor común el hecho de que el usuario o trabajador involucrado pueda realizar operaciones a distancia, sin tener que presentarse físicamente. Hay que tener en cuenta que en este proceso se maneja un flujo de datos sensibles para los implicados, por eso no es de extrañar que los organismos den tanta importancia a la seguridad informática.

Debido a las facilidades que brindan a los usuarios y demás favorecidos, la mayoría de los sistemas usados actualmente son distribuidos, o sea, dos o más nodos arquitectónicos u ordenadores conectados para la transmisión y/o recepción de datos a través de una red mediantes un protocolo prefijado por un esquema cliente-servidor. Dichas computadoras deberán poseer el software adecuado para que el sistema sea visto por los usuarios como una única entidad que brinda las opciones para las que ha sido creado.

Generalmente estos sistemas se dividen en módulos que además de implementar las funcionalidades para las que fueron concebidos, gestionan la seguridad individualmente en lugar de hacerlo de forma centralizada. Esto trae como consecuencia factores negativos como la duplicación de código fuente en cada uno de los componentes del sistema y la necesidad de que los usuarios se autentiquen cada vez que cambian de subsistema. Como podrá entenderse, la primera de ellas aumenta la carga de trabajo de los desarrolladores, retrasa la fecha de entrega del software y reduce su eficiencia; mientras que la segunda trae consigo el descontento de los usuarios.

Una solución adecuada a este problema podría lograrse gestionando la seguridad de aplicaciones distribuidas de forma centralizada.

Esta situación conlleva a plantear el siguiente problema científico: La gestión desordenada y dispersa de la seguridad de aplicaciones informáticas distribuidas está influyendo negativamente en la garantía de la autenticación, confidencialidad, integridad y el no-repudio.

Objeto de estudio: Seguridad de aplicaciones informáticas.

Para ello se planteó como objetivo de la investigación: Desarrollar un sistema de gestión de seguridad de aplicaciones informáticas distribuidas que permita garantizar la autenticación, confidencialidad, integridad y el no-repudio.

Campo de acción: La seguridad de aplicaciones informáticas distribuidas.

Para guiar la investigación se plantea la siguiente idea a defender: La gestión centralizada de la seguridad de aplicaciones informáticas distribuidas debe influir positivamente en *la garantía de la autenticación, confidencialidad, integridad y el no-repudio.*

La investigación se desarrollará a través de las siguientes tareas:

1. Elaborar el marco teórico de la investigación.
2. Realizar un estudio de los diferentes mecanismos de gestión de la seguridad y las aplicaciones que los implementan existentes en el mundo.
3. Proponer un subsistema para la gestión de la seguridad de forma centralizada en aplicaciones distribuidas.
4. Evaluar el subsistema propuesto.

Para realizar las tareas se emplearon los siguientes métodos:

Métodos teóricos:

- ✓ Análisis y síntesis: para el procesamiento de la información y arribar a las conclusiones de la investigación así como para precisar las características del software.
- ✓ Histórico - Lógico: permite, en la etapa facto perceptual, conocer desde sus orígenes hasta el instante actual, el objeto y campo de acción que se estudia.
- ✓ Sistémico: es un método teórico que sirvió para la descomposición del sistema en módulos que luego se integró para formar parte de la herramienta Subsistema para la gestión de seguridad en sistemas distribuidos resultante como un todo.

Métodos empíricos:

- ✓ Método de la observación científica.
  - o Fue el primer método utilizado por los científicos y en la actualidad continua siendo su instrumento universal. Permite conocer la realidad mediante la percepción sensorial directa de entes y procesos, para lo cual debe poseer algunas cualidades que le dan un carácter distintivo. Se utilizó para el estudio de la gestión de la seguridad en sistemas distribuidos.
- ✓ Método de la medición.
  - o Es el método empírico que se desarrolla con el objetivo de obtener información numérica acerca de una propiedad o cualidad del objeto, proceso o fenómeno, donde se comparan magnitudes medibles conocidas. Es la asignación de valores numéricos a determinadas propiedades del objeto, así como relaciones para evaluarlas y representarlas adecuadamente. Para ello se apoya

en procedimientos estadísticos. Se utilizó en la interpretación de las métricas de diseño y de las pruebas de unidad.

Aportes prácticos esperados del trabajo:

El subsistema que resulte de la investigación debe ser capaz de gestionar la seguridad de forma centralizada para las aplicaciones distribuidas, basándose en el uso y generación de certificados digitales en el entorno de una Infraestructura de Clave Pública.

La tesis está estructurada en tres capítulos:

En este capítulo se exponen de temas imprescindibles para el desarrollo de este trabajo, tales como: Seguridad Informática, Infraestructura de Clave Pública y Leyes que rigen la Seguridad Informática en Cuba. Además se hace una breve descripción de la metodología y las herramientas usadas, incluyendo los lenguajes de programación, para el desarrollo del subsistema.

En el Capítulo 2 se hace una descripción de la propuesta de solución de este trabajo. Se aborda la construcción de la solución; se presentan los diagramas de clases, se plantean los principios de diseño e implementación, tratamiento de excepciones y estándar de codificación que se tuvieron en cuenta para el desarrollo del sistema.

En el Capítulo 3 se describen las pruebas de unidad aplicadas al subsistema a través del framework NUnit y los resultados de la misma. Se detallan las métricas usadas para evaluar el diseño de clases y se muestran las salidas obtenidas de su aplicación.

Además esta tesis posee Conclusiones, Recomendaciones, Bibliografía, Anexos y Glosario de Términos.

Capítulo I

Fundamentación teórica

Capítulo I. Fundamentación teórica.

Introducción al capítulo.

En este capítulo se hace una exposición de temas imprescindibles para el desarrollo del Subsistema para la gestión de la seguridad en sistemas distribuidos, tales como: Seguridad Informática, Infraestructura de Clave Pública y Leyes que rigen la Seguridad Informática en Cuba.

De la misma forma se abordan algunos de los lenguajes de programación más utilizados en el mundo para el desarrollo de aplicaciones y los sistemas de gestión de bases de datos que se asocian a su funcionamiento. Se exponen las herramientas seleccionadas para el diseño e implementación de la propuesta y se hace una breve descripción de la metodología y las herramientas usadas para el desarrollo de la aplicación.

Seguridad Informática.

El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real se han de tener en cuenta múltiples factores, tanto internos como externos. (Aguirre, 2006)

La Organización Internacional para la Estandarización, (o en inglés, ISO, International Organization for Standarization), en su norma 7498, define la seguridad informática como una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos, donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene. El bien más preciado por cualquier institución es la información y de ahí que se han desarrollado protocolos y mecanismos adecuados, para preservar su seguridad.

La seguridad informática no es un producto, sino un proceso. No es un bien medible, en cambio sí se podrían desarrollar diversas herramientas para cuantificar de alguna forma la inseguridad informática. (Gutierrez, y otros, 2008)

El término seguridad informática está estrechamente relacionado con cuatro aspectos fundamentales de cualquier sistema computacional: autenticación, confidencialidad, integridad y el no-repudio. Uno de los mayores retos para establecer sistemas seguros es encontrar el balance correcto entre dichos aspectos. Es fácil mantener la confidencialidad de un sistema si nadie accede a él, pero la disponibilidad sería nula.

Autenticación (o autentificación)

Autenticar es sinónimo de autenticar (verbo derivado de auténtico); ambas acepciones son válidas. Sin embargo autenticar es un anglicismo que viene de "autentify". (Gutierrez, y otros, 2008)

Es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información. Por entidad se entiende tanto personas, como procesos o computadoras.

Constituye la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Constituye la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Existen varias formas de poder autenticarse:

1. Basada en claves.

2. Basada en direcciones.
3. Criptográfica.

De estas tres posibilidades la más segura es la tercera, pues en el caso de las dos primeras es posible que alguien escuche la información enviada y pueden suplantar la identidad del emisor de información.

Desde otro punto de vista se puede hablar de formas de autenticarse, como puede ser a través de la biometría (huellas digitales, retina del ojo, la voz...), por medio de contraseñas o claves, y por último utilizando algo que se posea, como un certificado digital.

Se llama autenticación fuerte a la que utiliza al menos dos de las tres técnicas mencionadas en el párrafo anterior, siendo bastante frecuente el uso de la autenticación biométrica, que como se indicó antes se basa en la identificación de personas por medio de algún atributo físico.

Confidencialidad

Es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. Igual que antes, los usuarios pueden ser personas, procesos, programas...

Para evitar que alguien no autorizado pueda tener acceso a la información transferida y que recorra la Red se utilizan técnicas de encriptación o codificación de datos.

Hay que mantener una cierta coherencia para determinar cuál es el grado de confidencialidad de la información que se está manejando, para así evitar un esfuerzo suplementario a la hora de decodificar una información previamente codificada.

Integridad de la información

Corresponde a lograr que la información transmitida entre dos entes no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales.

Mediante una firma digital se codifican los mensajes a transferir, de forma que una función, denominada hash, calcula un resumen de dicho mensaje y se añade al mismo.

La validación de la integridad del mensaje se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se añadió al final del mismo cuando se calculó por primera vez antes de enviarlo.

Mantener la integridad es importante para verificar que en el tiempo de viaje por la Red de la información entre el sitio emisor y receptor nadie no autorizado ha modificado el mensaje.

Servicios de no-repudio

Ofrecen una prueba al receptor del origen de la información recibida. Se aplica a la comunicación para no poder rechazar la autoría de un mensaje.

Con este aspecto se consigue que una vez que alguien ha mandado un mensaje no pueda renegar de él, es decir, no pueda negar que es el autor del mensaje.

Para el la realización de los procesos de un sistema es importante ya que garantiza la realización de las transacciones para las entidades o subsistemas participantes.

Es necesario identificar la información que debe conocer cada una de las entidades participantes en el proceso y con ello permitir la privacidad a las partes autorizadas para su uso.

Infraestructura de clave pública

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas.

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

En una operación criptográfica que use infraestructura PKI, intervienen conceptualmente como mínimo las siguientes partes:

- ✓ Un usuario iniciador de la operación
- ✓ Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, Autoridad de registro y sistema de Sellado de tiempo)
- ✓ Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

Las operaciones criptográficas de clave pública, son procesos en los que se utilizan unos algoritmos de cifrado que son conocidos y están accesibles para

todos. Por este motivo la seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o políticas de seguridad aplicados.

Es de destacar la importancia de las políticas de seguridad en esta tecnología, puesto que ni los dispositivos más seguros ni los algoritmos de cifrado más fuerte sirven de nada si por ejemplo una copia de la clave privada protegida por una tarjeta criptográfica (del inglés 'smart card') se guarda en un disco duro convencional de una computadora conectado a Internet.

Usos de la tecnología PKI

- ✓ Autenticación de usuarios y sistemas (login)
- ✓ Identificación del interlocutor
- ✓ Cifrado de datos digitales
- ✓ Firmado digital de datos (documentos, software, etc.)
- ✓ Asegurar las comunicaciones
- ✓ Garantía de no repudio (negar que cierta transacción tuvo lugar)

Tipos de certificados

Existen diferentes tipos de certificado digital, en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- ✓ Certificado personal, que acredita la identidad del titular.
- ✓ Certificado de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- ✓ Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- ✓ Certificado de persona jurídica, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- ✓ Certificado de atributo, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.).

Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:

- ✓ Certificado de servidor seguro, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- ✓ Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

Componentes

Los componentes más habituales de una infraestructura de clave pública son:

- ✓ **La autoridad de certificación** (o, en inglés, CA, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- ✓ **La autoridad de registro** (o, en inglés, RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
- ✓ **Los repositorios**: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.
- ✓ **La autoridad de validación** (o, en inglés, VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.
- ✓ **La autoridad de sellado de tiempo** (o, en inglés, TSA, TimeStamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
- ✓ **Los usuarios y entidades finales** son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmar digitales, cifrar documentos para otros usuarios, etc.)

Leyes vigentes.

La seguridad informática en Cuba se rige por:

- ✓ DECRETO-LEY Nº 199 SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN OFICIAL (ver anexo 1)

  Dado en el Palacio de la Revolución, en La Habana, a los 25 días del mes de noviembre de 1999 por Fidel Castro Ruz. Trata sobre la seguridad y protección de la información oficial que tiene como objetivo, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, cuyas normas deben cumplimentar tanto los órganos organismos, entidades o cualquier otra persona natural o jurídica residente en el territorio nacional, como las representaciones cubanas en el exterior.

- ✓ RESOLUCION No. 1/2000 del Ministerio del Interior. (ver anexo 2)

  Pone en vigor el reglamento sobre la seguridad y protección de la información oficial.

Ambos instrumentos tienen por objeto establecer los principios que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

Tratamiento de la Seguridad en algunos sistemas distribuidos.

En los sistemas distribuidos el aspecto seguridad es mucho más delicado que lo que normalmente es pues las conexiones se hacen de forma remota y no local, entonces suelen surgir problemas para controlar el acceso a los otros nodos.

A continuación se relacionan algunos ERP (Enterprise Resource Planning), con la descripción de cómo se implementa su seguridad.

Adempiere

La seguridad está basada en roles de usuario para cada uno de los subsistemas, la cual controla el acceso a Pantallas, Reportes y Procesos. Antes de acceder a cualquier dato, el usuario debe identificarse con un nombre de usuario y contraseña. Es mejorable la gestión de la seguridad pues no se implementa una forma de garantizar el no-repudio.

OpenERP

La seguridad está basada en autenticación de usuarios. El código que proporciona esta característica se repite en cada uno de los módulos, haciendo que la aplicación crezca innecesariamente. Tampoco garantiza el no-repudio.

CEDRUX

Aunque es un sistema que aun está en construcción implementa la seguridad en un módulo de forma centralizada. Sin embargo, para gestionar las peticiones o el flujo de información entre dos subsistemas usa toquen de seguridad que contienen toda la información que valida la autenticidad de la petición: nótese que no existe como garantizar entonces el atributo básico de la seguridad de no-repudio quedando el sistema expuesto a que terceros realicen ataques de intercepción, modificación o interrupción.

El subsistema Seguridad de CEDRUX cuenta con las siguientes funcionalidades:

- ✓ Configurar nomencladores.
    - Dominio.
    - Gestor de Bases de Datos.

- Bases de Datos.
- Esquemas.
- Idiomas.
- Temas.
- Escritorios.
- Expresiones.
- Claves

✓ Configurar servidores.

- Servidores.
- Bases de Datos.
- Gestores de Bases de Datos.
- Esquemas.

✓ Configurar sistemas.

- Sistemas.
- Funcionalidades.
- Acciones.
- Servicios que presta.
- Servicios que consume.
- Funciones.
- Parámetros.

✓ Configurar usuarios.

- Roles.
- Usuarios.
- Campos de perfil de usuario.
- Perfil de usuario.

El subsistema propuesto solo abarca la gestión de usuarios y subsistemas pues no se disponía de suficiente tiempo para implementar la configuración de nomencladores y la gestión de servidores.

Ninguno de estos ejemplos de sistemas distribuidos gestiona la seguridad de forma óptima, aunque CEDRUX tiene el logro de hacerlo ya de forma centralizada.

Protocolo SOAP

SOAP (Simple Object Access Protocol), proporciona un mecanismo estándar de empaquetar mensajes. Ha recibido gran atención debido a que facilita una comunicación del estilo RPC (Remote Procedure Calls) entre un cliente y un servidor remoto. (García, y otros, 2008)

Se convirtió en una recomendación de la W3C (World Wide Web Consortium) el 24 de junio de 2003, pero existen multitud de protocolos creados para facilitar la comunicación entre aplicaciones, incluyendo RPC de Sun, DCE de Microsoft, RMI de Java y ORPC de CORBA. Entonces, ¿por qué se presta tanta atención a SOAP?

Una de las razones principales es que ha recibido un increíble apoyo por parte de la industria. Es el primer protocolo de su tipo que ha sido aceptado prácticamente por todas las grandes compañías de software del mundo, como por ejemplo: Microsoft, IBM, SUN, Microsystems, SAP y Ariba.

Algunas de las ventajas de SOAP son:

- ✓ No esta asociado con ningún lenguaje: los desarrolladores involucrados en nuevos proyectos pueden elegir desarrollar con el último y mejor lenguaje de programación que exista pero los desarrolladores responsables de mantener antiguas aflicciones heredadas podrían no poder hacer esta elección sobre el lenguaje de programación que utilizan. SOAP no especifica una API, por lo que la implementación de la API se deja al lenguaje de programación, como en Java, y la plataforma como Microsoft .Net.
- ✓ No se encuentra fuertemente asociado a ningún protocolo de transporte: su especificación no describe como se deberían asociar los mensajes de SOAP con HTTP. Un mensaje de SOAP no es más que un documento XML (Extensible Markup Language), por lo que puede transportarse utilizando cualquier protocolo capaz de transmitir texto.
- ✓ No está atado a ninguna infraestructura de objeto distribuido: la mayoría de los sistemas de objetos distribuidos se pueden extender, y ya lo están alguno de ellos para que admitan SOAP.
- ✓ 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, SOAP aprovecha XML para la codificación de los mensajes, en lugar de utilizar su propio sistema de tipo que ya están definidas en la especificación esquema de XML. Y como ya se ha mencionado SOAP no define un medio de trasporte de los mensajes; los mensajes de SOAP se pueden asociar a los protocolos de transporte existentes como HTTP y SMTP.
- ✓ Permite la interoperabilidad entre múltiples entornos: SOAP se desarrollo sobre los estándares existentes de la industria, por lo que las aplicaciones que se ejecuten en plataformas con dicho estándares pueden comunicarse mediante mensaje SOAP con aplicaciones que se ejecuten en otras plataformas. Por ejemplo, una aplicación de escritorio que se ejecute en una PC puede comunicarse con una aplicación del back-end ejecutándose en un mainframe capaz de enviar y recibir XML sobre HTTP.

Anatomía de un mensaje de SOAP

SOAP proporciona un mecanismo estándar de empaquetar un mensaje. Un mensaje SOAP se compone de un sobre que contiene el cuerpo del mensaje y cualquier información de cabecera que se utiliza para describir le mensaje.

El elemento raíz del documento es el elemento Envelope. El ejemplo contiene dos subelementos, Body (cuerpo) y Header (cabecera). Un ejemplo de SOAP válido también puede contener otros elementos hijos en el sobre.

El sobre puede contener un elemento Header opcional que contiene información sobre el mensaje. En el ejemplo anterior, la cabecera contiene dos elementos que describen a quien compuso el mensaje, y posible receptor del mismo.

El sobre debe tener un elemento Body que contiene la carga de datos del mensaje. En el ejemplo el cuerpo contiene una simple cadena de caracteres.

Un mensaje debe estar dentro del sobre de SOAP bien construido. Un sobre se compone de un único elemento Envelope el sobre puede contener un elemento Header y debe contener un elemento Body. Si existe, la cabecera debe ser el elemento hijo inmediato del sobre, con el cuerpo siguiendo inmediatamente a la cabecera.

El cuerpo contiene la carga de datos del mensaje y la cabecera contiene los datos adicionales que no pertenecen necesariamente al cuerpo del mensaje.

Además de definir un sobre de SOAP, la especificación de SOAP define una forma de codificar los datos contenidos en un mensaje. La codificación de SOAP proporciona un mecanismo estándar para serializar tipos de datos no definidos en la parte 1 de la especificación del esquema de XML.

La especificación de SOAP también proporciona un patrón de mensaje estándar para facilitar el comportamiento de tipo RPC. Se emparejan dos mensajes de SOAP para facilitar la asociación de un mensaje de petición con un mensaje de respuesta.

La llamada a un método y sus parámetros se serializan en el cuerpo del mensaje de petición en forma de una estructura.

El elemento raíz tiene el mismo nombre que el método objetivo, con cada uno de los parámetros codificado como un subelemento.

El mensaje de respuesta puede contener los resultados de la llamada al método o una estructura de fallo bien definida. Los resultados de la llamada a un método se serializan en el cuerpo de la petición como una estructura. Por convenio, el elemento raíz tiene el mismo nombre que el método original al que se añade result. Los parámetros de retorno se serializan como elementos hijo, con el parámetro de retorno en primer lugar. Si se encuentra un error el cuerpo del mensaje de respuesta contendrá una estructura de fallo bien definida.

Metodología de desarrollo.

Las metodologías de desarrollo de aplicaciones informáticas proveen soluciones a un problema común: la complejidad del desarrollo de software. Imponen un proceso disciplinado sobre el desarrollo de software con el fin de hacerlo más predecible y eficiente.

A continuación una descripción de las metodologías valoradas:

SCRUM

Es una metodología ágil para la gestión de proyectos. “El precepto básico de esta metodología es que el mercado competitivo de los productos tecnológicos, además de los conceptos básicos de calidad, coste y diferenciación, exige también rapidez y flexibilidad”. (Takeuchi, 1999)

Sin embargo, más que una metodología de desarrollo de software, es una forma de auto-gestión de los equipos de programadores. Un grupo de programadores deciden cómo hacer sus tareas y cuánto van a tardar en ello. Scrum ayuda a que trabajen todos juntos, en la misma dirección, con un objetivo claro. Igualmente permite seguir el avance de las tareas a realizar, de forma que los "jefes" y clientes puedan ver día a día cómo progresa el trabajo.

Es una metodología que está empujando muy fuerte por la facilidad de implantación y por su agilidad en cuanto a cambios y lo que propiamente aporta en comparación con otras. Evita la burocracia y la generación documental: No significa esto que no se deba o no se pueda documentar, si no que no se exige documentar nada para iniciar un proyecto, algo que en otras metodologías es impensable. La idea principal es la de ponerse a trabajar prácticamente desde el primer momento y empezar a sacar frutos de ese trabajo para que el cliente vaya viendo los avances y se quede satisfecho con lo que se está haciendo y cómo se está haciendo.

Hay dos aspectos fundamentales a diferenciar, los actores y las acciones. Los actores de forma general, serán:

- ✓ Product Owner (Propietario del Producto): conoce y marca las prioridades del proyecto o producto.
- ✓ Scrum Master (Maestro del Scrum): es la persona que asegura el seguimiento de la metodología guiando las reuniones y ayudando al equipo ante cualquier problema que pueda aparecer. Su responsabilidad es, entre otras, la de hacer de paraguas ante las presiones externas.
- ✓ Scrum Team (Equipo de Scrum): son las personas responsables de implementar la funcionalidad o funcionalidades elegidas por el Product Owner.

- ✓ Usuarios o Clientes: son los beneficiarios finales del producto, y son quienes viendo los progresos, pueden aportar ideas, sugerencias o necesidades.

En el desarrollo del software es de vital importancia que el Usuario o Cliente se involucre, aunque no siempre lo entiende así.

Las acciones de Scrum forman parte de un ciclo iterativo repetitivo, por lo que el mecanismo y forma de trabajar que a continuación se indica, tiene como objetivo minimizar el esfuerzo y maximizar el rendimiento en el desarrollo. (Palacio, 2008)Las acciones fundamentales de Scrum son:

- ✓ Product Backlog (Pila de Tareas del Producto): corresponde con todas las tareas, funcionalidades o requerimientos a realizar. El Product Owner es la persona que se encarga de marcar las prioridades, y es al fin y al cabo, la persona que mantiene y actualiza dado el caso, la lista de tareas.

- ✓ Sprint Planning Meeting (Reunión de Planificación del Ciclo): es una reunión que tiene por objetivo, planificar el Sprint a partir del Product Backlog. El objetivo de esta reunión es la de mover las tareas del Product Backlog al Sprint Backlog. En esta reunión, suelen participar el Product Owner, el Scrum Master y el Scrum Team. De esta reunión surge el Sprint Goal, que es un pequeño documento o una breve descripción que indica lo que el Sprint intentará alcanzar.

- ✓ Sprint Backlog (Pila de Tareas del Sprint o Ciclo): corresponde con una o más tareas que provienen del Product Backlog de donde se saca una o más tareas que van a formar parte del Sprint Backlog. Estas se deben acometer (recomendado) en unas 2 ó 4 semanas. Eso debe de ser marcado antes de iniciar el Sprint. Una norma fundamental es que mientras un Sprint Backlog se inicia, éste NO puede ser alterado o modificado. Hay que esperar a que concluya el Sprint Backlog para realizar la correspondiente modificación o alteración cuya tarea, formaría parte de otro Sprint Backlog.

- ✓ Daily Scrum Meeting (Reunión Diaria de Scrum): es una tarea iterativa que se realiza todos los días que dure el Sprint Backlog con el equipo de desarrollo o de trabajo. Se trata de una reunión operativa, informal y ágil, de un máximo de 30 minutos, en la que se le hace 3 preguntas a cada integrante del equipo:

    - Qué tareas ha realizado desde la última reunión (¿qué he hecho?).

    - Sobre qué va a trabajar en el día actual (¿qué voy a hacer hoy?).

- Identificación de obstáculos o riesgos que impiden o pueden impedir el normal avance (¿qué ayuda necesito?). El Scrum Master, debe eliminar aquí cualquier obstáculo que encuentre.

"Cuando se ha finalizado un Sprint Backlog, se debe tener un entregable que se pueda mostrar y que evidencie los avances acometidos en el Sprint." (Takeuchi, 1999)Pero no acaban aquí las acciones o actividades…

- ✓ Sprint Review (Revisión del Sprint o Ciclo): se revisa en unas 2 horas como máximo el Sprint finalizado. Al llegar a este punto, se debe tener un entregable que el Cliente o el Usuario pueda valorar. En esta reunión, suelen asistir el Product Owner, el Scrum Master, el Scrum Team y personas que podrían estar involucradas en el proyecto. El Scrum Team es quién muestra los avances realizados en el Sprint.

- ✓ Sprint Retrospective (Retroalimentación del Ciclo): comienza luego de finalizar un Sprint Review. El Product Owner revisará con el equipo los objetivos marcados inicialmente en el Sprint Backlog concluido, se aplicarán los cambios y ajustes si son necesarios, y se marcarán los aspectos positivos (para repetirlos) y los aspectos negativos (para evitar que se repitan) del Sprint.

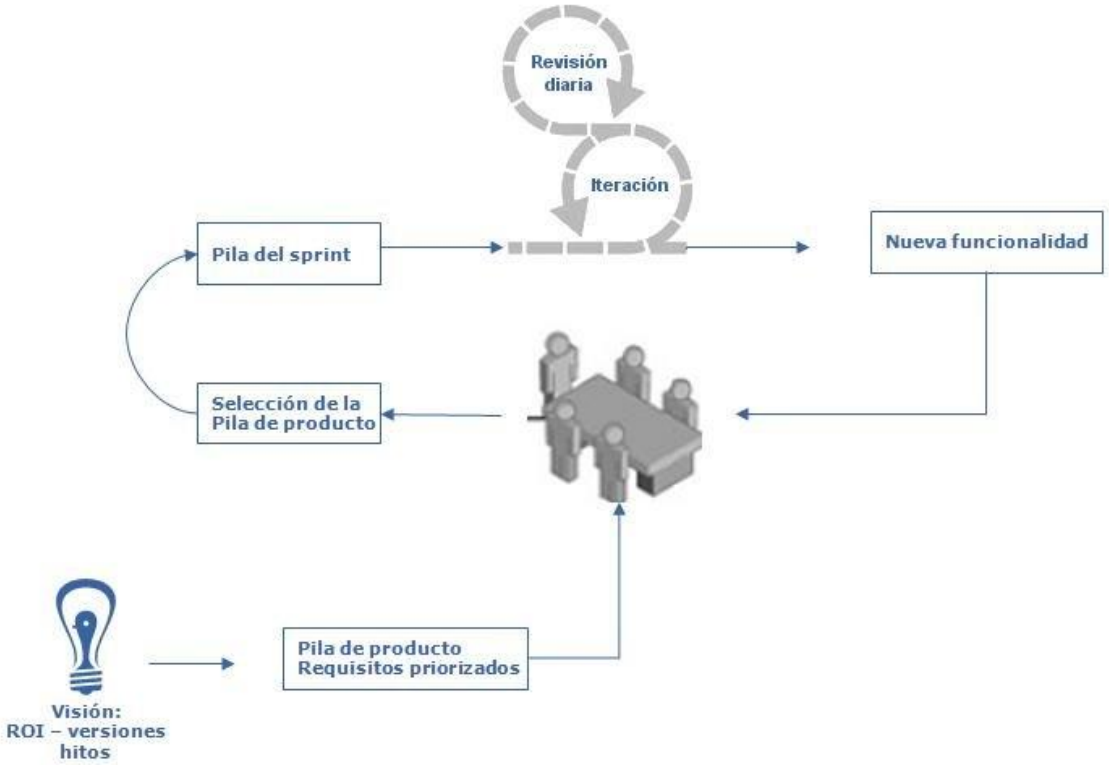


Figura 1: Ciclo de Scrum.

Una vez terminado el Sprint si en el Product Backlog no quedan tareas se planifica un descanso para el Scrum Team donde se resuelven posibles cuestiones vistas en el Sprint Retrospective. Comienza así otra fase en la que se comenzará nuevamente planificando un Sprint Planning Meeting.

Proceso Unificado de Desarrollo (RUP, Rational Unified Process)

RUP es el resultado de varios años de desarrollo y uso práctico en el que se han unificado técnicas de desarrollo, a través del UML, y trabajo de muchas metodologías utilizadas por los clientes. La versión que se ha estandarizado vio la luz en 1998 y se conoció en sus inicios como Proceso Unificado de Rational 5.0; de ahí las siglas con las que se identifica a este proceso de desarrollo.

En esta metodología se han unido las actividades en grupos lógicos definiéndose 9 flujos de trabajo principales. Los 6 primeros son conocidos como flujos de ingeniería y los tres últimos como de apoyo. En la Figura 2: RUP en dos dimensiones se representa el proceso, en ella se grafican los flujos de trabajo y las fases y muestra la dinámica expresada en iteraciones y puntos de control.

