SEGURIDAD EN LAS TIC: IDENTIDAD DIGITAL

SEGURIDAD EN LAS TIC: IDENTIDAD DIGITAL

Aportes desde CENDITEL

E. Mora, A. Araujo, V. Bravo, R. Sumoza
Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

CENDITEL
Ministerio para el Poder Popular para la Ciencia, Tecnología e Innovación

Publicación de la Fundación CENDITEL

Publicado por Fundación CENDITEL - MPPCTI.

Aquí deberíamos escribir la licencia de CENDITEL

Publicaciones de CENDITEL:

Seguridad en las TIC: Identidad Digital / Endira Mora . . . [et al.].
p. cm.—(Documentos CENDITEL)
"Licencia CENDITEL."
Incluye referencias bibliográficas e índice.
ISBN X-YYY-XYXYX-X (pbk.)
1. Referencia—Metodología. 2. Investigación

Impreso en la Repúblia Bolivariana de Venezuela.

10 9 8 7 6 5 4 3 2 1

A la creatividad

CONTRIBUYENTES

SUCERTE Superintendencia de Servicios de Certificación Electrónica
MPPCTI Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación

LISTA BREVE DE CONTENIDOS

CONTENIDOS

PARTE II APORTES DE CENDITEL EN LA SEGURIDAD VINCULADA A LA IDENTIDAD DIGITAL EN LAS TIC

LISTA DE FIGURAS

LISTA DE TABLAS

PRÓLOGO

Prólogo

PREFACE

Prefacio

RICHARD STALLMAN

Manhattan, Nueva York, Estados Unidos
Julio, 2014

AGRADECIMIENTOS

Le agradecemos a todos: ¡GRACIAS!

E. A. V. R.

ACRÓNIMOS

ISO	International Standard Office

GLOSARIO

Anonimato	Aun muy incomprendido.
Identidad	Sinónimo de cultura y algo. hgjgjk hhj jhhhj
Firma electrónica	Rúbrica hecha con ceros y unos

S˝MBOLOS

A Amplitud
& Símbolo lógico proposicional

$\mathcal{B}$ Número de pulsaciones

INTRODUCCIÓN

LINUS TORVALDS, ING.

Universidad de Helsinki
Finlandia

Aquí va todo el chalalá de la introducción para el índice. Aquí están dos citas: Una: [**?**] y la otra: [**?**].

Más chalalá.

$$ABCDEF\alpha\beta\Gamma\Delta \sum_{def}^{abc} \tag{I.1}$$

REFERENCIAS

1. J. S. Kilby, "Invention of the Integrated Circuit," *IEEE Trans. Electron Devices,* **ED-23,** 648 (1976).
2. R. W. Hamming, *Numerical Methods for Scientists and Engineers*, Chapter N-1, McGraw-Hill, New York, 1962.
3. J. Lee, K. Mayaram, and C. Hu, "A Theoretical Study of Gate/Drain Offset in LDD MOSFETs" *IEEE Electron Device Lett.,* **EDL-7**(3). 152 (1986).

PARTE I

FUNDAMENTOS

CAP´TULO 1

BASES DE LA IDENTIDAD DIGITAL

A. Araujo, V. Bravo y R. Sumoza

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

1.1 Conceptos básicos

Identidad Digital - ID

1. Es el conjunto de datos que describen y representan a un sujeto: persona, grupo de personas o cosas de manera única. Puede contener información sobre gustos, creencias, relaciones, tendencias, ideologías, y cualquier otro descriptor vinculado al sujeto.
2. Es la suma de toda la información disponible en formato digital de un sujeto (persona, grupo de personas, cosas).
3. Puede ser explicada como una percepción única o exclusiva de vida, con su integración a un grupo social, y con continuidad, la cual está acotada y formada por una sociedad. La identidad puede estar ligada a cualquier sujeto, ya sean seres humanos, personas jurídicas,y dispositivos electrónicos.

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

4. La identidad es un conjunto de atributos pertenecientes a un individuo que permiten diferenciarlo del resto de individuos que forman parte de un conjunto determinado. Por esta razón no existe una identidad única y universal, sino que pueden existir varias para un mismo individuo, según el conjunto y contexto al que se haga referencia. Incluso los valores de los atributos y los atributos mismos pueden cambiar en el tiempo.
5. La identidad digital denota la atribución de propiedades a una persona,los cuales son, desde el punto de vista técnico, operacionalmente accesible de forma inmediata, por su característica digital. El identificador de una identidad parcial digital puede ser una dirección de correo electrónico en un grupo de noticias o en una lista de correos.

Identidad Parcial

La identidad de cada persona está compuesta por muchas identidades parciales, las cuales representan a la persona en un contexto o rol específico. De esta forma, una identidad parcial es un subconjunto de atributos del conjunto que compone la identidad completa, formada por la unión de todos los atributos de esta persona. Desde un punto de vista técnico, estos atributos constituyen datos. Como se mencionó anteriormente estos atributos y los valores de la identidad parcial pueden variar en el tiempo. Un seudónimo puede considerarse como una identidad parcial. A pesar de que una identidad parcial no permite caracterizar a un individuo de forma única dentro de un conjunto específico, si puede, según la cantidad de atributos contenidos en el subconjunto, hacer posible tener varios contextos de aplicación del anonimato.

Identidad Virtual

Algunas veces se utiliza como sinónimo de identidad digital, pero dada su connotación de no-real, aparente y no-existente, este término es utilizado principalmente en ambientes multi-usuarios, o multi-jugadores masivos, es decir, en entornos de juegos virtuales.

Sociedad Digital

Es concepto moderno de sociedad progresiva que se forma como resultado de la adopción e integración de las TIC en ámbitos de hogar, de trabajo, de educación, de recreación. Las personas interactúan a través de diversos tipos de actividades, como el pago de los diversos servicios públicos, la gestión de sus cuentas, el pago de los impuestos, el acceso a información de su interés, el registro de empresas, obtención de tarjetas de identificación, autenticación, transacciones financieras, registros médicos, situación laboral, revisión de oportunidades de empleo, etc.

Rol

Desde el punto de vista de la sociología un rol o rol social constituye un conjunto de acciones conectadas o relacionadas, conceptualizadas por los actores en una situación social. Es frecuente definirlo como un comportamiento esperado en un contexto individual social dado.

Manejo de la ID

Con estas definiciones de identidad digital se logra distinguir entre dos instancias de los sujetos, la primera que les permite definirse asimismo (autodefinición interior y personal), y la segunda que los define en un contexto social con sus respectivos atributos, y que se mantiene para darles la posibilidad del acceso a la comunicación y que los ata de cierta manera a un control y un grado de consistencia con respecto al resto. La identificabilidad es el estado de ser identificable dentro de una conjunto de sujetos, que es el conjunto identificable.

El manejo de la ID implica la gestión de varias identidades parciales (usualmente denotadas por seudónimos) de un individuo. El establecimiento de la reputación es posible o cuando un individuo re-utiliza las identidades parciales. Un pre-requisito para la selección de una identidad parcial es el de conocer el contexto en el que la persona está actuando.

Sistema de manejo de la identidad

La tecnología basada en el manejo de la identidad en su esencia más amplia, se refiere a la administración y diseño de los atributos de las identidades. Se puede distinguir entre un sistema de manejo de identidad y una aplicación para el manejo de la identidad: La primera puede ser entendida como una infraestructura, y la segunda como un conjunto de componentes coordinados entre sí. Las aplicaciones para el manejo de la identidad son herramientas para manejar individualmente sus comunicaciones relevantes, las cuales pueden ser configuradas y operadas en el lado de los usuarios o en el lado de los servidores. El manejo de la identidad, soportado técnicamente, tiene que autorizar a los usuarios para reconocer diferentes tipos de comunicaciones o situaciones sociales, y acceder a ellas con respecto a su relevancia, funcionalidad y al nivel de riesgo de la privacidad y seguridad en función de hacer y asumir roles de forma adecuada. En general, las aplicaciones para el manejo de la identidad, específicamente en cuanto al manejo de las identidades parciales, representan los diferentes seudónimos con su respectivos datos de acuerdo a los diferentes roles que el usuario ha asumido y de acuerdo a los diferentes patrones de comunicación. En los casos donde se hace explícito el flujo de los datos personales, donde se le permite al usuario tener un mayor grado de control, la guía principal es la de "reconocer y escoger" su propia identidad, y se procura minimizar la cantidad de los datos utilizados. Esto significa que el usuario controla la relacionabilidad de sus datos personales. De acuerdo a una situación y contexto específico, tal sistema le da soporte al usuario en la selección de seudónimos que representen a sus identidades parciales.

Protección de la ID

Confidencialidad, privacidad, anonimato.

Privacidad vinculada a la ID

Anonimato

Seudonimato

No relacionabilidad

No observabilidad

Legislación vinculada a la ID

Firma Electrónica

Certificación Electrónica

1.2 Implicaciones

1.3 Identificación, autenticación

identificación, autenticación...

1.3.1 Técnicas de identificación y autenticación

Técnicas de identificación y autenticación...

1.3.1.1 Contraseñas Una contraseña es una palabra secreta que se utiliza en conjunto con un nombre de usuario o correo electrónico para obtener acceso a determinados recursos de un sistema informático. El sistema informático puede estar en la web, funcionar en un computador sin acceso a red, o ser un hardware dedicado tal como un cajero automático de banco, o un mecanismo de control para el acceso a un lugar físico.

Las contraseñas son quizás, el método más utilizado para identificar a personas en el mundo digital. El acceso al correo electrónico, a una sesión en una computadora, al sitio de un banco en internet, la acción para desbloquear un teléfono móvil, así como actividades que hacemos a diario con la computadora lo utilizan como sistema primigenio y en muchas ocasiones como único procedimiento disponible para este fin.

En primer lugar, para construir un sistema de contraseñas se necesita un almacén de datos, en el cual se guarden los elementos de información vinculados con la clave, y que pueden representar el ámbito de operación de un usuario dentro de un sistema informático, lo cual incluye esquemas de autorización para operar sobre objetos o acciones.

Generalmente los almacenes de datos para los esquemas de contraseñas se construyen usando archivos de texto (por ejemplo el usado por los sistemas Linux o Unix

que es un archivo */etc/passwd* o */etc/shadow*), o también es muy frecuente utilizar un conjunto de relaciones u objetos en una base de datos.

Algunas de las reglas básicas para almacenar contraseñas se muestran a continuación:

- Utilizar un nivel alto de seguridad para el resguardo de la base de datos acorde con las reglas generales de administración de servidores, sistemas de cómputo embebido o cualquier otro tipo de sistema donde resida el almacén de datos.
- No guardar las contraseñas en texto plano, en cambio utilizar algoritmos (con la suficiente fortaleza a ataques) de una sola vía para transformar las claves que ingrese el usuario
- Implementar políticas y protocolos de creación y asignación de claves tales como: vinculación a dos o más correo electrónico; prueba de fortaleza de contraseñas; monitorear los accesos de los usuarios por lugar, frecuencia; operaciones entre otras.
- Realizar auditorias periódicas a todo el proceso de gestión de claves.

Uno de los objetivos que debe tener cualquier sistema de protección es proveer al usuario de instrumentos para mejorar su interacción con los sistemas informáticos, descargándolo de tareas engorrosas o difíciles, sin que esta prerrogativa desmejore significativamente los niveles de seguridad. En este sentido, actualmente están disponibles varias tecnologías vinculadas con la gestión de contraseñas, que generalmente son implementadas por todos los navegadores para internet, Entre ellas están:

- **cookies**: son pequeñas cápsulas de información sobre los datos de acceso a una aplicación (sesión) .
- **recordación de claves**: Es una lista donde se encuentran asociadas las claves y usuarios con los sitios que se visitan en internet. Cuando el usuario visita un sitio que se encuentra en la lista, el navegador ingresa automáticamente el nombre de usuario y su clave en el formulario.
- **Sistemas centralizados o locales de gestión de claves**: son aplicaciones en la web o de uso local (computadora,tableta o teléfono móvil) para gestionar las claves de todos los sistemas al que el usuario ingresa desde sus dispositivos digitales.

Por otro parte, para que una contraseña sea resistente a ataques de fuerza bruta, debe contar con varias propiedades. Muchos sistemas validan las claves antes de que sean asignadas, pero no pueden asegurar de forma completa que la contraseña es inviolable dado que mucho de la responsabilidad de uso reside en el propietario de la clave: el usuario.

Generalmente para que una contraseña sea considerada fuerte, debe tener por lo menos las siguientes propiedades:

- Ser lo suficiente larga. Hoy en día, se considera ocho (8) caracteres la extensión mínima de una contraseña para la mayoría de los sistemas informáticos, este número puede disminuir si se acompaña con el uso de una tarjeta o elemento físico seguro (*token*).
- No ser una palabra de diccionario.
- Estar compuesta por letras minúsculas y mayúsculas,

Muchos sistemas informáticos cuentan entre sus políticas el cambio periódico de claves por parte de los usuarios, con respecto a ello Schneier en **??** considera que la política citada puede ser contraproducente y no se recomienda, debido a que si ya se cuenta con una contraseña fuerte no existe la necesidad de cambiarla.

Las contraseñas como método de control de acceso seguirá siendo por lo menos por unos cuantos años más el método más popular, por lo tanto se hace necesario prestar atención en los aspectos de gestión organizacional y técnica de este tipo de herramienta, logrando conectar de manera eficiente las políticas con las aplicaciones y con las personas, tomando en cuenta que no se debe disminuir la ergonomía significativamente en pro de la seguridad.

1.3.1.2 Certificados electrónicos A una persona que desea realizar un trámite o solicitar un servicio en una institución pública o privada generalmente se le exige que demuestre su identidad para ser atendido. La manera común en la que se demuestra la identidad de un individuo es a través de su documento de identidad o Cédula de Identidad. Por ejemplo, un pensionado del seguro social debe presentar su cédula de identidad para retirar dinero de su cuenta de banco, así como un solicitante de un préstamo para adquisición de vivienda principal debe presentar, entre otros requisitos, su cédula de identidad.

Todas las personas utilizan la cédula de identidad como un documento físico que garantiza su identidad ante otras personas, instituciones, empresas e inclusive ante otros países. En la figura 1.1 se muestra una cédula de identidad de un ciudadano de la República Bolivariana de Venezuela.

Figura 1.1 Cédula de identidad de la República Bolivariana de Venezuela.

En la sociedad digital en la que se desenvuelven los individuos en la actualidad, es necesario utilizar algún mecanismo que permita establecer su identidad digital.

Una alternativa es el certificado electrónico. Éste es un documento electrónico que tiene el objetivo de garantizar la veracidad de un conjunto de datos digitales. Así como la cédula de identidad incluye datos de una persona como nombres, apellidos, fecha de nacimiento y estado civil, los certificados electrónicos incluyen campos que permiten establecer la identidad digital de su titular y tienen un periodo de validez.

La cédula de identidad es emitida por una institución de gobierno en la que los ciudadanos confían siguiendo estándares que la hacen difícil de falsificar. Para los certificados electrónicos se busca mantener estas mismas características al ser emitidos por una entidad en la que tanto individuos como sistemas informáticos van a confiar.

Los certificados electrónicos son un elemento fundamental en el modelo de confianza denominado *Infraestructura de Clave Pública* (ICP). Este modelo describe una tecnología utilizada para establecer identidades a través de certificados electrónicos y permitir el intercambio de información segura entre partes que se comunican. La ICP agrupa programas o software, piezas de hardware y documentación relacionada a políticas para establecer lo que se puede hacer o no con certificados electrónicos.

Los certificados electrónicos están basados en la **criptografía**[1] de clave pública. Este tipo de criptografía se aprovecha del uso de un par de claves con características muy particulares para transmitir información de manera segura entre entidades que se comunican.

En una comunicación entre dos personas cada una genera un par de claves. El par de claves es tal que se complementan entre ellas; una porción de la clave va a ser conocida por las personas con quien se desea establecer la comunicación, llamada *clave pública*, y la otra porción de la clave va a ser secreta y protegida por el titular, llamada *clave privada*.

En la República Bolivariana de Venezuela existe una ICP jerárquica denominada *Infraestructura Nacional de Certificación Electrónica* y establecida en la Providencia Administrativa Número 016 del 05 de Febrero de 2007 de la Gaceta Oficial Número 38.636[2]. Esta jerarquía es supervisada y controlada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)[3], organismo adscrito al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación.

La *Infraestructura Nacional de Certificación Electrónica* está compuesta por los siguientes elementos:

- Autoridad de Certificación (AC) Raíz del Estado Venezolano. Primera autoridad de la infraestructura y se encarga de emitir, renovar, revocar y suspender los certificados electrónicos de los Proveedores de Servicios de Certificación.

- Autoridades de Certificación de los Proveedores de Servicios de Certificación (PSC). Entidades subordinadas a la Autoridad de Certificación Raíz del Estado Venezolano y se encarga de emitir, renovar, revocar y suspender los certificados

[1] AGREGAR EL CONCEPTO EN EL GLOSARIO
[2] http://www.tsj.gov.ve/gaceta/gacetaoficial.asp
[3] http://suscerte.gob.ve/

electrónicos a los signatarios y a sus Autoridades de Certificación subordinadas, en caso de tenerlas.

- Autoridades de Registro de los Proveedores de Servicios de Certificación. Entidades encargadas de controlar la generación de los certificados electrónicos de sus Autoridades de Certificación y comprobar la veracidad y exactitud de los datos suministrados por los signatarios. Generalmente las Autoridades de Registro y las Autoridades de Certificación de los PSC son vistos como una sola entidad de la ICP.

- Signatarios o titulares de certificados electrónicos emitidos por los PSC.

En la figura 1.2 se muestra un bosquejo de la Infraestructura Nacional de Certificación Electrónica.

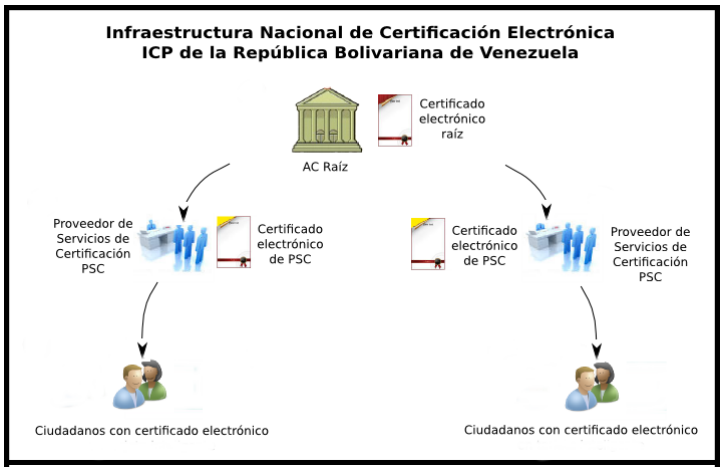

Figura 1.2 Infraestructura Nacional de Certificación Electrónica.

Cuando una persona desea obtener una identidad digital en la Internet puede recurrir a un PSC para que le venda y/o asigne un certificado electrónico de acuerdo a sus respectivos documentos de políticas de certificados y declaración de prácticas de certificación. Estos documentos establecen las normas y usos de los certificados electrónicos emitidos por cada Autoridad de Certificación. Hasta el momento de publicación de este libro, los PSC acreditados ante la SUSCERTE son los siguientes:

- Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico[4], organismo adscrito al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación.

[4]https://ar.fii.gob.ve

- Proveedor de Certificados (PROCERT[5]), C.A., primera entidad privada dentro de la República Bolivariana de Venezuela en ser acreditada ante el Estado Venezolano.

Los certificados electrónicos se utilizan principalmente para:

- Autenticación de usuarios. Los certificados electrónicos permiten demostrar la identidad digital de un usuario.
- Enviar y recibir información cifrada con terceros. Los certificados electrónicos de destinatarios permiten enviar información cifrada a través de algoritmos criptográficos.
- Firmar electrónicamente documentos. Se utiliza la clave privada asociada a un certificado electrónico para firmar electrónicamente cualquier documento electrónico.

Cuando existe una legislación asociada a los certificados electrónicos, éstos pasan a tener vinculación legal con la identidad de su titular a través de su firma electrónica. En el caso de la República Bolivariana de Venezuela, el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas electrónicas promulgado en el año 2001[6], crea mecanismos para que la firma electrónica tenga las misma eficacia y valor probatorio de la firma escrita a través del uso de certificados electrónicos de la Infraestructura Nacional de Certificación Electrónica. El concepto de firma electrónica se tratará con mayor detalle en la siguiente sección.

Una característica de los certificados electrónicos es que pueden ser emitidos tanto para individuos como para dispositivos de red. Uno de los usos más popular de los certificados es la validación de sitios web o nombre de dominio en la Internet, por ejemplo: *www.gobiernoenlinea.gob.ve*. Esto es considerado como una defensa contra acciones de falsificación que buscan tomar datos de los usuarios de estos sitios de manera masiva y que generalmente se coordinan con otros ataques como el *phishing*.

Los navegadores web son una de las principales herramientas utilizadas por los usuarios para tener acceso a la Internet tanto en computadores de escritorio como en dispositivos móviles. Están preparados para identificar los servidores que alojan una página web particular en el caso que se esté usando un certificado electrónico. Con el uso del certificado se intercambia información de manera segura con sus visitantes y además se garantiza que se están comunicando con el servidor correcto y no uno fraudulento.

En la figura 1.3 se muestra una captura de pantalla del sistema de banca en línea de un banco de la República Bolivariana de Venezuela que utiliza un certificado electrónico.

Los navegadores web mantiene un almacén de certificados de autoridades de certificación en las que confían para la emisión de certificados electrónicos. En el caso

[5]https://www.procert.net.ve/acprocert.asp
[6]http://www.tsj.gov.ve/legislacion/dmdfe.htm

Figura 1.3 Sistema de banca en línea que utiliza un certificado electrónico.

de la figura 1.3, el navegador muestra un indicador de color verde sobre la barra de dirección para mostrar al usuario que el certificado electrónico presentado es reconocido como válido. En el caso de que un usuario esté conectado a una página web con un certificado electrónico que el navegador no reconoce, éste último mostrará un mensaje que alerta al usuario de una posible comunicación con un sitio no confiable. El indicador puede variar de un navegador a otro pero mantiene su función de alertar al usuario.

Como resultado de ataques a portales web y algunas fallas de seguridad en la implementación de protocolos, servicios masivos de la Internet como correo electrónico y redes sociales utilizan certificados electrónicos para garantizar la identidad de los servidores con los que se comunican los usuarios e intercambiar la información cifrada.

Aunque un certificado electrónico no es un documento físico, sí es posible ver su contenido. El estándar X.509 versión 3 define los campos que un certificado electrónico tiene. Algunos campos son obligatorios y otros son extensiones que pueden o no aparecer en un certificado particular. A continuación se listan los campos comunes de un certificado electrónico X.509.

- Versión: Describe la versión del certificado codificado. La versión actual es la 3.

- Número de serie: Es un identificador único para el certificado electrónico emitido por una autoridad de certificación.
- Algoritmo de firma: Identificación del algoritmo criptográfico utilizado por la autoridad de certificación para firmar el certificado.
- Emisor: Identificación de la autoridad de certificación que emitió el certificado electrónico.
- Validez: Intervalo de tiempo durante el cual la autoridad de certificación mantiene información sobre el estado del certificado. El período de validez está representado por dos fechas: una fecha a partir de la cual la validez del certificado comienza y otra en la que termina. La validez de un certificado electrónico está definido en la documentación de políticas de certificado de una autoridad de certificación.
- Sujeto: Identificación del titular del certificado electrónico.
- Información de clave pública del sujeto: Mantiene la clave pública del sujeto e identifica el algoritmo con el cual se utiliza la clave.
- Identificador único de emisor:
- Identificador único de sujeto
- Extensiones: Secuencia de una o más extensiones que sirven para asociar atributos adicionales del sujeto.
- Algoritmo de firma de certificado: Identificador del algoritmo criptográfico utilizado por la autoridad de certificación para firmar el certificado electrónico.
- Firma electrónica del certificado: Valor de la firma electrónica del certificado electrónico. Al generar esta firma, la autoridad de certificación certifica la validez de la información.

En la figura 1.4 se muestran los detalles de los campos de un certificado electrónico de la Infraestructura Nacional de Certificación Electrónica visto en un navegador web.

Una forma de distribuir los certificados electrónicos es a través de dispositivos de usuario que permiten proteger los elementos del certificado. En la sección 1.3.1.4 se presentan algunos dispositivos como tarjetas inteligentes y token criptográficos que almacenan certificados electrónicos.

Anexo: Contenido de un certificado electrónico X.509 Versión 3 en formato de texto plano.

```
Certificate:
    Data:
        Version: 3 (0x2)
```

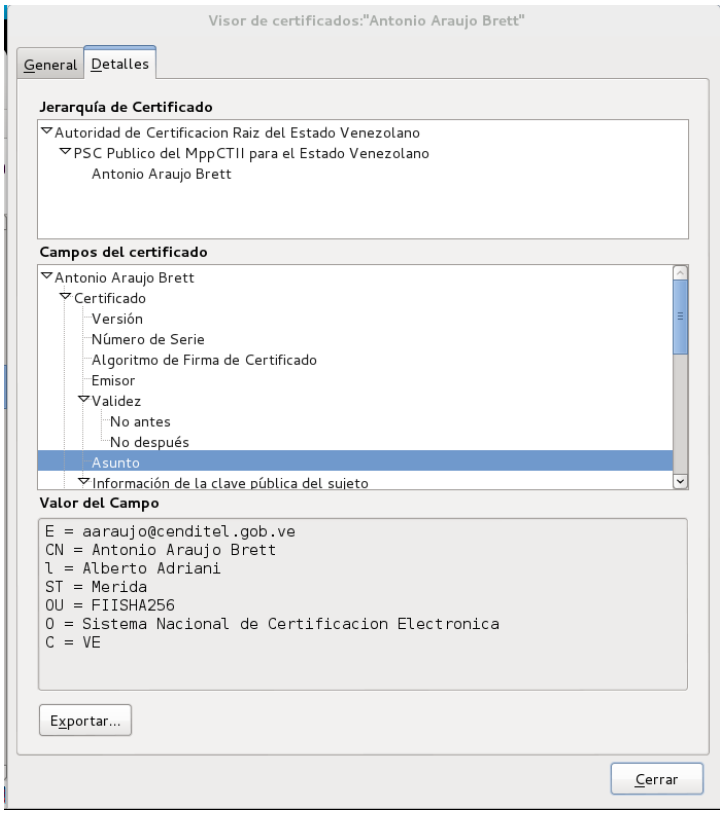

Figura 1.4 Detalles de los campos de un certificado electrónico.

```
    Serial Number: 5357 (0x14ed)
Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=VE, ST=Miranda, L=Baruta, O=Sistema Nacional
    de Certificacion Electronica, OU=Fundacion Instituto de
    Ingenieria, CN=PSC Publico del MppCTII para el Estado
    Venezolano/emailAddress=admin-pki@fii.gob.ve
    Validity
        Not Before: Apr  2 10:40:23 2012 GMT
        Not After : Apr  2 10:40:23 2013 GMT
    Subject: C=VE, O=Sistema Nacional de Certificacion
    Electronica, OU=FIISHA256, ST=Merida, L=Alberto Adriani,
    CN=Antonio Araujo Brett/emailAddress=aaraujo@cenditel.gob.ve
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
```

```
        Modulus:
            00:db:f4:30:58:bc:ce:30:50:9e:44:14:57:d6:eb:
            e9:cd:f6:90:a7:21:ec:b1:0e:73:af:0d:e7:05:1e:
            cd:a6:3b:1e:85:1a:86:1b:12:69:f9:28:28:4c:a0:
            1c:92:09:81:e0:a9:09:40:08:9e:60:89:12:c9:7b:
            96:f3:fd:99:49:52:5f:98:11:41:31:70:60:ca:55:
            de:73:4d:d8:05:c2:ac:d6:1c:9b:9a:2c:74:66:f3:
            e5:fa:ad:48:fc:7d:06:11:72:ed:bc:a4:35:cd:7e:
            50:69:eb:9d:75:01:06:a7:48:e7:58:40:11:0e:41:
            fa:50:03:4f:03:45:67:0d:c7:9a:25:c9:e3:32:86:
            99:64:18:31:d0:19:7d:45:ef:e4:f9:ec:46:12:65:
            7c:61:de:40:2c:c2:4d:2e:ab:dc:27:f2:7b:38:7b:
            81:47:20:ce:4f:6b:3b:a4:be:5b:7a:ef:f7:23:07:
            70:08:c6:6e:7b:4d:a9:6e:a3:c0:5b:0a:09:0d:72:
            ab:1e:cd:a7:f5:28:b4:4f:01:44:63:38:53:96:43:
            1e:8d:a8:9c:13:a2:84:30:44:41:a4:56:7c:7d:58:
            04:a7:58:a8:46:21:a7:16:64:fb:49:c7:0a:bc:7e:
            3a:3d:6a:df:ee:d7:0d:38:00:26:76:44:39:81:20:
            b2:7d
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication, E-mail Protection,
        Microsoft Smartcardlogin
    X509v3 Subject Key Identifier:
        E0:A4:9A:D5:A9:0F:EA:6B:CF:A1:1B:28:74:AD:8E:2A:AE:FD:88:
    X509v3 Authority Key Identifier:
        keyid:AA:94:98:5B:01:C8:17:18:50:28:B5:F6:E1:5F:FB:FC:89:
        DirName:/CN=Autoridad de Certificacion Raiz del
        Estado Venezolano/C=VE/L=Caracas/ST=Distrito
        Capital/O=Sistema Nacional de Certificacion
        Electronica/OU=Superintendencia de Servicios de
        Certificacion Electronica/emailAddress=acraiz@suscerte.go
        serial:0D

    Authority Information Access:
        OCSP - URI:http://publicador-psc.fii.gob.ve:2560/ocsp

    X509v3 Certificate Policies:
        Policy: 2.16.862.2.6
        Policy: 2.16.862.2.7.1
```

```
                CPS: http://publicador-psc.fii.gob.ve/dpc
                CPS: http://publicador-psc.fii.gob.ve/pc

            X509v3 Subject Alternative Name:
                othername:<unsupported>, othername:<unsupported>,
                othername:<unsupported>, othername:<unsupported>
            X509v3 Issuer Alternative Name:
                DNS:fii.gob.ve, othername:<unsupported>
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:https://publicador-psc.fii.gob.ve/crlsha256/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
         22:ca:a7:de:b7:30:27:b6:aa:95:67:c1:68:0a:5b:db:a6:a8:
         b5:ee:0b:b4:14:42:39:b7:d8:c5:13:7a:5b:7d:2d:66:49:54:
         0d:bc:e4:8a:25:b4:c8:af:87:60:9a:b4:22:a5:92:66:b6:4e:
         16:66:26:1d:06:76:1f:2b:af:e1:b0:7f:3f:4c:71:cd:75:99:
         66:14:84:01:da:40:18:40:8e:b3:0e:f8:4a:b6:b0:15:53:ef:
         40:28:69:1e:e9:dd:30:7d:80:22:c3:84:5f:16:d7:12:cf:a6:
         57:67:64:82:9d:b9:9c:43:e3:2b:d2:ed:bd:72:9e:6f:a4:f0:
         5b:6d:16:63:d1:9c:0e:68:eb:dd:45:db:57:7c:95:09:a0:53:
         d6:08:6b:ea:ae:95:24:8a:d1:eb:c7:99:46:f3:17:93:84:6c:
         6b:6b:06:97:3a:77:89:a6:ba:ff:3f:5b:aa:21:d8:55:11:25:
         ba:a7:65:a5:8e:9f:7d:f3:f2:7f:14:6a:af:eb:b0:7e:36:31:
         93:56:f9:0f:19:2f:27:ed:e7:0d:e4:b2:4f:05:f5:26:ad:76:
         c6:b2:b0:0e:4e:9b:e6:7f:5e:65:74:8d:9e:54:4c:6e:4b:aa:
         f1:de:85:86:a0:34:bc:bb:5b:7f:a9:1e:cf:ea:6b:a6:e0:66:
         3a:e2:48:2d:9e:ae:88:7c:69:da:26:26:bb:37:41:56:9a:5b:
         98:78:f6:d2:52:3c:28:9f:dc:5f:01:97:d7:d5:13:b6:00:31:
         07:d1:b4:3d:46:49:2c:68:02:4d:b7:fc:ef:b6:0e:7c:b8:19:
         4a:91:23:11:38:ea:f2:8a:8a:31:b4:1a:b6:34:ab:c3:d0:3a:
         4d:7f:67:ae:ae:04:e1:5e:f4:21:ee:63:83:4e:85:f0:87:13:
         9f:5b:f6:77:bc:90:c2:b7:a3:93:d9:75:d6:70:91:b0:94:4b:
         7f:2d:d7:d3:e6:ef:31:d8:de:54:62:fe:69:c5:10:95:8f:43:
         d6:ce:cf:a9:80:03:9a:87:81:c9:7e:0d:bd:85:2d:3b:11:57:
         7b:e1:88:28:b9:3c:ce:55:70:b0:11:59:34:2c:eb:51:de:15:
         24:42:2e:1a:e5:0a:30:6d:39:93:54:2d:f3:7b:5e:c6:a9:ca:
         b3:3d:13:56:d9:1b:bc:27:31:45:88:3d:e9:b3:40:d2:0e:1b:
         c1:3c:5e:4c:da:c6:bb:a3:4f:85:6a:8b:f0:b5:06:e7:2b:31:
         68:be:c4:6f:cf:a5:c9:75:79:98:b7:e4:6e:c9:34:b5:a7:c9:
         2a:6b:a6:f3:ef:f4:ba:c9:1e:b7:7f:cf:e9:8f:9e:ce:67:fb:
         c9:a9:f0:91:c3:33:95:00
```

1.3.1.3 Firmas electrónicas La firma electrónica es un algoritmo criptográfico que otorga a un documento digital la propiedad de integridad vinculada con la voluntad de aceptación de una persona jurídicamente hábil.

1.3.1.4 Dispositivos de usuario Una de las formas en que las personas demuestran su identidad en distintos entornos es a través de dispositivos tecnológicos. Los certificados de nacimiento, los documentos de identidad, las actas de matrimonio, los contratos y hasta los pasaportes utilizan algún tipo de tecnología; en este caso la palabra impresa sobre un papel.

Con el devenir de nuevas tecnologías, las personas han tenido que emplear mecanismos distintos para demostrar su identidad. Ahora es común tratar con sistemas informáticos en los cuales se realizan tareas tan cotidianas como comprar comida en un abasto o supermercado, pagar el servicio de agua, teléfono o energía eléctrica y hasta pagar los impuestos. El cambio en la forma de realizar las actividades cotidianas ha exigido que las personas empleen algún tipo de dispositivo para demostrar su identidad. En esta sección se describen algunos dispositivos de usuario que se emplean en la actualidad.

- Tarjetas como medio de almacenamiento seguro

  Uno de los medios más comunes para demostrar la identidad de las personas es a través de tarjetas de plástico PVC. Con un bajo costo, características de ergonomía y con mayor durabilidad que el papel, las tarjetas de plástico PVC son las más empleadas en la actualidad. Generalmente, la información asociada a la identidad de las personas está impresa en la tarjeta, y en algunos casos se agrega una fotografía. Esta tarjeta es emitida por la entidad que desea establecer la identidad de la persona y es intransferible.

  Existen distintos tipos de tarjetas empleadas para demostrar la identidad de las personas. A continuación se describen las más comunes.

  1. Tarjetas con cintas magnéticas.

     Son consideradas una de las primeras mejoras en las tarjetas que permitían el almacenamiento de datos digitales legibles sólo a máquinas. Se emplea una banda o cinta magnética en la cual se codifican los datos. Desde sus inicios las tarjetas débito y crédito, tanto de instituciones financieras públicas como privadas, utilizaban este tipo de tarjetas. En la figura 1.5 se muestra una tarjeta de débito con cinta magnética.

     Otro uso de las tarjetas con cintas magnéticas se pudo ver en la telefonía pública. En Venezuela, durante los años 80 y 90 la Compañía Anónima Nacional Teléfonos de Venezuela, CANTV, emitía tarjetas magnéticas de distintas denominaciones para teléfonos públicos. En la figura 1.6 se muestra una de las tarjetas emitidas por la CANTV.

     A pesar de su uso masivo, a las tarjetas con cinta magnética se le atribuyeron serias debilidades que permitían leer los datos almacenados, borrarlos e inclusive modificarlos si un atacante poseía el equipo necesario. Uno de los

Figura 1.5 Tarjeta de débito magnética.

Figura 1.6 Tarjeta magnética de telefonía pública.

ataques más comunes en estas tarjetas es la llamada "clonación de tarjeta", en la que el atacante podría copiar los datos de la cinta magnética con un dispositivo especializado e insertarlos en un nuevo plástico usurpando la identidad del titular. Ante esta situación, este tipo de tarjetas ha sido sustituido por otras con nuevos mecanismos de seguridad que se describen más adelante.

2. Tarjetas con tecnología de chip (Tecnología de tarjetas inteligentes)
   - Tarjetas de memoria. Permiten almacenar datos protegidos en un chip de circuito integrado contra manipulación y son útiles en aplicaciones donde el costo es una consideración principal. Fueron las primeras tarjetas inteligentes utilizadas de forma masiva para aplicaciones de telefonía. En el chip se almacenaba electrónicamente la cantidad de dinero de la que disponía el usuario para hacer llamadas.
     En Venezuela, la CANTV distribuía tarjetas de memoria prepagadas de distintas denominaciones para la telefonía pública. En la figura 1.7 se muestra una tarjeta de memoria con chip.
     Las tarjetas de memoria también pueden ser reutilizadas en algunas aplicaciones, por ejemplo para recargar el saldo de un usuario y mantener el plástico. Otros usos de estas tarjetas se describen en secciones posteriores de este capítulo.
   - Tarjetas con microprocesador.

Figura 1.7 Tarjeta de chip de telefonía pública.

A diferencia de las tarjetas de memoria, permiten almacenar claves y ejecutar algoritmos criptográficos en el microprocesador del chip. Las tarjetas con microprocesador utilizan un sistema operativo, similar al de los computadores, para realizar las operaciones internas.
Son utilizadas en telefonía celular, sistemas de pagos electrónicos, cifrado de datos y en firmas electrónicas (ver sección 1.3.1.3).
Entre las principales ventajas de este tipo de tarjetas están una mayor capacidad de almacenamiento, la posibilidad de mantener datos confidenciales y la habilidad de ejecutar algoritmos criptográficos.
Estas tarjetas tienen mecanismos de seguridad que minimizan los ataques contra este tipo de dispositivos como la mencionada "clonación de tarjetas". En general, el acceso a datos protegidos en el chip está restringido por dos características importantes: el Número de Identificación Personal (PIN por sus siglas en inglés) y la Clave de Desbloqueo Personal (PUK por sus siglas en inglés).

- El PIN es un código de seguridad que le permite bloquear y desbloquear la tarjeta para evitar que otro usuarios pueda tener acceso a su contenido.
- El PUK es un código que sirva para desbloquear la tarjeta y definir un nuevo PIN. Se emplea como mecanismo de seguridad cuando se introduce erróneamente el PIN más de un número establecido de veces.

En la figura 1.8 se muestran varias tarjetas con microprocesador.
Existe un conjunto de estándares asociados a la tecnología de tarjetas inteligentes o de microprocesador. Entre ellos están el ISO/IEC 7816 [7] para tarjetas inteligentes con contacto de la Organización Internacional para Estandarización (ISO por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC por sus siglas en inglés).
Las tarjetas de microprocesador pueden tener interfaces diferentes para comunicarse con los terminales o lectores para el acceso a

[7] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54089

Figura 1.8 Tarjetas con microprocesador.

la información protegida. Una interfaz de contacto o una interfaz sin contacto. En la primera, el chip de la tarjeta entra en contacto físico con el terminal o lector. En la segunda, el chip de la tarjeta no entra en contacto físico con el terminal o lector ya que se utiliza una comunicación inalámbrica entre ellos. A continuación se describen las tarjetas sin contacto.

– Tarjetas sin contacto
  Este tipo de tarjetas son utilizadas en entornos y aplicaciones donde las personas deben ser identificadas rápidamente. Algunos ejemplos de uso incluyen controles de acceso, transporte público, identificación de equipajes, entre otros. Las tarjetas sin contacto además de un chip poseen una antena incrustada que le permite establecer la comunicación con los lectores. En la figura 1.9 se muestra una tarjeta sin contacto.

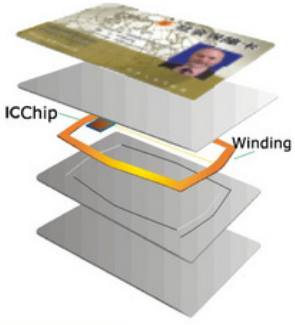

Figura 1.9 Tarjeta sin contacto.

El estándar principal de comunicaciones en tarjetas sin contacto es el ISO/IEC 14443 [8].

– Tarjetas Java Card
Un tipo de tarjetas inteligentes que se encuentra en muchas aplicaciones son las Java Card. Estas tarjetas utilizan la tecnología Java[9] sobre un chip para ejecutar múltiples aplicaciones. Los fabricantes de tarjetas inteligentes generalmente desarrollan su propia versión del sistema operativo Java o siguen especificaciones abiertas. Algunos fabricantes de tarjetas inteligentes y sistemas operativos conocidos son Gemalto[10] que sigue las especificaciones Java Card del Forum de Java Card[11], NXP[12] con JCOP, Giesecke & Devrient[13] con Sm@rtCafé Expert y Atos[14] con CardOS. Otro sistema operativo de tarjetas inteligentes es el MULTOS[15]. Este sistema está desarrollado por un conjunto de empresas a nivel mundial agrupadas en el Consorcio MULTOS que promueven el sistema operativo como estándar para tarjetas inteligentes en diferentes áreas de aplicación.
También es posible encontrar proyectos de software libre que permiten interactuar con tarjetas Java Card. El movimiento para el uso de tarjetas inteligentes en ambientes Linux[16] (MUSCLE por sus siglas en inglés), es un proyecto que define un marco de trabajo para el desarrollo de aplicaciones con tarjetas inteligentes en entornos Linux.

- Lectores de tarjetas

  Las tarjetas inteligentes requieren un dispositivo adicional para que su contenido pueda ser leído en un momento particular. Los lectores son dispositivos electrónicos de entrada que leen datos de medios de almacenamiento en forma de tarjetas. Existen lectores para tarjetas de memoria, tarjetas magnéticas y tarjetas inteligentes con interfaces de contacto, sin contacto o de interfaz dual (ambas interfaces en un mismo lector).

  Los lectores de tarjetas pueden conectarse a los computadores a través de distintas puertos como por ejemplo USB o serial. En las figuras 1.10, 1.11 y 1.12 se muestran algunos lectores de contacto, sin contacto y dual respectivamente.

[8] http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693
[9] http://www.java.com
[10] https://www.gemalto.com/
[11] https://javacardforum.com/
[12] http://www.nxp.com/
[13] http://www.gi-de.com
[14] http://atos.net/en-us/home.html
[15] http://www.multos.com/
[16] http://www.musclecard.com

Figura 1.10 Lectores de tarjetas inteligentes de contacto.

Figura 1.11 Lectores de tarjetas inteligentes sin contacto.

Al igual que las tarjetas inteligentes, para los lectores también existen estándares que especifican su operación. Entre estos estándares se encuentran: PC/SC (Personal Computer / Smart Card) con especificaciones para la integración de tarjetas inteligentes en computadores personales definidas por el PC/SC Workgroup [17] y el USB-CCID (Integrated Circuit(s) Cards Interface Device) con especificaciones para dispositivos USB que se comunican con tarjetas de circuitos integrados como tarjetas inteligentes definidas por el Grupo de Trabajo de Dispositivos (DWG por sus siglas en inglés) del Foro de Implementadores de USB[18] (USB-IF por sus siglas en inglés).