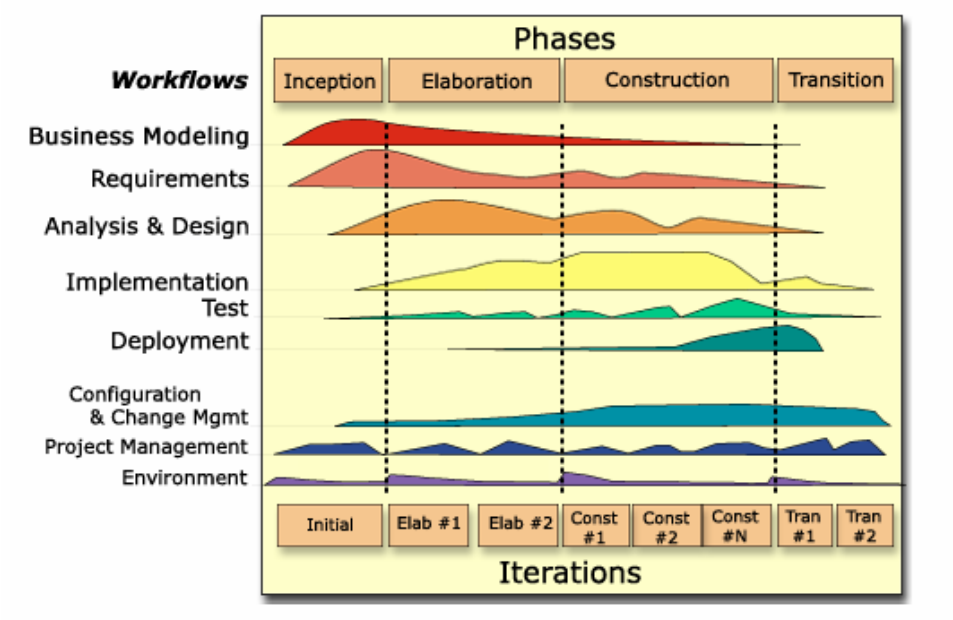


Figura 2: RUP en dos dimensiones

Características generales de RUP:

- ✓ Es un proceso pesado.
- ✓ Dirigido por casos de uso, donde se refleja lo que los usuarios futuros necesitan y desean representándose a través de los requerimientos.

- ✓ Centrado en la arquitectura, pues esta muestra la visión común del sistema completo en la que el equipo de proyecto y los usuarios deben estar de acuerdo.

- ✓ Iterativo e Incremental: RUP propone que cada fase se desarrolle en iteraciones. Una iteración involucra actividades de todos los flujos de trabajo aunque no sean completamente necesarios productivamente, haciendo el proceso menos ágil.

- ✓ Está pensado para equipos de desarrollo grandes en los que están muy bien definidos los roles, artefactos que generan y el nivel de detalle con que lo hacen en cada fase.

- ✓ Es necesario incluir a más personas en el equipo de desarrollo: Especialistas en los diseños y evolución de casos de uso, de los modelos de análisis y diseño, de los modelos de implementación, entre otros.

- ✓ Está basado mucho en la documentación. Por solo citar un ejemplo: Existe diferentes elementos de planificación (plan de desarrollo, plan de iteración, plan de calidad, entre otros).

- ✓ Si el conjunto de documentos y artefactos no son concebidos tal y como se plantea, dicha documentación solo servirá para ser archivada lo cual no genera valor respecto a la calidad del desarrollo, y evoluciona en problemas más complejos.

- ✓ Lo más importante en el desarrollo de un producto informático es el propio desarrollo, en RUP se gasta posiblemente demasiado tiempo para pasar a la fase de desarrollo.

De acuerdo a los datos anteriores se considera oportuno seleccionar SCRUM como la metodología que guie el desarrollo del producto. Esta permite ajustar el proceso productivo al tiempo disponible evitando la generación documental innecesaria y propone que el equipo que llevará adelante la tarea sea pequeño, concordando con la realidad. Las personas implicadas están completamente familiarizadas con ella por lo que no habrá que invertir tiempo y recursos en realizar una preparación previa para su uso.

Lenguajes de desarrollo

La selección del lenguaje es un paso sumamente importante a la hora de desarrollar un software, de la eficacia con que se lleve a cabo depende en gran medida el éxito que tendrá el producto final.

Se realizó un estudio de las fortalezas y debilidades de los lenguajes: Java, C++ y C# para seleccionar uno. No se afirma que uno es mejor o peor que otro, simplemente alguno se ajustará mejor a las necesidades reales del proyecto y de las personas involucradas; influenciado por el nivel de conocimientos que estas posean.

Java

Ventajas:

- Portabilidad alta: puede ejecutarse en diferentes plataformas.
- Amplia disponibilidad de IDEs.
- No usa apuntadores (o punteros)
- Posee mucho código disponible en la web
- Múltiples frameworks
- Mercado madurando constantemente e integrando tecnologías nuevas (servicios web, ajax, etc.)

Desventajas

- En móviles, no hay una estandarización de la Máquina Virtual, por lo que se requiere escribir mucho código para saber que librerías se pueden o no utilizar
- La Máquina Virtual es muy pesada sobre algunos Sistemas Operativos, por ejemplo: Windows.
- Existen picos de memoria difíciles de controlar. (2006)
- Debido a la portabilidad y modelo de seguridad de la Máquina Virtual no es apto para desarrollar aplicaciones que tengan que interactuar con las API (del inglés: Application Programming Interface) de los sistemas operativos.

C++

Ventajas:

- Permite desarrollar múltiples tipos de aplicaciones.
- Con los conocimientos adecuados se pueden hacer aplicaciones de alto rendimiento
- Multiplataforma

- Gran cantidad de compiladores, Idas, librerías y otros recursos disponibles
- Permite acceder a las API del Sistema Operativo
- Rico en características de Programación Orientada a Objetos (POO).
- Favorece la programación electrónica.

Desventajas:

- Requiere un nivel de conocimientos de programación muy alto.
- No hay una forma (directa) de hacer aplicaciones web.
- Los desarrollos toman más tiempo debido a su complejidad técnica.
- Exige saber muy bien cómo utilizar apuntadores de memoria.

C#

Con la realización de C# se pretendió que tuviese las ventajas de C, de C++, pero además la productividad que posee Java.

Ventajas

- Permite desarrollar aplicaciones de forma muy sencilla pues tiene una sintaxis fácil de manejar y aprender.
- Es flexible.
- Permite ahorrar tiempo ya que tiene una librería de clases muy completa y bien diseñada.
- Favorece la reutilización de código.
- Rico en características de Programación Orientada a Objetos (POO).
- Disponibilidad de Idas gratuitos que lo poseen (SharpDevelop y Visual Studio Express)
- Alta integración con el sistema operativo Windows
- Alta disponibilidad de recursos en la web.
- Lenguaje en evolución constante.

Desventajas

- Requiere que cada aplicación distribuida utilice exactamente las librerías del Framework correspondiente.
- Muy casado a plataformas Windows.

Cada uno de estos lenguajes ofrece diferencias en sus características. Teniendo en cuenta que no se cuenta con mucho tiempo para implementar el subsistema propuesto por esta investigación se escoge el lenguaje C# pues tiene una librería de clases muy completa y bien diseñada. Se añade que el desarrollador posee habilidades, amplios conocimientos y familiaridad para con dicho lenguaje; además existe gran cantidad de material de estudio sobre su uso apropiado.

Entorno de desarrollo integrado (IDE, Integrated Development Environment)

Un IDE es un entorno de programación que ha sido empaquetado como un programa de aplicación. Consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica (GUI). Los Idas pueden ser aplicaciones por sí solas o pueden ser parte de aplicaciones existentes.

Para el desarrollo del Subsistema para la gestión de la seguridad en sistemas distribuidos, se consideraron los Idas: Microsoft Visual Studio .NET y SharpDevelop ya que usan el lenguaje C# seleccionado anteriormente.

Se analizaron las características de cada uno a través de la siguiente tabla:

Propiedad	SharpDevelop 3.0	SharpDevelop 2.2	Visual Studio EE	Visual Studio 2008 TS
Completamiento de código	Si	Si	Si	Si
Pruebas de Unidad	Si	Si	No	Si
Lenguajes soportados	C#, VB.NET, Boo, F#, IronPython	C#, VB.NET, Boo	C#, C++, VB.NET, J#	C#, C++, VB.NET, J#
Documentación de ayuda	No	No	Si	Si
Referencias Web	Si	Si	Si	Si
Generación de código	Si	Si, pero no tan poderoso.	Si	Si
Lista de tareas	Si	Si	Si	Si
Lista de errores	Si	Si	Si	Si
Conversión de código	Si	Si	No	No
Historial de Navegación	Si	Si	Si	Si

Vista previa, documentación y generación XML	Si	Si	No	Si
Gratis	Si	Si	Si	No

Tabla 1: Comparación entre Idas de desarrollo

Analizando los factores en que se basa la comparación se puede observar que los cuatro IDEs poseen casi las mismas características haciendo compleja la elección.

Las facilidades de desarrollar Pruebas de unidad (a realizarse en el subsistema) y obtener Vista previa, documentación y generación XML; no están presentes en Visual Studio Express Editions. Ambos aspectos son significativos para el desarrollo del subsistema en cuestión, por lo que se descarta Visual Studio Express Editions. También se suprime SharpDevelop 2.2 porque se cuenta con SharpDevelop 3.0 que es una versión más estable, actual y mejorada del software.

Se arriba a la conclusión de que SharpDevelop 3.0 es el IDE que se usará para completar el desarrollo del subsistema pues posee las potencialidades que brinda Microsoft Visual Studio 2008 Team System y además remedia la situación desfavorable de éste, al ser gratis.

Sistemas de gestión de bases de datos.

Para desarrollar un sistema, generalmente, es necesario manejar cierto volumen de información que debe ser gestionada eficientemente para que la aplicación se nutra de los datos y funcione de forma correcta. Es lógico determinar que se necesite un lugar donde almacenar los datos y de un mecanismo que los manipule.

Se podrán lograr dichos objetivos usando un Sistema de gestión de bases de datos (SGBD), que no es más que una herramienta que permite que el usuario pueda administrar las bases de datos y a su vez los datos almacenados en las mismas de una forma sencilla, abstrayéndolo de las complejidades funcionales que ocurren en cada operación.

Un SGBD sirve de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

Entre los SGBD más usados actualmente están: PostgreSQL, MySQL, Microsoft SQL Server y Oracle.

A continuación se caracterizarán los dos primeros por ofrecer compatibilidad de uso con sistemas operativos libres.

PostgreSQL

Es un servidor de base de datos liberado bajo la licencia BSD (Berkeley Software Distribution).

Como muchos otros proyectos de código abierto (open source), el desarrollo de PostgreSQL no es manejado por una sola compañía sino que es dirigido por una comunidad de desarrolladores y organizaciones comerciales las cuales trabajan en su desarrollo, permitiendo que se desarrolle y expanda a gran velocidad y con mucha calidad. Dicha comunidad es denominada el PGDG (PostgreSQL Global Development Group).

Se diseñó como una base de datos orientada a objetos. Esto significa, que las tablas no son tablas, sino objetos, y las tuplas son instancias de ese objeto. Cuenta con un amplio conjunto de enlaces con lenguajes de programación (incluyendo C, C++, Java, Perl, PHP, Ruby, entre otros) Permite crear nuevos tipos de datos, hacer herencias entre objetos, tiene transacciones, integridad referencial, vistas, y multitud de funcionalidades, pero es lento y pesado.

PostgreSQL provee nativamente soporte para:

- ✓ Números de precisión arbitraria.
- ✓ Texto de largo ilimitado.
- ✓ Figuras geométricas (con una variedad de funciones asociadas)
- ✓ Direcciones IP (IPv4 e IPv6).
- ✓ Bloques de direcciones estilo CIDR.
- ✓ Direcciones MAC.
- ✓ Arrays.
- ✓ Claves ajenas también denominadas Llaves ajenas o Llaves Foráneas (foreign keys).
- ✓ Disparadores (triggers).
- ✓ Vistas.
- ✓ Integridad transaccional.
- ✓ Herencia de tablas.

Tiene incorporado la llamada MVCC, o Control de Concurrencia Multi-Versión (Multi-Version Concurrency Control), que es la tecnología que PostgreSQL usa para evitar bloqueos innecesarios.

Características adicionales:

- ✓ pg_dump selectivo: permite extraer vuelcos transaccionalmente consistentes de relaciones, seleccionando la inclusión y exclusión usando expresiones regulares.

- ✓ Criptografía: el módulo pgcrypto, soportando criptografía dentro de la base de datos, fue actualizado con los últimos algoritmos.

- ✓ Mejoras al SQL: nueva sintaxis, incluyendo UPDATE RETURNING, DROP IF EXISTS, ON COMMIT y nuevos comandos de propiedad («ownership») y permisos, para hacer más fácil el manejo de objetos de la base de datos en la línea de órdenes.

- ✓ Extracción de registros por lotes en psql: permite devolver filas a la consola en lotes en lugar de todas a la vez.

- ✓ Mejoras importantes en TSearch2: soporte de UTF-8, tesauros, soporte de reescritura de consultas e indexación GIN.

MySQL 5.0

Es un SGBD relacional, multihilo y multiusuario. Ofrece compatibilidad con PHP, Perl, C y HTML, y funciones avanzada de administración y optimización de bases de datos para facilitar las tareas habituales. Implementa funcionalidades Web, permitiendo un acceso seguro y sencillo a los datos a través de Internet. Incluye capacidades de análisis integradas, servicios de transformación y duplicación de datos y funciones de programación mejoradas.

Algunas de sus características son:

- ✓ Escrito en C y C++
- ✓ Trabaja bajo diferentes plataformas: AIX 4x 5x, Amiga, BSDI, Digital Unix 4x, FreeBSD 2x 3x 4x, HP-UX 10.20 11x, Linux 2x, Mac OS, NetBSD, Novell NetWare 6.0 , OpenBSD 2.5, OS/2, SCO OpenServer, SCO UnixWare 7.1.x, SGI Irix 6.x, Solaris 2.5, SunOS 4.x, Tru64 Unix y Windows 9x, Me, NT, 2000, XP, 2003
- ✓ Desarrollo de APIs para C, C++, Eiffel, Java, Perl, PHP, Python, Ruby, y Tcl
- ✓ Procesos MultiHilo. Capacidad de trabajar servidores con varios procesadores
- ✓ Alta velocidad en la utilización de joins y procesos de optimización

- ✓ Soporta muchos tipos de columnas para las tablas: FLOAT, DOUBLE, CHAR, VARCHAR, TEXT, BLOB, DATE, TIME, DATETIME, TIMESTAMP, YEAR, SET, ENUM y OpenGIS (Modelo Geométrico)
- ✓ Manejo de la memoria a través de manejo del buffer y cache
- ✓ Motores de almacenamiento independientes (MyISAM para lecturas rápidas, InnoDB para transacciones e integridad referencial)
- ✓ Soporte para Secure Socket Layer (capa del enchufe segura).
- ✓ Sub-SELECTs (o SELECTs anidados).
- ✓ Soporte completo para Unicode.

Habiendo analizado las características de ambos SGBD se selecciona para su utilización PostgreSQL por las facilidades abordadas anteriormente y dado que el software es desarrollado por una comunidad pública y el copyright del código está en poder del autor individual. MySQL es propietario y está patrocinado por una empresa privada, que posee el copyright de la mayor parte del código, o sea, tiene licencia que por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, y por otro aquellas empresas que quieran incorporarlo en productos privativos deben comprar una licencia específica que les permita este uso.

Otras herramientas usadas para el desarrollo del subsistema.

Enterprise Architect

Enterprise Architect (EA) combina el poder de la última especificación UML 2.1 con alto rendimiento, interfaz intuitiva, para traer modelado avanzado al escritorio, y para el equipo completo de desarrollo e implementación. Con un gran conjunto de características y un valor sin igual para el dinero, EA puede equipar a un equipo de desarrollo entero, incluyendo analistas, evaluadores, administradores de proyectos, personal del control de calidad, desarrolladores y más, por una fracción del costo de algunos productos competitivos. Es una herramienta comprensible de diseño y análisis UML, cubriendo el desarrollo de software desde el paso de los requerimientos a través de las etapas del análisis, modelos de diseño, pruebas y mantenimiento. EA es una herramienta multi-usuario, diseñada para ayudar a construir software robusto y fácil de mantener. Ofrece salida de documentación flexible y de alta calidad. (Sparxsystems, 2005)

EA Provee una generación poderosa de documentos y herramientas de reporte con un editor de plantilla completo WYSIWYG. Genera reportes detallados y complejos. Soporta generación e ingeniería inversa de código fuente para muchos lenguajes populares, incluyendo C++, C#, Java, Delphi, VB.Net, Visual Basic y PHP. También hay Add-ins gratis para CORBA y Python disponibles. Con un editor de código fuente con "resaltador de sintaxis" incorporado, permite navegar y explorar el modelo de código fuente en el mismo ambiente.

Microsoft Visio

Proporciona un entorno de dibujo dedicado y familiar que incluye una amplia gama de plantillas, formas y herramientas diseñadas para facilitar realmente la creación de una enorme variedad de diagramas empresariales y técnicos.

Fue usada para realizar y diseñar dibujos.

Microsoft Project

Microsoft Project es un Software de administración de proyectos desarrollado y vendido por Microsoft el cual esta creado para asistir a los administradores de proyectos en el diseño de planes, asignación de recursos a tareas, rastreo de progresos y análisis de cargas de trabajo.

En este trabajo se utilizó para desarrollar un diagrama de Gantt.

Conclusiones del capítulo.

En el presente capítulo se hizo una descripción de los conceptos asociados al problema, se valoró que no existe sistema capaz de gestionar de forma centralizada y eficiente la seguridad de sistemas distribuidos, siendo esta una deficiencia que pretende solucionar este trabajo de diploma con el desarrollo del subsistema propuesto. Igualmente se hace una descripción de las herramientas de desarrollo usadas y el por qué de su elección.

Como conclusión parcial se destaca la idoneidad de Scrum como Metodología Ágil de desarrollo de Software, Enterprise Architect como Herramienta de Modelado, PostgreeSQL como Gestor de Bases de Datos y SharpDevelop 3.0 como plataforma para desarrollar el subsistema en cuestión.

Capítulo II

Propuesta de solución

Capítulo II. Descripción de la propuesta de solución.

Introducción al Capítulo

En el presente capítulo se hace una descripción de la propuesta de solución de este trabajo, se detalla la arquitectura del sistema y se explican los principales artefactos de la metodología empleada y que debe tener el sistema propuesto.

Igualmente, se especifican los aportes prácticos y vías de solución de la situación problemática. Se realiza la construcción de la propuesta de solución desarrollando el Product Backlog, la planificación de los Sprint, los diagramas de clases de diseño asociados a los Sprint Backlog de Scrum y se valoran los principios de diseño, el tratamiento de excepciones, el estándar de codificación y la concepción de la ayuda que se trata en el subsistema.

Descripción del subsistema propuesto.

Arquitectura candidata

Los sistemas distribuidos basan su funcionamiento, generalmente, en una arquitectura orientada a servicios (no necesariamente SOA) que facilite la integración de cada uno de sus componentes y subsistemas entre ellos y con otros sistemas, tanto locales como externos. A continuación se muestra una vista genérica de cómo organizar servicios para este tipo de sistemas.

Figura 3. Forma de organización de los servicios e interfaces de un sistema distribuido.

La arquitectura del GeSeg debe ser capaz de interactuar con este tipo de organización por lo que se propone un estilo cliente servidor que se acople al funcionamiento de los servicios vistos anteriormente quedando de la siguiente manera:

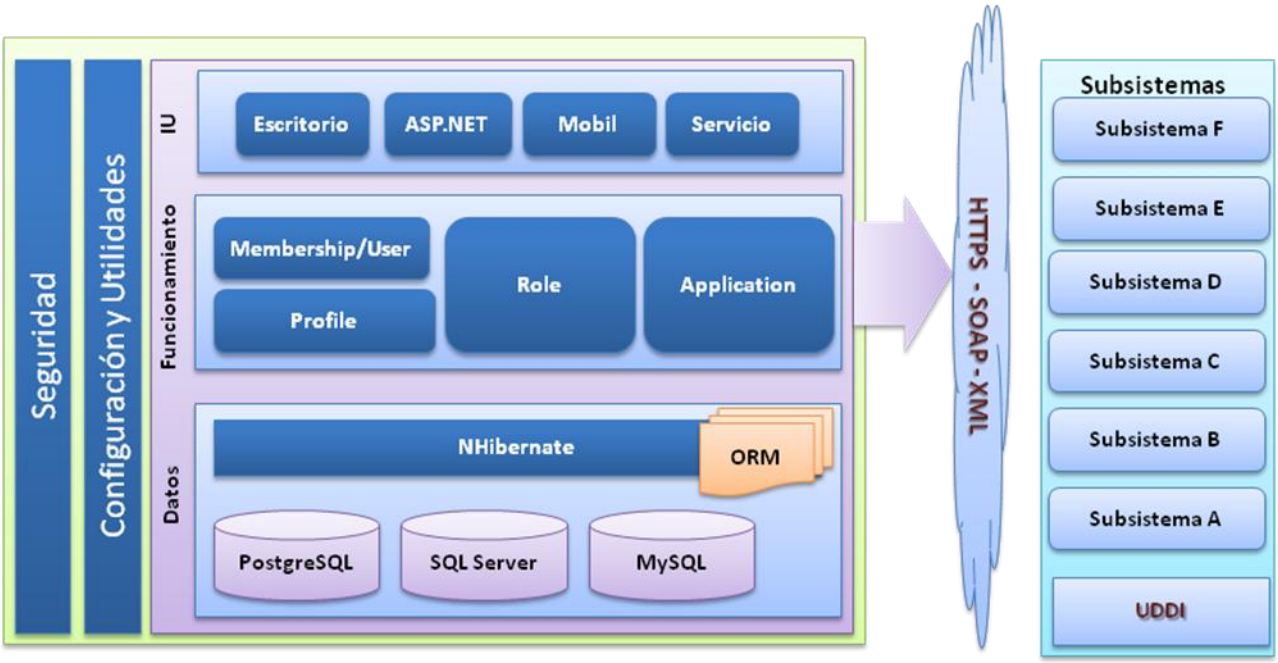


Figura 4. Estilo Cliente-Servidor con implementación en capas.

En el bloque de la izquierda se muestra el servidor y su distribución arquitectónica en 3 capas, a la derecha el lado del cliente que implementa su arquitectura propia basada en la figura 3.

Para garantizar el funcionamiento del subsistema en la mayoría de los gestores de bases de datos se modela una capa de datos con la implementación de cómo acceder a estos basándose en el uso de NHibernate, demostrando que no solamente funciona con el SGBD escogido, sino que con una simple configuración se puede usar cualquier otro. De tal forma en este bloque se incluyen los ficheros XML (file.hbm.xml) que mapean las entidades persistentes definidas por los requisitos y que implementan su solución en una o varias tablas del modelo de datos. Se incluyen además los DAO (Data Access Object).

En una capa superior, llamada capa de funcionamiento se implementan los proveedores de seguridad: usuario y perfiles, rol y aplicaciones. Estos proveedores son los responsables de gestionar adecuadamente el funcionamiento de los atributos de seguridad básicos y que han sido extendidos para el uso de los certificados digitales, cuya configuración se explica en el epígrafe Aportes prácticos y vías de solución, que forman parte del proveedor de usuarios y perfiles.

Por último se propone una capa de interfaces que puede ser implementada de forma particular en dependencia del tipo de aplicación distribuida y de sus requisitos de interfaz. La propuesta descrita en el presente trabajo de diploma esta enfocada en su aplicación en una aplicación web por lo que la variante sería la segunda de la figura.

Paralelamente al funcionamiento de las capas descritas se implementan las funcionalidades que permitan la configuración, parametrización y utilidades del sistema.

Autenticación

Mediante la sección de autenticación se obtienen credenciales de identificación tales como el nombre de usuario y la contraseña, al tiempo que se validan dichas credenciales ante alguna autoridad.

```
<system.web>
      <authentication mode="[Windows|Forms|Passport|None]">
            <forms name=".NAME" loginUrl="LogonPage.html"
                  defaultUrl="DefaultPage.html"
                  protection="[All|None|Encryption|Validation]"
                  path="path" timeout="minutes"
                  requireSSL="[true|false]">
                        <credentials passwordFormat="[Clear|MD5|SHA1]">
```

```
                        <user name="username"
            password="password"/>
                    </credentials>
            </forms>
            <passport redirectUrl="internal"/>
      </authentication>
</system.web>
```

Sin embargo, para el funcionamiento del subsistema propuesto debe trabajarse con la autenticación de formularios que hace referencia a un sistema en el que la solicitudes no autenticadas se redirigen a un formulario en el que los usuarios escriben sus credenciales. Una vez proporcionadas se envía el formulario, la aplicación autentica la solicitud y el sistema emite un vale de autorización de una cookie. Esta cookie contiene las credenciales o una clave para readquirir la identidad. Las solicitudes subsiguientes del explorador automáticamente incluyen la cookie.

```
<system.web>
      <authentication mode="Forms">
            <forms name=".GeSegAUTH" loginUrl="Login.html"
            defaultUrl="Default.html" protection="Validation"
            timeout="300"/>
      </authentication>
</system.web>
```

Autorización

La autorización determina si se debería conceder acceso a una identidad a un recurso concreto. Existen dos formas de autorizar el acceso a un recurso dado:

1. Autorización de archivos: FileAuthorizationModule realiza la autorización de archivos. Realiza una comprobación de la lista de control de acceso (ACL) del archivo de controladores para determinar si un usuario debe tener acceso al archivo. Los permisos de ACL se comprueban para la identidad de Windows (si se habilita la autenticación de Windows) del usuario o para la identidad de Windows del proceso de ASP.NET. Para obtener más información, vea Suplantación de ASP.NET.
2. Autorización de URL: UrlAuthorizationModule realiza la autorización de URL, que asigna usuarios y funciones a direcciones URL en aplicaciones ASP.NET. Este módulo se puede utilizar para permitir o denegar de forma selectiva el acceso a las partes arbitrarias de una aplicación (normalmente los directorios) para usuarios concretos o funciones.

Con la autorización de URL, permite o deniega explícitamente el acceso a un directorio determinado por nombre de usuario o función. Para ello, se crea una

sección authorization en el archivo de configuración para ese directorio. Para habilitar la autorización de URL, basta con especificar una lista de usuarios o funciones en los elementos permitir o denegar de la sección autorización de un archivo de configuración. Los permisos establecidos para un directorio también se aplican a sus subdirectorios, a no ser que los archivos de configuración de un subdirectorio los reemplacen.

```
<authorization>
      <[allow|deny] [users|roles]="[?|*]"/>
</authorization>
```

Proveedores personalizados

El funcionamiento del subsistema se basa en el uso de proveedores de Roles y Usuarios personalizados los cuales son implementados en el ensamblado que se provee; a continuación se muestra la configuración correcta para su uso, incluyendo los elementos mencionados hasta el momento:

```
<?xml version="1.0"?>

<configuration>
      <connectionStrings>
            <clear/>
            <add name="DefaultDB"
connectionString="DriverClass=NHibernate.Driver.SqlClientDriver;Dialec
t=NHibernate.Dialect.MsSql2005Dialect;Data
Source=localhost;Database=SecurityDB;User
ID=myUser;Password=myPassword;Trusted_Connection=true"/>
      </connectionStrings>
      <system.web>
            <!-- Authentication Mode -->
            <authentication mode="Forms">
                  <forms name=".ASPXAUTH" loginUrl="Login.aspx"
defaultUrl="Default.aspx" protection="Validation" timeout="300"/>
            </authentication>
            <!-- Membership Provider -->
            <membership defaultProvider="MembershipProvider">
                  <providers>
                        <clear/>
                        <add name="MembershipProvider" type="
Security.Membership.MembershipProvider, Security"
connectionStringName="DefaultDB" applicationName="MyAppName"
minRequiredNonAlphanumericCharacters="0" minRequiredPasswordLength="4"
requiresUniqueEmail="false"/>
                  </providers>
            </membership>
            <!-- Role Provider -->
            <roleManager enabled="true" defaultProvider="RoleProvider">
                  <providers>
                        <clear/>
                        <add name="RoleProvider"
connectionStringName="DefaultDB" applicationName="Default" type="
Security.Roles.RoleProvider, Security"/>
                  </providers>
            </roleManager>
```

```
            <!-- Profile -->
            <anonymousIdentification enabled="true"/>
            <profile defaultProvider="ProfileProvider">
                  <providers>
                        <clear/>
                        <add name="ProfileProvider" type="
Security.Profile.ProfileProvider, Security"
connectionStringName="DefaultDB" applicationName="Default"/>
                  </providers>
                  <properties>

<add name="ReceiveNotification" type="Boolean" defaultValue="True"
allowAnonymous="false"/>
                  </properties>
            </profile>
      </system.web>
      <location path="SecurePage.html">
            <system.web>
                  <authorization>
                        <deny users="?"/>
                  </authorization>
            </system.web>
      </location>
</configuration>
```

Vista de despliegue

A continuación se muestra una vista general del despliegue de un sistema distribuido el cual aplica el subsistema propuesto para gestionar su seguridad:

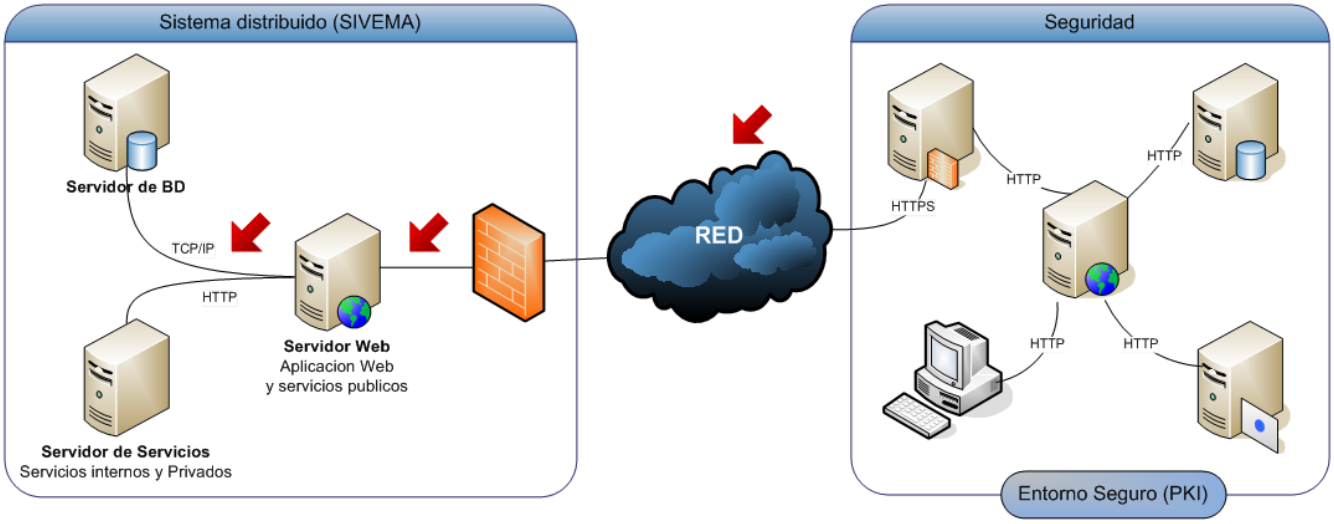


Figura 5. Vista de despliegue.