[17] http://www.pcscworkgroup.com
[18] http://www.usb.org/about/

Figura 1.12 Lector de tarjetas inteligentes de interfaz dual.

- Tokens Criptográficos

  También llamados token de seguridad, token de autenticación o simplemente token USB, son dispositivos similares a las tarjetas inteligentes en su arquitectura. Poseen un microprocesador criptográfico que permite realizar las mismas operaciones criptográficas y de autenticación que las tarjetas inteligentes a través de un puerto USB.

  A diferencia de las tarjetas inteligentes no utilizan un lector pero sí requieren la instalación de un controlador de hardware en el computador para que sea reconocido. A nivel del sistema operativo, el token criptográfico es visto como una tarjeta inteligente conectada a un lector de tarjetas virtual. En la figura 1.13 se muestran algunos token criptográficos utilizados en aplicaciones como certificación electrónica y firmas electrónicas.

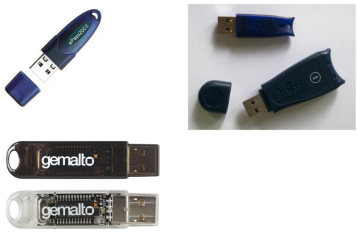

Figura 1.13 Tokens criptográficos.

También es posible encontrar tokens criptográficos en formato de tarjetas MicroSD o SD como se muestra en la figura 1.14. Las tarjetas MicroSD con

certificados electrónicos almacenados se pueden utilizar en teléfonos celulares para propósitos de autenticación o firma electrónica.

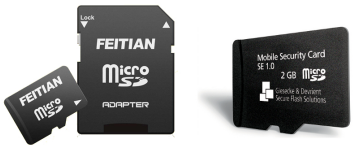

Figura 1.14 Tokens criptográficos en formato MicroSD y SD.

- Dispositivos de autenticación con contraseñas de un solo uso

  Este tipo de dispositivos representan una variación del mecanismo de autenticación con usuario y contraseña ya que la contraseña utilizada es válida para una sola sesión. Los dispositivos de autenticación con contraseñas de un solo uso (OTP por sus siglas en inglés), generan un código único y aleatorio para tener acceso a recursos o a sistemas.

  La generación de los códigos se realiza, principalmente, de acuerdo a varios enfoques existentes:

  – a través de algoritmos matemáticos con un reto que propone un servidor de autenticación al dispositivo.
  – basada en sincronización de tiempo entre el servidor de autenticación y el dispositivo.

  Tal como en las tarjetas inteligentes existen distintos fabricantes de dispositivos de contraseñas de un solo uso. En la figura 1.15 se muestran algunos de estos dispositivos.

- Chip SIM

  Es una tarjeta o módulo de identificación de suscriptor (SIM por sus siglas en inglés) que posee información relacionada al suscriptor de cada empresa prestadora de servicio de telefonía en el Sistema Global para las Comunicaciones Móviles (GSM por sus siglas en inglés). Datos como la clave del suscriptor usada para identificarse en la red, están protegidos en la tarjeta SIM.

  En general, el chip SIM está diseñado para proveer las siguientes funciones básicas:

  – Seguridad (identificación del suscriptor, autenticación de SIM y crifrado de datos).

Figura 1.15 Dispositivos de contraseña de un solo uso.

- Almacenamiento de datos (números de contactos, mensajes cortos, configuración del teléfono celular e información del suscriptor).
- Administración del suscriptor.

En la figura 1.16 se muestra una tarjeta SIM.

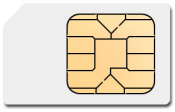

Figura 1.16 Tarjeta SIM de telefonía celular.

- Autenticación de dos factores

  En la actualidad existen organizaciones y empresas que proveen servicios en línea como correo electrónico, redes sociales, mensajería instantánea y hasta banca electrónica que utilizan alguna o varias formas de autenticación de dos factores. La idea es que sus usuarios tengan acceso a sus recursos y se minimice la suplantación de identidad.

  Aunque no es exactamente un dispositivo físico, la autenticación de dos factores utiliza distintos mecanismos para validar la identidad de un individuo al solicitarle alguna prueba adicional. Entre los mecanismos utilizados están el Servicio de Mensajes Cortos (SMS por sus siglas en inglés), una llamada telefónica, un correo electrónico, un token o dispositivo de hardware o una implementación de software[19]. Cuando un individuo desea autenticarse en un sistema informático presenta un identificador y contraseña como primer factor de autenticación. Luego el sistema envía un código, a través de uno de los mecanismos mencionados, que el usuario debe introducir como segundo factor de la auten-

[19] http://twofactorauth.org/

ticación. Si el código introducido es el correcto, el sistema permite el acceso al usuario a sus recursos.

La autenticación de dos factores puede ser utilizada en entornos como:

- Integración de sistemas.
- Acceso remoto y redes privadas virtuales (VPN por sus siglas en inglés).
- Administración de contraseñas.
- Cifrado de discos.
- Protección de servidores.

Desde Febrero de 2013 la Alianza de Identidad Rápida en Línea (FIDO Alliance[20] por sus siglas en inglés) agrupa a un conjunto de organizaciones y empresas que tienen como objetivo establecer estándares de interoperabilidad entre dispositivos de autenticación así como enfrentar el problema de crear y recordar múltiples nombres de usuarios y contraseñas para sistemas informáticos.

- Lectores biométricos

  Son dispositivos electrónicos capaces de leer características inherentes a los seres humanos para identificar y autenticar usuarios en un entorno particular. Es posible dar acceso a un espacio físico y/o recursos informáticos a través de lectores biométricos.

  Entre las características humanas empleadas por los lectores biométricos están:

  - Huella digital
  - Geometría de la mano
  - Patrones de líneas del Iris
  - Patrones de las venas encontradas en la parte trasera del ojo
  - Forma de la oreja
  - Rasgos faciales
  - Escritura

  Es común encontrar lectores biométricos de huellas digitales en aeropuertos, computadores portátiles e inclusive en registros electorales. En la figura 1.17 se muestran algunos lectores biométricos.

  Uno de los registros biométricos más conocidos es el que mantienen algunos países al momento de emitir los documentos de identidad a sus ciudadanos. En la República Bolivariana de Venezuela, se solicitan las huellas digitales a todos los ciudadanos al momento de emitirle la Cédula de Identidad. Todas las huellas digitales son registradas en un sistema de identificación de huellas automatizado (AFIS por sus siglas en inglés). Esta información puede ser consultada por las instituciones de gobierno para verificar la identidad de los ciudadanos venezolanos.

[20] https://fidoalliance.org/

Figura 1.17 Lectores biométricos.

Tabla 1.1 Indicadores del Servicio de Telefonía Móvil a nivel Nacional para el 2013.

Trimestre	Suscriptores	Suscriptores en uso	Población	Penetración (%)	Penetración activos (%)
I	31.355.824	30.195.345	29.787.406	105,27	101,37
II	31.543.806	30.442.724	29.891.188	105,53	101,85
III	31.718.539	30.547.569	30.001.687	105,72	101,82
IV	31.909.692	30.896.079	30.116.378	105,95	102,59

Usos comunes de dispositivos de usuario

- Telefonía móvil.

  De acuerdo a los indicadores del servicio de telefonía móvil a nivel nacional generados por la Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela, CONATEL, correspondientes al cuarto trimestre del 2013, el porcentaje de penetración de usuarios activos había sido de 102,59%. Se estimaron 103 líneas en uso del sistema de telefonía móvil por cada 100 habitantes.

  En la tabla 1.1 se presentan los datos de Número de suscriptores, suscriptores que están usando el servicio, la población total, el porcentaje de penetración y el porcentaje de penetración de usuarios activos basados en la población trimestral estimada a partir de la serie de Fuerza de Trabajo que publica el Instituto Nacional de Estadísticas, INE[21].

[21] http://www.ine.gov.ve/

Tabla 1.2 Proporción de suscriptores por tipo de tecnología móvil.

Tecnología	Proporción de suscriptores (%)
GSM	69,21
CDMA	30,79

Entre las tecnologías predominantes de telefonía móvil en Venezuela se encuentran la de Acceso Múltiple por División de Código (CDMA por sus siglas en inglés) y GSM que emplea un chip en el teléfono para el acceso a la red. De estas, GSM tiene mayor penetración en el país. En la tabla 1.2 se muestra la proporción de suscriptores por tipo de tecnología de acuerdo a las estadísticas preliminares del Sector Telecomunicaciones realizadas por la CONATEL, para el cuarto trimestre de 2013[22] con base en 31.909.692 suscriptores totales de telefonía móvil.

- Banca electrónica.

  Para el año 2014 todos los bancos de la República Bolivariana de Venezuela migraron su plataforma de tarjetas de débito, crédito y demás tarjetas de financiamiento de pago electrónico a tecnología de tarjetas con chip.

  En el año 2010, la Superintendencia de las Instituciones Bancarias (SUDEBAN) inició el proyecto de la incorporación del Chip electrónico en las tarjetas de débito, crédito y demás tarjetas de financiamiento de pago electrónico.

  En marzo del año 2012 la SUDEBAN exhortó a los ususarios de la banca a canjear sus tarjetas de débito y crédito por aquellas con el sistema de chip electrónico antes del 01 de Julio de ese año[23]. Este requerimiento de la SUDEBAN exigió la adaptación de cajeros automáticos y puntos de ventas para el soporte de las nuevas tarjetas en búsqueda de una reducción de los índices por fraude de clonación.

  Algunas instituciones públicas que dependen del Gobierno Bolivariano han utilizado tarjetas inteligentes para brindar a sus empleados el beneficio del bono de alimentación. A través de estas tarjetas los empleados pueden adquirir productos en abastos y supermercados con un mayor nivel de seguridad comparado con la emisión de tiquetes en papel. La figura 1.18 muestra una de las tarjetas emitidas por uno de las entidades bancarias del Estado Venezolano.

- Tarjetas de lealtad.

  Algunas organizaciones tanto públicas como privadas le otorgan a usuarios una tarjeta de lealtad. La tarjeta brinda beneficios a los usuarios que la portan a

[22] http://www.conatel.gob.ve/files/Indicadores/indicadores_2013/PRESENTACION_IV_TRIMESTRE_2013_2.pdf
[23] http://sudeban.gob.ve/webgui/root/documentos/notas-de-prensa/np-chip.pdf

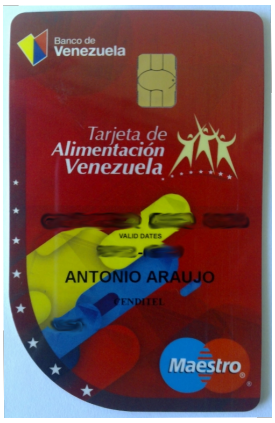

Figura 1.18 Tarjeta electrónica de alimentación.

diferencia de otros usuarios que, si bien pueden tener los beneficios, tal vez lo reciban con una menor prioridad a la de los portadores de la tarjeta. Generalmente se utilizan tarjetas que almacenan algunos puntos que luego pueden ser canjeados. Algunos ejemplos se encuentran en supermercados, tiendas por departamentos, ferreterías y tiendas de materiales de construcción, bibliotecas, etc.

- Certificación electrónica

  Con el despliegue de la Infraestructura Nacional de Certificación Electrónica la República Bolivariana de Venezuela cuenta con los Proveedores de Servicios de Certificación (PSC) que emiten certificados electrónicos a los ciudadanos. Como medida de seguridad la emisión de estos certificados se realiza en algún dispositivo de hardware como tarjetas inteligentes o token USB (ver sección 1.3.1.2). En las figuras 1.19 y 1.20 se muestra una tarjeta inteligente y un token USB utilizado por un PSC acreditado de la República Bolivariana de Venezuela.

Figura 1.19 Tarjeta inteligente para certificado electrónico.

- Otros usos generales.

Figura 1.20 Token USB para certificado electrónico.

Algunos usos generales de dispositivos de usuario incluyen tarjetas inteligentes para pasajes estudiantiles, licencias de conducir, carnet de identificación, control de acceso físico entre otros.

El Gobierno Bolivariano a través del Ministerio del Poder Popular para Transporte Terrestre gestiona el Proyecto Pasaje Preferencial Estudiantil como instrumento social para garantizar el acceso de los estudiantes al sistema de transporte público. El proyecto entrega a los estudiantes una tarjeta inteligente como sistema de pago electrónico a través del débito del pasaje, en sustitución del ticket o boleto de papel. La figura 1.21 muestra una tarjeta inteligente de un estudiante.

Figura 1.21 Tarjeta inteligente de pasaje estudiantil.

Cada tarjeta inteligente cuenta con la identificación del alumno, cédula de identidad y nombre de la institución donde cursa estudios. Es además, instransferible e individual, tiene una vigencia de 4 años, es renovable y también recargable.

Otro de los principales usos de las tarjetas inteligentes es el control de acceso físico. Se utiliza en oficinas, salones, bancos e instituciones públicas o privadas en las cuales se desea controlar el acceso a espacios físicos. Generalmente estas tarjetas tienen una interfaz sin contacto que utiliza la tecnología RFID. En la figura 1.22 se muestra una tarjeta de control de acceso físico y su respectivo lector.

Figura 1.22 Tarjeta y lector de control de acceso físico.

Pasaporte Electrónico Cada país emplea un documento con validez internacional para establecer la identidad de sus ciudadanos: el pasaporte. En la República Bolivariana de Venezuela la emisión del pasaporte para los ciudadanos está a cargo del Servicio Administrativo de Identificación, Migración y Extranjería (SAIME) organismo adscrito al Ministerio del Poder Popular para Relaciones Interiores y Justicia en el marco de la legislación existente: La Constitución de la República Bolivariana de Venezuela, Gaceta oficial N0. 5.908 de 19/02/2009 y la Ley Orgánica de Identificación (Artículos 29, 30, 31), Gaceta Oficial No. 34.458 del 14/06/2006.

Como resultado de un proceso de transformación iniciado en el año 2005, el Ejecutivo Nacional aprueba la ejecución del Proyecto de Transformación y Modernización de la Oficina Nacional de Identificación y Extranjería (ONIDEX) que se convirtió en el actual SAIME. Así mismo se inició la emisión del Pasaporte Electrónico para los ciudadanos en el año 2007.

El Pasaporte Electrónico de la República Bolivariana de Venezuela es un documento similar a cualquier pasaporte de papel pero con un conjunto de medidas de seguridad adicionales. Se utiliza una lámina de policarbonato con un circuito electrónico incrustado en ella. En la figura 1.23 se muestra un pasaporte electrónico.

A diferencia del pasaporte de papel, en el pasaporte electrónico todos los datos del ciudadano se encuentran almancenados en formato electrónico en un chip criptográfico sin contacto. Para garantizar la integridad de los datos así como el origen de los mismos se emplea la tecnología de firma electrónica (ver sección 1.3.1.3). SAIME firma electrónicamente todo la información asociada a un ciudadano y esta puede ser leída en cualquier oficina o punto de inmigración de un país para verificar su identidad.

Todas las especificaciones que deben cumplir los pasaportes electrónicos están definidas por la Organización de Aviación Civil Internacional[24] (ICAO por sus siglas en inglés). El documento identificado con el número 9303 contiene las especificaciones actuales de la ICAO para pasaportes legibles por máquinas. Se encuentra di-

[24]http://www.icao.int/

Figura 1.23 Muestra de pasaporte electrónico.

vidido en tres partes que describen los requisitos para documentos como pasaportes con datos almacenados en formato de reconocimiento óptico, con capacidades de identificación biométrica, máquinas lectoras de visas y máquinas lectoras de documentos oficiales de viaje. El documento está disponible para su revisión y libre distribución en el portal de la ICAO[25].

El Pasaporte Electrónico de la República Bolivariana de Venezuela posee en su anverso el símbolo que se muestra en la figura 1.24 . Este es un indicador visual de que el pasaporte es electrónico y que contiene un circuito integrado sin contacto, con capacidad de almacenamiento de datos de al menos 32Kb.

Figura 1.24 Símbolo de pasaporte electrónico según ICAO.

Los esfuerzos de la República Bolivariana de Venezuela en el proceso de actualización del pasaporte electrónico, permiten a los ciudadanos venezolanos entrar en algunos países del mundo sin necesidad de tramitar visas.

[25]http://www.icao.int/publications/pages/publication.aspx?docnum=9303

CAP´TULO 2

POL´TICAS DE SEGURIDAD

A. Araujo y V. Bravo

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

2.1 Políticas de seguridad de la información. Importancia.

test

2.2 Puestos de trabajo, centros de datos, seguridad lógica y física

test

2.3 Políticas de Seguridad de las Tecnologías de Información y Comunicación

Las políticas de seguridad en una institución representa una herramienta para mostrar a sus miembros la importancia y sensibilidad de la seguridad de la información. Estas políticas deben describir las características clásicas de la seguridad

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

de la información, que se definen sobre conceptos como confidencialidad, integridad, disponibilidad, autenticación, responsabilidad (no repudio); de esta manera, permitir la adaptación a nuevos paradigmas.

Sin embargo, es necesario dar un concepto, definición o contexto sólido respecto al concepto de *Seguridad* [**?**], en la cual pueden mostrarse las siguientes características:

Vicente Aceituno C., Seguridad de la información, Limusa, 2006.

- **Confidenciabilidad**, condición en la que sólo los usuarios autorizados tienen acceso al contenido de los datos.
- **Control de acceso**, se controla el acceso a recursos de usuarios autorizados.
- **Disponibilidad**, condición en la que se puede acceder a información o utilizar un servicio siempre que se necesite.
- **No repudio**, condición en la que se previene que una entidad involucrada en una comunicación niegue luego su participación en la misma.
- **Integridad**, condición en la que se garantiza que la información o mensaje no han sido alterado.

Las políticas de seguridad de la información deben seguir un proceso de actualización periódica sujeta a cambios pertinentes en la institución y relacionados a la contratación de personal, alta rotación del personal, cambio en la infraestructura, cambio o diversificación de las actividades y/o servicios de la institución, desarrollos de nuevos servicios, vulnerabilidades de algunos sistemas, nivel de confianza entre los miembros de la institución, numero de incidentes de seguridad, entre otras.

Ya que los seres humanos son los que realizan las actividades dentro de las instituciones, es importante que las poltíticas de seguridad no se conviertan en una forma de restricción o carga para ellos. Hay que tener en cuenta, que todas las soluciones tecnológicas implementadas por una institución (cortafuego, sistemas de detección de intrusos, dispositivos biométricos, entre otros) pueden resultar inútiles ante el desconocimiento, falta de información, mal uso de los controles de seguridad de la información, el no cumplimiento de las políticas de seguridad, desinterés o animo de causar daño de algún miembro desleal de la institución.

Las personas representan el eslabón más débil de la seguridad de la información **AGREGAR REFERENCIA**. Ellas pueden seguir o no las políticas de seguridad que fueron definidas y aprobadas en la institución, pueden realizar acciones que provoquen un agujero de seguridad en la red de la institución a través de instalación de software malicioso en las computadoras, revelación de información sensible a terceros entre otros. Según especialistas de la materia, el mayor porcentaje de fraudes, sabotajes, accidentes relacionados con los sistemas informáticos son causados desde

lo interno **AGREGAR REFERENCIA**, ya que las personas que pertenecen a la institución pueden conocer perfectamente los sistemas, sus barreras y sus puntos débiles.

El objetivo de este documento es proponer lineamientos generales a considerar desde el momento de definir las directrices de seguridad de la información de una institución de acuerdo a las necesidades, limitaciones que existe en ella, de manera de concretar las ideas en documentos que orienten las cciones de la institución.

2.4 Importancia de la Seguridad de la Información

Las instituciones deben entender que la seguridad de la información es un proceso que puede desarrollarse en ciclos iterativos, y no es una receta. Esto último, es entendido en los términos que no se genera una relación vivencial con la tecnología y sus actores y no se construye una experiencia que modifique nuestra visión como institución y seres humanos.

Entre los objetivos de la seguridad de la información se pueden destacar los siguientes:

- Minimizar y gestionar los riesgos. Detectar los posibles problemas y amenazas a la seguridad de la información.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones en los sistemas.
- Limitar la pérdida de información y recuperar sistemas en caso de un incidente de seguridad de la información.

Para cumplir con estos objetivos las instituciones deben contemplar tres planos de actuación: Técnico, Humano e Institucional.

Técnico:

- Consideración del nivel físico y lógico de la institución.
- Selección, instalación, configuración y actualización de las soluciones de hardware y software.
- Criptografía.
- Desarrollo seguro de aplicaciones.

Humano:

- Cultivo de buenas practicas de actuación ante la seguridad de la información.

- Sensibilización y formación del personal y directivos de la institución.
- Funciones, obligaciones, responsabilidades del personal.

Institucional:

- Definición e implementación de políticas, normas de procedimientos de seguridad de la información y planes de contingencias en casos de desastres en contexto de los activos de información.

2.5 Seguridad de la Información para Tecnologías Libres

Las potencialidades intrínsecas del software libre permiten incorporar elementos de seguridad en sistemas informáticos de instituciones, organizaciones y hasta usuarios finales. Entre estas potencialidades se incluyen:

1. La capacidad de analizar y estudiar las tecnologías subyacentes a las aplicaciones
2. La posibilidad de auditabilidad de los códigos fuentes
3. La frecuente corrección de errores y publicación de software gracias al apoyo de comunidades de usuarios y desarrolladores alrededor de las aplicaciones y herramientas, en comparación con otros modelos de desarrollo.
4. El rompimiento del paradigma de la seguridad por obscuridad.

La seguridad de la información en software libre sigue un modelo de desarrollo de software basado la en cooperación, la solidaridad, así como la creación de comunidades de seres humanos en torno a una tecnología.

En el mundo del software libre existen aplicaciones y herramientas con características y funcionalidades similares a las existentes en el software propietario; inclusive en algunos casos, se reconocen herramientas de software libre como mejores opciones **AGREGAR REFERENCIA**.

La adopción de software libre como alternativa para mejorar la seguridad de la información en organizaciones implica un cambio de pensamiento; un cambio del modelo imperante basado en compras de soluciones, por un modelo que incorpora tecnologías abiertas en búsqueda de la soberanía e independencia tecnológica.

2.6 Principio de Defensa en profundidad

Se refiere a una estrategia militar que tiene por objetivo hacer que el atacante pierda el empuje inicial y se vea detenido en sus intentos al requerir superar varias barreras

en lugar de una **AGREGAR REFERENCIA**. En informática consiste en el diseño e implementación de varias líneas de seguridad independientes dentro del mismo sistemas informático. De este modo, si uno de las líneas de seguridad logra ser traspasada por los atacantes, conviene disponer de líneas de seguridad adicionales que dificulten, debiliten, retrasen y que pueda ser detectado su acceso o control, no autorizado a los activos de la institución.

El enfoque tradicional de seguridad, que se presenta en la figura 2.1, establece una sola línea de seguridad al rededor de activos, que cubra la mayor área posible como por ejemplo: cortafuego, un sistema de autenticación, etc. Los problemas que presenta este enfoque, es que la línea de seguridad susceptible y puede tener vulnerabilidades dadas por: una mala configuración de sistema de protección, fallas del sistemas, etc. Una vez que es superada esta línea de seguridad, las formas de detener el ataque son mínimas.

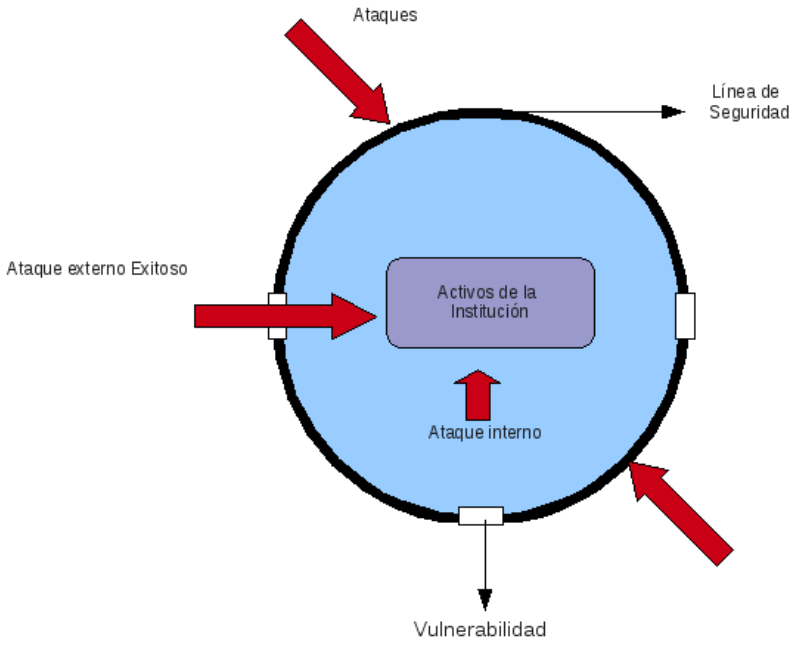

Figura 2.1 *Enfoque tradicional de Seguridad.*

Mientras que el enfoque de defensa en profundidad, como muestra la figura 2.2, establece múltiples líneas de seguridad, donde las vulnerabilidades de una linea de seguridad son cubiertas por las fortalezas de las otras.

Si no se puede detener el ataque, al atravesar una de las líneas de seguridad, se debilita el ataque, por que existe la posibilidad que se generen alertas y pueda ser detectado, se pudiese obtener información sobre su origen, naturaleza, anomalías y con esto se puede reforzar las otras líneas de seguridad, que podrían detener el ataque o que el mismo no genere pérdidas mayores a la institución, ademas permite, corregir en cierta medida la(s) vulnerabilidad(es) de las lineas de seguridad que fueron traspasadas.

Este enfoque permite cubrir varios de los puntos de riesgos de un sistema y dependiendo de la estructuración de las líneas de seguridad, lo protege de los ataques internos.

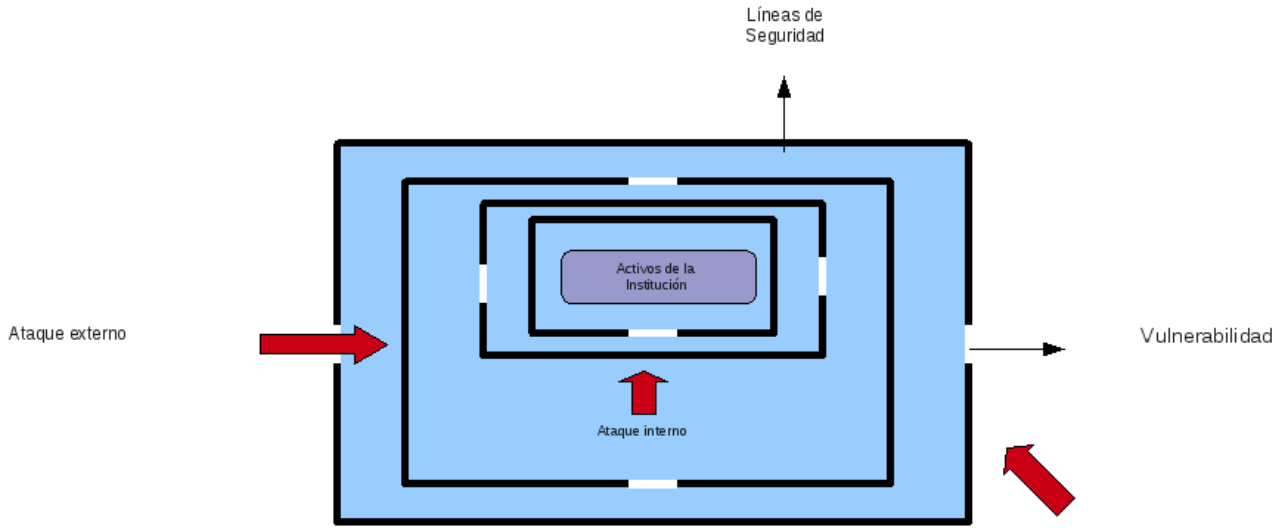

Figura 2.2 *Enfoque de defensa en profundidad.*

Dentro de una institución existe múltiples grupos de usuarios con diferentes actividades y responsabilidades, por lo que se requiere estructurar las líneas de seguridad, de manera que para cada grupo de usuario le corresponda una línea de seguridad y de esta manera, se logra incrementar la protección contra atacantes internos.

2.6.1 Los principios generales de la defensa en profundidad

- Engloba todas los aspectos organizacionales, técnicos, y de implementación.

- Las acciones a tomar deben estar coordinadas. Los medios implementados actúan gracias a una capacidad de alerta y difusión, tras una correlación de los incidentes.
- Las acciones a tomar deben ser dinámicas. Las políticas de seguridad contemplan la capacidad de reacción y planificación de acción ante incidentes.
- Las acciones a tomar deben ser suficientes. Cada medio de protección (organizacional, técnico) debe contar con: protección propia, medios de detección, procedimientos de reacción.
- Los activos deben protegerse en función a su sensibilidad y nivel de importancia a la institución, y tener como mínimo, tres líneas de seguridad.

2.7 Responsabilidad

Antes de que se apliquen las políticas de seguridad en una institución, deben ser aprobadas, publicadas, documentadas, y comunicadas a todos sus miembros. Estos son los responsables de la aplicación y cumplimiento de las políticas de seguridad en cada una de sus áreas.

Todas los roles y responsabilidades de la seguridad de la información deberían estar claramente definidas y documentadas; su asignación debería realizarse en concordancia con las políticas de seguridad. Las personas con responsabilidades en la seguridad de la información pueden delegar las tareas de seguridad a otros. No obstante, ellos siguen siendo responsables y debieran determinar si cualquier tarea delegada ha sido realizada correctamente.

No se recomienda que todas o la mayoría de las responsabilidades de la seguridad de la información y el manejo de las actividades críticas de la institución (ver sección 14.1) esté sobre en un grupo pequeño de personas, esto generaría una debilidad en la seguridad de la información, que por ejemplo se podría ver afectado el normal funcionamiento de la institución si este grupo pequeño de personas por alguna razón no puedisen atender sus compromisos con la institución.

2.8 Procesos para aumentar la adopción de seguridad de la información

Es esencial que las instituciones identifique claramente sus requerimientos de seguridad. La figura 2.3 muestra la relación entre los procesos a incluir para identificar los requerimientos de seguridad y alcanzar el objetivo de cumplir con metas sobre seguridad de la información. Entre los procesos se encuentran: Identificación y evaluación de los riesgos, revisión, monitoreo, selección e implementación de controles.

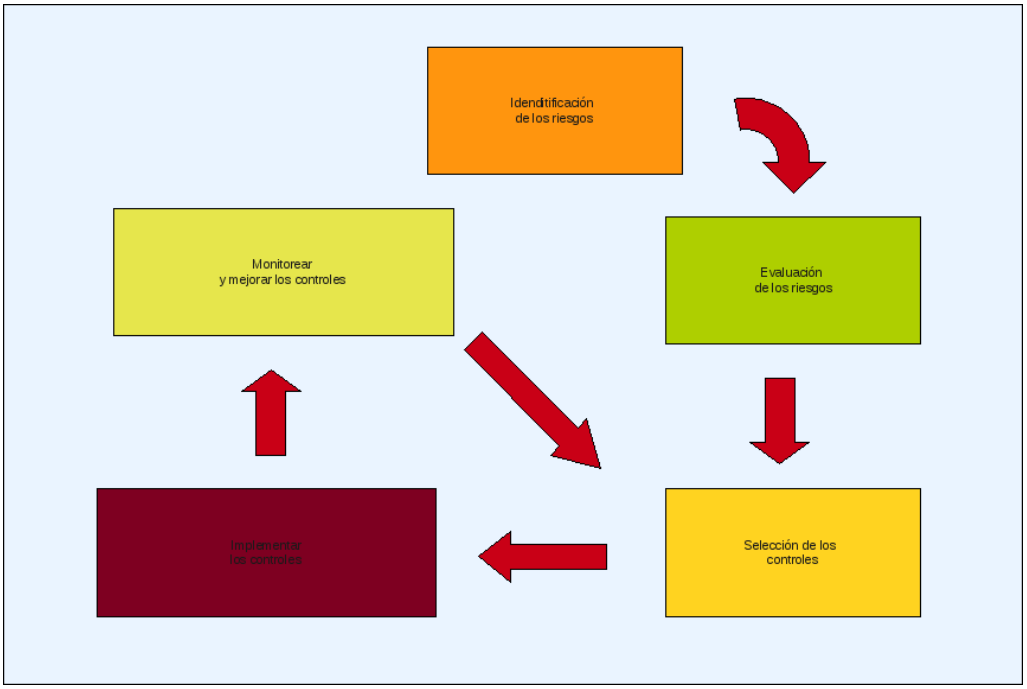

Figura 2.3 *Proceso de percepción de la Seguridad.*

2.8.1 Identificación de los riesgos

Es una medida que busca rastrear vulnerabilidades en los activos que puedan ser explotados por terceros. Es necesario la identificación de los riesgos que puedan existir en la institución, para la misma es importante considerar los distintos ámbitos para la implementación de la seguridad alrededor de donde se encuentra la información.

Entre los ámbitos se encuentra:

(a). **Técnico:** que se refiere al conocimiento que se tiene de configuración de los componentes de toda la infraestructura tecnológica de respaldo, comunicación, procesamiento, tránsito y almacenamiento de la información. Los activos en este ámbito son aplicaciones, equipo informáticos y de comunicación, datos, documentación, manuales, consumibles, servicios ofrecidos a usuarios internos como externos, requiriendo la realización de un inventario de los activos antes mencionados que permite:

- Tener un registro actualizado de los activos de la institución.
- Facilitar el análisis de las vulnerabilidades.

- Conocer la sensibilidad de la información que se manipula, clasificándola en función al grado de importancia para la institución.
- Identificar los posibles objetivos de los ataques o de los intentos de intrusión.
- Ser utilizado en caso de recuperación frente a un incidente grave de seguridad.

Asimismo será necesario identificar los distintos puntos de accesos a la red y los tipos de conexiones utilizadas.

(b). **Humano**: referido a la compresión de las maneras en que las personas se relacionan con los activos, y de la cultura que se tiene en materia de seguridad de la información. Así, es posible detectar cuáles vulnerabilidades provenientes de acciones humanas, y es posible dirigir recomendaciones para mejorar y garantizar la continuidad de las actividades de la institución. Este proceso pretende inicialmente identificar vulnerabilidades en los activos de usuario y de la organización, el nivel de acceso que las personas tienen en la red o en las aplicaciones, las restricciones y permisos que deben tener para realizar sus tareas con los activos. El nivel de capacitación y formación educativa que necesitan tener acceso para manipularlos, uso de buenas practicas de claves y contraseñas, nivel de responsabilidad y sensibilización de los miembros de la institución. Para su identificación debemos:

- Investigar la formación del personal en materia de seguridad
- Investigar sobre la cultura en materia de seguridad de la información que maneje la institución.

(c). **Físico:** pretende identificar la infraestructura física del ambiente en que los activos encuentran vulnerabilidades que puedan traer algún perjuicio a la información y a todos los demás activos. El enfoque principal de este ámbito de análisis son los activos de tipo organización, pues son los que proveen el soporte físico al entorno en que está siendo manipulada la información, Identificar posibles fallas en la localización física de los activos tecnológicos.

- Investigar sobre las condiciones físicas y ubicación donde se encuentran los equipos computacionales de la institución.
- Investigar sobre los servicios requeridos como electricidadd, comunicación, agua, etc.
- Controles de accesos físicos existentes
- Controles de protección y extinción de incendios

2.8.2 Evaluación de los riesgos de seguridad

Una vez identificados los riesgos de seguridad, se deben someter a evaluaciones para determinar, cuantificar, y priorizar los riesgos de la institución de acuerdo a los objetivos relevantes de la institución. La evaluación de los riesgos tiene como resultado

recomendaciones para la selección y/o corrección de los controles sobre los activos para que los mismos puedan ser protegidos. La evaluación de los riesgos de seguridad deben tener claro y definido el alcance que va a tener para que la misma sea efectiva.

La evaluación de los riesgos procura determinar:

- Amenazas al normal funcionamiento de la institución.
- El impacto que tendría el riesgo en la institución si llegara a ocurrir una amaneza.
- La posible frecuencia con la que podrían ocurrir amenazas.

Los resultados de la evaluación deben guiar y determinar las acciones en el tratamiento de los riesgos, esta evaluación puede que requiera ser realizada periódicamente, cuando se tengan cambios significativos; nuevos requerimientos de los sistemas, situaciones de riesgos, amenazas, vulnerabilidades, o cualquier cambio que podria influir en los resultados de la evaluación de los riesgos.

Las evaluaciones se pueden aplicar a toda la institución, parte de ella, un sistema información en particular, componentes específicos del sistema. Los riesgos deben ser aceptados por toda la institución de manera objetiva y con conocimiento. De ser necesario hay que transferir los riesgos a terceros como los son proveedores y/o aseguradores.

Hay herramientas para la evaluación de vulnerabilidades, que permiten conocer la situación real de un sistema y mejorar su seguridad, verificando que los mecanismos de seguridad funcionen correctamente. Con esta información obtenida es posible justificar la implantación de nuevas medidas de seguridad, así como de priorizar las medidas a implementar en función a las vulnerabilidades detectadas.

Dentro de las evaluaciones de la seguridad de los sistemas informáticos se realizan las pruebas de penetración internas y externas. Una prueba de penetración consta de las siguientes etapas:

- Reconocimiento del sistema para averiguar qué tipo de información podría obtener un atacante o usuario malicioso.
- Detección y verificación de las vulnerabilidades en los servidores estándar y en aplicaciones desarrolladas por la institución.
- Intento de explotación de las vulnerabilidades detectadas
- Generación de informes, con el análisis de los resultados

2.8.3 Selección de los controles

Una vez que se haya evaluado los riesgos de seguridad se decide el tratamiento que se le va a dar a los riesgos, seleccionando los controles que aseguren un nivel adecuado de seguridad para la institución. Se realiza una investigación sobre las posibles soluciones existentes para cada uno de los riesgos identificados de cada ámbito, por ejemplo, en el ámbito técnico se hace una investigación de la tecnología libre existente que cubra los riesgos identificados (cortafuegos, redes privadas virtuales, protocolos de comunicación seguros, sistemas de detección de intrusos de red y host, sistemas de escaneo de puertos, etc). En el ámbito humano, dictar charlas y dar cursos de seguridad de tal manera que se puedan sensibilizar a las personas que interactuan con los sistemas informáticos. En el ámbito físico, la instalación de circuitos de cámaras de cerradas, instalación de controles físicos, remodelación o reforzamientos del centro de datos.

Es importante considerar el gasto de los controles de seguridad, ya que el mismo debiera ser equilibrado con el daño probable que resulta de las debilidades en la seguridad de la información. Si el gasto del o los controles es mucho mayor al posible daño que pudiera resultar, la institución pudiera asumir el riesgo de ocurrir un incidente de seguridad por esa debilidad en la seguridad de la información y no colocar el o los controles de seguridad.

Existen controles que se consideran principios orientativos y esenciales, que proporcionan un punto de partida adecuado para implementar la seguridad de la información como es las políticas de seguridad. se deben considerar:

- Aprobar, documentar, publicar y comunicar las políticas de seguridad a todos los miembros de la institución de forma adecuada; charlas y/o cursos en materia de seguridad, etc.
- Asignar las responsabilidades de seguridad a miembros de la institución, en concordancia con las políticas de seguridad.
- Identificar los procedimientos de seguridad asociados a los activos de la institución.
- Definir y documentar los niveles de autorización.
- Registrar las incidencias y mejoras de seguridad.
- Desarrollar e implementar procedimientos de gestión de continuidad de actividades para disminuir la interrupción causada por los desastres y fallas de seguridad.
- Salvaguardar los registros de la organización. Se deben proteger los registros importantes de la organización frente a su pérdida, destrucción y/o falsificación.

- Sensibilización y formación de los mimbros de la institución en materia de seguridad de la información

2.8.4 Implementar los controles seleccionados

Es recomendable que los controles en el plano técnico de seguridad se implementen en un ambiente de pruebas antes de colocarlos en el ambiente de producción para no producir inconvenientes en los servicios informáticos.
Se deben configurar e implementar los controles de tal manera que existan varias líneas de seguridad independientes dentro del mismo sistemas informático para dar cabida al concepto de seguridad en profundidad (ver sección 5).

Hay otros controles esenciales en el plano institucional que dependen de la legislación aplicable en la institucion, como por ejemplo la protección de datos y privacidad de la información personal.

Los controles en el plano humano, como la sensibilización y formación de todos los miembros de la institución deben recibir una adecuada formación en seguridad, desde la directiva hasta los obreros e incluyendo cuando sea relevante, a los contratista y a terceras personas.
Se recomienda organizar charlas, cursos que permitan la formación en materia de seguridad de la información de acuerdo al área de actuación a los miembros de la institución los cuales permitan informar:

- El uso correcto de mecanismos y herramientas para procesar información.
- Actualización de nuevos controles y políticas de seguridad.
- El conocimientos de las vulnerabilidades existentes.

Esto permite aumentar la conciencia y conocimiento a los miembros de la institución con el objetivo de que puedan reconocer los problemas e incidentes de seguridad de la información, y responder adecuadamente a las necesidades según su rol dentro de la institución.

2.8.5 Monitorear y mejorar los controles de seguridad

Los controles de seguridad deberían ser revisados en periodos planificados o cuando ocurran cambios significativos que puedan afectar la eficiencia y eficacia de los controles.

Se recomienda la realización de pruebas y auditorias periódicas de seguridad. Esto constituye un elemento de gran importancia para poder comprobar la adecuada implantación de los controles de seguridad y medidas definidas en las políticas de

seguridad de la información. Para ello se debe realizar:

- Análisis de posibles vulnerabilidades de los sistemas informáticos, para localizar de forma automática algunas de las vulnerabilidades mas conocidas.
- Pruebas de intrusión, en las que no sólo se detecten las vulnerabilidades, sino que se trata de explotar las que se hayan identificados.
- Registros de incidentes de seguridad de la información.

Con esta información obtenida es posible justificar la implantación de nuevas medidas de seguridad, así como de priorizar las medidas a implementar en función a las vulnerabilidades detectadas.

Una prueba de penetración consta de las siguientes etapas:

- Reconocimiento del tipo de información que podría obtener un atacante o usuario malicioso.
- Detección y verificación de las vulnerabilidades en los servidores y en aplicaciones desarrolladas por la institución.
- Intento de explotación de las vulnerabilidades detectadas
- Generación de informes, con el análisis de los resultados

2.9 Grupo de seguridad de la información

Se propone la formación de un grupo de personas con conocimientos y formación profesional en ciencias de la computación e informática, que tendrá entre sus responsabilidades:

- Monitoreo y pruebas de seguridad a los puestos de trabajo y servidores de la institución, con el objetivo de detectar vulnerabilidades y generar reportes y recomendaciones.
- Investigación en temas relevantes y actuales en el área de seguridad de la información.
- Diseño de mecanismos para detección de ataques, prevención y recuperación de datos en casos de fallas.
- Coordinación de la implementación de controles de seguridad.
- Promoción y difusión del uso de herramientas y buenas prácticas en materia de seguridad de la información.

- Auditoria de seguridad, revisión de los registros y actividades de los sistemas para verificar y asegurar que se cumplen las políticas de seguridad y los procedimientos operativos establecidos. Detectar las infracciones y recomendar oportunamente modificaciones en los controles, políticas y procedimientos de seguridad.