La vista de despliegue de SIVEMA (en unas de sus variantes) muestra la forma en que el subsistema propuesto queda totalmente aislado en un entorno seguro, con la mayoría de los componentes de un PKI, para la realización de

sus funciones y brindando los servicios de seguridad a los subsistemas que se suscriban a este para garantizar la protección de sus vulnerabilidades (destacadas con flechas rojas en la figura).

Aplicando Scrum como metodología de desarrollo

Product Backlog / Pila de Tareas del Producto

El Product Backlog se considera el corazón de Scrum. Es básicamente una lista enumerada de requisitos o funcionalidades del producto, constituyendo una estimación inicial de los mismos. El Product Owner es responsable del contenido, priorización, y disponibilidad de este: nunca se acaba y es usado en la planificación del proyecto.

Se desarrolla paralelamente a medida que el producto y el ambiente en el cual se trabaja evoluciona, es dinámico; maneja constantemente los cambios para identificar que necesita el producto para ser: apropiado, competitivo, y útil. Mientras exista un producto, el Product Backlog también existe.

Id	Funcionalidad	Descripción	Estado
Requerimientos Críticos			
1	Gestionar subsistemas o aplicaciones	El subsistema debe ser capaz de gestionar las aplicaciones o subsistemas que conforman el sistema distribuido en el cual se piensa aplicar. Esta gestión debe incluir insertar, actualizar y eliminar aplicaciones.	**100%**
2	Gestionar roles de usuarios	Una vez creada las aplicaciones deben poder definirse grupos o roles de usuarios que podrán interactuar en todas o partes de estos subsistemas configurados. Incluye la inserción, modificación, eliminación y asociación de roles a subsistemas o aplicaciones.	**100%**
3	Gestionar usuarios	Debe ser posible crear, actualizar y eliminar usuarios, así como asociar estos a roles precreados y asociados a determinadas aplicaciones o subsistemas. Debe poderse identificar, autenticar y autorizar estos usuarios.	**100%**
Requerimientos Opcionales			
4	Gestionar perfiles	El subsistema debe ser capaz de gestionar perfiles para cada uno de los usuarios de manera tal que se logre una personalización de la apariencia de las sesiones de estos en el sistema distribuido al cual se aplica. Esta gestión incluye crear y actualizar el perfil de un determinado usuario precreado.	**100%**

Id	Funcionalidad	Descripción	Estado
5	Gestionar certificados	El sistema puede gestionar los certificados digitales con los que se trabajen. Para esto se deben permitir generar certificados y asociarlos a los usuarios del sistema. Esta funcionalidad puede ser subcontratada con el uso de terceros (uso de otro software especializado)	**60%**

Tabla 2. Pila de Tareas del Producto

Sprint Backlog / Pila de Tareas del Sprint

Una vez listo y chequeado el Product Backlog se puede pasar a realizar el Spring Backlog. Este último define de forma clara y comprensible las tareas que el equipo desarrollará para poder generar un incremento potencialmente funcional del producto. El equipo crea una lista inicial de estas tareas en la segunda parte del Sprint Planning Meeting. La duración de las tareas se define de acuerdo a la carga que encierren. Se recomienda que sean períodos cortos ya que demuestran agilidad: el ciclo de retroalimentación es breve, se obtienen más entregas de forma frecuente, en caso de error menos tiempo desarrollando en dirección incorrecta, o sea, se puede aprender y mejorar más rápido. Solamente el equipo puede cambiar el Sprint Backlog. A continuación se tabulan las planificaciones de cada uno de los Sprint creados para implementar el subsistema. Las columnas Estimado y Real hacen referencia al factor tiempo medido en días.

Pila del Sprint I (Acceso a Datos)					
Backlog	**Tarea**	**Módulo**	**Estado**	**Estimado**	**Real**
	Diseño y generación de la base de datos	General	100%	5	6
	Creación de DAO y los Mapeos de Nhibernate	General	100%	15	14
	Implementación de la capa de Acceso a Datos	General	100%	10	14

Tabla 3. Pila del Sprint I (Acceso a Datos)

Con la correcta culminación del Sprint I se tiene logrado el 30% de la solución total puesto que sus funciones son vitales para el funcionamiento de los demás. En este Sprint se garantiza el acceso a los datos de una forma segura y genérica de forma tal que pueda migrarse a cualquier otro gestor de Bases de Datos transparentemente y solo implicando un cambio en un XML de configuración para tener nuevamente funcional el sistema sobre el nuevo origen de datos.

Pila del Sprint II (Implementación)

Backlog	Tarea	Estado	Estimado	Real
1	Implementación de las funcionalidades del proveedor de aplicaciones.	100%	3	3
2	Implementación de las funcionalidades del proveedor de roles.	100%	4	5
3	Implementación de las funcionalidades del proveedor de usuarios	100%	7	6
4	Extensión de la implantación del proveedor de usuarios para garantizar la gestión de perfiles	100%	4	7
5	Implementación de un mecanismo de generación de los certificados a través del subsistema comunicándose con la herramienta especializada	60%	10	13

Tabla 4. Pila del Sprint II (Implementación)

La finalización de este Sprint garantiza que se implemente el código necesario para que funcione correctamente el subsistema.

Pila del Sprint III (Soporte y Optimización)				
Backlog	**Tarea**	**Estado**	**Estimado**	**Real**
	Parametrizar la Aplicación	100%	7	9
	Prueba y Corrección de Bugs	100%	10	7
	Documentación	100%	75	84

Tabla 5. Pila del Sprint III (Soporte y Optimización)

El Sprint III se concibe para dar soporte al desarrollo de la aplicación. Igualmente, en el se optimiza su funcionamiento parametrizando sus funcionalidades y logrando un mayor rendimiento de sus prestaciones. En este Sprint es donde se documenta y prueba al dedillo el correcto cumplimiento de las funcionalidades planteadas en el Product Backlog.

La figura siguiente muestra la planificación del tiempo para la etapa de desarrollo del software de acuerdo a las actividades recogidas en los tres Sprint documentados anteriormente

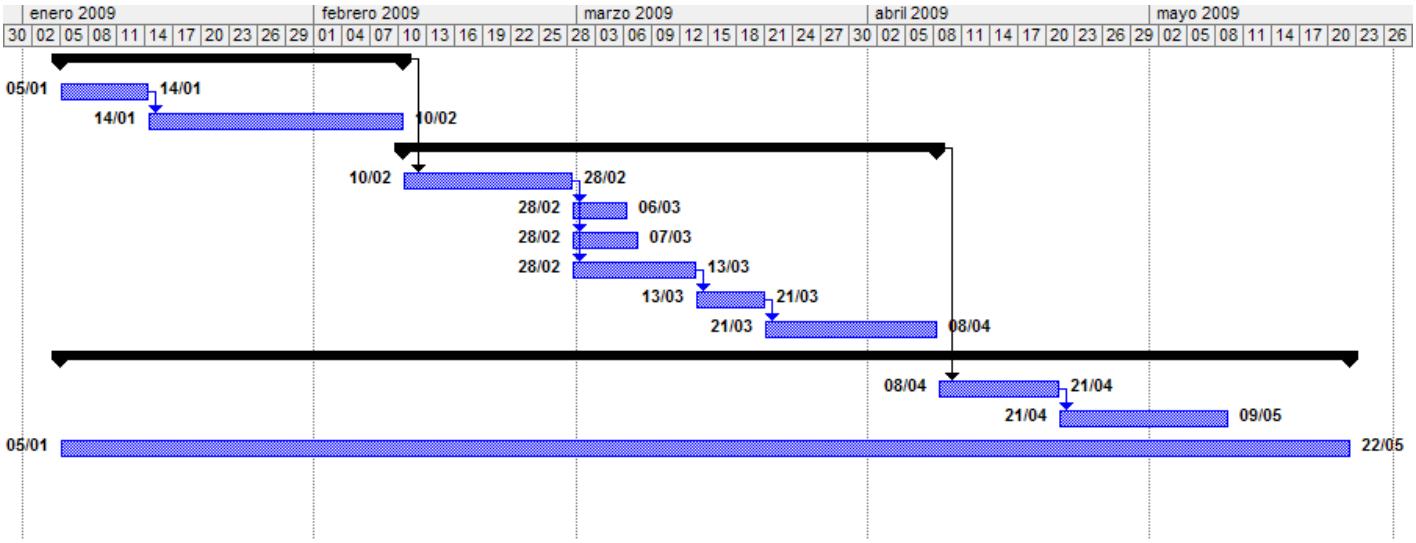


Figura 6. Diagrama de Gantt.

Existen requerimientos adicionales que la aplicación debe tener asociados al cumplimiento de las funcionalidades divididas en Sprint:

Requerimientos adicionales

- ✓ Usabilidad:
  - La puesta en marcha del Subsistema trae consigo la gestión centralizada de la seguridad de aplicaciones distribuidas brindando rapidez y confianza en las transacciones, haciéndolas mucho más eficientes.
- ✓ Software:
  - El servidor de base de datos debe ser PostgreSQL aunque puede instalarse cualquier otro especificándolo en la configuración del Subsistema.
- ✓ Portabilidad:
  - El subsistema se podrá utilizar en la mayoría de los sistemas operativos tales como Microsoft Windows 98/Me/2000/XP y en los de la gama GNU/Linux.
- ✓ Hardware:
  - Para trabajar con el subsistema de forma eficiente se necesita una máquina servidor que como mínimo debe tener las siguientes características: Pentium IV con 768 MB de RAM, un microprocesador a 3.00 GHz y una tarjeta de red Protocolo Ethernet 10/100 MB/s.
  - Para máquinas clientes: un procesador a 600 MHz y memoria RAM de 64 MB o superior. Deben estar conectadas en una red local de 10/100 MB o deben tener un módem de línea telefónica con una conexión a 128 Kbps.

Construcción de la propuesta de solución.

Diagrama de clases

A continuación se muestran las clases: User, Purpose, Role, Asigment, Application, Profile, Property y PropertyId. Además se pueden observar las relaciones que existen entre ellas.

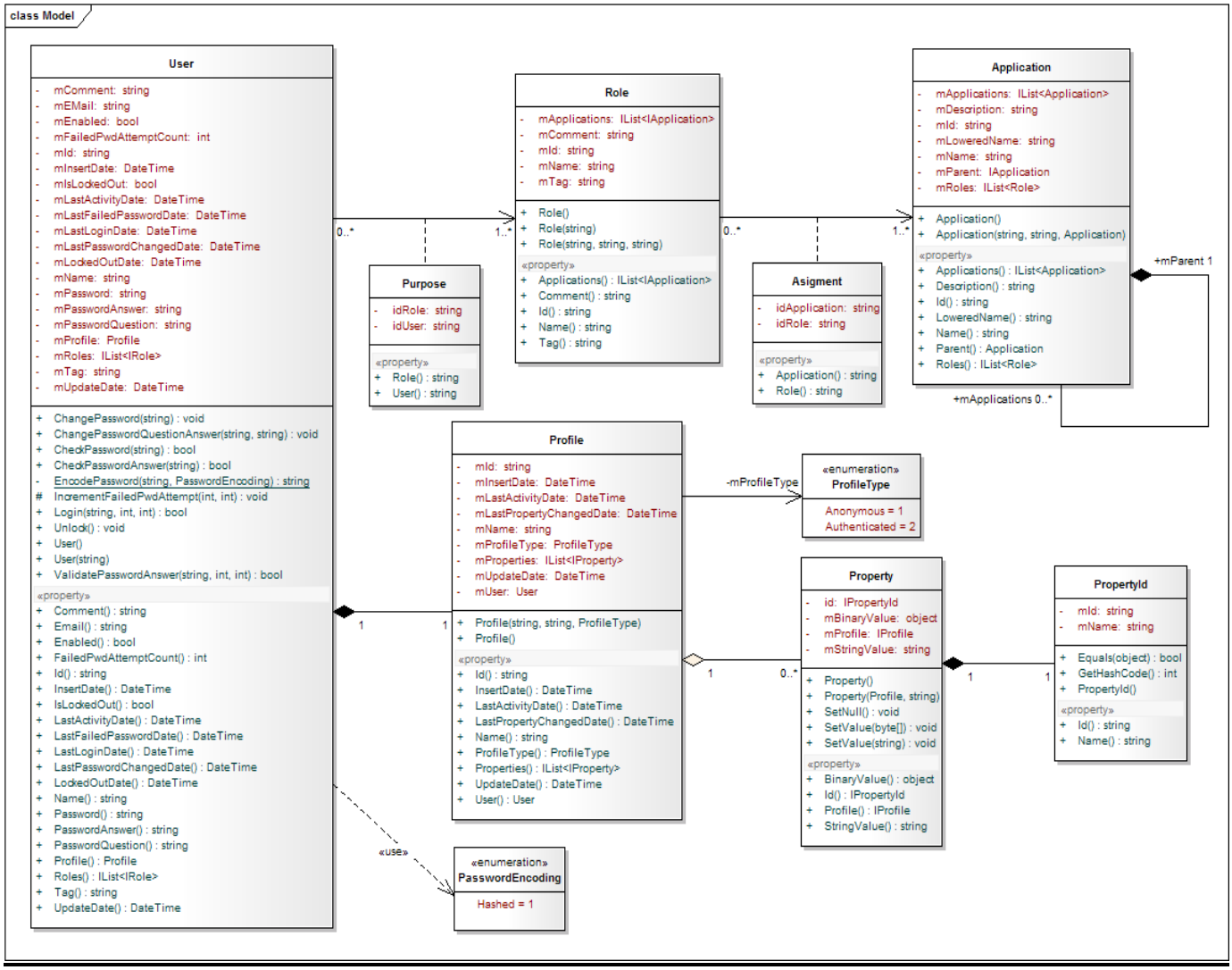


Figura 7. Entidades del negocio y sus relaciones.

Con la conceptualización de estas entidades se pretende lograr un entorno donde existan múltiples aplicaciones (o subsistemas) que conformen los sistemas distribuidos. Por cada una de estas existirán roles (o grupos de usuarios) con permisos determinados para realizar sus funciones registradas en la entidad Asigment.

Los usuarios del sistema deben tener algún rol para trabajar y por tanto quedan restringidos sus accesos solo a las aplicaciones a los que los roles tengan garantizado su acceso.
Por último se gestionan los perfiles de usuario con el objetivo de extender las características de estos y personalizar las aplicaciones. Con el uso de estos perfiles es que se gestionan los certificados personales en el caso de sistemas con estas características.

Diseño de la base de datos

A continuación se muestra la representación de las entidades persistentes que constituyen el dominio del subsistema descritas en la figura anterior así como las relaciones que se establecen entre ellas.

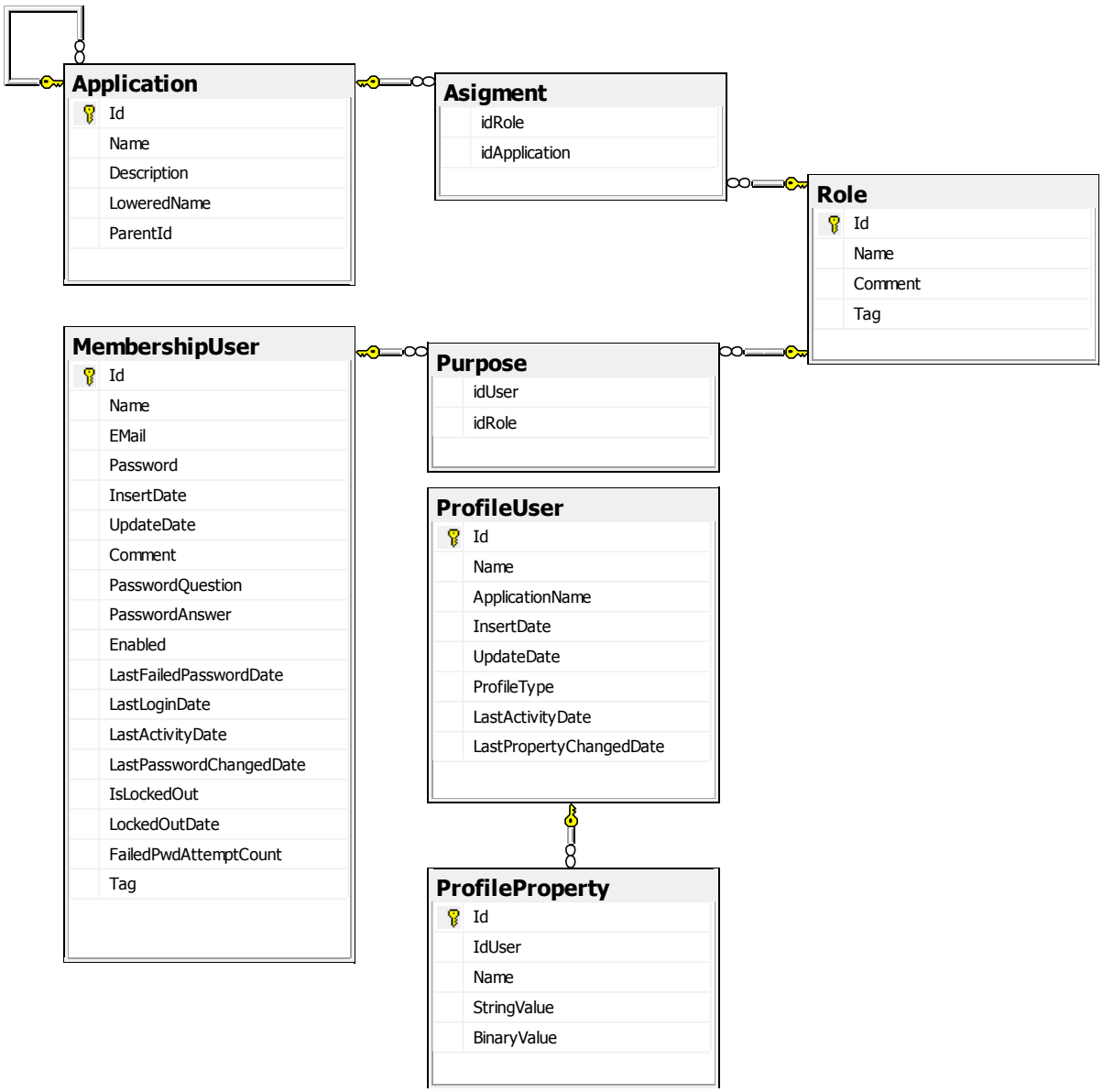


Figura 8. Modelo de la base de datos.

Principios del diseño de la aplicación.

Para el desarrollo del subsistema se tuvieron en cuenta los siguientes principios del diseño de aplicaciones:

1er Principio: Uso equiparable

El diseño es útil y vendible a personas con diversas capacidades.

Pautas para el Principio 1:

- ✓ Que proporcione las mismas maneras de uso para todos los usuarios: idénticas cuando es posible, equivalentes cuando no lo es.
- ✓ Que evite segregar o estigmatizar a cualquier usuario.
- ✓ Las características de privacidad, garantía y seguridad deben estar igualmente disponibles para todos los usuarios.
- ✓ Que el diseño sea atractivo para todos los usuarios.

2do Principio: Uso flexible

El diseño se acomoda a un amplio rango de preferencias y habilidades individuales.

Pautas para el Principio 2

- ✓ Que ofrezca posibilidades de elección en los métodos de uso.
- ✓ Que pueda accederse y usarse tanto con la mano derecha como con la izquierda.
- ✓ Que facilite al usuario la exactitud y precisión.
- ✓ Que se adapte al paso o ritmo del usuario.

3er Principio: Simple e intuitivo

El uso del diseño es fácil de entender, atendiendo a la experiencia, conocimientos, habilidades lingüísticas o grado de concentración actual del usuario.

Pautas para el Principio 3

- ✓ Que elimine la complejidad innecesaria.
- ✓ Que sea consistente con las expectativas e intuición del usuario.
- ✓ Que se acomode a un amplio rango de alfabetización y habilidades lingüísticas.
- ✓ Que dispense la información de manera consistente con su importancia.
- ✓ Que proporcione avisos eficaces y métodos de respuesta durante y tras la finalización de la tarea.

4to Principio: Información perceptible

El diseño comunica de manera eficaz la información necesaria para el usuario, atendiendo a las condiciones ambientales o a las capacidades sensoriales del usuario.

Pautas para el Principio 4

- ✓ Que use diferentes modos para presentar de manera redundante la información esencial (gráfica, verbal o táctilmente)
- ✓ Que proporcione contraste suficiente entre la información esencial y sus alrededores.
- ✓ Que amplíe la legibilidad de la información esencial.
- ✓ Que diferencie los elementos en formas que puedan ser descritas (por ejemplo, que haga fácil dar instrucciones o direcciones).
- ✓ Que proporcione compatibilidad con varias técnicas o dispositivos usados por personas con limitaciones sensoriales.

5to Principio: Con tolerancia al error

El diseño minimiza los riesgos y las consecuencias adversas de acciones involuntarias o accidentales.

Pautas para el Principio 5

- ✓ Que disponga los elementos para minimizar los riesgos y errores: elementos más usados, más accesibles; y los elementos peligrosos eliminados, aislados o tapados.
- ✓ Que proporcione advertencias sobre peligros y errores.
- ✓ Que proporcione características seguras de interrupción.
- ✓ Que desaliente acciones inconscientes en tareas que requieren vigilancia.

6to Principio: Que exija poco esfuerzo físico

El diseño puede ser usado eficaz y confortablemente y con un mínimo de fatiga.

Pautas para el Principio 6

- ✓ Que permita que el usuario mantenga una posición corporal neutra.
- ✓ Que utilice de manera razonable las fuerzas necesarias para operar.
- ✓ Que minimice las acciones repetitivas.
- ✓ Que minimice el esfuerzo físico continuado.

Tratamiento de Excepciones

El sistema perfecto e invulnerable no existe. Las excepciones son el mecanismo recomendado para propagar las que se produzcan durante la

ejecución de las aplicaciones (divisiones por cero, lectura de archivos no disponibles, etc.) Básicamente, son objetos derivados de la clase System.Exception que se generan cuando en tiempo de ejecución se produce algún error y que contienen información sobre el mismo.

Tradicionalmente, el sistema que en otros lenguajes y plataformas se ha venido usando para informar estos errores consistía simplemente en hacer que los métodos en cuya ejecución pudiesen producirse devolvieran códigos que informasen sobre si se han ejecutado correctamente o, en caso contrario, sobre cuál fue el error producido. Sin embargo, las excepciones proporcionan las siguientes ventajas frente a dicho sistema:

- ✓ Claridad:

  El uso de códigos especiales para informar de error suele dificultar la legibilidad del fuente en tanto que se mezclan las instrucciones propias de la lógica del mismo con las instrucciones propias del tratamiento de los errores que pudiesen producirse durante su ejecución.

  Como se verá, utilizando excepciones es posible escribir el código como si nunca se fuesen a producir errores y dejar en una zona aparte todo el código de tratamiento de errores, lo que contribuye a facilitar la legibilidad de los fuentes.

- ✓ Más información:

  A partir del valor de un código de error puede ser difícil deducir las causas del mismo y conseguirlo muchas veces implica tenerse que consultar la documentación que proporcionada sobre el método que lo provocó, que puede incluso que no especifique claramente su causa.

  Por el contrario, una excepción es un objeto que cuenta con campos que describen las causas del error y a cuyo tipo suele dársele un nombre que resuma claramente su causa. Por ejemplo, para informar errores de división por cero se suele utilizar una excepción predefinida de tipo DivideByZeroException en cuyo campo Message se detallan las causas del error producido

- ✓ Tratamiento asegurado:

  Cuando se utilizan códigos de error nada obliga a tratarlos en cada llamada al método que los pueda producir, e ignorarlos puede provocar más adelante en el código comportamientos inesperados de causas difíciles de descubrir.

Con el código adicional introducido a las aplicaciones por este motivo se afecta en alguna medida el rendimiento del sistema, sin embargo, es un pequeño sacrificio que merece la pena hacer pues ello asegura que nunca se producirán problemas difíciles de detectar derivados de errores ignorados.

En la figura se muestran las excepciones EMailDuplicatedExeption, EMailNotValidExeption, EMailRequiredExeption y UserNotFoundExeption que permiten realizar la validación de los usuarios q se registren en el sistema.

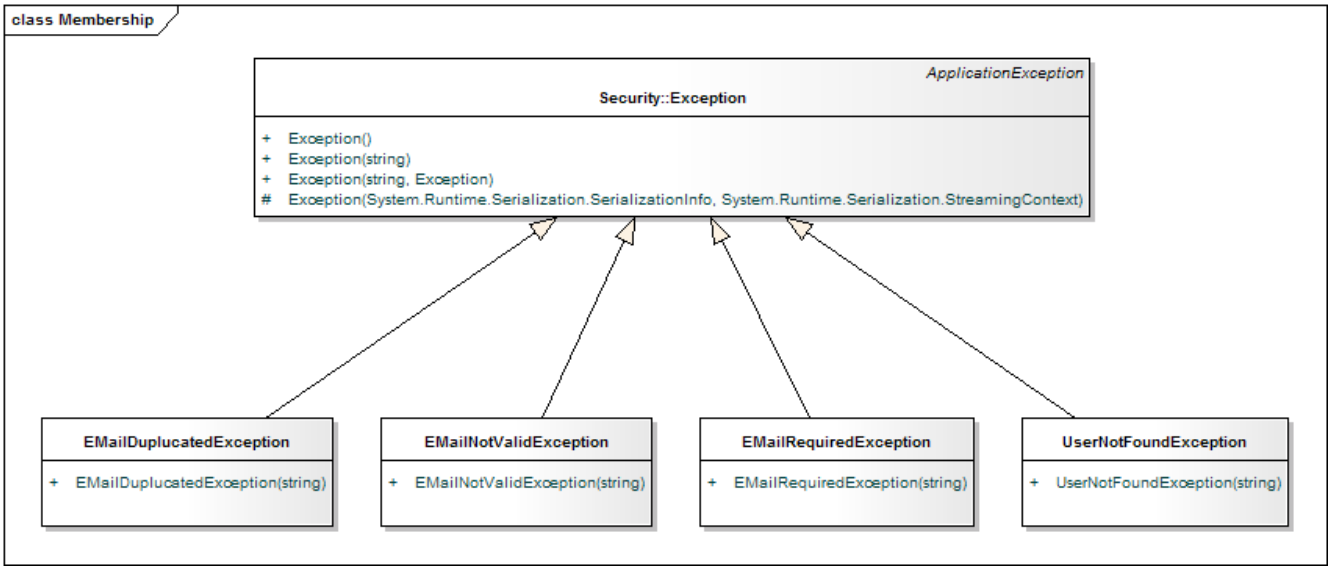


Figura 9. Excepciones utilizadas en el proveedor de membrecía.

En la figura se muestran las excepciones UserInRoleNotFoundException, ApplicationNotFoundException, y RoleNotFoundExeption que son utilizadas en el componente Role.

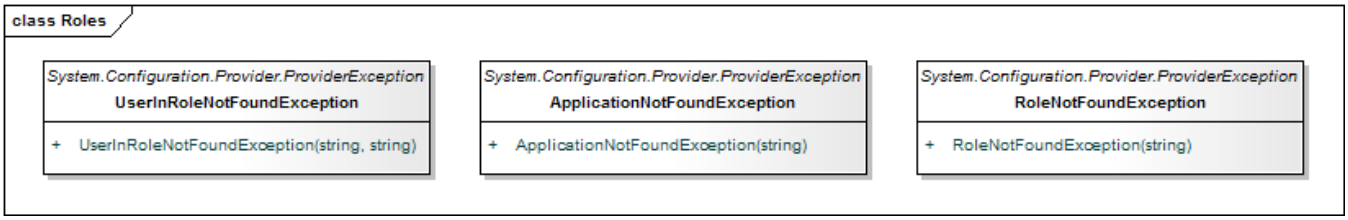


Figura 10. Excepciones utilizadas en el proveedor de roles.