2.10 Gestión de Contraseñas

Mantener las contraseñas en secreto o tener una contraseña lo suficientemente difícil de adivinar es uno de los problemas que se presenta. El uso de contraseñas es el mecanismo más utilizado para la autenticación en los sistemas y que representa uno de los puntos mas débiles en la seguridad de la información, ya que cuando se revelan las contraseñas, ya sea robo, espionaje, ingeniería social, engaño, extorsión, fuerza bruta, se puede acceder a los sistemas y provocar daños o alteraciones a los mismos y a la información.

Hay muchos usuarios que eligen contraseñas muy cortas o fácil de averiguar, a otros les asignan las contraseñas de 8 caracteres y seleccionadas aleatoriamente, que sería difícil de adivinar pero también sería difícil de recordar para muchos usuarios.

Existen algunas recomendaciones para la gestión de las claves, tales como:

(a). No solo se conformen con letras o números, es mejor utilizar la combinación de ambos grupos y que incluyan mayúsculas, minúsculas y caracteres especiales

(b). No se puedan con el usuario.

(c). Cambiar la clave periódicamente y no repetirlas.

(d). Usar diferentes claves para los distintos servicios.

(e). No utilizar palabras del diccionario.

(f). Deben ser mayor a 8 dígitos.

(g). No compartir las claves.

¿Cómo se puede generar una clave que sea fácil de recordar, que cumpla las normas descritas en el sección anterior, que no pueda ser desacubierta por cualquier atacante, y que además, no genere una carga para el usuario (en su generación, resguardo, utilización)?. Se han desarrollado sistemas que facilitan la generación y resguardo de claves, algunos no cumplen con todas las recomendaciones descritas en la sección anterior (no quiere decir que no sean seguras) pero presentan otros inconvenientes como: la portabilidad de las claves para ser usada desde otra máquina. Existe otros inconvenientes y tienen que ver con la responsabilidad de las personas

para generar y resguardar las claves, esto depende de sus costumbres, el contexto social, uso consciente, tipo de información que resguarda y el nivel de riesgo que implica.

2.10.1 Claves con menos de ocho dígitos

Existen 96 caracteres posibles a utilizar en una clave (letras minúsculas y mayúsculas, números, símbolos). En una clave con 8 dígitos existen 96^8 (7.213.895.789.838.336) posibilidades para adivinarla y analizando 1.000.000 posibilidades por segundo tardaría 228 años, en probarlas todas (peor de los casos).

Probablemente no se dispone de esa cantidad de tiempo para verificarlos por el método defuerza bruta. Existen métodos que reducen el tiempo de descubrimiento de las contraseñas, como probar primero con palabras de diccionarios, palabras que tenga relación con el usuario, ya que la mayoría de las contraseñas de los usuarios se conforman de esta manera.

Existen técnicas básicas para la selección de contraseñas. Se les puede explicar a los usuarios la importancia de usar contraseñas difíciles de adivinar, sensibilizándolos en las posibles implicaciones de una mala gestión de las contraseñas. Recomendaciones para la selección de las contraseña fuertes

Seleccionar una oración que sea fácil de recordar y a partir de ella generar la contraseña. Por ejemplo:

- Oración 1, *Mi hermana Sofía me regaló una poderosa computadora*
- Oración 2, *Pase todas las materias con 20 puntos*

Si tomamos los primer caracteres de cada palabra de la oración nos resultaría:

- Oración 1, `MhSmr1pc`
- Oración 2,`Ptlmc20p`

Si a esto se le incorpora reglas como por ejemplo, cambiar la `p` por algún símbolo, que para este caso será (%), entonces las oraciones quedarían:

- Oración 1, `MhSmr1%c`
- Oración 2, `%tlmc20%`

Como se puede notar, de esta manera se generaría una buena contraseña, que es difícil de adivinar por un tercero, y fácil de recordar para la persona ya que es generada a partir de oraciones particulares que se pueden recordar.

2.11 Qué se entiende por puesto de trabajo?

Al lugar físico y/o lógico donde al usuario se le asignan ciertos privilegios de accesos a los recursos que le permite el desarrollo y cumplimiento de las tareas, funciones y actividades que ejecuta para la institución. Los puestos de trabajos forman parte de los bienes/activos de la institución y debe existir una responsabilidad por parte de la persona asignada para su mantenimiento, correcto uso y funcionamiento.

2.12 Centro de datos

Se puede definir como una infraestructura y plataforma tecnológica (cómputo, almacenamiento y comunicaciones), que tiene como objetivo prestar la mayoría de los servicios informáticos y de comunicaciones a la institución. En el centro de datos se concentra y procesa todos los recursos lógicos con que opera la institución.

2.13 Que es seguridad lógica?

Se refiere a la aplicación de mecanismos y procedimientos para mantener el resguardo, la integridad de activos informáticos (archivos, sistemas, datos, etc.) y el acceso a personas autorizadas a los activos lógicos de la institución

Se debe definir que es activo lógico.

2.14 Qué es seguridad física?

Se refiere a los mecanismos de seguridad que generan barreras físicas y de control de los equipos computacionales como medida de prevención y protección de los activos informáticos de la institución, evitando el acceso no autorizado a los equipos y a los medios de almacenamiento de datos o cualquier desastre o contingencia.

2.15 Cuenta de usuario

Se refiere al permiso que se le asigna a un usuario de un determinado sistema, que le permite acceder y operar sobre el de forma remota, de acuerdo con unos roles definidos

Modificar. cuenta de usuario es diferente de permisos

2.15.1 Cuenta de usuario crítica

Son aquellas cuentas que dan accesos a recursos, servicios e información que se considere importante o vital para el normal funcionamiento de los recursos o servicios de la institución como por ejemplo: cuentas de administración de los equipos de computación (que en algunos sistemas se denomina “root”), entre otros.

2.16 Vulnerabilidades de los sistemas de información

Se refieren a los riesgos que tiene los sistemas informáticos, que pueden afectar la confidencialidad, integridad, disponibilidad de los datos y aplicaciones.

2.16.1 Causas de las vulnerabilidades de los sistemas informáticos

Entre las causas que se consideran responsables de las vulnerabilidades que afectan a los sistemas informáticos se tienen:

- Debilidad en el diseño de los protocolos utilizados en las redes, como por ejemplo los protocolos de transmisión de información en texto claro.
- Fallos en los diseños y/o codificación de los programas.
- Configuración inadecuada de los sistemas informáticos.
- Políticas de seguridad deficientes o inexistentes.
- Desconocimiento y falta de sensibilidad de los usuarios y de los responsables de informática. todas las soluciones tecnológicas que la institución pueden implementar (sistemas de detección de intruso, cortafuego, etc) resultan inútiles antes el desinterés, falta de información, falta de preparación en materia de seguridad. La falta de sensibilización de los directivos y responsables de la organización, que deben ser conscientes de la necesidad de destinar recursos a esta función
- Poca disponibilidad de herramientas, de fácil instalación, utilización, con detallada documentación.
- La incorrecta instalación, configuración y mantenimiento de los equipos

La institución podría utilizar herramientas para realizar análisis y evaluación de vulnerabilidades, que permitan conocer la situación real de los sistemas y de acuerdo con esa información se podrían reajustar las políticas de seguridad, implantación de mecanismos o medidas de seguridad.

2.17 Herramientas para la seguridad de la información

2.17.1 Cortafuego

Un cortafuego es un sistema que permite filtra las comunicaciones entre dos o más redes (por ejemplo la red de una institución (red privada) e Internet) a partir de unas reglas definidas de acuerdos con las políticas de seguridad de la institución, en procura de proteger la red y activos de la institución de ataques provenientes de una red que no es confiable como la Internet.

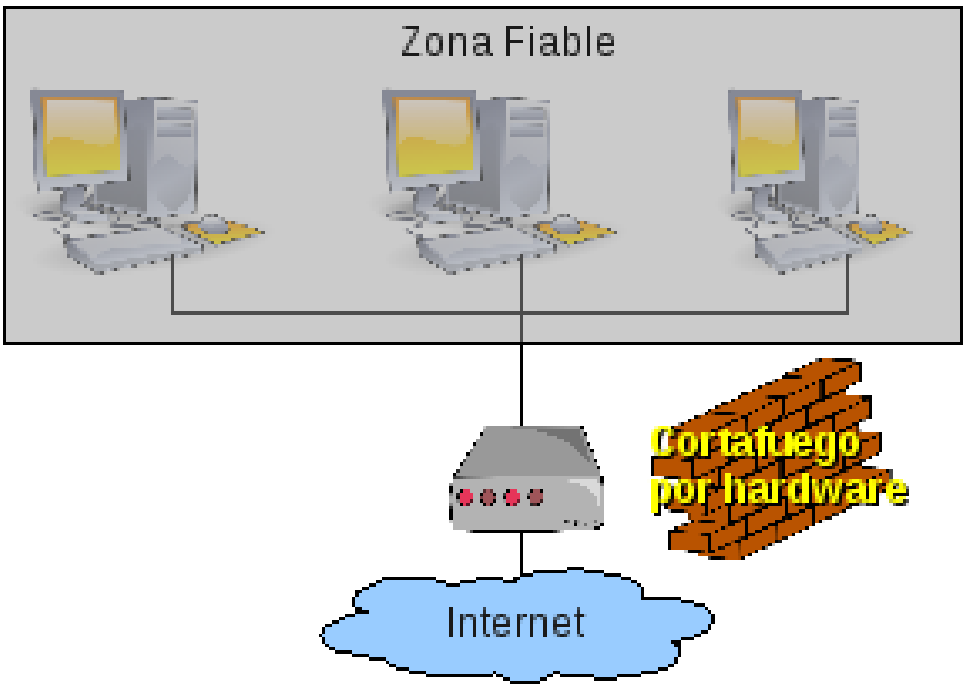

Figura 2.4 *Corta fuego por Hardware.*

Hay cortafuego por software y por hardware (Figura 2.4). En el cortafuego por software, hay que definir y probar la mayoría de las reglas, ocupa espacio y procesamiento en el servidor donde esta instalado, son mucho más baratos y por lo general son utilizados en instituciones pequeñas.

Todo el tráfico entrante y saliente de la institución debe pasar a través del cortafuego por lo que el administrador puede permitir o denegar el acceso a la Internet y a los servicios de la institución: un segmento de la red interna, una máquina en específico, de manera selectiva.

También se puede instalar un cortafuegos en un computador dentro de la red interna − *cortafuego personal* −, figuras 2.6, 2.7) que sólo controla el trafico que entra y sale de ese computador, de esta manera se pueden agregar reglas de filtrados a esa computadora, de acuerdo a la necesidad del usuario.

Cortafuego personal, es el término utilizado para los casos donde el área protegida se limita sólo al computador donde está instalado el cortafuego.

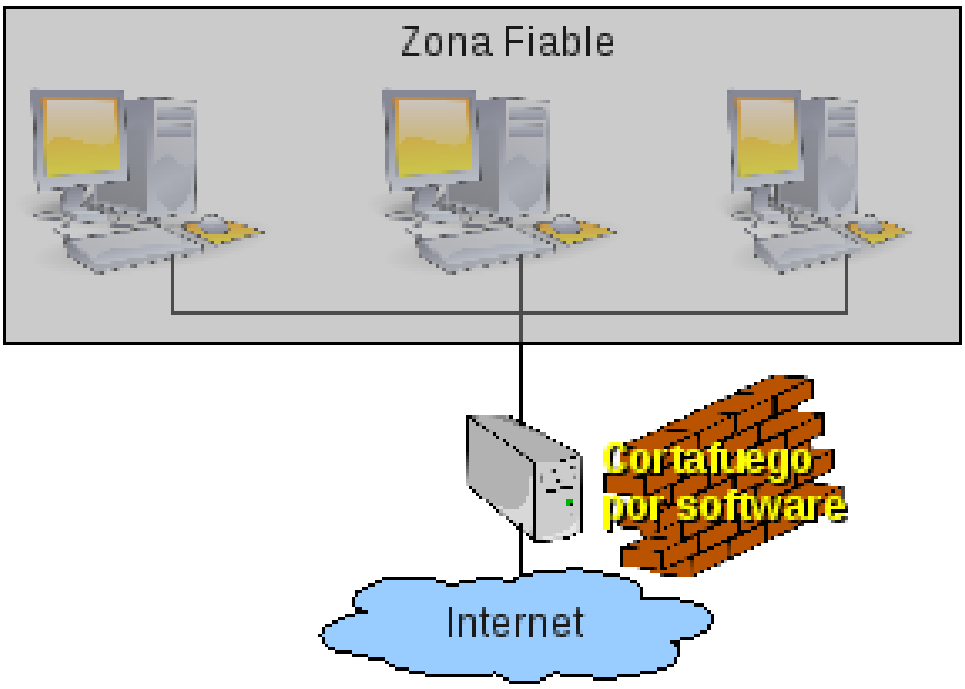

Figura 2.5 *Cortafuego por Software.*

2.17.2 Para qué sirve el cortafuego?

Es una herramienta de seguridad, que ofrece los siguientes servicios:

- Restringir el acceso a determinados programas, segmento de red de la institución, servicios de Internet, ciertas paginas web, bloqueando el tráfico no autorizado por la organización y no permitiendo ataques a las computadoras desde el exterior e interior de la red.
- Ocultar de los equipos internos de la institución, de forma que éstos no puedan ser detectados ante ataques que provengan del exterior. Asimismo pueden ocultar información sobre la topología de la red interna, los nombres de los equipos, tipo de protocolos utilizados, etc.
- Auditar y registrar el uso de la red.
- Mejorar el aprovechamiento del ancho de banda utilizado en la institución
- Monitorear los ataques o intentos de intrusión a la red de la institución.

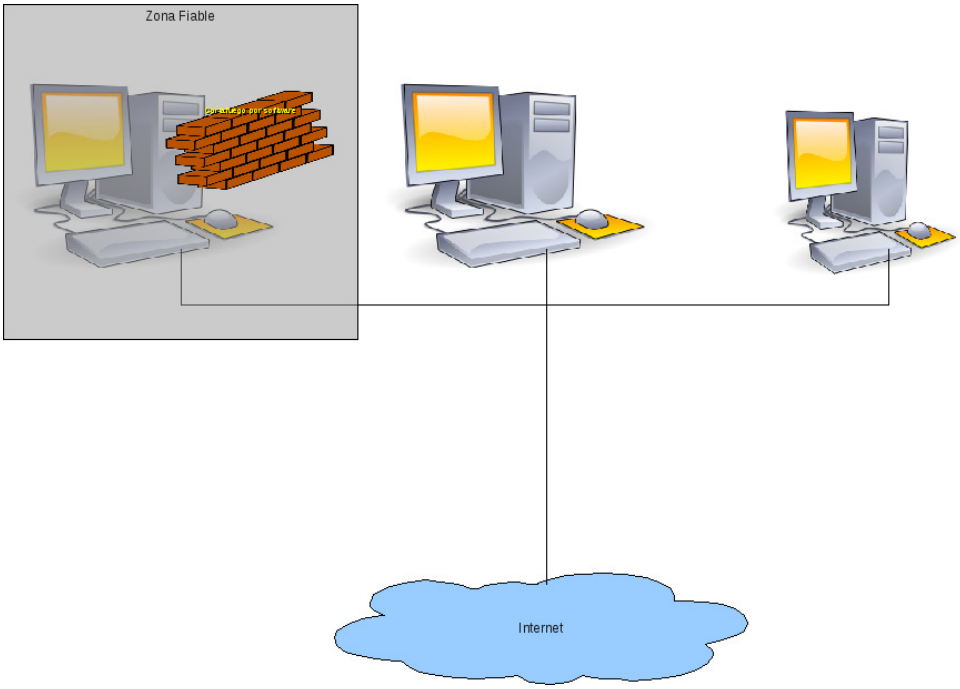

Figura 2.6 *Cortafuego personal.*

2.17.3 Consideraciones para la instalación y configuración de cortafuegos

Dentro de las políticas de seguridad de la información se deben considerar el uso de cortafuegos, donde se especifique configuración y la persona responsable de la administración.

Consideraciones para la Configuración de un cortafuego:

- Conocer los protocolos y servicios de la Internet.
- El equipo debe encontrarse libres de virus, de programas espías (spyware), programas maligno (malware).
- Análisis de los servicios requeridos de Internet y de la información que se maneja en los puestos de trabajos o servidores.
- Clasificación o estructuración de la red interna por zonas de acuerdo a las necesidades de seguridad.
- Mantener actualizado el cortafuego.

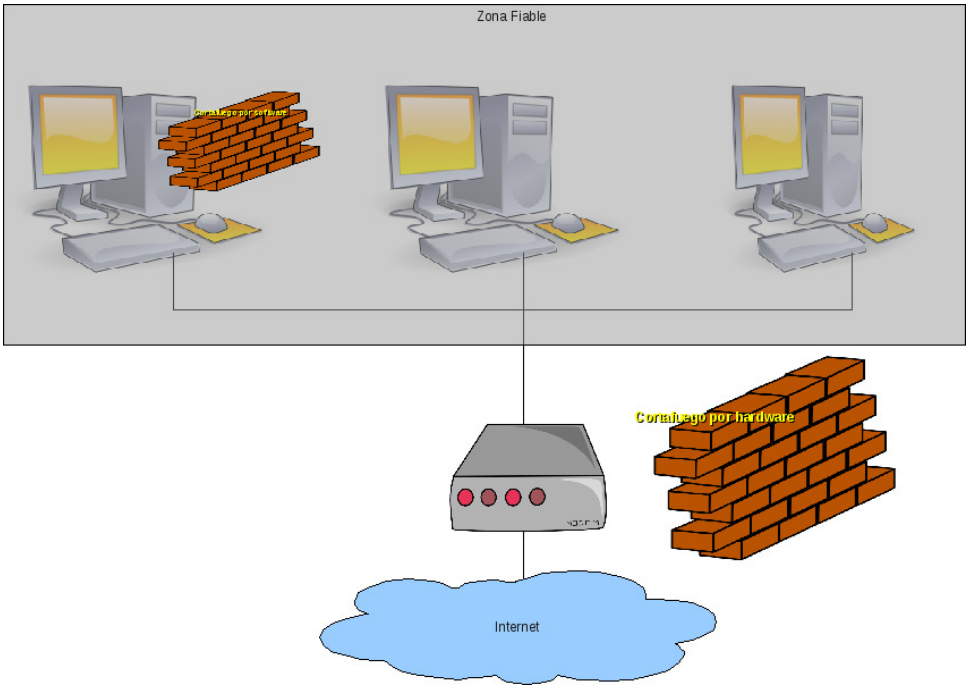

Figura 2.7 *Cortafuego personal combinado.*

Las reglas de filtrado son difíciles de difinir y de verificar, por lo que se deberían ser revisadas frecuentemente por los administradores de la red.

2.17.4 Sistemas de detección de intrusiones (IDS)

Estos sistemas se encargan de detectar y reaccionar de forma automática antes los incidentes de seguridad que tienen lugar en las redes y computadoras, que de acuerdo a unos patrones (comportamiento de actividades sospechosas) establecidos por defecto y los definidos por el administrador del sistema (de acuerdo a las políticas de seguridad), detectan y permiten prevenir la intrusión.

Revisar el siguiente párrafo El término vulnerabilidad hace referencia a la condición en los componentes de un sistema o en los procedimientos que afectan al funcionamiento del mismo posibilitando la consecución de una operación que viola la política de seguridad del sistema.

Funcionamiento básico de los IDS:

- Una fuente de eventos del sistema.

- Una base de datos con los patrones de comportamiento que se consideran como normales, así como los perfiles de posibles ataques.

- Motor de análisis de los eventos para detectar las evidencias de intento de intrusión.

- Módulo de respuesta, que de acuerdo al análisis de los eventos, realiza determinadas acciones.

La figura 2.8 muestra la estructura funcional básica del IDS.

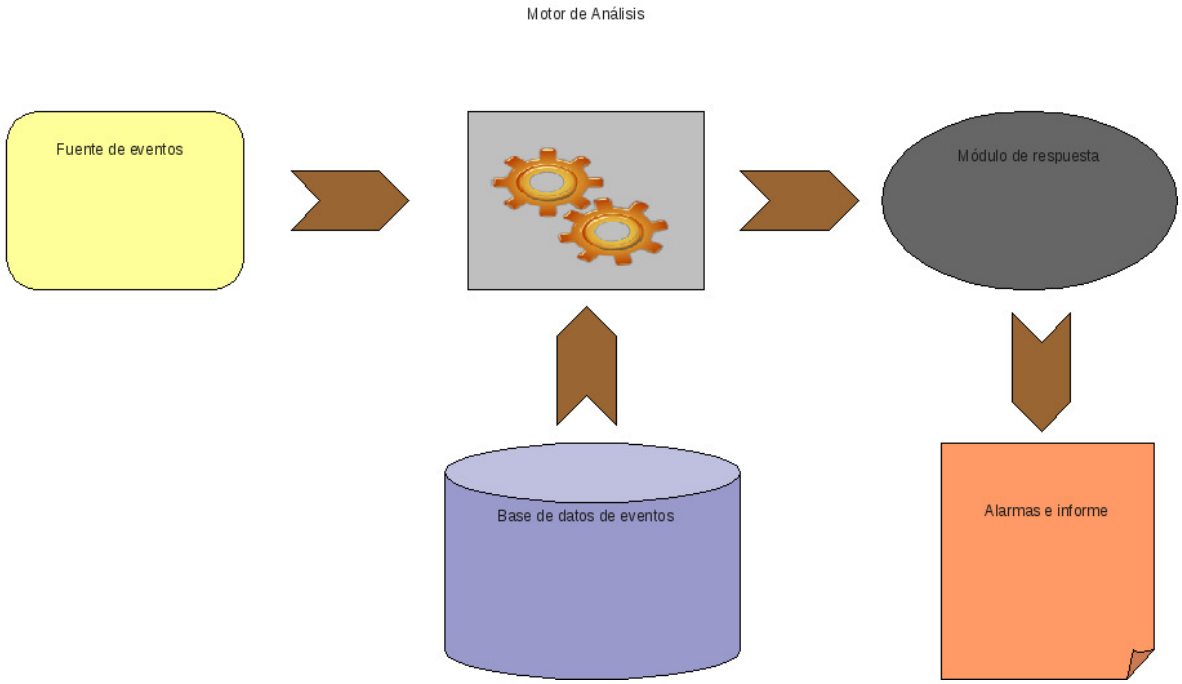

Figura 2.8 *Estructura funcional básica del IDS.*

Los IDS pueden presentar problemas y limitaciones, podrían generar falsas alarmas, ya sean falsos negativos, que se producen cuando los IDS no pueden detectar algunas actividades relacionadas con incidentes de seguridad que está ocurriendo en la red o en los equipos informáticos, o bien falsos positivos, que se presenta cuando los IDS registran y generan alertas sobre determinadas actividades que no resultan problemáticas, ya que son normal en el funcionamiento de los sistemas.

2.18 Identificación de los riesgos a terceros

Cuando exista la necesidad de otorgar acceso a terceras personas se debe llevar acabo una evaluación de los riesgos que representan para determinar las implicaciones en la seguridad y los requerimientos de controles. Para cada grupo de terceras personas se debería llevar la evaluación y definición de los controles de seguridad.
Se requiere considerar el tipo de acceso requerido (físico, lógico); de acuerdo a las actividades que va a realizar en la institución, si se va a requerir del uso de activos lógicos de la institución, y/o acceso a determinadas áreas, que pueden ser vitales a la institución, y de acuerdo a esto, tener la certeza de permitirlo o no.

Para este tipo de riesgos se recomienda:

- Los medios de procesamientos de información a las cuales necesita tener acceso (equipos muy especializados, delicados, sensibles, costosos).
- Evaluar la información a la que se accede, medido en diferentes aspectos (Económicos, sociales, morales, entre otra).
- Especificarle a las terceras personas las costumbres de la institución y de las personas que trabajan en ella en materia de la seguridad de la información, en relación con a las costumbres de la comunidad, y otros visitantes.
- Evaluar el nivel de confianza, entendido como qué tanto se confíe en que terceros no dañen o usufructúen los activos de información de la institución. Esto puede realizarse utilizando una historia detallada de incidentes de seguridad, a la cuál pueda aplicarse herramientas estadísticas.
- Configurar los recursos informáticos requeridos.
- Cargar los procesos en la realización de la actividades para el cumplimientos de las políticas de seguridad.
- Especificar el nivel de seguridad físico (espacio físico) en su estancia en la institución y en realizar las actividades de acuerdo con los niveles de confianza,
- Disponibilidad de una red inalámbrica o cableada con sólo determinados servicios de acuerdo a las necesidades de las personas.
- Estbalecer las responsabilidades de la institución por actos de las personas que utilicen recursos de la institución como el uso del correo institucional, acceso a la información confidencial de la institución a terceros, ataques o intento de intrusión contra equipos utilizando la red de la institución.

2.19 Seguridad lógica en los puestos de trabajo

Entre las recomendaciones de controles para los puestos de trabajo se debe proponer al personal:

- Determinar y clasificar el grado de criticidad de la información que se maneja en los sistemas de almacenamiento ubicados en los puestos de trabajo.
- La contraseña de administración de los equipos de computación (que en algunos sistemas se denomina “root”), sólo debe ser conocida por las personas responsables del puesto de trabajo; debe ser seleccionada siguiendo las recomendaciones propuestas en la sección 2.10.
- Realizar cambios de las contraseñas cuando se tenga el menor indicio de vulnerabilidad o se sospeche que personas no autorizadas tenga el acceso o conocimiento de la misma
- No utilizar la misma clave para diferentes sistemas de autenticación en el puesto de trabajo: correo electrónico, usuarios del sistema operativo (root), aplicaciones
- Definir políticas para generar, eliminar, y modificar las claves de usuarios en los puestos de trabajo evitando la carga de trabajo para las personas.
- Mantener el sistema operativo y aplicaciones actualizadas.
- Utilizar herramientas y procedimientos que verifiquen la integridad y la fuente de los paquetes a instalar (mecanismos de verificación de integridad y autoría).
- Utilizar el correo institucional con métodos criptográficos para proteger la confidencialidad e integridad de los mensajes.
- Establecer políticas referentes al bloqueo automatico de las sesiones de trabajo cuando no se encuentre el responsable del puesto.
- Recomendar la instalación y configuración de cortafuegos de software personales para incrementar la seguridad en el puesto de trabajo.

2.20 Seguridad lógica en el centro de datos

- Seleccionar los protocolos de comunicaciónen función a las necesidades de la institución.
- Segmentar la red de la institución por grupos de usuarios, servicios internos y externos, para tener un mayor control y seguridad de la misma.
- Utilizar sistemas de detección de intrusos, para detectar el acceso no autorizado a los activos de la institución.
- Respaldar la información local y de los servidores de forma periódica.
- Cerrar todas las sesiones de red después de ser utilizadas.

- Controlar el acceso remoto a los equipos de la red institucional a través de herramientas seguras.
- Utilizar sistemas de controles de cambios para verificar las modificaciones realizadas en los equipos de computación.
- Utilizar buenas prácticas de seguridad en el uso y selección de las contraseñas (ver sección 2.10).
- Utilizar contraseñas para proteger el acceso a la configuración de hardware básica de los equipos.
- Configurar los servidores de manera segura:
  - Desactivar servicios y cuentas que no vayan a ser utilizadas.
  - Instalar los últimos parches de seguridad y actualizaciones publicados por el fabricante. Convendría comprobar su correcto funcionamiento en otra maquina de pruebas antes de la máquina de producción.
  - Utilizar sólo los protocolos y servicios necesarios.
  - Activar los registros de actividades de los servidores (logs).
  - Disponer de una copia de seguridad completa del sistema operativo de cada servidor tras una configuración correcta.
  - Instalar herramientas que permitan comprobar la integridad de los archivos del sistema.
  - Modificar el mensaje de inicio de sesión para evitar que no se pueda mostrar información sobre la configuración y recursos del sistema a un posible atacante.
- Llevar un control de registro y des-registro de los usuarios con sus respectivos roles y niveles de acceso a los activos de la institución
- Eliminar o bloquear inmediatamente los privilegios de acceso de los usuarios que han cambiado de área, departamento o han dejado la institución.

2.21 Seguridad física en los puestos de trabajo

Entre algunas de las recomendaciones se tienen:

- De acuerdo a la información que se maneje se determinará la ubicación y seguridad física de los puestos de trabajo. la información que es confidencial y con un limitado acceso de personas, se recomienda que los puestos de trabajo deben estar ubicados en locales cerrados, utilizando perimetros de seguridad.
- Los equipos deben contar con fuentes o suministros de poder (UPS), para regular la corriente y proporcionar energía eléctrica continua. Un pico de tensión

alta puede ocasionar que se queme algún componente eléctrico de la computadora, o los pequeños y repetidos picos de voltajes pueden acortar la vida útil de los componentes de la computadoras.

- Los equipos deben estar ubicados en un ambiente de trabajo adecuado (temperatura, humedad, polvo, según las características de las computadoras).

- Las ubicación de las equipos (cpu, ups) y el cableado no deben ser golpeados. Los cables no pueden ser pisados ni cortados, ni se les colocar otros objetos encimas o contra ellos.

- Mientras se esté trabajando en el puesto, se debe tener cuidado al consumir alimentos y/o ingerir líquidos.

- Contar con planes de mantenimiento de los equipos de los puestos de trabajos, en concordancia especificaciones de valores y servicios recomendadas por el proveedor de los equipos, de esta manera se pueda alargar la vida útil de los equipos y se pueden detectar a tiempos posibles fallas.

2.22 Seguridad física en el centro de dato

Para establecer la seguridad física se deben tener en consideración varios aspectos (físico, lógico y ambiental) que permitirán una configuración apropiada y segura para el centro de datos. En ssta área por lo general se encuentra un alto porcentaje de los activos de la institución. En él concentran y se procesan todos los recursos lógicos con que opera la institución. Para configurar un buen centro de datos se debe considerar:

2.22.1 Servicios que presta o prestará el centro de datos:

- Tipos de servicios a prestar tanto a los usuarios internos como externos.

- Cantidad de usuarios que requiere ingresar y permanecer en el centro. Tipo de usuarios que se beneficiarán de los servicios prestados.

- Estimación de crecimientos al futuro (incluir nuevos servicios internos, externos que requiera la instalación de nuevos equipos computación).

- Especificar las características y especificaciones técnicas de los equipos.

Con esta información se pueden establecer las relaciones con la capacidad de procesamiento, cantidad de equipos computacionales requerido, espacio físico y acondicionamiento del espacio (aire acondicionado, capacidad de la planta eléctrica, etc.)

2.22.2 Ubicación y condición física del centro de datos

La selección de la ubicación de un centro de datos, es un factor determinante en su correcto funcionamiento, puesto que de esto depende la mayor protección y seguridad de una de las áreas más importantes de cualquier institución.

Para la ubicación del centro de datos se recomienda que:

- Se encuentre alejado de instalaciones eléctricas como radares, microondas, etc. para que no influyan en el funcionamiento de los equipos de computación del centro de datos.
- Se encuentre lejos de estaciones de materiales volátiles, estaciones de servicio (bombas de gasolina), por que representan peligros por incidentes intencionado o fortuitos.
- Se encuentren en lugares no desolados o desprotegidos.

Entre los factores inherentes a la localidad hay que considerar:

- Si el terreno donde se encuentra ubicado presenta problemas de hundimiento
- Si existen condiciones climatológicas adversas (áreas de constantes lluvias y descargas eléctricas, altas temperaturas, etc.)
- Si está ubicada en un área con constantes actividades sísmicas.
- Si está ubicada en áreas de inundaciones.

Además se debe contar con todos los servicios que requiere el centro de datos para: comunicación, procesamiento y almacenamiento de datos.

- Líneas telefónicas.
- Instalaciones eléctricas.
- Antenas de comunicación, etc.

2.22.3 Especificaciones técnicas del centro de datos

Se debe considerar:

- Espacios amplios disponibles por la institución con todos los servicios que requiere el centro de datos.
- El acceso de los equipos de computación y del personal al centro de datos, debe ser lo más cómodo y seguro posible, para evitar que se presenten incidentes, como por ejemplo: en los traslados de los equipos de computación

- Buen diseño de las instalaciones de suministro eléctrico, que garantice el suministro y la disponibilidad de la energía eléctrica estable, y además sea independiente del resto de la instalaciones del edificio del la institución.
- Se debe contar con un acondicionamiento térmico del local que controle la humedad y la temperatura requeridas por los equipos computacionales del centro de datos
- Instalación de pisos falso, para evitar que las descargas eléctricas afecten a los equipos por su característica conductiva, y para una óptima distribución de cableado, canaletas, aire acondicionado.
- Se debe considerar la resistencia del piso falso que soporte el peso de los equipos de computación y personal que se encuentra en el centro de datos
- Se debe sellar herméticamente para preservar las condiciones térmicas del local del centro de datos y para evitar la entrada de cualquier sustancias extraña que pueda generar algún incidente.
- Contar con sistemas de aterramiento, que permiten absorber las descargas eléctricas.
- Para las paredes y techos del centro de dato se recomienda usar pintura plásticas lavables para poderlos limpiarlos fácilmente y evitar las erosión, la altura del techo debe estar entre los 2,70m y 3,30m para permitir la movilidad del aire dentro del centro de datos.
- Debe contar con ductos lisos y sin desprendimiento de partículas con el paso del aire que pudiera afectar a los equipos de computación
- El cableado del centro de datos se recomienda que esté dispuesto por debajo del piso falso, ubicado de forma separada en función al tipo de cable (de alto voltaje, de bajo voltaje, de telecomunicación, y los de señales para dispositivos de detección de fuego).
- Evitar conectar múltiples dispositivos en el mismo tomacorreinte para evitar sobrecargas en los circuitos eléctricos del centro de datos.
- Se deben evaluar al momento de diseñar un centro de datos el suministro eléctrico, ya que si no se efectúa un buen cálculo sobre la carga que se va a utilizar, podría ocasionar serios problemas al utilizar los equipos.
- Se requiere de la disposición de planta generadora de corriente para evitar la paralización de las actividades del centro de datos en los periodos de corte de energía eléctrica. Las características de las platas eléctricas y su instalación, estará en función a las necesidades eléctricas del centro de datos.
- Contar con fuentes o suministro de poder (UPS) para proteger a los equipos electrónicos por fluctuaciones de poder.

2.22.4 Control de acceso físico al centro de datos

Los sistema de control de acceso debe ser un sistemas flexibles y confiables para el control, monitoreo, registro, verificación de los datos de acceso para permitir el acceso solo al personal autorizado a las instalaciones o áreas restringidas de la institución. Los sistema de control de acceso, involucran al personal de seguridad, a la política de seguridad, al hardware y el software.

Se recomienda hacer tomar en cuenta lo siguiente:

- Identificar personal que entra y sale del centro de datos.
- Durante la noche, el fin de semana, los descansos o cambios de turnos el control de debe ser sean tan estricto como en el horario normal.
- Se debe identificar, controlar y vigilar las actividades que realizan las terceras personas durante su estadía en el centro de datos. Entre las personas que se consideran como terceras personas están, los visitantes, personal de limpieza, personal de mantenimiento de los diferentes equipos.
- Instalación de Torniquetes.
- Utilizar cerraduras electromagnéticas.
- Utilizar circuitos cerrados de televisión
- Utilizar detectores de movimiento.
- Utilizar tarjetas de identificación.
- Utilizar control de aperturas de puertas
- Utilizar control de acceso mediante sistemas electrónicos con tarjetas de proximidad

2.22.5 Aire acondicionado

Los equipos modernos de computación generan grandes cantidades de calor. Se debe prever de un sistema de aire acondicionado para mantener una temperatura un clima adecuado que permita que los equipos funcionen bien. Se debe considerar lo siguiente:

- El aire acondicionado debe ser exclusivo para el centro de datos por las condiciones especiales que se requieren.
- Se debe contar con aire acondicionado de respaldo, en el caso que el principal presente problemas. Con esto se evita que se tengan que apagar los equipos computacionales y se asegura la disponibilidad de los servicios que presta en centro de datos.

- Tener los controles y las alarmas de temperatura y humedad que permitan la detección y la acción oportuna de corrección de los niveles de temperatura y humedad sin afectar los equipos de computación del centro de dato
- Tener ls suficiente capacidad de los equipos de aire acondicionado en función de las necesidades de los equipos instalados en el centro de datos y su posible tasa de crecimiento
- Considerar los riesgo que representa los aires acondicionado, el mal funcionamiento ocasiona que los equipos sean apagados, se pueden producir Incendios y inundaciones

2.22.6 Protección, detección y extinción de incendios

Para los centros de datos se tiene las siguientes consideraciones para proteger, detener y extinguir los incendios:

- El materiales de las paredes deben ser antifuego
- Techo resistente al fuego
- Canales y aislante resistente al fuego
- Sala y área de almacenamiento de equipos impermeables
- Sistema de drenaje en el piso firme
- Detectores de fuego alejado del aire acondicionado
- Alarmas de fuego conectado al sistema de detección temprana de humo

2.23 Especificación de las Políticas de seguridad de la información en el centro de datos

En el momento de especificar las políticas de seguridad de los sistemas informáticos para el personal de la institución requiere contemplar los siguientes aspectos:

- Especificar los procedimientos para la creación de nuevas cuentas críticas.
- Especificar niveles de acceso físico y lógico de los recursos computacionales de la institución, para establecer quiénes están autorizados para realizar determinadas actividades y operaciones; a qué datos, aplicaciones y servicios, desde qué máquina puede acceder, quiénes pueden acceder a los centros de datos.
- Especificar los procedimientos para eliminar/bloquear las cuentas y los posibles escenarios que puedan incurrir en esta medida.

- Establecer el personal que delegará la responsabilidad del control de: usuarios, claves, entre otros, en los momentos cuando no esté el responsable principal.
- Especificar políticas de respaldo y recuperación ante incidentes para garantizar el continuo funcionamiento de los sistemas de la institución.
- Especificar los procedimientos para respaldar o eliminar información o sistemas de los equipos de computación (ver sección 2.24).
- Especificar las posibles violaciones y consecuencias derivadas del incumplimiento de las políticas de seguridad. **revisar**.
- Especificar las sanciones a los responsables por la violación de las políticas de seguridad.
- Clasificar la información e identificar los activos de la institución. **¿Para qué?**.

Entre las actividades y responsabilidades que se deben delegar y considerar para las políticas de seguridad se tienen:

- Mantener en óptimas condiciones el funcionamiento de la red para garantizar su disponibilidad.
- Revisar periódicamente el estado físico del cableado horizontal y vertical de la red de la institución.
- Realizar periódicamente mantenimientos preventivos y correctivos a los equipos de telecomunicaciones. Se recomienda que el mantenimiento se realice semestral, además deberá ser registrado en bitácoras.
- Supervisar y mantener adecuadamente las instalaciones de la infraestructura de red.
- Solucionar los problemas relacionados con conflicto de direcciones IP.
- Administrar y operar los Servidores de la Red.
- La red institucional no será instrumento de experimentos que pongan riesgo la integridad de la información.
- Configurar y supervisar los equipos de comunicaciones.
- Construir un mapa de red y actualizarlo ante cambios.
- Asegurar las contraseñas críticas como: administrador (root), aplicaciones como cortafuegos, servidores, entre otros.
- Ubicar los equipos en salas (centro de datos) con acceso restringido y medidas de seguridad física, utilizando estándares o certificaciones.

2.24 Políticas de Respaldo y recuperación

Se requiere contar con políticas de respaldo y recuperación para garantizar el continuo funcionamiento de los sistemas de las instituciones. La recuperación de los sistemas posterior a la interrupción de índole natural o accidental como incendios, mal funcionamiento de los sistemas, errores humanos, entre otros, resulta necesario, requiriendo de una acción rápida para poner nuevamente disponible el servicio y de esta manera asegurar la disponibilidad.

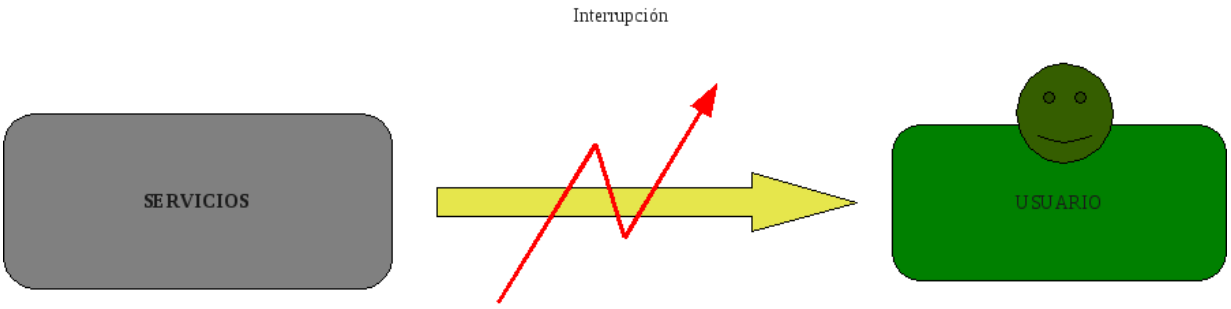

Figura 2.9 *Interrupción de los servicios.*

Para garantizar la disponibilidad de los servicios es necesario contar con planes de contingencias ante desastres y para esto se requiere aplicar las políticas de respaldo y recuperación. En la figura 2.9 se muestra un bosquejo sobre la interrupción de servicios.

2.24.1 Normas para las políticas de respaldo y recuperación

- Las copias de respaldo de datos y archivos de servidores deben ser realizadas y supervisadas por personal debidamente autorizado.
- Debe existir para todo los activos de información de la institución, la documentación de los procedimientos de respaldo y recuperación.
- Planificar las copias de respaldo que se deben realizar en función del volumen y del tipo de información generada por los sistemas informáticos
- Todas las copias de respaldo y medios de almacenamiento utilizados, deben estar bien identificadas con información tal como: a qué equipo de computación pertenece, contenido de la copia de respaldo, fecha y hora de ejecución del respaldo, cronogramas de ejecución del respaldo, tipo de respaldo (completos, incrementales, diferenciales), cuantos medios de almacenamiento fueron uti-

lizados, identificación de la persona que ejecuta el respaldo, ubicación asignada para su almacenamiento, personas responsables del almacenamiento.

- Establecer los sistemas o técnicas que se van a emplear para garantizar la privacidad e integridad de los datos que se guarden.
- Se debe contar con un lugar de resguardo para los respaldos, físicamente seguro y que posean controles de acceso.
- Generar en un tiempo determinado dos copias de los respaldos, unas de esas copias, se debe resguardar en otros sitio fuera del edificio, este sitio debe igualmente cumplir con determinados características de seguridad al sitio principal. Además el acceso y traslado de las copias deben ser realizados por personal debidamente identificado y autorizado para ejecutar el procedimiento.
- Efectuar las pruebas de recuperación en un tiempo determinado y definido para verificar el estado de los soportes y el correcto funcionamiento de los procedimiento de copias de respaldo.
- Para los casos de aplicaciones críticas se recomienda implementar técnicas de sincronización automática, por hardware y software de forma que si la aplicación principal deja de funcionar la otra aplicación espejo tome el control inmediatamente o en un tiempo mínimo requerido para su ejecución.

2.25 Gestión de Incidentes de seguridad

Cualquier evento que pueda ocasionar la interrupción o degradación de los servicios de los sistemas. Estos incidentes pueden ser intencionados, por error de aplicación de las políticas y procedimientos de seguridad, de desastre natural o del entorno como las inundaciones, incendios, tormentas, fallos eléctricos entre otros.