En la figura se muestra la excepción ProfileValueNotSupportedExeption que es utilizada en el componente Profile.

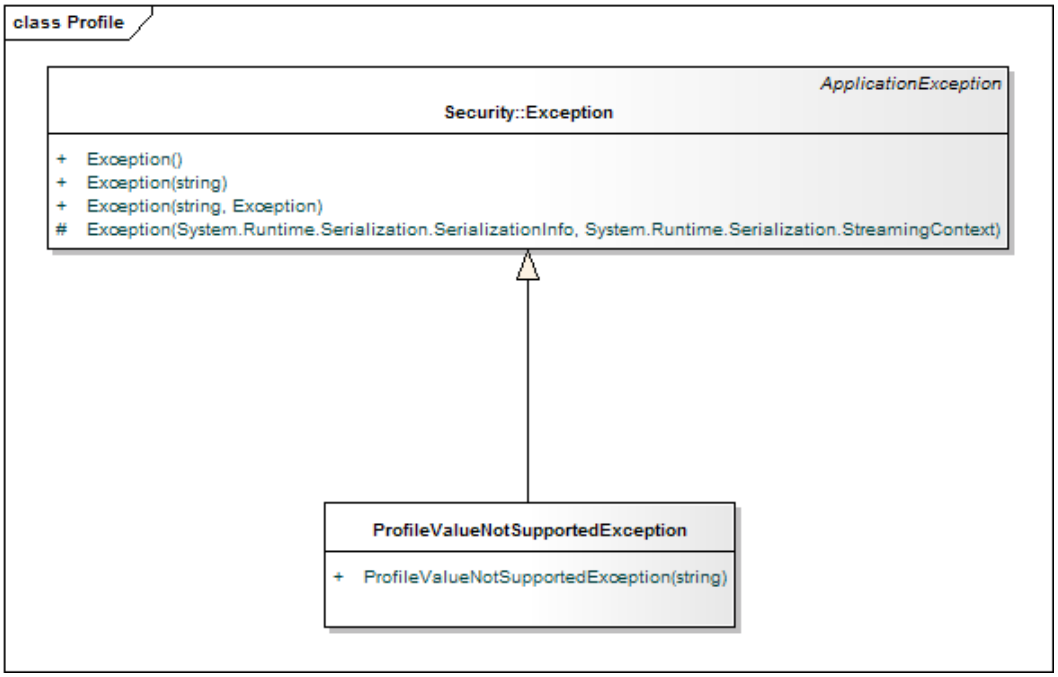


Figura 11. Excepción utilizada en el proveedor de perfiles.

General

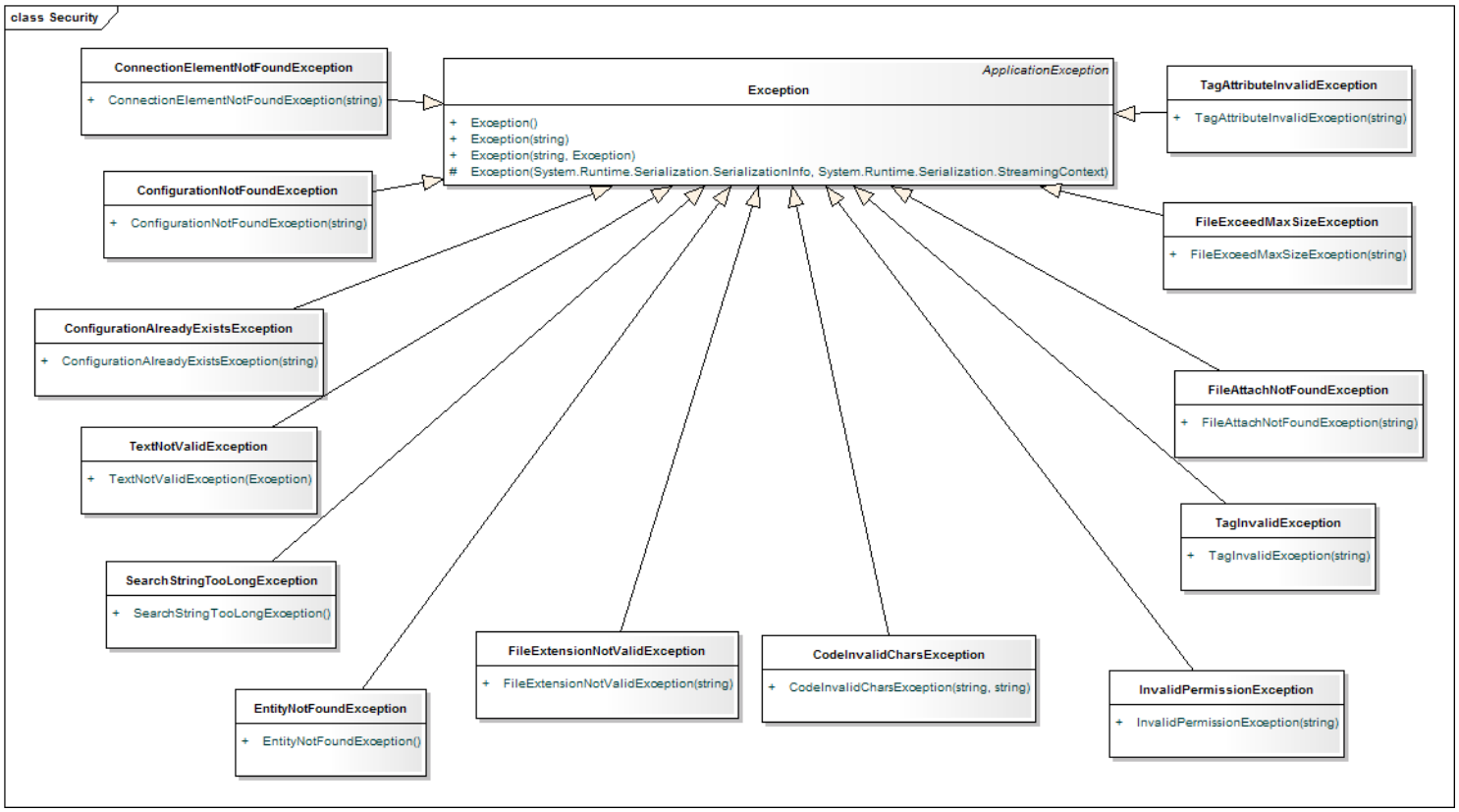


Figura 12. Vista general de excepciones generales.

En la figura se muestra un conjunto de otras excepciones generales que son utilizadas en el subsistema.

Estándar de codificación

El estándar de codificación centra en las guías de estilo para programación en lenguaje C# aunque puede ser utilizado en muchos otros lenguajes y entornos para establecer las convenciones a utilizar.

1. Organización de los ficheros
   1.1. Archivos fuente
        Cada clase debe estar en un solo archivo, y un archivo no puede contener más de una clase. Si bien, en un archivo, junto con su clase se pueden definir los elementos relacionados, por ejemplo: las excepciones que puede lanzar.
   1.2. Árbol de directorios y espacio de nombres
        El espacio de nombres de los objetos se verá reflejado en el árbol de directorios del código fuente. Así, la clase Y10K.AyeAye.Switch, tendrá su código en Y10K/AyeAye/Switch.cs. Si una clase abstracta contiene código útil y además de ella heredan otras clases, como las de especialización, se tendrá el fichero con extensión cs correspondiente a la clase abstracta y, en el mismo nivel, el directorio con el nombre de la clase abstracta que contendrá las clases herederas.
2. Indentación
   2.1. Longitud de línea
        No se mantendrá, siempre que sea posible, la longitud de la línea más allá de los 80 caracteres.
   2.2. Dividir líneas: siempre que sea necesario dividir una línea en dos, se utilizarán las siguientes convenciones:
        Si hay una lista de elementos separados por comas, se dividirá tras una coma.
        Si se trata de una expresión, se dividirá tras uno de los operadores.
        Preferentemente, una expresión se dividirá en niveles superiores, antes que en inferiores.
        La línea dividida se alineará con el nivel dentro del que se ha producido la división.
   2.3. Espaciados de indentación
        Dada la disparidad que hay sobre la cantidad de espacios de indentación, se utilizarán tabuladores, los cuales pueden usarse con muchos editores para representarse con distintas cantidades de

espacios y, sobretodo, se convierten en una pulsación por indentación.

3. Declaraciones
   3.1. Número de declaraciones por línea
   Por definición, nunca se utilizará una misma línea para más de una definición, la cual cosa facilita los comentarios relativos al elemento declarado.
   3.2. Inicialización
   Siempre que sea posible las variables se inicializarán en la misma línea de declaración
   3.3. Declaración de clases e interfaces: Para definir las clases e interfaces, se seguirán las siguientes reglas:
   No se usará ningún espacio entre el nombre de un método y el paréntesis de abertura de la lista de parámetros.
   La llave de abertura que contiene el código se escribe sola en la línea siguiente a la definición del prototipo. Igualmente, la llave de cierre correspondiente se escribe sola en la última línea.
4. Sentencias
   4.1. Sentencias simples
   Cada línea contendrá no más de una sentencia, aunque, según lo explicado en el apartado 3, una sentencia puede estar en más de una línea
   4.2. Sentencias de retorno
   La sentencia return no utiliza paréntesis.
   4.3. Sentencia de selección básica(if/if...else/if...else if...else)
   Las llaves de inicio de un bloque de código se ponen al final de la sentencia if, else o else if. Las llaves de cierre van en líneas independientes. Cuando una sentencia else o else if vaya tras un bloque de código, la sentencia se colocará en la misma línea que la llave de cierre.
   4.4. Sentencias de bucle for o foreach
   De forma similar a las sentencias de selección, la llave de abertura de bloque se colocará tras la sentencia de definición del for o foreach, y la de cierre en una línea independiente.
   4.5. Sentencias de bucle while o do while
   De modo idéntico al for, pero en el caso del do while, el while se colocará en la misma línea que la última llave.
   4.6. Sentencias de selección múltiple (switch)
   Respecto a lo que concierne a las llaves, se colocarán como en el resto de casos. Respecto al código y la línea break, éstas irán con una indentación más que la línea case correspondiente, que irá con una indentación más que la línea de switch.
   4.7. Sentencias de captura y tratamiento de excepciones (try/catch/finally)

El tratamiento de las llaves de bloque será como en el resto de sentencias.

5. Espacios en blanco
   5.1. Líneas en blanco: Se pueden utilizar líneas en blanco para separar grupos de líneas que tengan cierta relación lógica. Dos líneas en blanco seguidas se usan para:
      Separar secciones de código en un fichero.
      Separar definiciones de clases e interfaces dentro de un fichero.
   5.2. Una línea en blanco separa...
      Métodos.
      Definiciones de variables locales dentro del método.
      Bloques de código que no guarden relación directa.
   5.3. Separaciones entre términos
      En una lista de parámetros, se pondrán espacios tras las comas, pero nunca tras o antes de los paréntesis. En las asignaciones, se pondrán espacios antes y después del =. En las expresiones, se utilizarán espacios sólo cuando sean estrictamente necesarios y para separar las distintas expresiones.
   5.4. Separaciones en las declaraciones
      Se procurará mantener una estructura tabulada para las líneas de declaraciones de variables, de manera que leer la información sea fácil. En el ejemplo siguiente se puede observar cómo mantener dicha estructura, pero hay que tener en cuenta que para el espaciado, hay que utilizar espacios, no tabuladores:

```
string name = “Mr. Ed”;
int myValue = 5;
Test aTest = Test.TestYou;
```

6. Nomenclatura: Es importante tener presente que no se utilizará la notación húngara para absolutamente nada, exceptuando la codificación de GUI, donde se puede utilizar, pero detallando los tipos en sufijos detallados (cancelButton, por ejemplo).
   6.1. Nomenclatura para las clases
      El nombre de una clase debe componerse de sustantivos. Se utilizará capitalización Pascal. No se utilizará ningún prefijo de clase.
   6.2. Nomenclatura para interfaces
      Se nombrarán con sustantivos o adjetivos que describan el comportamiento. Capitalización Pascal. Se prefijan con una I, en mayúsculas, y la palabra que sigue también va en mayúsculas.
   6.3. Nomenclatura para enumeraciones
      Se utilizará Pascal tanto para los nombres de los valores como para los nombres de tipo. No se utilizarán ni prefijos ni sufijos. Se utilizarán sustantivos en singular.

6.4. Nomenclatura para constantes y para atributos de sólo lectura

Se utilizará Pascal con sustantivos o abreviaciones de sustantivos.

6.5. Nomenclatura para parámetros y atributos normales

Se utilizarán nombres descriptivos, destacando el significado antes que la tipología del parámetro. En este caso se utiliza capitalización Camel.

6.6. Nomenclatura para variables

Se utilizará Camel. Cuando se utilicen contadores triviales, se utilizarán nombres como i, j, k, m, n,...

6.7. Nomenclatura para métodos

Los métodos se nombrarán con verbos, en Pascal.

6.8. Nomenclatura para propiedades

Se utilizarán sustantivos, en Pascal.

6.9. Nomenclatura para eventos

Los eventos tendrán como sufijo EventHandler y se utilizarán dos parámetros, denominados sender y e. Se utilizará Pascal. Se utilizarán verbos en tiempos pasado y presente para dar una idea del significado del evento.

7. Prácticas de programación

7.1. Visibilidad

Preferentemente se codificarán los atributos de clase y de instancia como privadas, de modo que existirán métodos accesores.

7.2. La magia está prohibida

No se utilizarán números que puedan ser reemplazados por constantes. Esto es únicamente para que, si se presentara el caso de que el número tuviera que se modificado, sólo hay que modificarlo en un lugar.

8. Comentarios

Se utilizará solamente el formato //, nunca se utilizará el /*...*/. Cuando haya que comentar un bloque de líneas, se utilizarán tantos // al principio de línea como convenga, como si se tratase de un # en un shell script.

Aportes prácticos y vías de solución.

Configuración

Los proveedores de función y pertenencia se configuran para utilizar una base de datos en la cual se almacenan los datos de usuarios y permisos de los mismos para la aplicación. En el archivo de configuración de la aplicación cliente se debe especificar una cadena de conexión y varias opciones. Al proveedor de pertenencia se le da el nombre MembershipProvider y al proveedor de funciones se le da el nombre RoleProvider.

Para configurar la aplicación para el uso de estos proveedores se debe crear un fichero de configuración en la carpeta raíz con los siguientes elementos:

```
<?xml version="1.0"?>
<configuration>
      <system.web>
      </system.web>
</configuration >
```

Lo primordial a tener en cuenta es la configuración de la cadena de conexión a la base de datos del sistema o la propia de seguridad (si existiera alguna). En la sección de configuración debe incluirse los valores de la manera siguiente:

```
<connectionStrings>
      <clear/>
      <add name="DefaultDB"
      connectionString="DriverClass=NHibernate.Driver.SqlClientDriver;
      Dialect=NHibernate.Dialect.MsSql2005Dialect;Data
      Source=SERVIDOR;Database=BASE_DATOS;User
      ID=USUARIO;Password=CONTRASENNA;Trusted_Connection=true"/>
</connectionStrings>
```

Usar certificados de GeSeg en una Aplicación Distribuida

En el presente acápite se describe como configurar un servidor de internet, tomando como base el IIS (aunque la configuración es similar para el resto) para poder pedir al usuario que utilice un certificado emitido por la el sistema de gestión de seguridad propuesto.

SSL

SSL es un protocolo que permite la comunicación del navegador con el servidor a través de un canal seguro. Este canal seguro se consigue encriptando las comunicaciones y su función es impedir que terceras personas intercepten lo que se está enviando y nos espíen para conseguir nuestros datos privados.

En general, se distingue si se accede a una página web sobre SSL cuando se utilice el protocolo https en lugar de http. Además, el navegador generalmente recalcará que la página web es segura mediante un icono de un candado, en el que se puede pinchar para ver en detalle la información sobre el certificado de seguridad. Para activar el soporte https para páginas web en el IIS (ver anexo 3).

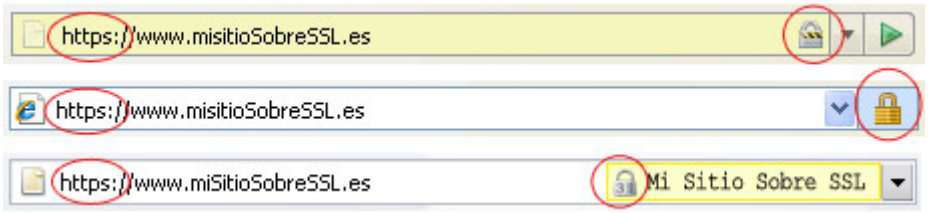


Figura 13. Ejemplo donde el navegador declara la página web segura.

Una vez que se tiene un certificado digital funcionando en el servidor, se puede acceder a los subsistemas publicados tanto por http como por https; sin embargo, constituye un requisito para maximizar la seguridad que siempre se realice por la vía cifrada. Para restringir el acceso a los subsistemas por https (ver anexo 4).

Certificado digital

El circuito de flujo de los certificados para el sistema que se propone es el siguiente:

1. El cliente accede a la url https://.... (para la cual es necesario un certificado de cliente).
2. El servidor envía su certificado al cliente para establecer el canal seguro. El cliente debe confiar en la entidad que ha generado ese certificado y comprobar que es válido. En caso de no confiar aparecerá un mensaje en el explorador indicándonoslo (la mayoría de la gente no lo lee).
3. Una vez que el cliente ha confiado en el servidor, se establece el canal seguro.
4. El servidor tiene configurado que para el recurso que intenta ver el cliente es necesario que presente un certificado de cliente, emitido por una entidad certificadora en la que él confíe y además que está en la lista de los certificados admitidos para el recurso en cuestión.
5. El explorador del cliente recibe estas condiciones del servidor y muestra una ventana con los certificados instalados que cumplan los requisitos del servidor.
6. El usuario elige su certificado y éste es mandado al servidor.
7. El servidor comprueba la lista de revocación de certificados de la entidad que emitió el certificado para ver si sigue siendo válido.
8. En caso que el certificado sea válido, podrá acceder al recurso y en la sesión tendrá guardado el certificado para usarlo.

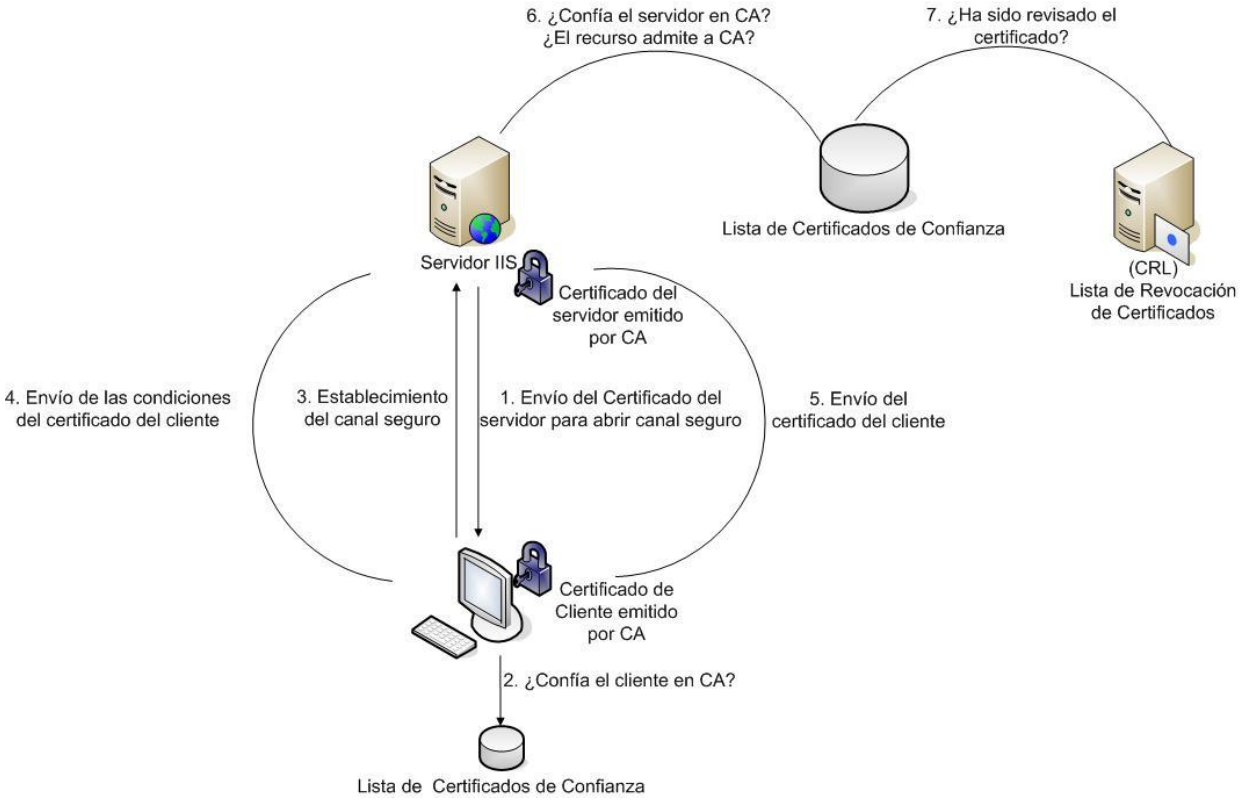


Figura 14. Flujo de los certificados durante una petición de servicio en una aplicación distribuida.

La clave del asunto es la confianza entre los diferentes elementos (cliente y servidor). Por tanto se debe partir de configurar el servidor de aplicación para requerir al cliente el certificado generado por el GeSeg como entidad certificadora en cada una de las comunicaciones o peticiones realizadas.

Aspectos a configurar para el uso del sistema propuesto:

1. IIS para requerir y aceptar certificados de los clientes generados por el GeSeg (ver anexo 5).
2. Confiar en GeSeg como entidad certificadora (ver anexo 6).
3. Incluir al GeSeg como entidad válida para el sistema, en la CTL (Certificate Trusted List) (ver anexo 7).

Firmar llamadas SOAP

Como punto culminante de la garantía de la seguridad se propone firmar las llamadas SOAP utilizando la extensión para servicios web WS 3.0 de Microsoft y los certificados digitales del GeSeg.

La idea es poder realizar cada llamada asegurando que el contenido de la misma no ha sido manipulado en el camino.

Figura 15. Proceso de firma de peticiones con el certificado del cliente.

Siguiendo esta filosofía el GeSeg se convierte en una especie de pasarela de certificados de los clientes o subsistemas que se comunican mediante servicios web. Para realizar esto se firman las llamadas SOAP con el certificado usando el estándar XMLSignature siguiendo políticas y filtros.

Cuando se realiza una llamada a un servicio, ésta es interceptada por una clase que define lo que hay que realizar con dicha llamada antes de que salga. Cuando se recibe una respuesta, es interceptada igualmente, y lo mismo pasa cuando se definen los servicios web.

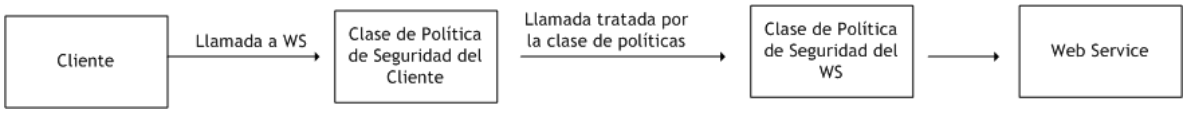


Figura 16. Secuencia de una llamada de un Cliente a un Servicio Web.

Para lograr el comportamiento del sistema descrito:

1. Se crea una clase que controla la entrada y salida de mensajes SOAP desde el cliente. Esta clase tiene que heredar de SecurityPolicyAssertion. La clase posee cuatro métodos, uno para cada situación: salida/entrada para el cliente y salida/entrada para el servicio.
2. Se crea una clase que hereda de SendSecurityFilter que es la que realmente firma la petición. En esta lo que se hace es obtener el token del certificado y añadirle la firma al mensaje SOAP, haciendo override del método SecureMessage.
3. Al realizar las llamadas a los servicios, la política intercepta el mensaje de salida, ejecuta el método "SecureMessage()" y firma la petición.

Conclusiones del capítulo.

En el este capítulo se abordó profundamente la propuesta de solución en la que se basa este trabajo, se explicaron los principales artefactos de la metodología empleada asociados al desarrollo del subsistema. Igualmente, se realizó la construcción de la propuesta de solución desarrollando el 100% de las funcionalidades descritas en el Product Backlog; y se valoran los principios de diseño que se tratan en el subsistema.

El subsistema propuesto ha implementado el total de las funcionalidades propuestas y queda listo para ser objeto de las pruebas pertinentes para su validación.

Capítulo III

Validación de la solución propuesta

Capítulo III. Validación de la propuesta de solución.

Introducción al Capítulo

En el presente capítulo se explican los resultados de los indicadores de seguridad: autenticación, confidencialidad, integridad y el no-repudio. Se hace una descripción de las pruebas de unidad aplicadas al subsistema a través del framework NUnit. Se detallan las métricas usadas para evaluar el diseño de clases y se explican los resultados obtenidos de su aplicación.

Resultados de los indicadores de seguridad

A través del subsistema producto de esta investigación, que hace uso de los certificados digitales, se garantiza el adecuado funcionamiento de los atributos de seguridad: autenticación, confidencialidad, integridad y el no-repudio.

Al contar con una Entidad Certificadora que genera tres tipos de certificados de acuerdo a su destinatario: a usuario, a subsistema y a servidor se aseguran las comunicaciones en todo el sistema distribuido.

Autenticación

Para garantizar la correcta gestión de este atributo se implementaron satisfactoriamente los mecanismos de identificación y de autorización de usuarios. Se asegura que un usuario que no existe en el contexto del sistema, o incluso uno que si existe pero que introduzca incorrectamente su contraseña, no ingrese al mismo.

Confidencialidad

Cuando se crea un rol se le conceden permisos de acceso a aplicaciones que en su totalidad conforman el sistema distribuido. Los usuarios creados para ese rol heredan los permisos de acceso a las aplicaciones. De esta forma nadie que no esté identificado dentro del rol que tiene permisos para acceder a determinada funcionalidad puede hacerlo.

Para enviar un documento el emisor lo encripta con la clave pública del receptor y lo envía por la red. Este documento está totalmente protegido en su viaje pues sólo se puede descifrar con la clave privada correspondiente, conocida solamente por el receptor. Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en texto claro.

A través del algoritmo MD5 se logra encriptar las contraseñas de usuarios, el resultado es guardado en la base de datos para que cada vez que el usuario se autentique su contraseña sea encriptada y comparada con el resultado almacenado anteriormente. De esta forma si algún extraño logra interceptar el mensaje en el intermedio del proceso sólo obtendrá la cadena generada por el MD5, no pudiendo desencriptarlo pues este es un algoritmo de un solo sentido.

Integridad

Para lograr que la información transmitida entre dos entes del sistema distribuido no sea modificada por un tercero, el mensaje se encripta y es firmado haciendo uso del certificado digital. La firma se logra con una función de dispersión unidireccional (hash), que resume o identifica probabilísticamente la información en una cadena. Entonces el mensaje se envía por la red, cuando

este llega se le vuelve a comprobar el hash, si concuerda corrobora que no ha cambiado el mensaje y se ha conservado la integridad de los datos.

No-repudio

Es usado el certificado digital, firmado con la clave privada de la autoridad de certificación, con el objetivo de identificar a una persona, subsistema o servidor cuando hace una petición o llamada a una determinada funcionalidad, de modo que nunca podrá negar que ha realizado una determinada operación.

También se asegura este atributo haciendo uso de la firma digital teniendo en cuenta que sólo su propietario es capaz de generarla y lo identifica de forma única. Cuando un usuario firma un mensaje ya no puede rechazar que ha sido autor del mismo.

Métricas aplicadas a la solución propuesta

Con el propósito de lograr una validación del diseño e implementación utilizado para dar solución al problema inicial, y basado en los argumentos antes expuestos sobre la importancia y uso de las métricas como medidor de la legibilidad, reutilización, limpieza y buenas prácticas de diseño e implementación, se decide hacer uso de las series propuestas por Chidamber y Kemerer (CK), así como las que proponen Lorenz y Kidd.

Árbol de Profundidad de Herencia (APH) serie de métricas de CK

A medida que el APH crece, es posible que clases de más bajos niveles hereden muchos métodos. Esto conlleva dificultades potenciales, cuando se intenta predecir el comportamiento de una clase. Una jerarquía de clases profunda (el APH es largo) también conduce a una complejidad de diseño mayor. Por el lado positivo, los valores APH grandes implican un gran número de métodos que se reutilizarán. (Pressman, 2002)

Resultados obtenidos de la aplicación de la métrica al sistema:

Algunos autores sugieren que umbrales mayores de 6 para el resultado de la aplicación de esta métricas constituye un abuso de la herencia, se puede concluir que el diseño propuesto de la solución no es complejo porque el mayor nivel obtenido de la aplicación de la métrica al sistema fue de 2 por lo tanto no es difícil de dar mantenimiento y existe un bajo acoplamiento entre las clases.

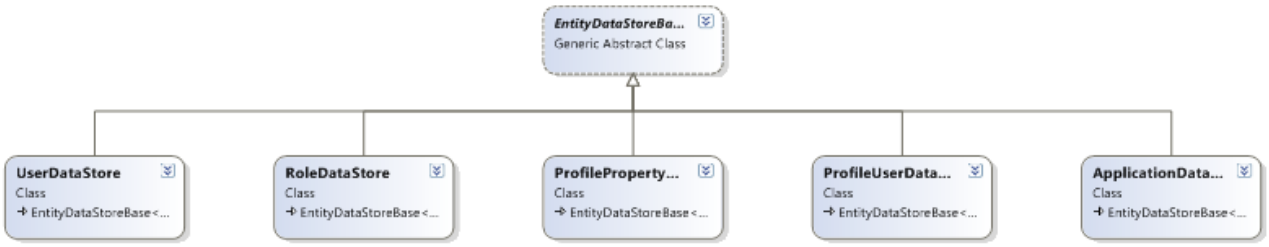


Figura 17. Niveles de herencia de los DataStore.

Número de descendiente (NDD) serie de métricas de CK

A medida que el número de descendientes crece, la reutilización se incrementa, pero además es cierto que cuando el NDD crece, la abstracción representada por la clase predecesora puede diluirse. Esto significa que existe una posibilidad de que algunos descendientes no sean miembros, realmente apropiados de la clase predecesora. A medida que el NDD crece, la cantidad de pruebas (requeridas para ejercitar cada descendiente en su contexto operativo) se incrementará también. (Pressman, 2002)

Resultados obtenidos de la aplicación de la métrica al sistema:

Como resultado de la aplicación de la métrica NDD al sistema se tiene como resultado que el máximo nivel para NDD es de 2, valor que se encuentra dentro de los umbrales definidos para algunos autores donde se especifica que existe una baja reutilización sin afectar el nivel de abstracción de la clase predecesora.

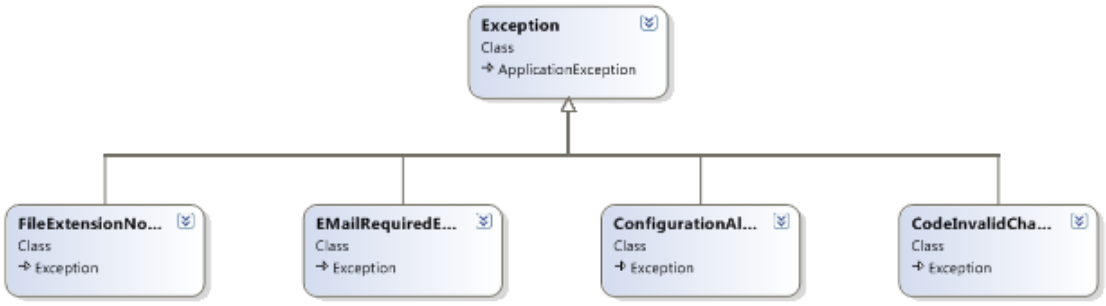


Figura 18. Niveles de herencia de las excepciones.

Carencia de cohesión en los métodos (CCM) serie de métricas de CK

Cada método dentro de una clase, C, accede a uno o varios atributos (también llamados variables de instancia), CCM es el número de métodos que accede a uno o varios de los mismos atributos. Si no existen métodos que accedan a los mismos atributos, entonces CCM = 0.

En general, los valores altos para CCM implican que la clase debe diseñarse mejor descomponiendo en dos o más clases distintas. (Pressman, 2002)

Resultados obtenidos de la aplicación de la métrica al sistema:

Después de aplicar la métrica CCM a las clases más importantes dentro del sistema (EntityDataStoreBase y MembershipProvider), se puede arribar a la conclusión que dichas clases tomadas como muestra para la métrica en cuestión, presentan un nivel de CCM de 1 y 3 respectivamente. Este resultado representa un nivel medio para los umbrales o medidas que proponen algunos autores en el campo de la métrica y el diseño.

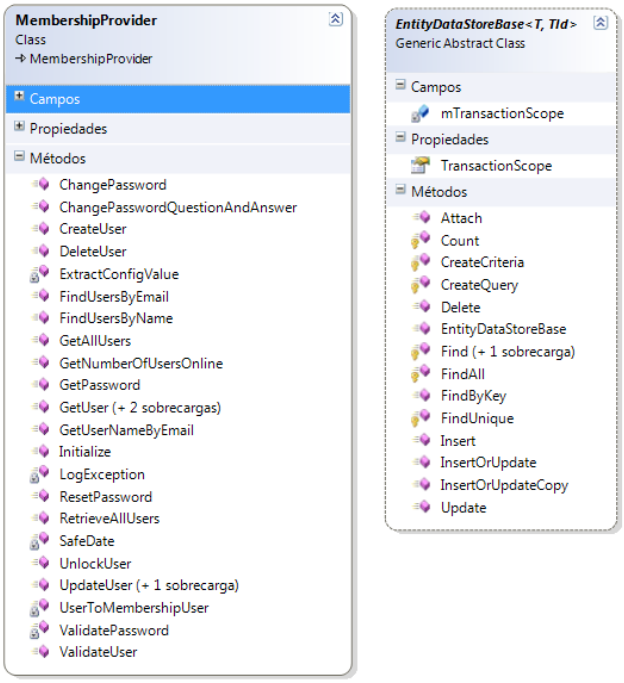


Figura 18. CCM aplicado a EntityDataStoreBase y MembershipProvider

Tamaño de clase (TC) propuesta por Lorenz y Kidd

El tamaño general de una clase puede medirse determinando las siguientes medidas:

- ✓ El total de operaciones (operaciones tanto heredadas como privadas de la instancia), que se encapsulan dentro de la clase.
- ✓ El número de atributos (atributos tanto heredados como privados de la instancia), encapsulados por la clase.

Valores grandes de TC representa gran responsabilidad de la clase. Esto implica la reducción de la reutilización de la clase y complica la implementación

y las pruebas. De forma general, operaciones y atributos deben ser ponderados al determinar el tamaño de la clase. Para valores pequeños de TC para una clase existe mayor posibilidad de que la clase pueda ser reutilizada. (Pressman, 2002)

Parámetros de calidad	Valores Grandes de TC
Reutilización	Reduce la reutilización de la clase
Implementación	Complica la implementación
Complejidad de las pruebas	Hace compleja las pruebas del sistema
Responsabilidad	La clase debe tener bastante responsabilidad

Tabla 6: Parámetros de calidad para valores grandes de TC.

Medidas o umbrales aplicados:

Número de operaciones y/o atributos TC	Umbral
Baja	<= 20
Media	>20 y <=30
Alta	>30

Tabla 7: Umbrales para TC.

Medidas para las principales clases de la solución:

No	Clase	Métodos	Responsabilidad	Complejidad	Reutilización
1	ApplicationProvider	10	Media	Media	Media
2	ApplicationDataStore	3	Baja	Baja	Alta
3	RoleProvider	15	Media	Media	Media
4	RoleDataStore	2	Baja	Baja	Alta
5	MembershipProvider	22	Alta	Alta	Baja
6	UserDataStore	5	Baja	Baja	Alta
7	HttpModuleCheckValidUser	2	Baja	Baja	Alta
8	ProfileProvider	14	Media	Media	Media
9	ProfileUserDataStore	3	Baja	Baja	Alta
10	ProfilePropertyDataStore	3	Baja	Baja	Alta
11	Section	1	Baja	Baja	Alta
12	AssemblyMappingCollection	2	Baja	Baja	Alta
13	Log	4	Baja	Baja	Alta
14	InterceptorBase	13	Media	Media	Media
15	Interceptor	2	Baja	Baja	Alta
16	EntityHelper	1	Baja	Baja	Alta
17	EntityDataStoreBase	12	Media	Media	Media
18	TransactionScope	5	Baja	Baja	Alta
19	ConnectionParameters	8	Baja	Baja	Alta

Tabla 8: Clases a las que se les aplicó la métrica TC

Resultados obtenidos de la aplicación de la métrica al sistema:

Llevando los resultados obtenidos a un gráfico de por ciento obtenemos que del total de clases analizadas existe un 63% de clases entre con menos de 5

procedimientos, un 11% con menos de 10, un 21% con menos de 15 y un 5% con menos de 25 procedimientos lo que implica un resultado positivo según los parámetros de calidad propuestos para esta métrica

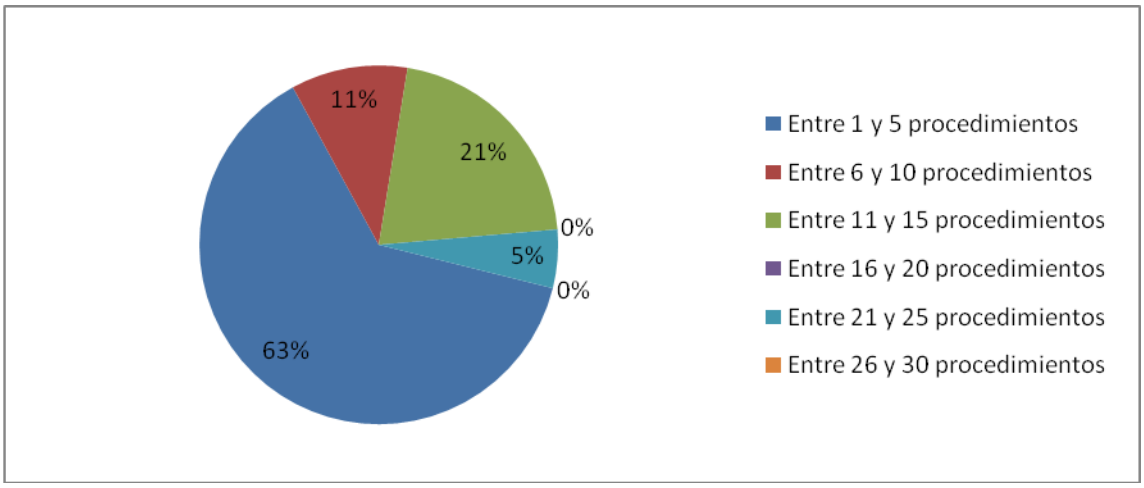


Figura 19. Gráfico de resultado de TC

No. de Operaciones Redefinidas para una Sub-Clase (NOR) propuesta por Lorenz y Kidd

NOR es la medida del número de operaciones que una subclase redefine de su superclase o clase padre, un valor grande para el NOR, generalmente indica un problema en el diseño, o sea si el NOR es grande el diseñador ha violado la abstracción representada por la superclase. Esto provoca una débil jerarquía de clases y un software orientado a objetos, que puede ser difícil de probar y modificar. (Pressman, 2002)

Clase	Calidad del Diseño	Complejidad del Mantenimiento.	Cantidad de Pruebas	Violación de ARS
ApplicationProvider	Buena	Baja	Baja	Baja
ApplicationDataStore	Buena	Baja	Baja	Baja
ApplicationNotFoundException	Buena	Baja	Baja	Baja
RoleProvider	Aceptable	Media	Media	Media
RoleDataStore	Buena	Baja	Baja	Baja
RoleNotFoundException	Buena	Baja	Baja	Baja
UserInRoleNotFoundException	Buena	Baja	Baja	Baja
MembershipProvider	Aceptable	Media	Media	Media
UserDataStore	Buena	Baja	Baja	Baja
HttpModuleCheckValidUser	Buena	Baja	Baja	Baja
UserNotFoundException	Buena	Baja	Baja	Baja
EMailRequiredException	Buena	Baja	Baja	Baja
EMailNotValidException	Buena	Baja	Baja	Baja
EMailDuplucatedException	Buena	Baja	Baja	Baja
ProfileProvider	Aceptable	Media	Media	Media
ProfileUserDataStore	Buena	Baja	Baja	Baja
ProfilePropertyDataStore	Buena	Baja	Baja	Baja
ProfileValueNotSupportedException	Buena	Baja	Baja	Baja

Section	Buena	Baja	Baja	Baja
AssemblyMappingCollection	Aceptable	Media	Media	Media
Log	Buena	Baja	Baja	Baja
InterceptorBase	Buena	Baja	Baja	Baja
Interceptor	Aceptable	Media	Media	Media
EntityHelper	Buena	Baja	Baja	Baja
EntityDataStoreBase	Buena	Baja	Baja	Baja
TransactionScope	Buena	Baja	Baja	Baja
ConnectionParameters	Buena	Baja	Baja	Baja
Exception	Buena	Baja	Baja	Baja
RoleDataStore	Buena	Baja	Baja	Baja
ConfigurationNotFoundException	Buena	Baja	Baja	Baja
ConfigurationAlreadyExistsException	Buena	Baja	Baja	Baja
ConnectionElementNotFoundException	Buena	Baja	Baja	Baja
EntityNotFoundException	Buena	Baja	Baja	Baja
TextNotValidException	Buena	Baja	Baja	Baja
SearchStringTooLongException	Buena	Baja	Baja	Baja
InvalidPermissionException	Buena	Baja	Baja	Baja
FileAttachNotFoundException	Buena	Baja	Baja	Baja
FileExceedMaxSizeException	Buena	Baja	Baja	Baja
FileExtensionNotValidException	Buena	Baja	Baja	Baja
CodeInvalidCharsException	Buena	Baja	Baja	Baja
TagInvalidException	Buena	Baja	Baja	Baja
TagAttributeInvalidException	Buena	Baja	Baja	Baja

Tabla 9: Clases a las que se les aplicó la métrica NOR.

Otra vista o representación en la que se puede mostrar los datos obtenidos después esta métrica, es una vista del comportamiento del porciento de las subclases que redefinen funcionalidades de clases padres, contra las clases que no redefinen funcionalidades.

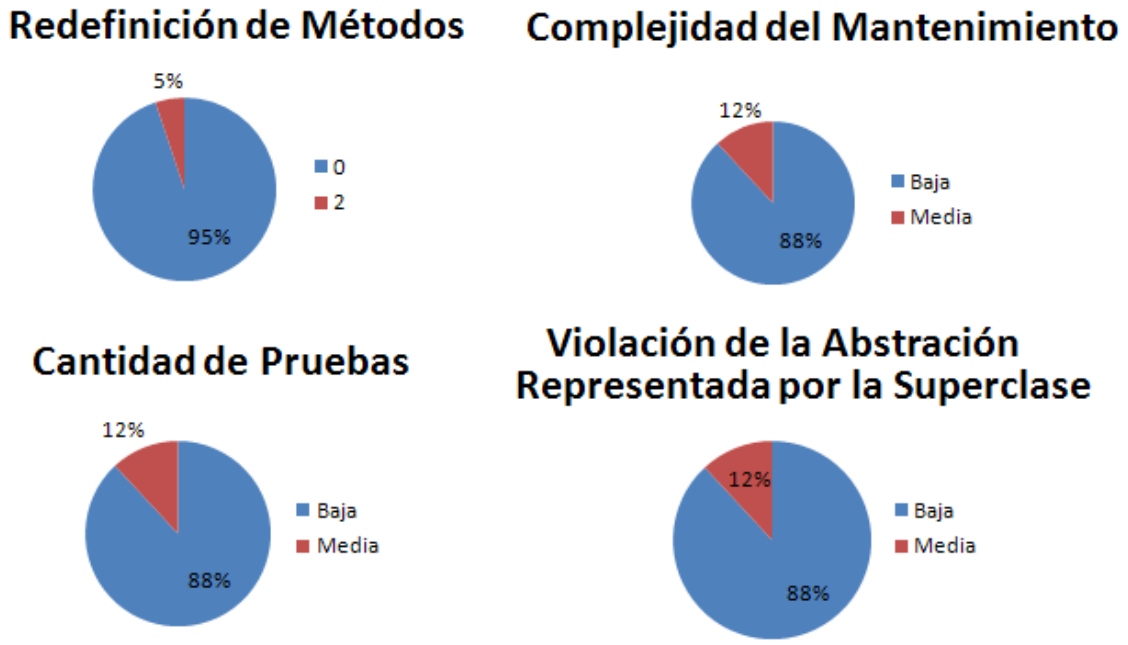


Figura 20. Gráfico del no. de Operaciones Redefinidas para una Sub-Clase (NOR)

Pruebas de unidad.

A pesar de que las pruebas no pueden asegurar la ausencia de defectos, ya que sólo pueden demostrar que existen defectos en el software, son parte fundamental antes de entregar el software final.

Estas son aplicadas para diferentes tipos de objetivos, en diferentes escenarios o niveles de trabajo. Se distinguen los niveles: prueba de desarrollador, independiente, de integración, de sistema, de aceptación y de unidad.

Al subsistema se le aplicaron varias pruebas de unidad las cuales constituyen una forma de probar el correcto funcionamiento de un módulo de código. Sirven además para asegurar que cada uno de los elementos que lo conforman funcione correctamente por separado. Estas pruebas ayudan a crear aplicaciones robustas y reducir la cantidad de errores. Proporcionan cinco ventajas básicas:

1. **Fomentan el cambio**: facilitan que el programador cambie el código para mejorar su estructura, puesto que permiten hacer pruebas sobre los cambios y así asegurarse de que los nuevos cambios no han introducido errores.
2. **Simplifica la integración**: permiten llegar a la fase de integración con un grado alto de seguridad de que el código está funcionando correctamente. De esta manera se facilitan las pruebas de integración.
3. **Documenta el código**: las propias pruebas son documentación del código puesto que ahí se puede ver cómo utilizarlo.
4. **Separación de la interfaz y la implementación**: dado que la única interacción entre los casos de prueba y las unidades bajo prueba son las interfaces de estas últimas, se puede cambiar cualquiera de los dos sin afectar al otro, a veces usando objetos mock (mock object) para simular el comportamiento de objetos complejos.
5. **Los errores están más acotados y son más fáciles de localizar**: dado que se tienen pruebas unitarias que pueden desenmascararlos.

Framework NUnit.

El proceso de pruebas se concentra principalmente en validar la codificación a través del framework de software libre NUnit, que se encarga de realizar pruebas a módulos o segmentos de código para verificar que funcionen apropiadamente, permitiendo escribir las pruebas de una manera sencilla y simple.

NUnit es una herramienta que se encarga de analizar ensamblados generados por SharpDevelop, interpretar las pruebas inmersas en ellos y ejecutarlas. Utiliza atributos personalizados para interpretar las pruebas y provee además

métodos para implementarlas. En general, NUnit compara valores esperados y valores generados, si estos son diferentes la prueba no pasa, caso contrario la prueba es exitosa. NUnit carga en su entorno un ensamblado y cada vez que lo ejecuta, o mejor, ejecuta las pruebas que contiene, lo recarga. Esto es útil porque se pueden tener ciclos de codificación y ejecución de pruebas simultáneamente, así cada vez que se compile no tiene que volver a cargar el ensamblado al entorno de NUnit si no que este siempre obtiene la última versión del mismo. NUnit ofrece una interface simple que informa si una prueba o un conjunto de pruebas fallaron, pasaron o fueron ignorados.

Existen algunos atributos NUnit expuestos por el framework que ayudan a marcar diferentes áreas de las clases para realizar pruebas. Estos son los atributos básicos.

- *[TestFixture]:* Con este atributo se informa que la clase es una clase de prueba y expone métodos para pruebas.
- *[SetUp]:* Se utiliza para marcar un método que se usará para instanciar objetos comunes que luego serán usados por los demás métodos. Solo puede existir un método con el atributo SetUp.
- *[Test]:* Especifica un método dentro de una clase como un método de prueba. Dentro de una clase marcada como TestFixture pueden haber varios métodos con el atributo Test.
- *[TearDown]:* Luego que las pruebas han sido ejecutadas el método con el atributo TearDown es el encargado de limpiar el ambiente, por ejemplo aniquilar objetos.

Resultados de las pruebas aplicadas a los proveedores de seguridad.

A continuación se muestran algunas de las pruebas aplicadas a los proveedores implementados:

```
[NUnit.Framework.Test]
public void ApplicationProviderTest()
{
    // Creating a Test Application
    BasKet.Security.Roles.ApplicationProvider ap = new BasKet.Security.Roles.ApplicationProvider();
    ap.CreateApplication("TestApplicationName", "TestApplicationDescription", null);

    // Retrieving all Applications to delete the Test Application
    BasKet.Security.Roles.ApplicationProvider ap = new BasKet.Security.Roles.ApplicationProvider();
    IList<BasKet.Security.Model.Application> al = ap.RetrieveApplications();

    // Finding and deleting the Test Application
    foreach (BasKet.Security.Model.Application app in al)
        if (app.Name.ToLower().Equals("testapplicationname"))
            ap.DeleteApplication(app.Id);
}
```

Esta prueba verifica el comportamiento del proveedor de aplicaciones sobre el cual se realizan las operaciones básicas Create, Retrieve, Update y Delete, (CRUD).

El método siguiente demuestra un CRUD sobre el proveedor de roles. Nótese la importancia de la creación previa de una aplicación para poder probar la asignación de roles a aplicaciones que forman parte del sistema distribuido en cuestión.

```
[NUnit.Framework.Test]
public void RoleProviderTest()
{
    // Creating a Test Role
    BasKet.Security.Roles.RoleProvider rp = new BasKet.Security.Roles.RoleProvider();
    System.Web.Configuration.RoleManagerSection configSection =
        (System.Web.Configuration.RoleManagerSection)System.Web.Configuration.
        WebConfigurationManager.OpenWebConfiguration("/Web").GetSection("system.web/roleManager");
    System.Collections.Specialized.NameValueCollection nvc = configSection.Providers[0].Parameters;
    rp.Initialize("", nvc);
    rp.CreateRole("TestRoleName", "TestRoleDescription", "TestRoleAbbreviation");

    // Authorizing the TestRole to ApplicationForTestRole
    List<string> apps = new List<string>();
    apps.AddRange("ApplicationForTestRole".Split(','));
    List<string> roles = new List<string>();
    roles.Add("TestRoleName");
    ap.AddRolesToApplications(roles.ToArray(), apps.ToArray());

    // Finding and deleting the TestRole
    List<BasKet.Security.Model.Role> rls = rp.RetrieveAllRoles();
    foreach (BasKet.Security.Model.Role role in rls)
        if (role.Name.ToLower().Equals("TestRoleName"))
            System.Web.Security.Roles.DeleteRole(role.Id, false);
}
```

Por último se muestra la prueba implementada para el proveedor de membrecía de usuarios. En esta prueba se incluye el escenario de cambiar la pregunta y contraseña de seguridad como muestra de funcionalidades apartes del CRUD.

```
[NUnit.Framework.Test]
public void MembershipProviderTest()
{
    System.Web.Security.MembershipCreateStatus status;
    System.Web.Security.MembershipUser user = System.Web.Security.Membership.
        CreateUser("test", "testpwd", "test@test.test", "question", "answer", true, out status);

    if (System.Web.Security.Membership.ValidateUser("test", "testpwd") == false)
        throw new ApplicationException("Password or user not valid");

    //Name must be case insensitive, password case sensitive
    if (System.Web.Security.Membership.ValidateUser("TesT", "testpwd") == false)
        throw new ApplicationException("Password or user not valid");

    user.ChangePasswordQuestionAndAnswer("testpwd", "question2", "answer2");
    System.Web.Security.Membership.UpdateUser(user);

    bool found = false;
    MembershipUserCollection list = System.Web.Security.Membership.FindUsersByName("test");
    foreach (MembershipUser listItem in list)
    {
        if (listItem.UserName == "test")
            found = true;
    }

    if (found == false)
        throw new ApplicationException("User created not found");
}
```

Finalmente se puede observar en la figura que se muestra a continuación, la interfaz de NUnit que muestra la correcta ejecución de las pruebas aplicadas al subsistema y los resultados satisfactorios de las mismas.

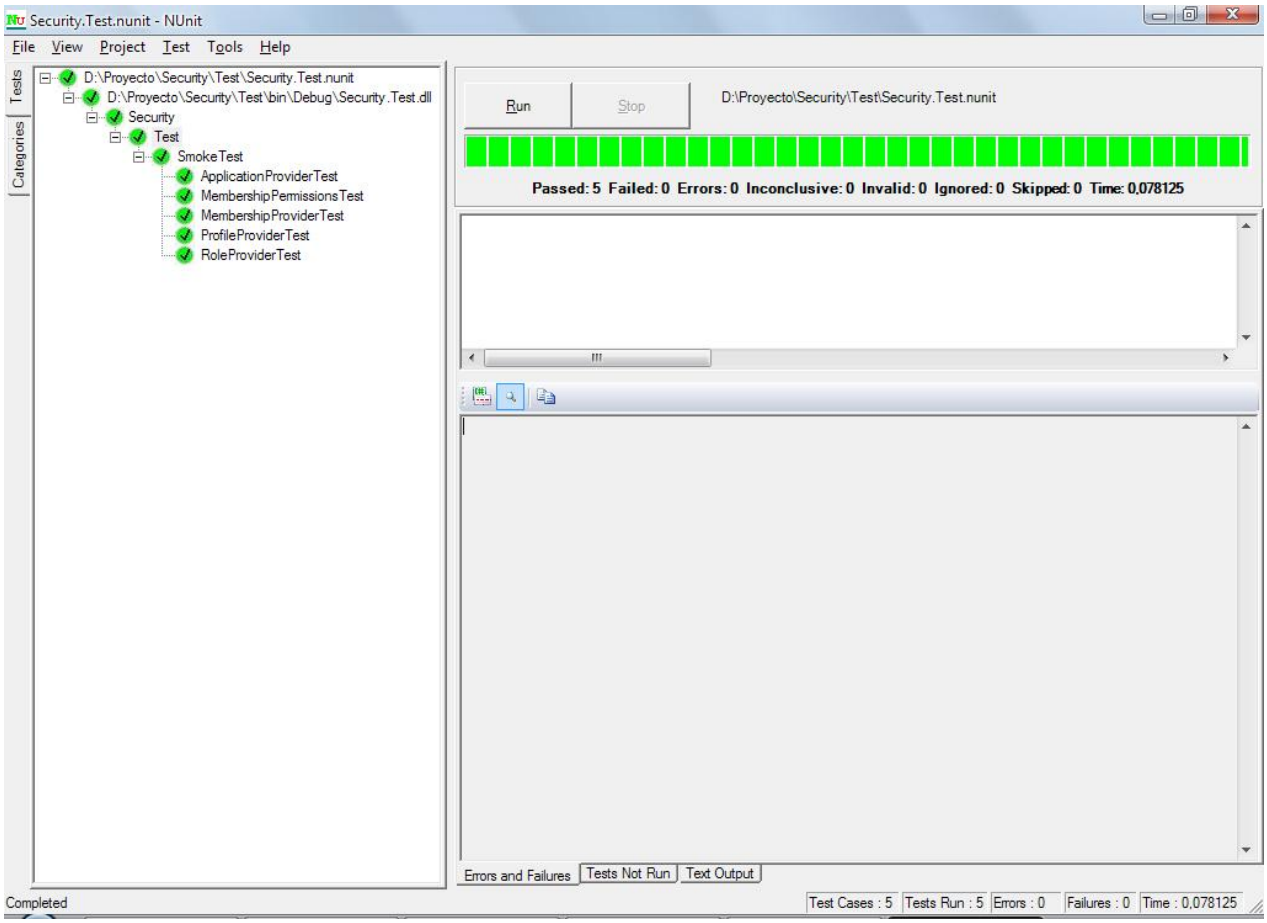


Figura 21. Ejecución de las pruebas de unidad con NUnit

Conclusiones del capítulo.

En el este capítulo se trataron los resultados de los indicadores de seguridad y se documentaron las pruebas realizadas al código del subsistema, específicamente las de unidad, basándose en el framework NUnit. Además se aplicaron métricas al diseño de las clases de la serie Chidamber y Kemerer (CK) y de la serie Lorenz y Kidd.

Se demostró que la gestión centralizada de la seguridad de los sistemas distribuidos haciendo uso de los certificados digitales garantiza la autenticación, confidencialidad, integridad y el no-repudio.

Una vez aplicadas las pruebas que demuestran el correcto funcionamiento tanto de sus elementos por separado como del subsistema como un todo descritas en el capítulo y los resultados positivos de estas se arriba a la conclusión de que el subsistema obtenido está apto para ser desplegado en un entorno real.

Conclusiones.

Como resultado de la investigación se destacan las siguientes conclusiones:

1. La gestión centralizada de la seguridad de los sistemas distribuidos haciendo uso de los certificados digitales garantiza la autenticación, confidencialidad, integridad y el no-repudio.
2. Se desarrolló una herramienta que gestiona de forma centralizada la seguridad de los sistemas distribuidos.
3. La metodología utilizada para el diseño y desarrollo de la aplicación resultó eficiente y queda disponible para su utilización en sistemas similares.

Recomendaciones.

Se recomienda basado en el resultado de la investigación:

1. La implantación y uso del sistema en la UCI para valorar su despliegue a mayor escala.
2. Ampliar las funcionalidades del subsistema a configurar nomencladores y gestionar servidores.
3. Realizar un manual de usuario y/o una ayuda con el objetivo de facilitar el trabajo con el subsistema.
4. El uso del subsistema como material de apoyo para impartir asignaturas como “Seguridad Informática” y cursos optativos como “Redes”.
5. Desarrollar nuevas versiones incursionando en el uso de otras metodologías como RUP o XP para hacer una comparación de los resultados obtenidos.

Bibliografía.

2006. Adictos al trabajo. [En línea] 24 de 11 de 2006. http://www.adictosaltrabajo.com/tutoriales/pdfs/SharpDevelop.pdf.

Aguirre, Jorge Ramió. 2006. *Libro electrónico de Seguridad Informática y Criptografía.* Madrid : s.n., 2006. ISBN: 84-86451-69-8.

Alvarez, Miguel Angel. 2004. desarrolloweb.com. [En línea] 2004. http://www.desarrolloweb.com/articulos/1557.php.

2009. c#Code. [En línea] 2009. http://www.icsharpcode.net/OpenSource/SD/Features.aspx.

2009. ConnectionStrings. [En línea] 2009. http://www.connectionstrings.com/.

García, Jimeno y Teres, María. 2008. *Hacker.* Madrid : s.n., 2008. ISBN: 9788441523234.