Entre las actividades y tareas que se deben tener en cuenta están las siguientes:

2.25.1 Antes del incidente de seguridad:

- Se debe contar con equipo de solución: sera el equipo encargado de activar y coordinar el plan de contingencia. Este equipo debe estar constituido por personas que cuenten con la experiencia y formación necesaria que pueda dar respuesta ante cualquier incidente de seguridad. Debe existir una lista de números telefónicos y direcciones actualizadas para la ubicación de las personas que conforman este equipo en el momento que ocurra un incidente de seguridad.
- Identificación de las áreas criticas y/o operativas de la institución, para la misma se consideran los servicios, equipos, aplicaciones, infraestructura, existentes dentro de la institución.

- Hacer inventario de los equipos y servicios. Se requiere de una descripción detallada como por ejemplo la ubicación, configuración, características, y procedimientos de respaldo y recuperación.

- Considerar todos los posibles escenarios de incidentes de seguridad que puedan ocurrir en cada área crítica identificada. Los mismos deben estar bien documentados.

- Describir clara y detalladamente los planes de contingencia de todos los posibles escenarios de incidentes de seguridad, donde se indiquen los procedimientos de actuación necesarias para la restauración rápida, y eficiente.

- Efectuar reuniones al menos una vez al año para la revisión del plan de contingencia, en función de evaluarlas y/o actualizarlas.

- Detección de incidentes de seguridad. La institución debe prestar especial atención a los indicadores de incidentes de seguridad, como una actividad a contemplar dentro del plan de respuesta a incidentes. E ntre estos indicadores tenemos:

  – Cambio de configuración de los equipos de red como: activación de nuevos servicios, puertos abiertos no autorizados, etc.

  – Caída en el rendimiento de la red o algún servidor debido a un incremento inusual del trafico de datos.

  – Caída o mal funcionamiento de servidores como: reinicio inesperado, fallos en algún servicio.

  – Existencias de herramientas no autorizadas en el sistema.

  – Aparición de nuevas cuentas de usuarios o registro de actividades inusuales en algunas cuentas como: conexión de usuarios en horarios poco usuales.

2.25.2 Durante el incidente de seguridad:

- Análisis del incidente de seguridad, para determinar el alcance (aplicaciones afectadas, información confidencial comprometida, equipos afectados, entre otras), para ayudar al equipo de solución a tomar soluciones adecuadas y permitan establecer prioridades en las actividades que se deben llevar a cabo. **describir cuáles**.

- Puesta en marcha el plan de contingencia de acuerdo al incidente de seguridad presentado.

- Contención, erradicación y recuperación. El equipo de solución debe de llevar a cabo una rápida actuación para evitar que el incidente de seguridad vaya a tener mayores consecuencias a la institución.

2.25.3 Después del incidente de seguridad:

- Análisis y revisión del incidente. Causas del incidente, valoración inicial de los daños y sus posibles consecuencias
- Una completa documentación del incidente facilitará su posterior estudio. Entre los aspectos que debe tener reflejado la documentación se tiene:
  - Descripción del tipo de incidente: ataque a la seguridad, procedimientos de seguridad, desastres naturales.
  - Hechos registrados (como por ejemplo: logs de los equipos)
  - Daños producidos en los sistemas informáticos
  - Decisiones y actuación del equipo de respuesta
  - Lista de evidencias obtenidas durante el análisis y la investigación
  - Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en un futuro
- Actualización de los planes de contingencia de ser necesario
- Realizar un seguimiento o monitoreo del sistema en busqueda de vulnerabilidades omitidos o recreados luego de la recuperación de los sitemas.
- Aplicación de Informática forense. Esta proporciona los principios y técnicas que facilitan la investigación de los eventos informáticos ocurridos, mediante la identificación, captura, reconstrucción y análisis de evidencias. Entre las etapas para el análisis forense se tienen:
  - Identificación y captura de las evidencias
  - Preservación de las evidencias
  - Análisis de la información obtenida
  - Elaboración de informe con las conclusiones del análisis forense

2.26 Plan de Recuperación antes Desastres

El Plan de Recuperación ante Desastre es un elemento que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operatividad mínima luego de una contingencia, en donde se vean afectados los procesos y recursos informáticos que funcionen en la Institución.

Los desastres pueden ser naturales o accidentales como incendios, inundaciones, corte en el suministro de energía eléctrica, etc. El plan de recuperación antes desastres debe especificar los objetivos y prioridades a tener en cuenta por las instituciones. Es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento de los sistemas informáticas de la

institución, así como de la recuperación de los datos, aplicaciones y servicios básicos. La practica de recuperación que se acostumbra a realizar es:

- Disponibilidad de un centro alternativo para la ubicación de los principales recursos informáticos (servidores, aplicaciones, bases de datos, entre otros). Este centro debe contar con las mismas medidas de seguridad que las instalaciones principales de la institución.
- Existencia de políticas de respaldo y recuperación.
- Herramientas para llevar a cabo una replicación de los documentos y las bases de datos.
- Detección y respuesta al desastre en el centro principal, adoptando las medidas de contención previstas dependiendo del tipo de desastre: incendio, inundación, explosión, entre otros.
- Traslado de las actividades a un centro alternativo, junto con el personal necesario para la puesta en marcha de los servicios, equipos informáticos, copias de seguridad más recientes y con las medidas de seguridad que correspondan, entre otros.

2.27 Seguridad en redes

después de includes

CAP´TULO 3

PRIVACIDAD

R. SUMOZA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

3.1 Consideraciones sobre Privacidad

No es necesario apelar a los artículos de la carta sobre los Derechos Humanos establecida por la Organización de las Naciones Unidas para darse cuenta que cada una de las personas que habitan este planeta tiene el derecho de decidir sobre el destino de su información privada. Esto incluye no sólo decidir quién, cómo, dónde y cuándo terceras partes puedan tener acceso a sus datos en general, sino que se debe prestar una particular atención a los que están relacionados con la identidad, el perfil social, cultural, personal, etc.

Tanto en las organizaciones privadas, como en las públicas, y a nivel individual, la protección de la información no sólo debe incluir los aspectos típicamente enmarcados dentro de la integridad, confidencialidad y disponibilidad de los datos, sino que debe ampliarse al resguardo de la privacidad donde, entre otros, se procura evitar que se develе la identidad de las partes comunicantes. Se han desarrollado varias estrategias, mecanismos, técnicas y sistemas que tienen esto como objetivo, y que

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

pueden enmarcarse en lo que se denomina las tecnologías que mejoran la privacidad (Privacy Enhancing Technologies).

Este tipo de tecnologías han tenido sus frutos en escenarios de diversa índole, que van desde aplicaciones militares, donde se procura evitar que el enemigo pueda descubrir las conexiones estratégicas, pasando por aplicaciones científicas/comerciales, que evitan revelar información sobre las comunicaciones hechas entre socios científico/comerciales, hasta las aplicaciones de particulares que le ayudan a mantener en privado sus datos personales: los referentes a su salud, su estado financiero, sus preferencias de consumo, etc. Uno de los puntos críticos de la privacidad es el encubrimiento de la identidad de las partes comunicantes, es decir, es la procura de que las comunicaciones sean anónimas: Anonimato.

Cada una de las técnicas y mecanismos utilizados tienen sus ventajas y desventajas en cuanto al perfil de ataque considerado. Es decir, dependiendo del tipo de atacante que se considere, cada una de éstas posee un conjunto de fortalezas y debilidades asociadas. Adicional al perfil del atacante, se debe incluir su radio de acción, esto quiere decir, que se debe considerar su capacidad para manejar ciertos volúmenes de usuarios, su heterogeneidad, su distribución y localización.

Además se debe considerar el tipo de comunicación anónima que se desea o necesita entablar: mensajería instantánea, correos electrónicos, servicios web, etc.

3.2 Técnicas para proporcionar privacidad

Tal como se menciona en [50] las personas en general utilizan Internet para poder comunicarse, para el envío de correo electrónico, para la investigación en diversas áreas de interés, para la interacción con distintos organizamos públicos y/o privados, etc. Al mismo tiempo, gran cantidad de estos organismos públicos y privados en distintas regiones del planeta buscan maximizar la interacción electrónica en todos los niveles entre los usuarios y sus centros tecnológicos, intercambiando información a través del uso de bases de datos controladas por ellos mismos, buscando utilizar el poder de la informática para tener el control de la información concerniente a innumerables aspectos relacionados a los individuos, tales como las preferencias en sus consumos diarios, la interacción con su alrededor, sus estilos de vida, sus opiniones, sus preferencias, y todo esto en niveles que en gran medida son desconocidos por los mismos usuarios. En respuesta a lo anterior, y procurando minimizar este tipo de control, se han propuestos diferentes mecanismos y sistemas que buscan reforzar o mejorar la privacidad (Privacy Enhancing Technologies) del individuo (visto en un contexto amplio, es decir, pudiéndose considerar como individuo a un conjunto de personas, e incluso a organizaciones completas). Este tipo de tecnologías pueden asistir a los organismos en su cumplimiento de los principios de protección de la privacidad establecido en los derechos humanos[25], dándole a los usuarios mayor poder para controlar su información, pudiendo éstos decidir cómo y cuándo puede ser utilizada por terceras partes. Existen sistemas tales como los navegadores web anónimos y servicios especiales de correo electrónico que le permiten comunicarse sin necesidad de revelar su verdadera identidad. Los sistemas para el manejo de la

identidad potencialmente le permiten a los individuos acceder a los servicios y recursos sin tener que proveer información sobre ellos. Esto implica involucrar a una o varias organizaciones sobre las cuales se deba tener cierto grado de "confianza", y que puedan verificar la identidad de los usuarios, y además puedan generar cierto tipo de certificación electrónica que no contenga información sobre la identidad, pero que permita acceder a los recursos y servicios ofrecidos por terceras partes.

Las tecnologías que mejoran o refuerzan la privacidad no son sólo aquellas destinadas a proveer un cierto grado de anonimato, sino que se extienden a la protección y mejora de la privacidad en general del individuo, incluyendo el cumplimiento de sus derechos sobre la protección de sus datos, en este sentido se pueden mencionar como ejemplos de este tipo de tecnología los siguientes:

- Los sistemas de acceso biométrico encriptado, que permite el uso de las huellas dactilares como mecanismo para autenticar la identidad de un individuo sin necesidad de retener su huella dactilar actual.
- Los accesos a los datos personales de los usuarios en linea seguros.
- Programas que permiten a los navegadores detectar automáticamente las políticas de privacidad de los sitios web y las comparan con las preferencias expresadas por los usuarios.
- Sistemas de alertas y avisos que son anexados a la misma información y que previenen su uso en caso del no cumplimiento de las políticas de privacidad.

3.2.1 Anonimato

Para establecer un concepto simple de Anonimato es conveniente utilizar la configuración de un sistema general de comunicación tradicionalmente compuesto por un emisor, un receptor, quienes utilizan una red de comunicación para transmitir un mensaje. En la figura 2.1 se muestra el diagrama general de este modelo.

Figura 2.1: Configuración del Sistema General.

Este sistema está delimitado por los componentes antes mencionados, por lo cual los involucrados que se encuentren fuera de esta delimitación, en cada uno de los casos que se describen se consideran participantes externos.

Cada uno de los casos de estudio presentados serán considerados desde la perspectiva del atacante, quien puede monitorear las comunicaciones, estudiar sus patrones, e incluso puede hacer cambios al manipular el contenido. El atacante puede estar dentro del sistema o puede ser uno de los participantes externos.

En todas las definiciones de los términos relacionados con las tecnologías asociadas a la mejora o refuerzo de la privacidad, se considera un sujeto (subject) a una entidad (ente o ser) que tiene la posibilidad de actuar en el sistema, por ejemplo, un ser humano, una persona jurídica, un computador, etc.

Un sujeto es anónimo cuando no puede ser identificado dentro de un conjunto de sujetos, denominado el conjunto anónimo. Este conjunto está conformado por todos los posibles sujetos que pueden causar (o estar relacionados con) una acción. No

ser identificado significa que ese sujeto no puede ser caracterizado de forma única o particular dentro de ese conjunto. Un sujeto actúa anónimamente cuando, desde el punto de vista del adversario, su acción no puede relacionarse con su identidad, dado que hay un conjunto de sujetos que podrían ser los causantes potenciales de la acción (y el adversario no puede distinguir a su verdadero causante). El anonimato debe permitirle a un sujeto utilizar un recurso o servicio sin revelar su identidad, esto implica que el anonimato por si mismo no procura proteger la identidad de un usuario en un ámbito general, lo que pretende es evitar que otros usuarios o sujetos no puedan determinar la identidad de un usuario cuando éste genera una acción u operación en particular.

Con respecto a las entidades que podrían generar una acción, el conjunto anónimo se conforma por los sujetos que pueden generar una acción en un instante de tiempo específico; desde el punto de vista de las direcciones o ubicaciones de las entidades, el conjunto anónimo está conformado por los sujetos que pueden estar relacionados a una ubicación o dirección. Lo anterior quiere decir que el anonimato se podría clasificar según las entidades involucradas o según la ubicación de las mismas.

De esta forma, para permitir el anonimato de un sujeto siempre tiene que existir un conjunto apropiado de sujetos que posean potencialmente los mismos atributos. Ser los emisores y los receptores de mensajes particulares son ejemplos de estos atributos. Un emisor de un mensaje puede ser anónimo sólo si constituye parte de un conjunto de emisores potenciales (con atributos similares), el cual es su conjunto anónimo, y puede ser un subconjunto de todos los sujetos a nivel global quienes pueden enviar un mensaje en un tiempo específico. Lo mismo aplica para los receptores de mensajes. Este esquema se representa en la figura 2.2. El conjunto anónimo es relativo al tiempo, es decir, puede variar según los cambios que se den en el sistema.

Con lo anterior se especifica que existe un conjunto anónimo para el emisor de un mensaje, existe otro conjunto anónimo para el receptor de ese mensaje, y estos conjuntos puedes ser disjuntos, pueden solaparse o pueden ser el mismo conjunto.

Figura 2.2: Conjuntos Anónimos.

Por otro lado el anonimato además de estar relacionado al conjunto anónimo y al tiempo en el que se está ejecutando la acción, también tiene relación al contexto donde se aplica, es decir, un sujeto puede ser anónimo en relación al contexto envío y recepción de correos electrónicos, pero puede no serlo en ese mismo instante de tiempo para el contexto interacción con una base de datos. Esto se debe a que según el contexto de estudio pueden existir distintos atributos que caractericen al conjunto anónimo, y por ende al anonimato del sujeto.

Como se mencionó el conjunto anónimo está directamente relacionado con el atacante, esto quiere decir, que el conjunto anónimo se delimita según el grado de conocimiento que posee el atacante. De esta forma, el fin último del anonimato es procurar que el atacante posea la misma información antes y después de su ataque.

Dado que el anonimato es dependiente del contexto, definido por sus atributos, las variaciones del mismo podrían cambiar los niveles de anonimato. Si se pretende diferenciar entre "niveles" de anonimato, es necesario poder cuantificarlo (medirlo) con el fin de poder hacer distinciones entre distintos sistemas anónimos.

3.2.1.1 Técnicas de Anonimato Tal como se mencionó en el apartado anterior el anonimato de un sujeto es el estado de no ser identificable dentro de un conjunto de sujetos, denominado el conjunto anónimo. También se ha mencionado, ver [1], que el emisor de un mensaje puede ser anónimo sólo dentro de un conjunto de potenciales emisores, lo que correspondería al conjunto anónimo del emisor, el cual a su vez puede ser un subconjunto de todos los sujetos a nivel mundial quienes podrían enviar mensajes en determinados instantes de tiempo. Este tipo de anonimato es llamado anonimato del emisor. Lo mimo ocurre para el receptor, quien puede ser anónimo sólo dentro de un conjunto de receptores posibles, llamado el conjunto anónimo del receptor, y a este tipo de anonimato es llamado anonimato del receptor. Además hay un tercer tipo de a anonimato, el de relación, el cual consiste en tener la propiedad de no poder relacionar quién se comunica con quién. La no relacionabilidad significa que dentro del sistema las distintas entidades, aquí denominadas ítems de interés o IDI (mensajes, emisores, receptores, etc.) no están ni más ni menos relacionadas con respecto a la información que se tenía antes de que el adversario ejecute un ataque (información a priori). En otras palabras, el anonimato del emisor/receptor puede o ser definido como las propiedades de que un mensaje particular no sea relacionado a cualquier emisor/receptor, y que cualquier mensaje no sea relacionado a un emisor/receptor en particular, entonces el anonimato de relación es la propiedad de no poder relacionar o determinar quién se comunica con quién.

El anonimato se fortalece mientras más grande sea su conjunto anónimo, y mientras más uniforme sea la distribución de probabilidad de la ejecución de las acciones por parte de los sujetos dentro del conjunto, es decir, el nivel de anonimato no sólo depende del tamaño del conjunto sino también de la probabilidad de que un sujeto en particular pueda generar cierta acción. De esta forma se puede definir el entorno de acción que acota las técnicas de anonimato para las comunicaciones: Colectar un conjunto apropiado de usuarios para que un usuario en particular pueda ser anónimo cuando se comunica con los demás.

Los sujetos no pueden tener el mismo nivel de anonimato contra todos los tipos de ataques posibles generados por participantes internos o externos. El conjunto de los posibles sujetos y la probabilidad de que ellos puedan causar una acción puede variar dependiendo del conocimiento del atacante. Se asume que desde el punto de vista del atacante, el nivel de anonimato sólo puede decrementar, es decir, se asume que el atacante no olvida la información que tiene y que ha logrado recolectar durante su observación e influencia sobre la comunicación en el sistema.

Para definir las diferentes técnicas de anonimato se utilizan los siguientes criterios:

Objetivo de la protección Define cuál tipo de anonimato puede ser provisto (del emisor, del receptor, o de la relación).

Nivel de seguridad Se debe definir cuál es el nivel de seguridad alcanzado por el objetivo de la protección (la seguridad desde la perspectiva de la teoría de la información o incondicional y la seguridad criptográfica/computacional con los supuestos asociados a mecanismos como los de clave pública).

Modelo de atacante Contra qué tipo de atacantes protege el sistema (externos, participantes, proveedores de servicios).

Modelo de confianza En quién confía el usuario: en los proveedores de servicios, en los participantes externos, en otros usuarios, etc.

Redes de mezcla Esta idea se describe en [12]. El método utiliza criptografía de clave pública y fue diseñado para que los sistemas de envío de correo electrónico proveyeran anonimato del emisor, del receptor y de relación sin necesitar un servicio de confianza central (por ejemplo una autoridad certificadora). En general, los mezcladores o Mixes pueden ser entendidos como una cadena de proxies seguidos uno detrás del otro. Se considera que el atacante puede observar todas las comunicaciones y puede controlar todos los mixes a excepción de uno.

Topología Mix: Este concepto funciona aun cuando se dispone de un solo mix. Pero en este caso el usuario debe confiar en este mix. Típicamente hay más de un mix en la red organizados en forma de cadena. Existen diferente métodos para organizar la cooperación dentro de la red. Uno de ellos puede ser que cada mix existe independientemente en la red y los participantes libremente deciden a través de cuál de ellos enrutarán sus mensajes. Así cada nodo puede comunicarse con el resto conformando lo que se denomina una topología de red mix o red de mezcla.

Otra posibilidad es utilizar una cadena de mixes predefinida. A esta cadena se le denomina mix en cascada. Además de los dos extremos antes mencionados, se pueden utilizar variaciones que resulten en diseños híbridos. Un análisis y comparación de ambas ideas se presenta en [17, 9].

En una red mix, el usuario puede decidir con cuáles mixes desea interactuar, proveyendo de esta manera un buen nivel de escalabilidad y flexibilidad. Además, debido a que los usuarios escogen aleatoriamente los mixes, un atacante no podrá determinar cuáles de ellos debería controlar para poder observar un mensaje enviado, para esto debería controlar gran parte de la red.

Por otro lado, un atacante sabe con exactitud cuáles mixes debe controlar en una red en cascada (mix en cascada). Este diseño es vulnerable a los ataques de denegación de servicio, ya que al detener un solo mix en la red, lograr detener todo el sistema.

Por otro lado en [9] exponen que la red mix (pero no la red en cascada) es vulnerable a ciertos tipos de atacantes con altos niveles de control, es decir, que controlan a todos los mixes a excepción de uno. Mencionan que este tipo de red es vulnerable a los ataques $n - 1$. Otra desventaja es que algunos mixes puede que no sean casi utilizados (se subutilizan) y otros se sobrecarguen. Los objetivos de protección que se logran son el de anonimato del emisor, y el de relación.

Provee protección contra atacantes que pueden observar toda la red y que pueden controlar muchos mixes. Es susceptible a ataques de denegación de servicio y ataques $n - 1$. Desde el punto de vista de la confianza, se debe confiar en al menos un mix de la ruta seleccionada.

Funcionalidad Básica: En este enfoque los usuarios o clientes no envían sus solicitudes directamente al servidor (o a otro destino), sino que las envía a nodos (en-

rutadores) intermedios denominados mix. Para poder ocultar la comunicación de los participantes, los mixes no envían instantáneamente los mensajes que reciben, en vez de esto, los mixes almacenan varios mensajes de diferentes clientes por un tiempo definido, los transforman, y luego si los reenvían simultáneamente a los servidores de destino o a otros mixes en la red. Un observador que puede ver todos los mensajes entrantes y salientes de un mismo mix no podrá determinar cuáles mensajes de entrada corresponden a cuáles mensajes de salida. Los fundamentos que consolidan la seguridad de los mixes se muestran en la figura 2.12

Figura 2.12: Fundamentos que sustentan las redes mix.