2005. GeoCities. [En línea] Yahoo, Marzo de 2005. http://www.geocities.com/mailsoftware42/db/.

Gutierrez, Diego, Juan y López, Angel. 2008. *Seguridad de Redes Locales (guía práctica).* Madrid : s.n., 2008. ISBN: 9788441523739 .

2009. Hibernate. [En línea] Red Hat Middleware, 2009. https://www.hibernate.org/.

Kniberg, Henrik. 2007. *Scrum y XP desde las trincheras. Como hacemos Scrum.* 2007. ISBN: 978-1-4303-2264-1.

2006. La Revista Informatica. [En línea] 2006. http://www.larevistainformatica.com.

Leyet, Osmar y Rodríguez, Iosmel. 2008. *Desarrollo de una herramienta generadora de ficheros de mapeo para la persistencia de objetos relacionales basada en Nhibernate.* La Habana : s.n., 2008.

Lockhart, Andrew. 2007. *Seguridad de Redes: Los mejores trucos.* Madrid : s.n., 2007. ISBN: 9788441521858.

López, Manuel José Lucena. 2005. *Criptografía y Seguridad en Ordenadores.* Madrid : s.n., 2005.

Luján, Rafael Lozano. 2006. *Sistemas Gestores de Bases de Datos.* 2006.

Mauri, Antonio y Pérez, Abel. 2008. *Estrategia de Migración hacia Sitemas Gestores de Bases de Datos Libres.* La Habana : s.n., 2008.

Microsoft. 2009. MSDN .Net Framework Developer Center. [En línea] 2009. http://msdn.microsoft.com/en-us/library/system.security.cryptography.aspx.

—. 2008. SQL Server 2008. [En línea] 2008. http://www.microsoft.com/latam/sqlserver/productividad.aspx.

2008. MySQL. [En línea] Sun Microsystems, 2008. http://www.mysql.com/why-mysql/.

NHibernate Forge. [En línea] http://nhforge.org/Default.aspx.

2007. NUnit. [En línea] 2007. http://www.nunit.org/index.php.

Palacio, Juan. 2008. *Flexibilidad con Scrum.* Madrid : s.n., 2008.

2009. PHP Builder. [En línea] WebMediaBrands, 2009. http://www.phpbuilder.com/columns/tim20000705.php3.

2009. PostgreSQL. [En línea] PostgreSQL Global Development Group, 2009. http://www.postgresql.org/about/.

Proenza, Yuniel. 2006. *Arquitectura de Seguridad para aplicaciones Web Empresariales .* Ciudad de la Habana : s.n., 2006.

Ruiz, Santiago Gómez. 2009. Protalia. [En línea] 2009. http://www.protalia.com/articulos/52_53_54_55_56_57.pdf.

2008. Scrum Alliance. *Scrum Alliance Inc.* [En línea] 2008. http://www.scrumalliance.org/articles/122--tips-for-creating-a-good-sprint-backlog.

2008. Scrum Alliance. [En línea] Scrum Alliance Inc, 2008. http://www.scrumalliance.org/articles/99-implementing-scrum--questions-to-answer-before-you-begin.

2008. Scrum Alliance. [En línea] Scrum Alliance Inc, 2008. http://www.scrumalliance.org/articles/99-implementing-scrum--questions-to-answer-before-you-begin.

2009. SharpDevelop. [En línea] SharpDevelop Community, 2009. http://community.sharpdevelop.net/blogs/mattward/pages/VisualStudioExpressComparison.aspx.

2008. SQL Server 2008. [En línea] Microsoft, 2008. http://www.microsoft.com/latam/sqlserver/seguridad.aspx.

Takeuchi, Hirotaka. 1999. *Scrum.* 1999.

1999-2009. Todo expertos. [En línea] 1999-2009. http://www.todoexpertos.com/categorias/ciencias-e-ingenieria/ingenieria-informatica/respuestas/291165/comparativa-sistemas-gestores-bases-de-datos.

Valdés, Yandy. 2005. *Subsistema Gestión de Seguridad.* La Habana : s.n., 2005.

Zambrano, Donel Vázquez. 2008. *Sistema de Ventas Mayoristas.* La Habana : s.n., 2008.

Anexos.

Anexo 1: DECRETO-LEY Nº 199 SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN OFICIAL

GACETA OFICIAL REPUBLICA DE CUBA

CONSEJO DE ESTADO

FIDEL CASTRO RUZ. Presidente del Consejo de Estado de la República de Cuba.

HAGO SABER: Que el Consejo de Estado ha acordado lo siguiente:

POR CUANTO: Los servicios especiales extranjeros dedican cuantiosos recursos, medios sofisticados y fuerzas cada vez más preparadas en la obtención de informaciones de interés, lo que hace necesario fortalecer las medidas establecidas para la seguridad y protección de la Informaci6n oficial que pudiera ser útil para los planes subversivos y agresivos contra la República de Cuba.

POR CUANTO: Los cambios que se han producido a partir de la reorganización de los organismos de la Administración Central del Estado y la creación de las nuevas formas de relaciones económicas, aconsejan la introducción y puntualización de medidas encaminadas a lograr una mejor eficiencia en la protección de la información oficial.

POR CUANTO: El desarrollo de las comunicaciones y tecnologías de información en el país exige, para transmitir y almacenar información oficial clasificada, la aplicación de medidas de Protección Criptográfica y de Seguridad Informática, cuyo diseño y aplicación requieren de una alta especialización y centralización estatal.

POR CUANTO: La Ley número 1246 del Secreto Estatal del 14 de mayo de 1973 sobre la Protección del Secreto Estatal y su Reglamento, puesto en vigor por el Decreto número 3753 del 17 de enero de 1974; el Decreto número 3787 del 23 de septiembre de 1974 que puso en vigor los Reglamentos Gubernamentales para el Servicio Cifrado Nacional y para el Servicio Cifrado Exterior, así como otras disposiciones complementarias en esta materia, requieren ser adecuadas a las nuevas condiciones y cambios que tienen lugar en el país, en función de lograr una mayor seguridad y protección de la información oficial.

POR TANTO: El Consejo de Estado, en uso de la atribución que le confiere el Artículo 90, inciso c) de la Constitución de la República, resuelve dictar el siguiente:

DECRETO-LEY No.199 SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN OFICIAL

CAPITULO 1

OBJETIVOS Y DEFINICIÓN.

ARTICULO 1.-El presente Decreto-Ley tiene como objetivo, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, cuyas normas deben cumplimentar tanto los órganos, organismos, entidades o cualquier otra persona natural o jurídica residente en el territorio nacional, como las representaciones cubanas en el exterior.

ARTICULO 2.-El Sistema para la Seguridad y Protección de la Información Oficial comprende la clasificación y desclasificación de las informaciones, las medidas de seguridad con los documentos clasificados, la Seguridad Informática, la Protección Electromagnética, la Protección Criptográfica, el Servicio Cifrado y el conjunto de regulaciones, medidas, medios y fuerzas que eviten el conocimiento o divulgación no autorizados de esta información.

ARTICULO 3.-En el presente Decreto Ley se emplean, con la acepción que en cada caso se expresa, los términos y definiciones siguientes:

a) Acceso: Facultad o autorización que se otorga a una persona y que le permite conocer información oficial clasificada para el ejercicio de sus funciones.

b) Auditoria a la Seguridad Informática: Es el proceso de verificación y control mediante la investigación, análisis, comprobación y dictamen del conjunto de medidas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve por medio de las tecnologías de información.

c) Compartimentación: Acción de dar a conocer lo que compete a cada persona, de acuerdo al acceso a la información oficial que le sea otorgado.

d) Documento: Cualquier objeto físico capaz de proporcionar información o datos que puedan ser transferidos del conocimiento de una persona a otra.

e) Entidad: Toda organización administrativa, comercial, económica, cooperativa, privada o mixta, residente en el territorio nacional, así como las organizaciones sociales y de masas del país.

f) OCIC: Oficina para el Control de la Informaci6n Oficial Clasificada

g) Plan de Contingencia: Documento básico contenido dentro del Plan de Seguridad Informática, mediante el que se establecen las medidas para establecer y dar continuidad a los procesos informáticos ante una eventualidad o desastre.

h) Plan de Evacuación, Conservación y Destrucción de la Información Oficial: Documento básico que establece las medidas organizativas y funcionales para la evacuación, conservación o destrucción de la información oficial, que por sus características es necesario preservar o destruir al declararse una situación excepcional o producirse una catástrofe.

i) Plan de Seguridad Informática: Documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en un órgano, organismo o entidad, a partir de las políticas y conjunto de medidas aprobadas sobre la base de los resultados obtenidos en el análisis de riesgo previamente realizado.

j) Plan de Seguridad y Protección de la Información Oficial Clasificada: El documento básico que establece el conjunto de medidas organizativas. Administrativas, preventivas y de control dirigidas a garantizar la seguridad y protección de la información oficial clasificada e impedir su conocimiento u obtención por personas no autorizadas o por los servicios especiales extranjeros.

k) Protección Criptográfica: Proceso de transformación de información abierta en información cifrada mediante funciones, algoritmos matemáticos o sucesiones lógicas de instrucciones, con el objetivo de su protección ante personas sin acceso a ella.

l) Seguridad Informática: Conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información.

m) Señalización: Acción de consignar de forma visible y expresa la categoría de clasificación o término que le corresponde a la información.

n) Servicio Cifrado: Actividad que realiza mediante un conjunto de regulaciones, medidas organizativas y técnicas y medios para la protección criptográfica de la información oficial clasificada que se tramita o almacena a través de las tecnólogas de la información.

o) Tecnólogas de la Información: Medios técnicos de computación o comunicación y sus soportes de información, que pueden ser empleados para el procesamiento, intercambio, reproducción o conservación de la información oficial.

CAPITULO II DE LA AUTORIDAD COMPETENTE

ARTICULO 4.- EL Ministerio del Interior es el organismo encargado de regular, dirigir y controlar la aplicación de la política del Estado, y del Gobierno en cuanto a la Seguridad y Proteccl6n de la Información Oficial y para el cumplimiento de estas funciones tiene las atribuciones siguientes:

a) dictar normas y procedimientos en materia de Seguridad y Protección de la Información Oficial;

b) establecer los requisitos para elaborar los Planes de Seguridad Informática, de Contingencia, de Seguridad y Protección de la Información Oficial Clasificada y de Evacuación, Conservación y Destrucción de la Información Oficial para Situaciones Excepcionales y otras que puedan poner en riesgo la seguridad y protección de la información oficial;

c) certificar aquellas entidades que brinden servicios se Seguridad Informática y Criptográfica a terceros, así como la utilización, distribución o comercialización de herramientas de Seguridad Informática;

d) regu1ar y aprobar la producción de productos criptográficos; la aplicación de los Sistemas de Protección Criptográfica y la investigación y desarrollo científico en esta disciplina;

e) realizar inspecciones, auditorias y controles de la Seguridad y Protección a la Información Oficial, incluyendo la Criptografía y la Seguridad Informática;

f) promover la formación de personal calificado y el desarrollo de la ciencia y la tecnología en materia de seguridad y Protección a la Información Oficial, la Seguridad Informática y la Criptografía;

g) realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Decreto-Ley, tal y como se establece en el articulo 66 de la Constitución de la Repúblicl1 de Cuba.

CAPITULO III INFORMACIÓN OFICIAL.

ARTÍCULO 5.- La Información Oficial es aquella que posee un órgano, organismo, entidad u otra persona natural o jurídica residente en el territorio nacional o representaciones cubanas en el exterior, capaz de proporcionar, directa o indirecta datos o conocimientos que reflejan alguna actividad del Estado o reconocida por éste y que pueda darse a conocer de cualquier forma perceptible por la vista, el oído o el tacto.

ARTÍCULO 5.1.- La Información Oficial constituye un bien del órgano, organismo o entidad que lo posea.

ARTÍCULO 6.- La Información Oficial, a los fines de establecer las medidas para su seguridad y protección, se divide en tres grupos:

a) CLASIFICADA.

b) LIMITADA

c) ORDINARIA.

SECCIÓN PRIMARIA Información Oficial Clasificada.

ARTICULO 7.- La información Oficial Clasificada es la que posee un órgano, organismo, entidad u otra persona natural o jurídica y que requiere de medidas de Protección definidas por Ley, por contener datos o informaciones cuyo conocimiento o divulgación no autorizada puede ocasionar daños o entrañar riesgos para el Estado o para su desarrollo político, militar, económico, científico, técnico, cultural, social o de cualquier otro tipo.

ARTÍCULO 8.-La Información Oficial Clasificada tiene las categorías de: SECRETO DE ESTADO, SECRETO Y CONFIDENCIAL.

ARTICULO 9.-La categoría SECRETO DE ESTADO es aquella cuyo conocimiento o divulgación no autorizada puede poner en peligro la seguridad, integridad, estabilidad o el funcionamiento del Estado.

ARTICULO 10.-La categoría de SECRETO es aquélla cuyo conocimiento o divulgación no autorizada puede causar perjuicios en las esferas política, militar, económica, científica, técnica, cultural, social o cualquier otra de importancia para el funcionamiento del Estado.

ARTICULO 11.-La categoría .CONFIDENCIA es aquélla cuyo conocimiento o divulgación no autorizada puede ocasionar daños a la producción, de bienes, los servicios y en general a la gestión de cualquiera de ellos.

ARTÍCULO 12.-El tratamiento a la información oficial clasificada mediante tecnologías de la información o de comunicación en las representaciones y delegaciones cubanas fuera del territorio nacional, se rige por medidas especiales de Protección Criptográfica y Seguridad Informática establecidas y controladas por el Ministerio del Interior.

ARTICULO 13.-Los cargos que requieren acceso a información oficial clasificada son determinados por el nivel de dirección administrativa facultada para ello.

ARTICULO 14.-El documento que información oficial clasificada deberá tener la señalización de la categoría que le corresponda, según lo establecido en el artículo 8.

ARTICULO 15.-Toda persona con acceso a información oficial clasificada mantendrá la debida compartimentación y se responsabilizara con protegerla y no divulgarla sin la autorización correspondiente.

ARTÍCULO 16.-La información oficial clasificada no puede ser modificada, alterada o destruida sin la debida autorización.

SECCIÓN SEGUNDA Información Oficial Clasificada

ARTICULO 17.- La Información Oficial Limitada es aquella que sin poder ser conceptuada como clasificada, por su importancia o carácter sensible para el objeto social del órgano, organismo, o entidad u otra persona natura1 o jurídica que la posee, no resulta conveniente su difusión pública y debe 1imitarse su acceso a personas determinadas que no podrán destruirla, divulgarla ni modificarla sin la correspondiente autorización.

ARTICULO 18.-La Información Oficial Limitada se determina por el Jefe del órgano, organismo, entidad o persona natural o jurídica que la genera; se señala con el término LIMITADA, y se establecen medidas para su seguridad y protección.

ARTICULO 19.- Quien tenga acceso a información oficial limitada mantendrá la debida compartimentación y no podrá divulgarla sin la autorización correspondiente.

SECCIÓN TERCERA Información Oficial Ordinaria.

ARTICULO 20.- La información Oficial Ordinaria es aquella que posee un órgano, organismo o entidad, cuyo conocimiento o divulgación no autorizada no produce daños o riesgos para su funcionamiento.

CAPITULO IV CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN OFICIAL

SECCIÓN PRIMERA De la clasificación y desclasificación.

ARTÍCULO 21.-La Clasificación es el proceso mediante el cual se determina la categoría correspondiente a una información oficial, de acuerdo con el grado de afectación que su conocimiento o divulgación no autorizada pueda producir.

ARTÍCULO 22.-La desclasificación es el proceso mediante el cual se le suprime la categoría de clasificación a una información oficial clasificada, al desaparecer los elementos que le dieron ese carácter.

SECCIÓN SEGUNDA Comisión estatal para la Clasificación y Desclasificación de la Información Oficial.

ARTICULO 23.- Se crea la Comisión estatal para la Clasificación y Desclasificación de la Información Oficial, en lo adelante "la Comisión", la cual elabora y somete a la aprobación del Comité Ejecutivo del Consejo de Ministros su reglamento y la Lista general para la Clasificación y Desclasificación de la Información oficial, así como ejecuta y controla los procesos para la clasificación y desclasificación de la información oficial.

ARTICULO 23.1.- Esta Comisión esta presidida por el Ministerio del Interior e integrada además por un representante, de cada órgano u organismo que ocupen cargos de dirección de Viceministros u otros equivalentes. Los representantes de la Comisión tienen carácter permanente y son designados por el jefe del órgano u organismo que representan.

SECCIÓN TERCERA Lista general para la clasificación y desclasificación de la Información oficial.

ARTÍCULO 24.-La Lista General para la Clasificación y Desclasificación de la Información Oficial es el documento oficial donde se define el conjunto de asuntos considerados clasificados en la república de Cuba.

ARTÍCULO 25.- A la Lista general solo tiene acceso los jefes de los órganos, organismos o entidades del estado y el personal autorizado por estos, que por sus funciones así lo requieran.

ARTICULO 26.-Toda modificación que requiera efectuarse a la Lista general debe someterse a consulta de la Comisión Estatal para la Clasificación y Desclasificación de la Información Oficial, que la elevará al Comité Ejecutivo del Consejo de Ministros para su aprobación.

SECCIÓN CUARTA Lista interna para la Clasificación y Desclasificación de la Información Oficial.

ARTICULO 27.-La Lista Interna para la Clasificación y Desclasificación de la Información Oficial es el documento oficial contentivo de las Informaciones que se generan en cada órgano, organismo y entidad que constituyen asuntos definidos en la Lista. General.

ARTICULO 28.- Cada órgano, organismo o entidad según corresponda elabora su Lista Interna, la que es aprobada y puesta en vigor por Resolución u otra disposición del Jefe correspondiente.

ARTÍCULO 28.1.-A la Lista Interna tienen acceso los dirigentes, funcionarios y personal en general de los órganos, organismos y entidades que en atención a la función que realicen deben utilizar Información Oficial.

ARTICULO 29.-Toda modificación que se requiera efectuar a la Lista Interna, cuando afecte la Lista General será sometida a consulta de la Comisi6n, que la elevará al Comité Ejecutivo del Consejo de Ministros para su aprobación.

CAPITULO V RESPONSABILIDADES DE LOS ÓRGANOS, ORGANISMOS y ENTIDADES

ARTICULO 3O.- Los Jefes de órganos organismos y entidades aseguran en controlan y exigen e1 cumplimiento de lo estab1ecido en e1 Sistema para la Seguridad y Protección de la Información Oficial.

ARTÍCULO 31.- Los Jefes de órganos, organismos y entidades en cada instancia están en 1a obligación de:

a) educar, preparar y concienciar al personal subordinado en mantener la debida discreción y compartimentación en cuanto a la Información Oficial C1asificada o Limitada que conozca en razón de su cargo, así como de cumplir

todas las medidas que se establezcan en materia de Seguridad y Protección de esta información:

b) ejercer especial control sobre el uso de los medios de computación portátl1 y soportes magnéticos, cámaras, cassettes de video y televisión, rollos fotográficos, grabadoras y cintas fuera de los locales de trabajo, cuando contengan Información Oficial Clasificada o Limitada;

c) designar al personal que responde por la dirección, ejecución y control de la seguridad y protección de la Información Oficial Clasificada y Limitada;

d) designar una o mis personas si se requiere, con la idoneidad adecuada para que supervise y contrate el cumplimiento de las medidas de Seguridad Informática y Criptográfica establecidas en los lugares donde se procesa, intercambia, reproduce o conserva información oficial, a través de las tecnologías de información;

e) garantizar que se proceda, ante la ocurrencia de hechos constitutivos de violaciones del Sistema para la Seguridad y Protección de la Información Oficial Clasificada o Limitada, a la aplicación de las medidas correspondientes e informarlo de inmediato al órgano competente del Ministerio del Interior;

f) preparar al personal vinculado con la Seguridad y Protección a la Información Oficial y la Seguridad Informática;

g) aprobar los Planes de Seguridad Informática, de Contingencia, de Seguridad y Protección a la Información y de Evacuación, Conservación y Destrucc16n de la Información Oficial Clasificada y Limitada.

ARTÍCULO 32.- El Jefe de cada órgano, organismo, o entidad, en correspondencia con el volumen de la Información Oficial Clasificada, crea la Oficina para el Control de la Información Clasificada OCIC o designa la persona que se responsabiliza con la orientación y control del cumplimiento de las medidas para la seguridad y protección a esta información.

ARTÍCULO 33.- Los Jefes de órganos, organismos o entidades en cada instancia son los únicos facultados para autorizar a1 personal con acceso a la Información Oficial Clasificada y Limitada que le competa en cada momento de acuerdo a las funciones que desempeña.

ARTÍCULO 34.- El Jefe es el único que puede autorizar dar a conocer Informaci6n Oficial Clasificada generada en su órgano, organismo o entidad, procediendo de acuerdo a la categoría de clasificación que posea la misma.

ARTICULO 35.- Los Jefes de órganos organismos o entidades, aseguraran que la Información Oficia1 Clasificada se tramita con Protección Criptográfica y decidirán cuándo, por los riesgos que su conocimiento pueda producir, deba ser tratada en contactos personales exclusivamente.

ARTÍCULO 36.- Los dirigentes administrativos deben incluir en los planes económicos anuales y perspectivos los recursos financieros y materiales necesarios para la adquisición, instalación y mantenimiento de las medidas, medios técnicos y físicos requeridos para la Seguridad y Protección de la Información Oficial.

CAPITULO VI PROTECCIÓN CRIPTOGRÁFICA.

ARTICULO 37.- El Ministerio del Interior es el organismo encargado de representar al país en las relaciones de colaboración científica y tecnológica en la esfera de la Criptografía con países y organizaciones internacionales.

ARTICULO 38.- Es facultad del Ministerio del Interior autorizar la divulgación, promoción, elaboración de información, realización de eventos e intercambios de o sobre los Sistemas de Protección Criptográfica. Los intereses que al respecto puedan presentarse serán coordinados y solucionados con dicho Ministerio.

ARTICULO 39.- Corresponde al Ministerio del Interior autorizar el diseño, producción, importación y comercialización de Sistemas de Protección Criptográfica y prestación de estos servicios a órganos, organismos y entidades estatales.

ARTICULO 40.- Corresponde al Ministerio del Interior realizar las actividades de investigación y desarrollo para el diseño, producción, análisis, evaluación y aprobación de los Sistemas de Protección Criptográfica y los criptomateriales y de las aplicaciones criptográficas contenidas en los Sistemas Automatizados o de Comunicaciones.

ARTÍCULO 41.- La realización de estudios o investigaciones científicas y tecnológicas en interés de la Criptografía, por parte de personas naturales o jurídicas, se hará por necesidades y solicitud del Ministerio del Interior, o a iniciativa de aquellas, previa consulta y aprobación de dicho Ministerio, el que además certificará la aplicación de todo Sistema de Protección Criptográfica.

ARTÍCULO 42.- El Ministerio del Interior es el organismo encargado de regular, dirigir y controlar el Servicio Central Cifrado Internacional del Estado y Gobierno Cubano.

CAPITULO VII SEGURIDAD INFORMÁTICA

ARTICULO 43.- En los órganos, organismos o entidades donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información, se cumplirán las medidas que se requieran para su seguridad y protección, en correspondencia con las normas y regulaciones emitidas por el Ministerio del Interior

ARTICULO 44.- Todos los órganos, organismos o entidades donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información tienen que elaborar, aplicar y mantener actualizados permanentemente los Planes de Seguridad Informática y de Contingencia, acorde con lo establecido por el Ministerio del Interior para la seguridad informática y por el de la Industria Sidero Mecánica y la Electrónica para la seguridad técnica de los sistemas informáticos.

ART1CULO 45.- El Ministerio del Interior es el organismo competente para realizar Auditoria a la Seguridad Informática y el facultado para autorizar a otros órganos, organismos o entidades u otras personas naturales o jurídicas a realizarlas.

ARTÍCULO 46.- Se prohíbe procesar, reproducir o conservar Información Oficial Clasificada con la categoría de Secreto de Estado en las tecnologías de información conectadas en redes de datos.

ARTÍCULO 47.- Se prohíben las conductas que se describen a continuación:

a) Crear o diseminar programas malignos.

b) El acceso no autorizado a redes de datos.

c) Conectar tecnologías de información que procesen Información Oficial Clasificada a las redes datos de alcance global.

ARTÍCULO 48.- La violación de lo establecido en los Artículos 46 y 47 será puesta en conocimiento de la autoridad administrativa que corresponda a los efectos de la aplicación de la medida que proceda, sin perjuicio de cualquier otra responsabilidad en que pudiere haberse incurrido.

ARTICULO 49.- En los órganos, organismos o entidades donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información, se designa una o más personas en su caso, con la

idoneidad requerida para que supervise y controle el cumplimiento de las medidas de Seguridad Informática establecidas.

CAPÍTULO VIII PROTECCIÓN ELECTROMAGNÉTICA

ARTÍCULO 50.- La Protección Electromagnética tiene como objetivo disminuir el riesgo que encierra las fugas de señales electromagnéticas contentivas de Información Oficial Clasificada o Limitada, emitidas por los sistemas Informáticos durante su explotación. Comprende locales, medios y circuitos apantallados, sistemas de filtraje de señales, barreras técnicas y medidas complementarias.

ARTICULO 51.- Los Sistemas de Protección electromagnéticas serán desarrollados y producidos en entidades nacionales autorizadas bajo el cumplimiento de normas y certificación emitidas por el Ministerio del Interior.

ARTICULO 52.- Las entidades que adquieran tecnólogas de información por vías diferentes a las entidades nacionales autorizadas al efecto deberán, previo a su empleo, solicitar al Ministerio del Interior su homologación o certificación en relación a la Protección Electromagnética.

ARTICULO 53.- La aplicación de los Sistemas de Protección Electromagnética en las entidades estará en correspondencia con los requerimientos de protección a la Información Oficial y de Seguridad Informática.

DISPOSICIONES ESPECIALES.

PRIMERA: Se faculta al Ministerio de las Fuerzas Armadas Revolucionarias para el desarrollo, reglamentación, aplicación y control de los Sistemas de Protección Criptográfica y de Seguridad Informática de uso propio.

SEGUNDA: El Ministerio del Interior presentará al Comité ejecutivo del Consejo de Ministros, en un plazo de 180 días contados a partir de la fecha de aprobación del presente Decreto-Ley, la correspondiente propuesta para establecer el sistema de contravenciones en la materia que por éste se regula.

DISPOSICIONES FINALES.

PRIMERA: Se faculta al Ministerio de las Fuerzas Armadas Revolucionarias y del Interior, según corresponda, para adecuar en lo que resulte necesario, la aplicación de las disposiciones establecidas en este Decreto-Ley, en

correspondencia con las particularidades de las funciones, misiones y características en la información de dichos organismos.

SEGUNDA: El Ministerio del Interior emitirá el Reglamento y demás disposiciones complementarias del presente Decreto-Ley en un plazo que no exceda los 90 días, contados a partir de la fecha de su aprobación y queda facultado para dictar cuantas otras disposiciones resulten necesarias para su mejor cumplimiento.

TERCERA: Se derogan la Ley número 1246 del Secreto Estatal del 14 de mayo de 1973 y el Decreto número 3753 del 17 de enero de 1974 que puso en vigor el Reglamento para la ejecución de la Ley del Secreto Estatal, así como el Decreto número 3787 del 23 de septiembre de 1974 que puso en vigor los Reglamentos Gubernamentales para el Servicio Cifrado Nacional y para el Servicio Cifrado Exterior; la Resolución del 25 de mayo de 1973 del Comandante en Jefe en su condición de Primer Ministro, creando la Comisión Estatal para la Clasificación y Desclasificación de la Información y cuantas disposiciones se opongan al cumplimiento del presente Decreto Ley.

CUARTA: El Sistema para la Seguridad y Protección de la Información Oficial que se establece, comenzará a regir una vez transcurridos 180 días contados a partir de la publicación del presente Decreto-Ley en la Gaceta Oficial de la República.

Dado en el Palacio de la Revolución, en la ciudad de La Habana, a los 25 días del mes de noviembre de 1999.

Fidel Castro Ruz.

Anexo 2: Decreto-Ley Nº 199

RESOLUCION No. 1/2000

DEL MINISTRO DEL INTERIOR

QUE PONE EN VIGOR EL REGLAMENTO SOBRE LA SEGURIDAD Y PROTECCION DE LA INFORMACION OFICIAL

POR CUANTO: El Consejo de Estado ha aprobado el Decreto Ley No. 199 de 25 de noviembre de 1999, mediante el cual se establece y regula el Sistema de medidas en materia de Seguridad y Protección de la Información Oficial.

POR CUANTO: El Decreto Ley No. 199 de 25 de noviembre de 1999 sobre la Seguridad y Protección de la Información Oficial, en su Disposición Final Segunda faculta al Ministerio del Interior a emitir los Reglamentos y demás disposiciones complementarias que resulten necesarias para su mejor cumplimiento.

POR CUANTO: En los órganos, organismos y entidades resulta necesaria la instrumentación y aplicación de medidas de seguridad y protección a la información oficial que obstaculicen e impidan el acceso a estas informaciones por parte de los Servicios Especiales Extranjeros y personas no autorizadas.

POR TANTO: En uso de las facultades que me están conferidas,

RESUELVO:

PRIMERO: Poner en vigor el Reglamento sobre la Seguridad y Protección de la Información Oficial que se establece a continuación.

REGLAMENTO

SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA

INFORMACIÓN OFICIAL

CAPITULO I

DE LA AUTORIDAD COMPETENTE

ARTICULO 1: El presente Reglamento establece las normas que rigen la Seguridad y Protección de la Información Oficial que deben aplicarse en los órganos, organismos, entidades y sus dependencias o cualquier otra persona natural o jurídica residente en el territorio nacional, como las Representaciones Cubanas en el Exterior. A los efectos de este Reglamento, cuando se mencione Decreto Ley, se refiere al Decreto Ley No. 199 de 25 de noviembre de 1999 sobre la Seguridad y Protección de la Información Oficial.

ARTICULO 2: La Dirección de Protección del Ministerio del Interior, es el órgano rector especializado encargado de ejecutar y controlar en el marco de

su competencia el cumplimiento de la política establecida en el Decreto Ley y en este Reglamento en materia de Seguridad y Protección de la Información Oficial.

CAPITULO II

DE LA INFORMACIÓN OFICIAL CLASIFICADA

SECCIÓN PRIMERA

Personal con acceso a la Información Oficial Clasificada

ARTICULO 3: La Información Oficial Clasificada solamente puede ser conocida por las personas autorizadas para ello.

ARTICULO 4: Los órganos, organismos, entidades y sus dependencias, se responsabilizan con mantener actualizado el control de las personas con acceso a Información Oficial Clasificada, en las instancias que les correspondan.

ARTICULO 5: Toda persona a la que se le autorice el acceso a la Información Oficial Clasificada está obligada a firmar el **"Acta de responsabilidad"** donde se hace constar su obligación a no divulgar las informaciones que conoce.

SECCIÓN SEGUNDA

Facultad para otorgar acceso a la Información Oficial Clasificada

ARTÍCULO 6: Corresponde la facultad para otorgar acceso a la Información Oficial Clasificada hasta la categoría:

Secreto de Estado al dirigente máximo de los órganos, organismos y entidades.

Secreto a los viceministros, vicepresidentes o dirigentes de cargos equivalentes en los órganos, organismos, entidades y sus dependencias.

Confidencial a los directores o dirigentes de los cargos equivalentes en los órganos, organismos, entidades y sus dependencias.

ARTÍCULO 7: La facultad de otorgar el acceso a los extranjeros a la Información Oficial Clasificada corresponde solamente al dirigente máximo de los órganos, organismos y entidades. En aquellas entidades que

organizativamente estén integradas a un órgano u organismo central esta facultad le corresponderá al máximo dirigente de éstos.

ARTÍCULO 8: El funcionario responsable en otorgar el nivel de acceso a la Información Oficial Clasificada tendrá la obligación de determinar en cada caso las informaciones a las cuales autoriza su conocimiento.

SECCIÓN TERCERA

Organización y funciones del personal responsabilizado con la dirección, ejecución y control de la Seguridad y Protección de la Información Oficial Clasificada

ARTÍCULO 9: De acuerdo a lo establecido en el Decreto Ley, los dirigentes de los órganos, organismos, entidades y sus dependencias, designan el cargo o persona con la idoneidad requerida que debe responder por la dirección, ejecución y control de la seguridad y protección de la Información Oficial Clasificada de acuerdo a la estructura, volumen y valor de las informaciones que se tramitan en dichos lugares.

ARTÍCULO 10: Corresponde al Jefe, Especialista, Técnico de Seguridad y Protección o persona designada, las funciones de organizar, asesorar y controlar el cumplimiento de lo establecido en el Decreto Ley, en este Reglamento y demás disposiciones complementarias que emanen del Ministerio del Interior.

ARTÍCULO 11: El Jefe, Especialista, Técnico de Seguridad y Protección o persona designada para organizar, asesorar y controlar las medidas de seguridad y protección a la Información Oficial Clasificada tiene las funciones siguientes:

a) asesorar y controlar el cumplimiento del Decreto Ley, este Reglamento y demás disposiciones complementarias, así como las emanadas de la Comisión Estatal para la Clasificación y Desclasificación de la Información Oficial,
b) organizar, asesorar y controlar la aplicación y cumplimiento de las medidas de seguridad y protección a la Información Oficial Clasificada en los órganos, organismos, entidades y sus dependencias,
c) organizar, dirigir y supervisar el funcionamiento y trabajo del personal de la Oficina para el Control de la Información Oficial Clasificada (OCIC) o persona designada para realizar estas funciones,
d) asesorar, exigir y controlar el uso correcto de la Lista Interna para la Clasificación y Desclasificación de la Información Oficial a fin de proteger las informaciones de valor,
e) participar y asesorar en la elaboración y actualización de la Lista Interna para la Clasificación y Desclasificación de la Información Oficial,

f) asesorar y exigir por el cumplimiento de las obligaciones que se establecen en este Reglamento para los dirigentes administrativos y las comunes de todo el personal,
g) definir los lugares y bienes donde se elabore, procese, tramite, transmite, reproduce y conserve la Información Oficial Clasificada en los órganos, organismos, entidades y sus dependencias, con el fin de aplicar las medidas de seguridad y protección correspondientes,
h) planificar y realizar el control al cumplimiento de lo establecido para la seguridad y protección a la Información Oficial Clasificada en todas las instancias del aparato central y demás dependencias del órgano, organismo o entidad a la que pertenezca,
i) analizar, actuar e informar al Jefe administrativo y al órgano correspondiente del Ministerio del Interior sobre los hechos constitutivos de violaciones de la legislación penal, contravencional y laboral vigentes en relación con las medidas de seguridad y protección de la Información Oficial Clasificada y crear una comisión ante cada hecho, que se encargue de investigarlo,
j) planificar, elaborar y ejecutar planes de preparación del personal que está a cargo del control de esta actividad y controlar su cumplimiento,
k) asesorar y controlar el cumplimiento de las medidas establecidas de Seguridad y Protección de la Información Oficial Clasificada en los eventos nacionales e internacionales que se organicen a su nivel o en los que participe.
l) instruir al personal con nivel de acceso a Información Oficial Clasificada que viaje al exterior según la metodología establecida a esos efectos,
m) asesorar el trabajo para la divulgación de la Información Oficial.
n) asesorar, la elaboración del Plan de Seguridad y Protección de la Información Oficial.
o) asesorar la elaboración del Plan de Evacuación, Conservación y Destrucción de la Información Oficial Clasificada y Limitada para Situaciones Excepcionales y Catástrofes.
p) trabajar coordinada y sistemáticamente con el Responsable de Seguridad Informática a fin de evitar hechos que atenten contra el procesamiento, transmisión y almacenamiento de datos por medios de computación; y
q) ante la ocurrencia de hechos que constituyan violaciones de la Seguridad Informática relacionadas con la Información Oficial Clasificada o Limitada, investigar las causas, condiciones y efectos, tomando las medidas correspondientes e informar a los órganos competentes del Ministerio del Interior.

CAPITULO III

DE LA INFORMACIÓN OFICIAL LIMITADA

ARTÍCULO 12: El dirigente máximo del órgano, organismo, entidad y sus dependencias en cada instancia determina cual de las informaciones oficiales que genera debe identificarse como Limitada y cuando pierde esa condición.

ARTÍCULO 13: El dirigente en cada instancia determina las medidas que deben adoptarse para controlar la Información Oficial Limitada que genere.

ARTÍCULO 14: Al dirigente en cada instancia, le corresponde la facultad para otorgar acceso a la Información Oficial Limitada y disponer las medidas para su seguridad y protección.

ARTICULO 15: El dirigente máximo del órgano, organismo, entidad y dependencia le asignará al Jefe, Especialista, Técnico de Seguridad y Protección o persona designada, las funciones relacionadas con el control y protección de la Información Oficial Limitada.

ARTÍCULO 16: Cada órgano, organismo o entidad determina los procedimientos para el control de la elaboración, reproducción, acceso, conservación y destrucción de la Información Oficial Limitada.

CAPITULO IV

DE LA INFORMACIÓN OFICIAL ORDINARIA

ARTICULO 17: Los Jefes de órganos, organismos o entidades, y de Seguridad y Protección a esos niveles, dispondrán la revisión periódica de la Información Oficial Ordinaria, en cualquier soporte, con el objetivo de detectar informaciones no clasificadas por la no aplicación de las regulaciones establecidas en la Lista General e Interna de Clasificación y Desclasificación de la Información Oficial, así como aquellas informaciones no identificadas como Limitadas.

CAPITULO V

DE LA CLASIFICACIÓN Y DESCLASIFICACIÓN DE LA INFORMACIÓN OFICIAL

SECCIÓN PRIMERA

Proceso de Clasificación y Desclasificación de la Información Oficial

ARTICULO 18: El proceso de clasificación es aquel mediante el cual se determina la categoría correspondiente a una información oficial, teniendo en

cuenta que su divulgación o conocimiento no autorizado pueda ocasionar daños o entrañar riesgos para el país o su desarrollo en el orden político, militar, económico, científico, técnico, cultural, social o de cualquier otro tipo. El proceso de clasificación también comprende señalar en un documento la categoría de clasificación correspondiente.

ARTICULO 19: El proceso de desclasificación es aquel mediante el cual se suprime la categoría de clasificación correspondiente a una información oficial, al desaparecer los elementos que le dieron dicha categoría o por el vencimiento del período de permanencia de clasificación que se señala en la Lista General o Interna para la Clasificación y Desclasificación de la Información Oficial.

ARTICULO 20: La desclasificación de una Información Oficial Clasificada contenida en la Lista Interna, que se genere en un órgano, organismo o entidad, cuyo período de permanencia sea "Hasta que se autorice su desclasificación", solo podrá ejecutarse de acuerdo a la categoría de clasificación que posea, con la aprobación de los niveles de dirección siguientes:

Secreto de Estado.....Comité Ejecutivo Consejo de Ministros

Secreto.....Dirigente máximo del órgano, organismo, o entidad

Confidencial.....Viceministros, directores o cargos equivalentes.

ARTICULO 21: Los dirigentes de los órganos, organismos o entidades quedan responsabilizados con elevar para su análisis a la Comisión Estatal para la Clasificación y Desclasificación de la Información Oficial, en lo adelante Comisión Estatal, las modificaciones y propuestas de clasificación o desclasificación que consideren hacer a la Lista General.

ARTICULO 22: El dirigente máximo de un órgano, organismo o entidad decide que se proteja como clasificada una información oficial, aun cuando no esté contenida en su Lista Interna, y si afecta la Lista General eleva su propuesta de clasificación a la Comisión Estatal.

ARTÍCULO 23: Las propuestas de clasificación y desclasificación de la información oficial recogidas en los artículos 21 y 22 se elevan por la Comisión Estatal al Comité Ejecutivo del Consejo de Ministros para su aprobación y puesta en vigor, cuando afecte la Lista General.

SECCIÓN SEGUNDA

De las negociaciones y su clasificación

ARTICULO 24: Toda información oficial que se genere derivada de los asuntos tratados y acuerdos adoptados con países, empresas, firmas, entidades y personalidades extranjeras, como resultado de viajes al exterior o contactos, con el objetivo de efectuar relaciones comerciales, económicas y financieras, negociaciones, creación de empresas extranjeras privadas o mixtas u otras formas de asociaciones económicas internacionales, así como representaciones o firmas extranjeras, será debidamente clasificada por el funcionario o dirigente representante de la parte cubana.

ARTÍCULO 25: Las Informaciones Oficiales Clasificadas o Limitadas que, por necesidades de las negociaciones, deba tener acceso la parte extranjera, serán autorizadas con arreglo a lo establecido en los artículos 5, 7 y 14 de este Reglamento. Asimismo se garantizará que la parte extranjera no acceda a otras Informaciones Oficiales Clasificadas o Limitadas que no resulten necesarias, antes, durante o después de las negociaciones oficiales.

CAPITULO VI

DE LA RESPONSABILIDAD DE LOS ORGANOS, ORGANISMOS Y ENTIDADES

SECCIÓN PRIMERA

Obligaciones de los dirigentes administrativos

ARTICULO 26: Los dirigentes administrativos tienen la responsabilidad de cumplir y hacer cumplir lo dispuesto en el Decreto Ley, este Reglamento, las disposiciones complementarias y además, las obligaciones siguientes:

a) crear las condiciones materiales y de organización que garanticen la aplicación y el cumplimiento de lo establecido en el Decreto Ley, este Reglamento y demás disposiciones complementarias,
b) crear en el personal subordinado un estado de conciencia propicio a la observancia de la discreción y la compartimentación, en cuanto a las Informaciones Oficiales Clasificadas y Limitadas que conozca en razón de su cargo, así como de cumplir todas las medidas que se establezcan en materia de seguridad y protección de esta información,

c) incorporar al sistema de preparación de los cuadros administrativos, especialistas y demás funcionarios, las regulaciones establecidas para la seguridad y protección a la información oficial,
d) cumplir y hacer cumplir la clasificación correcta de la información oficial que se genere en su ámbito de trabajo, de acuerdo a la Lista Interna,
e) proponer al nivel que corresponda la clasificación y desclasificación de la información oficial que se genera en su ámbito de acuerdo a lo establecido en los artículos 20, 21 y 22 de este Reglamento,
f) cumplir las regulaciones establecidas para la Protección Criptográfica y el Servicio Cifrado cuando sea necesario trasmitir Información Oficial Clasificada por los medios de comunicación,
g) aprobar la información destinada a la divulgación, con el fin de evitar que por error se divulgue Información Oficial Clasificada y Limitada, por los medios masivos de difusión,

h) autorizar por escrito la reproducción o destrucción de documentos clasificados que se generan, tramitan o conservan en el lugar,
i) garantizar que se cumplan las medidas establecidas para la seguridad y protección de la Información Oficial Clasificada o Limitada que se procesa, intercambia, reproduce o conserva a través de las tecnologías de información; y
j) garantizar que se proceda ante la ocurrencia de violaciones de las medidas de seguridad y protección a la Información Oficial Clasificada y Limitada, y aplicar las medidas administrativas correspondientes e informar a sus instancias superiores y al órgano competente del Ministerio del Interior.

ARTICULO 27: El dirigente máximo tiene la obligación de autorizar la reproducción o destrucción de los documentos Secreto de Estado que se generen en su ámbito. Cuando el documento Secreto de Estado se haya recibido de otro órgano, organismo o entidad para reproducirlo se requiere la autorización del dirigente máximo del lugar donde se generó.

SECCIÓN SEGUNDA

Obligaciones del personal con acceso a Información Oficial Clasificada.

ARTÍCULO 28: El personal con acceso a Información Oficial Clasificada está en la obligación de:

a) conocer y cumplir las normas establecidas para la seguridad y protección de la Información Oficial Clasificada, contenidas en el Decreto Ley, este Reglamento y demás disposiciones complementarias,
b) firmar la recepción de los documentos que contengan Información Oficial Clasificada y en las entregas y devoluciones exigir la firma de quien lo recibe,

c) clasificar la información cuando se elabore un documento de acuerdo con las categorías establecidas en la Lista Interna,
d) impedir que los documentos contentivos de Información Oficial Clasificada o Limitada, con los cuales se está trabajando, sean conocidos por personas no autorizadas,
e) guardar los documentos clasificados en los lugares o muebles con las medidas de seguridad requeridas,
f) entregar a la Oficina para el Control de la Información Oficial Clasificada (OCIC) o persona responsabilizada con el control de la Información Oficial Clasificada, cualquier soporte utilizado como borrador,
g) observar el máximo cuidado en la custodia de documentos clasificados, el sello personal y otros medios y materiales que les hayan sido entregados en evitación de su pérdida, extravío o cualquier otra violación,
h) comprobar antes de transmitir una Información Oficial Clasificada, de forma oral, escrita o automatizada, que el destinatario esté autorizado a tener acceso a ella, las condiciones de privacidad del lugar donde se realice la transmisión y la utilización del medio de protección establecido para ello,
i) cerrar y sellar los locales, archivos, buroes, u otros muebles o lugares, donde obre documentación clasificada, utilizando las medidas y medios técnicos según corresponda,
j) comprobar en los locales donde está aplicada la técnica de alarma, que ésta quede activada al concluir el horario de trabajo,
k) guardar con la protección debida las llaves de muebles y locales donde obren documentos clasificados,
l) comprobar antes de abrir los lugares y depósitos donde se elaboren, custodien, o trasladen documentos clasificados, si los puntos de cierre habilitados con el sistema de sellaje, presentan signos de haber sido violados,
m) entregar en la Oficina para el Control de la Información Oficial Clasificada (OCIC) o a la persona responsabilizada con el control de documentos clasificados, los que obren en su poder antes de salir al exterior, de vacaciones, por traslado u otros motivos de ausencia temporal o definitiva del puesto de trabajo,
n) entregar de inmediato a la Oficina para el Control de la Información Oficial Clasificada (OCIC) o a la persona responsabilizada con el control de los documentos clasificados, los que haya recibido en otro lugar, para su registro y control,
o) comunicar al Jefe de Seguridad y Protección las personas que no tienen acceso a una Información Oficial Clasificada y muestren interés en conocerla, así como cuando cometa o conozca de cualquier violación, y
p) facilitar la información que se solicite en la ejecución de supervisiones que se realicen por el personal facultado para ello.

SECCIÓN TERCERA

Obligaciones comunes a todo el personal

ARTÍCULO 29: El personal que labore, visite o acuda a cualquier órgano, organismo, entidad o sus dependencias, está en la obligación de cumplir todas las medidas establecidas para proteger la Información Oficial Clasificada y Limitada.

ARTICULO 30: La persona que cometa o tenga conocimiento de la violación de cualesquiera de las medidas establecidas para la seguridad y protección de la Información Oficial Clasificada y Limitada, está en la obligación de comunicarlo a su Jefe inmediato y éste al Jefe de Seguridad y Protección del lugar donde trabaja o la persona responsabilizada a estos efectos y a su jefe inmediato superior, así como preservar el lugar del hecho si es necesario, hasta tanto se presenten las autoridades competentes.

CAPITULO VII

TRATAMIENTO A LA INFORMACIÓN OFICIAL CLASIFICADA Y LIMITADA

SECCIÓN PRIMERA

Elaboración, impresión, reproducción, recepción, registro, tramitación, transmisión, archivo, almacenamiento, conservación, destrucción, borrado y evacuación de la Información Oficial Clasificada y Limitada

ARTICULO 31: Cuando se elabore en un órgano, organismo, entidad o dependencia una Información Oficial Clasificada y el ejecutor considere que no pueda otorgársele acceso o reproducirse sin su autorización, lo hará constar en el propio documento.

ARTICULO 32: El envío de documentos clasificados se efectuará mediante los correos oficiales o personas autorizadas e instruidas para realizar esta función, y en los vehículos destinados a transportar esta documentación solo podrán viajar las personas debidamente autorizadas.

ARTICULO 33.1: El documento clasificado o limitado destinado al conocimiento de una persona se identificará con la letra (**P) (personal)** a continuación de la categoría o señalización que le corresponda de acuerdo a la información que contenga.

2. El destinatario de este tipo de documento será el único facultado para determinar si otra persona, por necesidades de trabajo, deba tener acceso al mismo teniendo en cuenta los niveles de acceso establecidos.

ARTICULO 34: En los órganos, organismos, entidades y sus dependencias, se establecerán las medidas que permitan prevenir y detectar cualquier acción que atente contra la compartimentación, integridad y disponibilidad de la Información Oficial Clasificada y Limitada relacionadas con la elaboración, impresión, reproducción, recepción, registro, tramitación, transmisión, archivo, almacenamiento, conservación, destrucción, borrado y evacuación de la Información Oficial Clasificada y Limitada mediante equipos de computación, filmación, grabación, o cualesquiera medios técnicos que garanticen la seguridad y protección de los programas, aplicaciones, soportes, equipos y locales donde éstos se instalen.

ARTICULO 35.1: Los soportes magnéticos que contengan Información Oficial Clasificada o Limitada existentes en los órganos, organismos, entidades y sus dependencias serán debidamente inventariados.

2. Para el control de los soportes magnéticos se entiende por inventario la especificación de los datos que permitan conocer: el número consecutivo, fecha de comienzo de explotación, categoría o señalización, informaciones, asuntos, números de registros de los documentos, nombre de los ficheros donde están contenidos y las observaciones que se consideren necesarias.

ARTICULO 36: Los soportes magnéticos que contengan Información Oficial Clasificada, serán registrados en la Oficina para el Control de la Información Clasificada (OCIC) o por las personas responsabilizadas con el control de este tipo de información.

ARTICULO 37: Los soportes destinados para la Información Oficial Clasificada no podrán utilizarse para la Información Oficial Limitada ni Ordinaria.

ARTICULO 38: En las Normas y Procedimientos para el registro, tramitación y control de la información oficial, se establecen las medidas de seguridad y protección para su tratamiento en todos sus procesos.

SECCIÓN SEGUNDA

Traslado de Información Oficial Clasificada al extranjero

ARTICULO 39: El traslado de Información Oficial Clasificada al extranjero o de éste a nuestro país, se realizará solamente a través del Sistema de Correo Diplomático del Ministerio de Relaciones Exteriores de la República de Cuba o por la persona autorizada, de acuerdo con las normas establecidas al respecto.

ACUERDO 40: La transmisión de Información Oficial Clasificada al extranjero o de éste a nuestro país, a través de las tecnologías de información, solo se hará utilizando el Servicio Cifrado del Ministerio del Interior.

ARTICULO 41: El traslado de Información Oficial Clasificada al extranjero o de éste a nuestro país, se realizará, de acuerdo a la categoría de clasificación con la autorización expresa de los niveles de dirección siguientes:

Secreto de Estado el órgano y organismo donde se genera esta información, con la consulta previa del nivel superior de dirección del Comité Ejecutivo del Consejo de Ministros al cual esté subordinado.

Secreto el dirigente máximo del órgano, organismo o entidad. Aquellas entidades que organizativamente estén integradas a un organismo u órgano central esta facultad le corresponderá al máximo dirigente de éstos.

Confidencial el viceministro o cargo equivalente de dirección del órgano, organismo o entidad, donde se genera esta información.

CAPITULO VIII

MEDIDAS DE SEGURIDAD Y PROTECCIÓN PARA LOS BIENES MUEBLES E INMUEBLES DE LOS ORGANOS, ORGANISMOS Y ENTIDADES DONDE EXISTA INFORMACIÓN OFICIAL CLASIFICADA Y LIMITADA.

ARTICULO 42: Los bienes muebles e inmuebles que resulten esenciales para la seguridad y protección de la Información Oficial Clasificada contarán con las medidas de seguridad y protección establecidas en este Reglamento.

ARTICULO 43: A los efectos de este Reglamento, los bienes muebles e inmuebles existentes en los órganos, organismos, entidades y sus dependencias, serán aquellos donde se realicen los procesos de elaboración, impresión, reproducción, recepción, transmisión, tramitación, archivo, almacenamiento, conservación, destrucción y evacuación de la Información Oficial Clasificada.

ARTICULO 44: La seguridad y protección de los bienes muebles e inmuebles, donde exista Información Oficial Clasificada se llevará a cabo mediante la adopción de medidas internas y externas.

ARTICULO 45: Se entiende por medidas de seguridad internas, a los efectos de este Reglamento, aquellas que se aplican para impedir el acceso de personas no autorizadas a los bienes muebles e inmuebles donde existe Información Oficial Clasificada.

ARTICULO 46: Las medidas de seguridad internas que serán aplicadas en los bienes muebles e inmuebles donde existe Información Oficial Clasificada serán las siguientes:

a) sellar con el sello personal de quien los utiliza,

b) organizar el control centralizado de las llaves garantizando su permanencia física en los órganos, organismos, entidades y sus dependencias.
c) cumplir las normas complementarias establecidas para la evacuación o destrucción de la información oficial clasificada en caso de desastres, amenazas o cualquier peligro,
d) reparar y limpiar los bienes por personas seleccionadas y en presencia del personal que labore en el lugar,
e) mantener una temperatura estable, relativamente baja y donde se evite la humedad,
f) equipar con medios de detección de intrusos y extinción de incendios, y
g) donde se encuentre en elaboración o conservación la Información Oficial Clasificada que por sus características debe estar expuesta o no pueda moverse, cubrir y sellar sus puntos de cierre, para evitar el acceso de personas no autorizadas.

ARTICULO 47: Se entiende por medidas de seguridad externas, a los efectos de este Reglamento, aquellas que se aplican para proteger debidamente los bienes muebles e inmuebles donde existe Información Oficial Clasificada.

ARTICULO 48: Las medidas de seguridad externas que serán aplicadas en los lugares y bienes muebles e inmuebles, donde exista Información Oficial Clasificada serán las siguientes:

a) proveer de cierre de seguridad, sistema de sellaje y alarmas en las puertas y ventanas,
b) construir las paredes y techos con materiales sólidos que impidan el acceso a personas no autorizadas, y
c) habilitar en la Oficina para el Control de la Información Oficial Clasificada (OCIC) o archivo central una ventanilla o lugar para la entrega, lectura y recibo de los documentos con el fin de evitar el acceso de personas no autorizadas.

ARTICULO 49: En cada lugar se aplicarán las medidas de seguridad y protección internas y externas que sean necesarias de acuerdo al valor, volumen y vigencia de la Información Oficial Clasificada, teniendo en cuenta las características y condiciones existentes.

ARTICULO 50: En horas laborables solo tienen acceso a la Oficina para el Control de la Información Oficial Clasificada (OCIC) o lugar donde se tramita, archiva, almacena y conserva la Información Oficial Clasificada, el dirigente máximo de cada lugar, las personas a quienes él autorice y las que laboran en ella. Fuera de este horario el dirigente máximo debe definir el personal facultado a entrar en este local, siempre que exista una razón que lo justifique y se deje constancia de ello.

ARTICULO 51: Las medidas para la seguridad y protección de los bienes muebles e inmuebles donde la Información Oficial sea Limitada, están determinados por el dirigente máximo de cada lugar.

CAPITULO IX

ORGANIZACIÓN DE LA OFICINA DE CONTROL DE LA INFORMACIÓN OFICIAL CLASIFICADA (OCIC) Y FUNCIONES DEL PERSONAL QUE LABORA EN LA MISMA.

SECCIÓN PRIMERA

Organización

ARTICULO 52.1: Las oficinas para el Control de la Información Oficial Clasificada (OCIC) serán organizadas atendiendo a la estructura propia de cada órgano, organismo, entidad o sus dependencias, pudiendo ser en el aparato central una oficina o varias al nivel de dirección que lo requiera, de acuerdo al volumen de información y a las características de las mismas.

2. En los órganos, organismos y entidades la Información Oficial Clasificada deberá estar centralizada en la Oficina para el Control de la Información Oficial Clasificada (OCIC). De forma excepcional se autorizará su descentralización en aquellas áreas que por razones muy justificadas, dada la dinámica y gestión del trabajo así lo requiera. En estos casos el Jefe de la Oficina para el Control de la Información Oficial Clasificada (OCIC) o persona responsabilizada mantendrá un control sistemático sobre la misma.

ARTICULO 53: La Oficina para el Control de la Información Oficial Clasificada (OCIC) contará con un Jefe o responsable que responde por la aplicación y cumplimiento de las funciones asignadas a la misma y tendrá bajo su dirección administrativa al personal subordinado que labora en dicha oficina.

ARTICULO 54: En los casos en que la Información Oficial Clasificada que exista en los órganos, organismos, entidades y dependencias. sea poco numerosa y no se requiera de una Oficina para el Control de la Información Oficial Clasificada (OCIC), se designará una persona que desempeñe las funciones establecidas en este Reglamento.

ARTICULO 55: Cuando se produzca el cambio o sustitución de un Jefe de Oficina para el Control de la Información Oficial Clasificada (OCIC) o persona designada para el control de la Información Oficial Clasificada se procederá a realizar la entrega mediante acta que registre el estado y comprobación física de los documentos clasificados, siendo suscrita por el personal entrante y saliente.

SECCIÓN SEGUNDA

Funciones

ARTÍCULO 56: El Jefe de la Oficina para el Control de la Información Oficial Clasificada (OCIC), o persona responsabilizada tiene las funciones siguientes:

a) controlar la elaboración, impresión, reproducción, recepción, registro, acceso, tramitación, transmisión, archivo, conservación, almacenamiento, destrucción, borrado y evacuación de la documentación clasificada, incluyendo cuando se realicen todos estos procesos por medio de computación, audio, video, filmación o por cualquier otra vía,
b) dar un número de registro a todo documento que se genere o reciba, el cual lo identificará en cualquier proceso,
c) asesorar y exigir por el uso correcto de la Lista Interna para la Clasificación y Desclasificación de la Información Oficial,
d) efectuar controles para comprobar el estado de cumplimiento de las medidas de seguridad y protección establecidas en este Reglamento,
e) asesorar e instruir al personal con nivel de acceso a la Información Oficial Clasificada,
f) controlar la preparación del personal con acceso a Información Oficial Clasificada que viaja al exterior o se vincula con extranjeros,
g) asesorar la aplicación de la metodología que se establezca ante la ocurrencia de violaciones de las medidas de seguridad y protección a la Información Oficial Clasificada,
h) informar las violaciones detectadas, al Jefe de Seguridad y Protección del nivel correspondiente,
i) cumplir las normativas para la implantación y aplicación del modelaje de registro, tramitación y control de documentos clasificados,
j) realizar muestreos a la Información Oficial Limitada y Ordinaria con el objetivo de detectar violaciones en el uso de la Lista Interna para la Clasificación y Desclasificación de la Información Oficial,
k) participar en el proceso de elaboración de los Planes de protección de la Información Oficial Clasificada, y
l) establecer coordinaciones de trabajo permanentes con el Responsable de Seguridad Informática para ejercer el control de las medidas de seguridad sobre la Información Oficial Clasificada en las tecnologías de información.

CAPITULO X

PROHIBICIONES RELATIVAS AL ACCESO A LA INFORMACION OFICIAL CLASIFICADA Y LIMITADA

SECCIÓN PRIMERA

Prohibiciones al personal con acceso a Información Oficial Clasificada y Limitada.

ARTÍCULO 57: Al personal con acceso a Información Oficial Clasificada y Limitada se le prohíbe:

a) conceder o participar en entrevistas con representantes de instituciones, órganos de prensa, radio, cine, televisión, o cualquier personal nacional o extranjera para tratar temas que impliquen brindar Información Oficial Clasificada y Limitada, sin la autorización del nivel facultado para ello,
b) sostener conversaciones relacionadas con la Información Oficial Clasificada que conozca, con o en presencia de personas no autorizadas a su acceso o permitirles escuchar la que haya sido grabada,
c) permitir a personas no autorizadas el acceso visual o conocer Información Oficial Clasificada contenida en fotos, filmaciones, soportes magnéticos, gráficos, maquetas o cualesquiera otras formas de objeto físico que la contenga, y
d) trasmitir Información Oficial Clasificada por canales abiertos de comunicación, sin que esté previamente cifrada.

ARTÍCULO 58: Con el fin de garantizar el cumplimiento de las medidas establecidas para la seguridad y protección de la Información Oficial Clasificada y Limitada relacionadas con la tramitación, transmisión, conservación, almacenaje y control de la misma, además de las señaladas en el Artículo anterior, se establecen las prohibiciones siguientes:

a) elaborar, procesar, reproducir, almacenar y transmitir Información Oficial Clasificada a través de medios automatizados, electrónicos u otros, sin la protección requerida o sin el sistema de Servicio Cifrado del Ministerio del Interior,
b) enviar documentos clasificados a personas que no requieren conocer su contenido para el ejercicio de sus funciones,
c) destruir documentos clasificados sin previamente romperlos o triturarlos, de acuerdo a sus características, así como realizar su destrucción o borrado sin cumplir las medidas establecidas para ello,

d) acumular documentos para su destrucción sin las medidas de seguridad y protección establecidas,
e) extraer documentos clasificados sin la autorización correspondiente,
f) dejar documentos clasificados en lugares o muebles donde puedan ser observados por personas que no tengan autorización de acceso a la información contenida en ellos o no reúnan condiciones de seguridad,
g) reproducir, modificar, borrar o destruir Información Oficial Clasificada, contenida en soportes magnéticos, sin la autorización del funcionario facultado para ello y sin cumplir las medidas establecidas.
h) conservar sin control los borradores de documentos clasificados.
i) elaborar, trabajar o trasladar documentos clasificados hacia los domicilios u otros lugares no autorizados, y
j) fotografiar, fotocopiar, grabar y filmar Información Oficial Clasificada sin la autorización del funcionario facultado para ello.

ARTICULO 59: Se prohíbe transmitir Información Oficial Limitada por canales abiertos sin la autorización del funcionario facultado para ello.

SECCIÓN SEGUNDA

Prohibiciones comunes a todas las personas nacionales o extranjeras

ARTICULO 60.1: A todas las personas naturales nacionales o extranjeras se les prohíbe:

a) penetrar en una Ofician para el Control de la Información Oficial Clasificada (OCIC) sin estar comprendido en el nivel de acceso correspondiente,
b) introducir, extraer o permitir que se introduzcan o extraigan, sin la debida autorización, en los lugares donde se trabaje con Información Oficial Clasificada, medios de comunicación, de computación y sus soportes o cualesquiera otros medios capaces de contener, grabar o reproducir información,
c) introducir o extraer cámaras fotográficas o de filmación, grabadoras, videos, bultos o paquetes, sin la debida autorización,
d) tomar fotos, filmar o ejecutar obras artísticas, en lugares de interés para la defensa, sin la debida autorización y control,
e) obtener sin autorización, copias de llaves de locales o muebles donde obre Información Oficial Clasificada.

2. Se prohíbe además tomar fotos, filmar o ejecutar obras artísticas a los edificios o instalaciones que a continuación se mencionan, salvo que medie autorización expresa de la autoridad competente:

a) órganos, organismos, entidades o dependencias, donde se elaboren productos de interés para la defensa, o se experimenten tecnologías de

producción de elementos que se consideren innovaciones en el proceso tecnológico científico;
b) construcciones militares de cualquier índole, polígonos, aeropuertos y puertos militares, con la excepción de los que se determinen por el gobierno que tienen carácter público. La prohibición regirá también cuando las obras se encuentren en proceso de construcción;
c) armamento militar y técnica de combate con las excepciones de los mostrados en los desfiles militares; y
d) las construcciones militares, el armamento y la técnica de combate sólo podrán ser filmados o fotografiados por el personal militar autorizado en operaciones de servicio.

CAPITULO XI

REGULACIONES RELATIVAS A LAS PERSONAS CON ACCESO A LA INFORMACION OFICIAL CLASIFICADA Y LIMITADA

SECCION PRIMERA

Regulaciones para la salida al exterior del personal con acceso a Información Oficial Clasificada y Limitada

ARTICULO 61: El personal con acceso a la Información Oficial Clasificada para salir al exterior en viaje turístico, problemas familiares o cualquier otro motivo personal, debe obtener la aprobación previa de los niveles de dirección que se establecen en este Reglamento.

ARTICULO 62.1: Corresponde autorizar la salida temporal o definitiva al exterior por cualquier motivo, a personas con acceso a Información Oficial Clasificada, en correspondencia con la categoría de clasificación a los niveles siguientes:

SECRETO DE ESTADO: En los órganos y organismos el miembro del Consejo de Ministros que atiende el órgano u organismo que genere la información. Para la Fiscalía General de la República y el Tribunal Supremo Popular el Consejo de Estado.

SECRETO - CONFIDENCIAL: El máximo dirigente del órgano, organismo o entidad. Aquellas entidades que organizativamente estén integradas a un órgano u organismo central esta facultad le corresponderá al máximo dirigente de éstos.

2. Cuando el motivo de la salida al exterior se deba a las funciones propias del cargo que desempeña la persona, la autorización corresponde al máximo dirigente del órgano, organismo o entidad.

3. En todos los casos cuando el acceso sea a la Información Oficial Limitada, cada órgano, organismo, entidad o dependencia definirá los niveles de dirección que autorizan la salida al exterior por cualquier motivo.

SECCIÓN SEGUNDA

Regulaciones al personal con acceso a Información Oficial Clasificada

ARTICULO 63: El personal con acceso a Información Oficial Clasificada solo podrá tener relaciones de trabajo directas, incluidas las entrevistas, o por correspondencia con ciudadanos o representantes de instituciones extranjeras, residentes o no en el territorio nacional, así como con miembros de la comunidad cubana en el exterior, cuando esté autorizado por el dirigente máximo del órgano, organismo o entidad o por los funcionarios en quienes delegue.

ARTÍCULO 64: El personal con acceso a Información Oficial Clasificada deberá solicitar la autorización correspondiente para:

a) tener relaciones personales, por correspondencia u otros medios de comunicación con ciudadanos o representantes de instituciones extranjeras residentes o no dentro o fuera del territorio nacional, así como con miembros de la comunidad cubana en el exterior, y

b) tener relaciones personales, por correspondencia u otros medios de comunicación con estaciones de radio o televisión, órganos de prensa, publicaciones u otras instituciones similares radicadas en el extranjero o con sus representantes en el territorio nacional.

ARTICULO 65: Corresponde la facultad de autorizar las solicitudes a que se refiere el artículo anterior a los mismos niveles de dirección que se establecen en el Artículo 9 de este Reglamento, a los efectos que se corresponda con la categoría de clasificación de la información oficial a la que el solicitante tiene acceso.

ARTICULO 66: Todo equipo o artículo que se obtenga en donación, obsequio o compra, antes de ser utilizado para procesar información oficial, dentro o fuera del territorio nacional, debe informarse al Jefe inmediato superior con el fin de tomar las medidas técnicas y de revisión correspondientes.

CAPITULO XII

DE LA ATENCIÓN A LOS VISITANTES NACIONALES O EXTRANJEROS

ARTICULO 67: Los órganos, organismos, entidades y sus dependencias, establecerán condiciones adecuadas para recibir y atender a diplomáticos y representantes, periodistas, comerciantes, turistas extranjeros y cualesquiera otras personas que en calidad de visitantes acudan a sus instalaciones, de manera que no tengan acceso a la Información Oficial Clasificada o Limitada, cuando no cuenten con la autorización del nivel de dirección facultado para ello.

CAPITULO XIII

SOBRE LA SUPERVISION DE LA SEGURIDAD Y PROTECCION A LA INFORMACION OFICIAL

SECCION PRIMERA
De la supervisión a la información oficial

ARTICULO 68: Se entiende por supervisión de la seguridad y protección a la información oficial la acción de comprobar el cumplimiento de las medidas establecidas en el Decreto Ley, este Reglamento y en las disposiciones complementarias para su ejecución.

ARTICULO 69: La supervisión de la seguridad y protección a la información oficial se realizará mediante controles, inspecciones y auditorías.

ARTICULO 70: La supervisión a la información oficial tiene los objetivos siguientes:

a) comprobar y evaluar el cumplimiento de la política establecida en el Decreto Ley No. 199/99, de las medidas reguladas en este Reglamento y demás disposiciones complementarias dictadas para su ejecución.
b) evaluar el nivel de conocimientos, control y aplicación de la base legal y reglamentaria establecida por parte del personal dirigente y administrativo de los órganos, organismos, entidades y dependencias objetos de supervisión.
c) identificar las amenazas, riesgos y vulnerabilidades que presenta el sistema de seguridad y protección de la información oficial y las posibilidades de acceso de personas no autorizadas y de los Servicios Especiales Extranjeros.
d) valorar la gestión, atención, control e influencia que ejercen las instancias y niveles superiores sobre esta materia; y
e) detectar la existencia de informaciones de valor sin clasificar, pérdidas y extravíos de documentos clasificados y demás violaciones de las medidas de seguridad y protección de la información oficial y aplicar las medidas disciplinarias y multas que correspondan conforme a la Ley y los Reglamentos.

SECCIÓN SEGUNDA
El Control

ARTICULO 71: El control constituye una forma de supervisión que se organiza por distintos niveles del Estado, del órgano, organismo o entidad a sus dependencias y por los órganos especializados del Ministerio del Interior, con el propósito de comprobar el cumplimiento de las medidas y normas establecidas que rigen la seguridad y protección de la información oficial.

ARTÍCULO 72.1: El Jefe, Especialista y Técnico de Seguridad y Protección de los órganos, organismos y entidades, podrán realizar controles a las entidades y dependencias subordinadas, pudiendo aplicar el régimen contravencional si están expresamente facultados por la legislación vigente.

2. El Jefe de la Oficina para el Control de la Información Oficial Clasificada (OCIC) o persona responsabilizada está facultada para realizar controles en las áreas bajo su atención.

ARTICULO 73: Una vez concluido el control se aplicarán las medidas disciplinarias correspondientes, y se fijará el plazo para erradicar las deficiencias señaladas.

SECCIÓN TERCERA
La Inspección

ARTICULO 74.1: La inspección constituye una forma de supervisión que se efectúa periódicamente por Inspectores del Ministerio del Interior con el propósito de verificar el estado de cumplimiento de las medidas que regulan la seguridad y protección de la información oficial.

2. La inspección se organiza de acuerdo a los intereses del órgano o instancia que la realiza.

ARTICULO 75: La inspección se programa, organiza y comunica oportunamente, o puede realizarse de forma sorpresiva, o ante la detección o evidencia de violaciones que aconsejen su realización.

ARTÍCULO 76: Una vez concluida la inspección se aplicarán las medidas correspondientes y se recomendarán las que cada órgano, organismo, entidad o dependencia debe adoptar, así como el plazo que se concede para erradicar las deficiencias señaladas.

ARTICULO 77: Los Inspectores del Ministerio del Interior en las inspecciones que realicen a los órganos, organismos, entidades y dependencias tienen las facultades y atribuciones siguientes:

a) organizar y realizar la inspección con aviso previo o sin él.
b) acceder y revisar todas las informaciones oficiales clasificadas, limitadas y ordinarias existentes en cualquiera de los niveles de dirección de los órganos, organismos, entidades y sus dependencias,
c) determinar responsabilidades e imponer las multas para las que estuviere facultado, a los infractores de las medidas de seguridad y protección de la información oficial conforme a lo establecido en la Ley y sus Reglamentos,
d) proponer sanciones y recomendar medidas administrativas a la dirección de los órganos, organismos, entidades y dependencias que contribuyan a mejorar la eficiencia de la seguridad y protección de la información oficial; y
e) evaluar el estado, organización, control, nivel de cumplimiento, aplicación y funcionamiento de las medidas de seguridad y protección de la información oficial establecida en el Decreto Ley, este Reglamento y demás disposiciones complementarias.

SECCIÓN CUARTA

La Auditoría

ARTICULO 78: La auditoría constituye una forma de supervisión que se efectúa con previo aviso o de modo sorpresivo y se realiza por personal profesional del órgano especializado del Ministerio del Interior, capaz de verificar, comprobar, revisar y evaluar las deficiencias, insuficiencias, amenazas, riesgos y vulnerabilidades existentes en el control y aplicación de las medidas establecidas para la seguridad y protección de la información oficial.

ARTICULO 79: La auditoría a cargo del personal del órgano especializado del Ministerio del Interior comprende la inspección, verificación, control y comprobación en el órgano, organismo, entidad o dependencia auditada de la política, medidas y regulaciones establecidas en el Decreto Ley No. 199, este Reglamento y demás disposiciones complementarias en materia de seguridad y protección de la información oficial.

ARTICULO 80: El personal especializado del Ministerio del Interior en la realización de auditorías a órganos, organismos, entidades y sus dependencias en materia de seguridad y protección a la información oficial, tienen las facultades y atribuciones siguientes:

a) organizar, planear, dirigir y ejecutar auditorías con o sin programas o guías de trabajo previamente elaboradas;
b) determinar la confiabilidad, eficacia y funcionamiento de las medidas de seguridad y protección de la información oficial y verificar su cumplimiento;
c) orientar y supervisar el trabajo y ejercer el control sobre el personal dirigente y administrativo vinculado a la ejecución de la auditoría.

d) solicitar al personal de la entidad auditada, la presentación de informaciones por escrito y declaraciones, acerca de las cuestiones relacionadas con la auditoría; y
e) elaborar informe y dictamen de la auditoría realizada.

CAPITULO XIV
SOBRE LAS DISPOSICIONES COMPLEMENTARIAS PARA LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN OFICIAL.

ARTICULO 81: En todos los órganos, organismos, entidades y dependencias se emitirán dentro del marco de su competencia y sobre la base de lo establecido en el presente reglamento, las disposiciones específicas que permitan el cumplimiento de las medidas de seguridad y protección de la información oficial.

ARTICULO 82: Las disposiciones que complementan el conjunto de medidas de seguridad y protección de la información oficial son las siguientes:

a) Normas y procedimientos para el registro, tramitación y control de la información oficial;
b) El Plan de Evacuación, Conservación y Destrucción de Documentos Clasificados y Limitados para Situaciones Excepcionales y Catástrofes;
c) El Plan de Seguridad y Protección de la Información Oficial Clasificada y Limitada;
d) Instrucciones para los portadores de Información Oficial Clasificada que viajan al exterior;
e) Metodología para la investigación de los hechos;
f) Metodología para la revisión, actualización y elaboración de las Listas Internas de Clasificación y Desclasificación de la Información Oficial;
g) Procedimientos para la divulgación de la información oficial.

SEGUNDO: El Viceministro del Interior emitirá las Instrucciones complementarias que resulten necesarias para el cumplimiento del presente Reglamento.

TERCERO: La presente Resolución entrará en vigor a partir de la fecha de su publicación en la Gaceta Oficial de la República.

CUARTO: Comuníquese a los Jefes de Organismos de la Administración Central del Estado, Presidentes de Institutos, al Presidente del Tribunal Supremo Popular, al Fiscal General de la República, dirigentes de las Organizaciones Políticas y de Masas, a los Presidentes de los Consejos de las Administraciones Provinciales y del Municipio Especial Isla de la Juventud y a cuantas personas naturales o jurídicas corresponda.

Dada en Ciudad de La Habana a los _26___ días del mes de__diciembre____ del año 2000 “Año del 40 Aniversario de la decisión de Patria o Muerte”.

Ministro del Interior

General de Cuerpo de Ejército

Abelardo Colomé Ibarra

Reg. AO4321

Anexo 3: ¿Cómo activar el soporte https para páginas web en el IIS?

Para activar el soporte https para páginas web en IIS se deben seguir los siguientes pasos:

1. En la consola de administración del IIS, se selecciona propiedades del "Sitio Web predeterminado" (Default Web Site), en la pestaña de Seguridad, se accede a "Certificado de servidor..." (Server Certificate...).
2. Se abre un asistente, en el que se debe seleccionar "Crear un certificado nuevo" (Create a new certificate) y en la siguiente pantalla "Preparar la petición ahora pero enviarla más tarde" (Prepare the request now, but send it later).
3. A continuación se escoge como longitud de clave 2048 bits y se proveen todos los datos necesarios. De este paso se obtiene una petición de certificado "certreq.txt".
4. Para obtener un certificado, se debe emitir usando el sistema de gestión de seguridad propuesto que parte del uso de OpenSSL. Ver anexo 2.
    a. Generar la clave privada: *openssl genrsa -des3 -out clavePrivada.pem 2048* (pedirá una contraseña para proteger la clave).
    b. Crear el certificado digital con la información pertinente: *openssl req -new -x509 -key clavePrivada.pem -out certificado.pem -days 3650* (Certificado válido durante 10 años, *3650 días*).
    c. Crear el certificado para el solicitante: *openssl x509 -req -days 3650 -in certreq.txt -CA certificado.pem -CAkey clavePrivada.pem -CAcreateserial -out certificado.crt*
5. En la ventana de certificados del IIS seleccionar la opción de "Procesar la petición pendiente e instalar el certificado".

6. En la siguiente pantalla del asistente indicar la ruta del certificado creado (certificado.cer) y finalizar el proceso.

Anexo 4: ¿Cómo restringir el acceso a los subsistemas por https?

Para restringir el acceso a los subsistemas por https se deben seguir los siguientes pasos:

1. Acceder a las propiedades de la aplicación en la consola de administración del IIS.
2. En la pestaña de seguridad pulsar el botón editar en el apartado "Comunicaciones seguras" y marcar la casilla "Requerir canal seguro (SSL)" (Require secure channel (SSL).

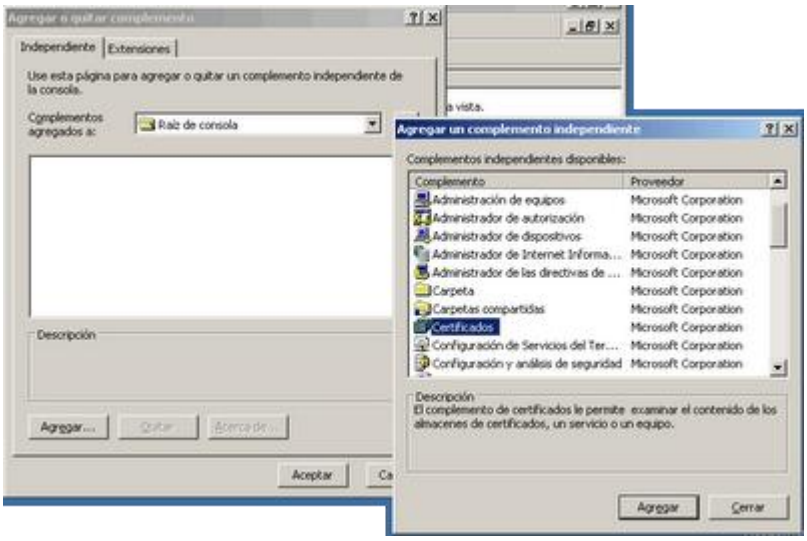
Anexo 5: ¿Cómo configurar IIS para requerir y aceptar certificados de los clientes generados?

Para requerir el certificado del cliente se debe ir al "Administrador de Servicios de IIS", buscar el recurso, sitio web o directorio virtual que necesitará certificado y pulsar en "Propiedades" del menú contextual. En la pestaña "Seguridad de Directorios" pulsar sobre el botón "Modificar" de la parte inferior. Aparecerá la siguiente pantalla:

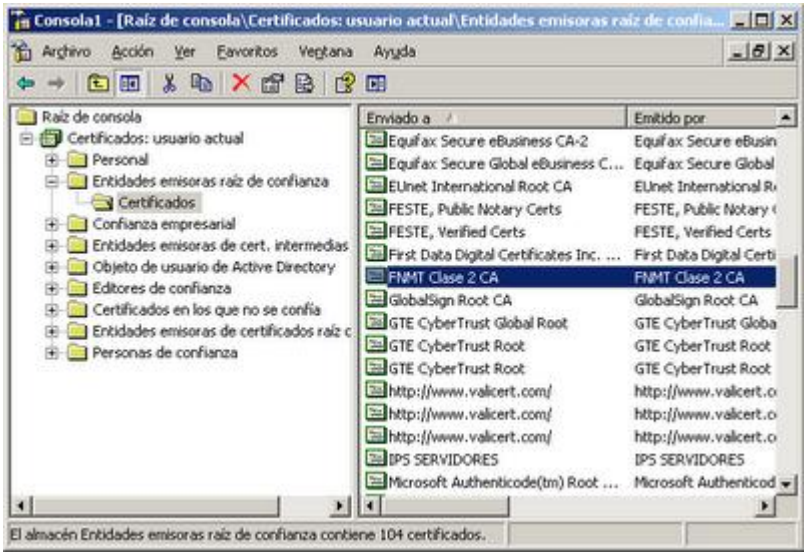
Marcar la opción "Requerir Canal Seguro" y "Requerir Certificados de Cliente". Pulsar sobre Aceptar. Ahora el IIS espera un certificado del cliente para acceder al recurso, sin embargo, todavía no se ha especificado que debe confiar en GeSeg como entidad certificadora. Ver anexo 4.

Anexo 6: ¿Cómo especificar que se confíe en el GeSeg como entidad certificadora?

Abrir una consola mmc (Ejecutar--> mmc), Archivo-->Agregar o Quitar Complemento. En la pantalla que aparece pulsar de nuevo sobre Agregar y seleccionar el complemento "Certificados":



Pulsar sobre "Agregar", seleccionar la opción "Mi Cuenta de usuario" y cerrar la pantalla de agregar complementos. En la consola mmc, expandir "Entidades emisoras raíz de confianza-->Certificados" y buscar al GeSeg:



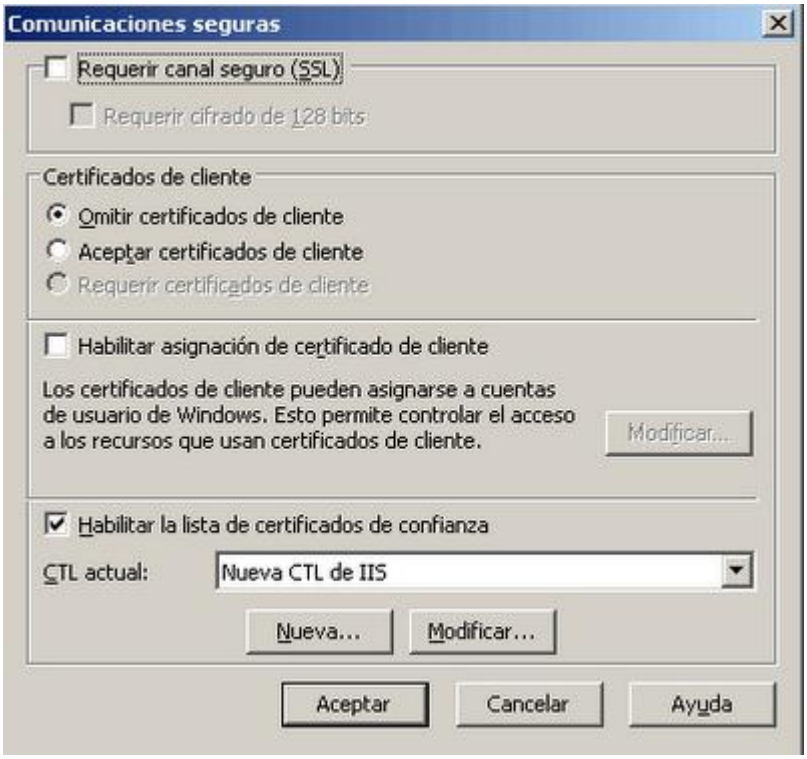
En caso que no esté, pulsar con el botón derecho sobre "Certificados" y elegir "Todas las tareas-->Importar". Saltará un asistente para importar un certificado, seleccionar el fichero generado por GeSeg y siguiente hasta el final.

Una vez importado, ver las propiedades del certificado y habilitar la opción "Autenticación del Cliente". De esta forma se habilitan los certificados que sirvan como certificados de cliente.

Con esto se ha dado confianza al GeSeg como entidad certificadora (CA Root), sin embargo, todavía no funciona porque se debe incluir al GeSeg como entidad válida para el sistema, en la CTL (Certificate Trusted List). Ver anexo 5.

Anexo 7: ¿Cómo incluir al GeSeg como entidad certificadora válida del Sistema?

Abrir la consola del IIS e ir a las propiedades del sistema certificado. Seleccionar la pestaña "Seguridad de Directorios" y pulsar sobre el botón "Modificar" de la parte inferior. Aparecerá la pantalla siguiente:



En la parte inferior se tiene la lista de certificados de confianza, pulsar sobre "Modificar" y en la lista que aparece, pulsar sobre "Agregar desde el almacén" e incluir el del GeSeg. Pulsar "Siguiente" hasta el final.

Glosario de términos.

Organización Internacional para la Estandarización: La Organización Internacional para la Normalización, o ISO por sus siglas en inglés, nace el 23 de febrero de 1947. Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

ISO es una red de los institutos de normas nacionales de 160 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra, Suiza, que coordina el sistema. Está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental.

Infraestructura de clave pública: En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

Certificado digital: Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

El certificado contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Protocolo: Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras distintas, dos de ellas conectadas en la misma red pero con protocolos diferentes no podrían comunicarse jamás.

HTTP: El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web. HTTP define la

sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

XML: siglas en inglés de Extensible Markup Language (lenguaje de marcas), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C).

SMTP: Simple Mail Transfer Protocol (SMTP), Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

Hibernate: es una herramienta de Mapeo objeto-relacional para la plataforma Java que facilita el mapeo de atributos entre una base de datos relacional tradicional y el modelo de objetos de una aplicación, mediante archivos declarativos (XML) que permiten establecer estas relaciones.

NHibernate: es la conversión de Hibernate de lenguaje Java a C# para su integración en la plataforma .NET.

Framework: es una estructura de soporte definida, mediante la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, puede incluir soporte de programas, bibliotecas y un lenguaje interpretado entre otros software para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

Sistema Operativo: Un sistema operativo es un software de sistema, es decir, un conjunto de programas de computación destinados a realizar muchas tareas entre las que destaca la administración eficaz de sus recursos.

API: representa una interfaz de comunicación entre componentes software. Se trata del conjunto de llamadas a ciertas bibliotecas que ofrecen acceso a ciertos servicios desde los procesos y representa un método para conseguir abstracción en la programación, generalmente (aunque no necesariamente) entre los niveles o capas inferiores y los superiores del software. Uno de los principales propósitos de una API consiste en proporcionar un conjunto de funciones de uso general, por ejemplo, para dibujar ventanas o iconos en la pantalla.

Programación Orientada a Objetos (POO): es un paradigma de programación que usa objetos y sus interacciones para diseñar aplicaciones y programas de computadora. Está basado en varias técnicas, incluyendo herencia, modularidad, polimorfismo y encapsulamiento. Su uso se popularizó

a principios de la década de 1990. Actualmente son muchos los lenguajes de programación que soportan la orientación a objetos.

GUI: La interfaz gráfica de usuario (en Idioma inglés Graphical User Interface, GUI) es un tipo de interfaz de usuario que utiliza un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz. Habitualmente las acciones se realizan mediante manipulación directa para facilitar la interacción del usuario con la computadora.

Microsoft Corporation: es una empresa multinacional estadounidense, fundada en 1975 por Bill Gates y Paul Allen. Dedicada al sector de la informática, con sede en Redmond, Washington, Estados Unidos. Microsoft desarrolla, fabrica, licencia y produce software y equipos electrónicos. Siendo sus productos más usados el Sistema operativo Microsoft Windows y la suite Microsoft Office.

GNU GPL: La Licencia Pública General Reducida de GNU, o más conocida por su nombre en inglés GNU Lesser General Public License es una licencia de software creada por la Free Software Foundation. Los contratos de licencia de la mayor parte del software están diseñados para jugar con su libertad de compartir y modificar dicho software.

URL: significa Uniform Resource Locator, es decir, localizador uniforme de recurso y se refiere a la dirección única que identifica a una página web en Internet.

Indentación: es un anglicismo (de la palabra inglesa indentation) de uso común en informática. Significa mover un bloque de texto hacia la derecha insertando espacios o tabuladores para separarlo del texto adyacente.

En los lenguajes de programación de computadoras, se utiliza para mejorar la legibilidad del código fuente por parte de los programadores, teniendo en cuenta que los compiladores o intérpretes raramente consideran los espacios en blanco entre las sentencias de un programa. Sin embargo, en ciertos lenguajes de programación como Haskell, Occam y Python, la indentación se utiliza para delimitar la estructura del programa permitiendo establecer bloques de código.

Métrica: es cualquier medida o conjunto de medidas destinadas a conocer o estimar el tamaño u otra característica de un software o un sistema de información, generalmente para realizar comparativas o para la planificación de proyectos de desarrollo. Un ejemplo ampliamente usado es la llamada métrica de punto función.