Preprocesamiento: Transformación de los mensajes

El objetivo principal de la transformación de los mensajes es evitar que un atacante pueda trazar (descubrir su recorrido) un mensaje a través de la comparación de los patrones de bits correspondientes a los mensajes que entran y salen de un mix. Para poder enviar un mensaje, el cliente primero lo debe preparar. Para esto, el primer paso que debe dar es escoger el camino por el cual se transmitirá el mensaje, este camino estará compuesto por los mixes que haya escogido, y debe incluir el orden específico de reenvíos antes de que llegue a su destino final. Para mejorar la seguridad del sistema, se recomienda utilizar más de un mix en cada camino. El siguiente paso, es utilizar las claves públicas de los mixes escogidos para cifrar el mensaje, en el orden inverso en el que fueron escogidos, es decir, el mensaje se cifra primero con la clave pública del ultimo mix, luego con la del penúltimo, y así hasta cifrar por ultima vez con la clave pública del primer mix en el camino seleccionado. Cada vez que se cifra se construye una capa, y se incluye la dirección del siguiente nodo (ya sea el destino final u otro mix). Así cuando el primer mix obtiene el mensaje preparado, lo descifra con su clave privada, y obtiene la dirección del siguiente nodo al que debe reenviarle el resto del contenido que quedó después de su descifrado.

Este esquema puede ser descrito de la siguiente manera:

$A_1, ..., A_n$ pueden ser la secuencia de las direcciones y $c_1, ..., c_n$ la secuencia de la claves de cifrado conocidas públicamente y pertenecientes a la secuencia $Mix_1, ..., Mix_n$ escogidos por el emisor. Incluso c_1 puede ser una clave secreta en un sistema de cifrado simétrico. A_{n+1} puede ser la dirección del receptor o del destino final del mensaje, al cual se le denomina, por simplificación, Mix_{n+1}, y c_{n+1} sería su clave de cifrado. $z_1, ..., z_n$ puede ser una secuencia de bits aleatorias. El emisor crea los mensajes N_i que son recibidos por el Mix_i, y en la base del mensaje N es lo que el receptor final debe recibir (Mix_{n+1}) supuestamente:

$$N_{n+1} = c_{n+1}(N) \tag{3.1}$$

$$N_i = c_i(z_i, A_{i+1}, N_{i+1}) para i = n, ..., 1 \tag{3.2}$$

El emisor le envía N_1 al Mix_1. Después que se decodifica, cada mix recibe la dirección del siguiente mix y el mensaje que está destinado a ese siguiente mix. Debido a las implementaciones de los sistemas de clave pública o asimétrica se necesitan las cadenas aleatorias de bits. Para asegurar que un atacante no pueda trazar un mensaje (seguir su trayectoria) a través de un mix, es necesario que todos los pares de entrada-salida de los mensajes no tengan características que permitan identificarlos,

por ejemplo, el tamaño de los mismos. Una solución a esto es establecer tamaños fijos para los mensajes, y cuando los mensajes tengan un tamaño inferior al fijado, se deberán rellenar con información falsa, y cuando lo superan se deberán fragmentar en varias piezas.

Reordenamiento: Mezclas por grupos (pool) o mezclas por cantidad (batch): Cuando un mix opera en modo "por cantidad" o "batch", éste recolecta un número fijo n de mensajes, cifrándolos y reordenándolos antes de reenviarlos a todos en un solo envío. En contraste, un mix que opera en modo “por grupos” o “pool” tiene siempre un número n de mensajes almacenados en su memoria temporal o “buffer” denominado “pool”. Si un nuevo mensaje llega al mix, entonces se escoge aleatoriamente y se reenvía uno de los mensajes almacenados. El número n representa al tamaño del “pool”.

Prueba de reenvío: Uno de los tipos de ataques más frecuentes es el denominado ataque de reenvíos. Un atacante podrá copiar un mensaje que desea monitorear y enviarle una o varias copias de éste al mix. Estas copias del mensaje podrían tomar el mismo camino en la red que el mensaje original, dado que los algoritmos de envío y descifrado trabajan determinísticamente. Así puede ser encontrado un patrón característico del mensaje sólo con observar la red. Con el fin de evitar este tipo de ataque, las copias de los mensajes deben ser identificadas y eliminadas a través de un filtro. Una posibilidad para identificar los mensajes inválidos es a través del uso de estampas de tiempo. Cuando un mix obtiene un mensaje, también obtiene una etiqueta que le informa la franja de tiempo durante la cual el mensaje es válido. Si el mensaje llega muy tarde (después de lo que la franja de tiempo le indica), el mix niega el reenvío del mensaje. Otra posibilidad es que el mix almacene una copia de los mensajes que ya haya enviado, y así los los mensajes nuevos que lleguen pueden ser comparados con esta base de datos. Por razones de seguridad y rendimiento, es conveniente restringir el tamaño de esta base de datos. Los mensajes deberían ser almacenados por un corto período de tiempo antes de que se borren.

Tráfico de relleno o dummy: Aun cuando ninguna información está siendo transmitida, es posible enviar información falsa en la red. Esto tendría el mismo efecto de no enviar ningún mensaje, pero un observador (atacante) no podría distinguir entre los mensajes reales de los que se envían como relleno. El envío de este tipo de mensajes de relleno es denominado tráfico dummy. Con respecto a la idea de los mixes, un mix podrá aleatoriamente enviar tráfico dummy a otro en la red. Este mecanismo también beneficiaría a los mix que trabajan en el modo batch, ya que normalmente estos mixes tienen que esperar hasta que un número predefinido de mensajes hayan llegado antes de que todos los mensajes sean reenviados simultáneamente, y evitaría los posibles retrasos que podrían ocurrir cuando no hayan envíos suficientes de mensajes al mix, y éste puede hacer su respectivo reenvío es decir, el tráfico dummy evitaría estos retrasos, ya que si no hay suficientes mensajes reales enviados, el número de mensajes necesarios para hacer el reenvío se pudiese alcanzar con los mensajes de relleno.

Anonimato del receptor (Direcciones de retorno no trazables): El hecho de permitir que un receptor pueda permanecer anónimo se le caracteriza por tener una dirección de retorno que no pueda ser registrada o trazada por un atacante. Esta di-

rección de retorno es un mensaje especial que tiene que ser creado por el receptor y tiene que ser utilizado por el emisor para el envío del mensaje al receptor anónimo. La idea de base de este tipo de direccionamiento es que el receptor, y no el emisor, define sobre cuáles mixes y el orden a ser utilizado para la entrega de cierto mensaje de respuesta. La dirección de retorno preparada por el receptor contiene una clave simétrica para cada mix en el camino que éste utilizará para cifrar el mensaje enviado por el emisor. Finalmente, el receptor recibirá un mensaje cifrado múltiples veces con claves simétricas como él mismo especificó. Dado que el receptor conoce todas las claves simétricas, para poder desarrollar esta técnica, éste puede descifrar el mensaje. Dado que la claves simétricas son desconocidas por el emisor y la codificación del mensaje cambia en cada uno de los mixes (debido al cifrado), el emisor no puede trazar el mensaje hacia el receptor.

Este esquema se explica de la siguiente forma: $A_1, ..., A_m$ pueden ser la secuencia de las direcciones y $c_1, ..., c_m$ pueden ser la secuencia de las claves públicas conocidas de la secuencia de mixes $Mix_1, ..., Mix_m$ escogida por el receptor, donde c_m puede ser una clave secreta de un sistema de cifrado simétrico. El mensaje añadido a la dirección de retorno pasará por estos mixes en orden ascendiente dependiendo de sus índices. A_{m+1} puede ser la dirección del receptor llamado Mix_{m+1}. De forma similar, al emisor se le llama Mix_0. El receptor crea una dirección de retorno no trazable (k_0, A_1, R_1) donde k_0 es una clave de un sistema de cifrado simétrico generada para este propósito. Mix_0 se supone que utiliza esta clave para codificar el contenido del mensaje con el fin de garantizar que el Mix_1 no sea capaz de leer este mensaje. R_1 es parte de la dirección de retorno, la cual se transmite a través del Mix_0 y contiene el mensaje generado y que ha sido cifrado utilizando k_0. R_1 inicialmente se crea escogiendo aleatoriamente un único nombre de la dirección de retorno en un esquema recursivo como el que se muestra a continuación:

- R_j es la parte de la dirección de retorno que será recibida por el Mix_j.
- k_j es la clave de un sistema de cifrado simétrico, con el cual Mix_j codifica la parte legible del mensaje.

$$R_{m+1} = e \tag{3.3}$$

$$R_j = c_j(k_j, A_{j+1}, R_{j+1}) \, para \, j = m, ..., 1. \tag{3.4}$$

El mensaje N_j está constituido por la parte de la dirección de retorno R_j y el contenido I del mensaje (codificado varias veces) generado por el emisor (también llamado parte I_j del contenido). Los mensajes N_j son creados por el Mix_{j-1} y son enviados al Mix_j de acuerdo al siguiente esquema recursivo. Estos son creados y enviados por el emisor Mix_0 y así, en secuencia, se pasan a través de los mixes $Mix_1, ..., Mix_m$

$$N_1 = R_1, I_1; \; I_1 = k_0(I) \tag{3.5}$$

$$N_j = R_j, Ij;\ I_j = k_{j-1}(I_{j-1})\, para\, j = 2, ..., m+1 \tag{3.6}$$

El receptor Mix_{m+1} recibe e, $N_{m+1} = e(km(...k1(i))...)$ y puede descifrar y extraer el contenido I ya que conoce todas las claves secretas k_j asignadas para el nombre e de la parte de la dirección de retorno en el orden correcto.

Verificación del tamaño del conjunto anónimo: Si un atacante bloquea el mensaje de un participante específico, este mensaje se aísla del conjunto anónimo. Lo mismo sucedería si un atacante rodea a un participante específico, manipulándolo a través de la generación de mensajes con fines "ilícitos" para el sistema. Este tipo de ataque es conocido como el ataque de mezcla o $n-1$. No existe una solución específica contra este tipo de ataques en ambientes abiertos, como por ejemplo en aquellos donde los participantes entran y salen del sistema a su discreción. Se podría utilizar una protección básica si el mix puede identificar a cada participante, así de una forma confiable el mix puede verificar si los mensajes que tiene almacenados en su memoria temporal ("buffer") fueron enviados por un número relativamente adecuado de usuarios.

Canales Mix: Los canales mix son utilizados para manejar en tiempo real las cadenas continuas de datos o que contengan sólo pequeños retrasos a través de una cadena de mixes. Para este caso, es necesario que se divida el ancho de banda: una parte para la señalización y otra parte para el envío de los datos, ambos utilizados para la transmisión del mensaje.

Se podría asumir que existe un sólo canal para la señalización, y varios canales para la transmisión de datos. Con el fin de establecer el canal, se envía un mensaje sobre el canal de señalización, el cual contiene la clave k_i que deberá ser utilizada entre el emisor y el Mix_i, la cual se cifra de forma asimétrica por la clave pública de dicho mix. Con esto, se define un canal de igual forma para todos los mixes, sobre el cual será transmitido el mensaje.

Se podría utilizar un canal para el envío y otro canal para la recepción. Un canal de envío es análogo a un cifrado híbrido: el emisor establece un canal, y codifica continuamente su información N, transformándola en $k_1(k_2(...k_m(N)...))$ y enviándola al mix Mix_1. Cada mix Mix_i para $(i = 1, ..., n-1)$ decodifica los mensajes recibidos continuamente utilizando k_i y transmitiendo el resultado de la decodificación al mix Mix_{i+1}. El mix Mix_m crea el mensaje en texto plano en el fin de la cadena. Esto le permite al emisor enviar anónimamente los mensajes, pero en este caso el receptor no será anónimo. Un canal de recepción es en realidad un canal de envío el cual se utiliza en dirección opuesta, es decir, el receptor es el que establece el canal. El emisor le envía al mix Mix_m la cadena N de información que no está especialmente codificada por el mix Mix_m, luego lo codifica utilizando la clave k_m y conduce $k_m(N)$ un paso atrás, hacia el mix Mix_{m-1}. Los otros mixes hacen lo mismo, por ejemplo, el mix Mix_1 envía la cadena $k1(...km(N)...)$ codificada. Dado que el receptor conoce todas la claves públicas k_i, tiene la disponibilidad de descifrar N. Esto le permite al receptor recibir los mensajes anónimamente mientras que el emisor no es anónimo.

Para alcanzar ambos niveles de anonimato, en [54] sugieren la creación de canales Mix como enlaces de los canales de envío y recepción. El emisor establece un canal de envío que finaliza en el mix Mix_m y el receptor establece un canal de recepción que inicia en el Mix_m. El mix Mix_m traspasa las cadenas de información que llegan por el canal de envío hacia el canal de recepción. Los canales que están supuestamente enlazados, se etiquetan con una marca común que se recibe consistentemente en ambos canales que establecen los mensajes asociados al mix Mix_m. Los datos transferidos están coordinados con un mensaje de entrada al mix cifrado asimétricamente, el cual contiene la información del mix que conecta a los dos canales, y el usuario emisor del mensaje de entrada al mix actúa como un emisor o un receptor. Cada mix en la cadena puede descifrar este mensaje de entrada al mix y en el último paso, el texto plano se difunde a todos los suscriptores. Ahora, los canales pueden ser establecidos utilizando los mensajes de establecimiento de ambos participantes. Estos escogen los mixes por el canal de transferencias de datos del mix Mix_m y los mantienen en secreto. Así todos conocen sólo la mitad del camino y el mix Mix_m reenvía los mensajes entrantes del canal de envío del mix al canal de recepción del mix. Cada emisor/receptor debe tener el mismo número de canales de envío/recepción, porque de lo contrario serían observables, por tal razón convendrá utilizar canales "dummy".

Enrutamiento cebolla Este mecanismo fue propuesto y estudiado en [46, 67, 68]. Es equivalente a una red de mixes, pero en el contexto de enrutamiento basado en circuitos. En vez de enrutar cada paquete separadamente, el primer mensaje lo que hace es abrir un circuito, etiquetando una ruta. Cada mensaje que tiene una etiqueta en particular se enruta por un camino predeterminado. Finalmente, un mensaje se envía para que cierre o clausure un camino. Con frecuencia se hace referencia a flujo anónimo como la información que viaja por estos circuitos. Su objetivo es dificultarle la tarea al análisis de tráfico, uno de los tipos de ataques más conocidos. Este sistema procura proteger la no relacionabilidad de dos participantes que se comunican a través de terceras partes, y procura proteger la identidad de las partes comunicantes. En vista de que las redes ISDN son difíciles de implementar en Internet, lo que procuró el enrutamiento cebolla es adaptar esta idea distribuyendo la red anónima y adaptándola para que se ejecute en el tope del modelo TCP/IP. El primer mensaje enviado en la red se cifra en capas, que pueden ser descifradas en una cadena de enrutadores cebolla (onion routers, OR) los cuales utilizan sus respectivas claves privadas.

El primer mensaje tiene el material que debe ser compartido entre el emisor y los enrutadores, también las etiquetas y la información de direccionamiento del próximo nodo. Tal como sucede en los mixes de Chaum, se provee la no relacionabilidad a nivel de bits, de esta forma el camino que toma el primer mensaje no es trivial de seguir con sólo observar el patrón de bits de los mensajes.

También se propuso un tipo de enrutamiento dinámico donde los enrutadores que reenvían el flujo a través del camino establecido no se especifican únicamente en el mensaje inicial, esto con el fin de incrementar el anonimato. Los datos que circulan por la red en un circuito establecido están cifrados con claves las simétricas de los

enrutadores. Las etiquetes se utilizan para indicar a cuál circuito pertenece cada paquete. Se utilizan etiquetas diferentes para los distintos enlaces, asegurando así la no relacionabilidad, y además las etiquetas de los enlaces también se cifran utilizando una clave que se comparte entre los pares de enrutadores OR. Lo anterior previene los ataques de observadores pasivos que puedan determinar cuáles paquetes pertenecen al mismo flujo anónimo, pero no le oculta la información a un enrutador que pueda ser subversivo.

OR es susceptible a un conjunto de ataques, tal como el ataque de tiempo. Esto se debe a que los patrones pudiesen ser analizados por un atacante en ausencia de un gran volumen de tráfico pesado. Para este sistema se afirma proveer anonimato en la navegación web la cual requiere comunicaciones con baja latencia, por tal razón se ha excluido toda la dinámica de los mezcladores o mixes, dado que pudiese incrementar demasiado los tiempos de respuesta. En ausencia de este tipo de características, lo hace vulnerable a distintos tipos de ataques superados por los mixes, por ejemplo el ataque de correlación del tráfico de mensajes, donde se pudiese determinar cuáles mensajes entrantes corresponden con los salientes, con respecto a un enrutador.

Los enrutadores se pueden configurar para que trabajen sólo con un determinado subconjunto de clientes, ya sea por zonas o de forma particularizada. Además se puede configurar para que trabajen sólo con un subconjunto de otros enrutadores.

Tor: la segunda generación de OR

El proyecto OR fue retomado en el año 2004, con el diseño e implementación de lo que se denominó la "segunda generación del onion router" o TOR, por sus siglas en inglés, la propuesta se muestra en [31]. Su política es la del reenvío de flujo TCP sobre una red de reenvíos, y junto con la ayuda de otra herramienta, el Privoxy (http://www.privoxy.org), está especialmente diseñada para el tráfico web.

Este sistema utiliza una arquitectura de red tradicional: una lista de servidores voluntarios se obtiene desde un servicio de directorio ofrecido por otro(s) servidor(es). De esta forma, los clientes crean caminos utilizando al menos tres nodos intermedios escogidos de forma aleatoria dentro de la lista, y sobre los cuales se hace la comunicación de la información. A diferencia de la arquitectura anterior, donde se enviaba y distribuía el material criptográfico, TOR utiliza un mecanismo interactivo: el cliente se conecta con el primer nodo, y le solicita a éste que se conecte con el segundo nodo, de esta forma un canal bidireccional se utiliza en cada paso para desarrollar un intercambio de claves autenticado DF (Diffie-Hellman). Este garantiza el reenvío en forma secreta y la resistencia a la compulsión, debido principalmente a que solo son necesarias claves de corta duración. Este mecanismo fue inicialmente propuesto en Cebolla (ver [10]), y no está cubierto en la patente de OR (ver [67]).

Otra notable diferencia entre TOR y los intentos anteriores por anonimizar el tráfico de flujo, es que TOR no ofrece seguridad contra los atacantes que pueden observar la red entera, es decir, contra atacantes pasivos globales. Un conjunto de técnicas de Análisis de Tráfico (ver [18, 42, 61, 73, 69]) han sido desarrolladas a través de los años para trazar el flujo de tráfico continuo viajando por redes de baja latencia como TOR. En estos estudios se ha demostrado que este tipo de ataques son muy difícil de contrarrestar, a menos que se utilicen técnicas que implicarían latencias elevadas, o que requieran la inyección de grandes cantidades de tráfico cubierto

(tráfico inservible o "dummy"), los cuales representan soluciones muy costosas. Por esta razón en TOR se opta por obtener un nivel de seguridad que se pueda alcanzar en un sistema altamente utilizable y muy económico de utilizar (ver [3, 45]). Como resultado si un adversario puede observar el flujo entre dos puntos de la red, pudiese de forma trivial generar el mismo tráfico, y lograr ataques del tipo "tagging". Sin embargo, dada esta vulnerabilidad, aun se necesita estimar la probabilidad de que un adversario pueda estar monitoreando la red en múltiples puntos sobre un camino o ruta establecida.

TOR también ofrece mecanismos para ocultar los servidores. Un servidor oculto abre una conexión anónima y la utiliza para publicar un punto de contacto. Si un cliente quiere contactar a un servidor, debe conectarse con un punto de contacto y negociar un canal anónimo separado del que se utiliza para el reenvío de la comunicación actual. Un ataque propuesto en [51] demuestra la vulnerabilidad de esta idea. La intuición detrás de este ataque está en el hecho de que un adversario puede abrir múltiples conexiones hacia un mismo servidor oculto, y secuencialmente o en paralelo podría controlar el flujo hacia ese servidor. Para esto, el atacante necesitaría controlar al menos un enrutador, y debe esperar a que el servidor escoja una de las conexiones de su enrutador como un primer nodo de un camino anónimo cualquiera.

CAP´TULO 4

FUNDAMENTOS JUR´DICOS

E. MORA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

4.1 El ordenamiento jurídico venezolano y las nuevas tecnologías de la información

test

4.1.1 Ley de Mensajes de Datos y Firmas Electrónicas, Ley de Infogobierno, Ley de Interoperabilidad y Ley Especial Contra los Delitos Informáticos

test

4.2 La insuficiencia de las regulaciones jurídicas existentes

test

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

PARTE II

PUBLICACIONES DESDE CENDITEL

CAP´TULO 5

CERTIFICACIÓN ELECTRÓNICA

V. Bravo y A. Araujo

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

A continuación el contenido del artículo de ROOTVE

Una Autoridad de Certificación Raíz (AC Raíz) es un componente que tiene el rol de ser el punto más alto de confianza en una estructura jerárquica denominada Infraestructura de Clave Pública (ICP). Una ICP provee de certificados digitales bajo estándar X.509 a personas, direcciones IP y direcciones en la Web; proporcionando seguridad lógica, y vinculación legal a las transacciones que realiza el propietario del certificado en la Internet. La confianza reside en la protección a través de esquemas fuertes de seguridad física y lógica de la clave privada que permite la emisión de estos certificados. Este trabajo muestra el proceso de desarrollo de una aplicación para gestionar el componente mencionado utilizando bibliotecas, herramientas, compiladores, sistemas operativos y licencias compatibles con los principios del software libre. En primer lugar, se determinan los requisitos a ser satisfechos en función de una descripción general de las funciones y características de una Autoridad de Certificación; posteriormente, se dise nan funcionalidades y se especifican requisitos, con el objetivo de producir una visión formal de los procesos a automatizar. Se dedica una sección a la implementación que consiste, en la codificación en un lenguaje de

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

programación, de los procesos previstos en las etapas anteriores, como también, de la incorporación de mecanismos fuertes de validación de identidad de usuarios, registro de eventos, firma de acciones por parte de los administradores de la aplicación, y especificación de conexiones con hardware especializado, como tarjetas inteligentes. Finalmente, se muestra el despliegue y configuración de la aplicación, que involucra la instalación en un ambiente seguro (bóveda o centro de datos) y el enlace de la AC Raíz con los demás componentes de la infraestructura.

A Certification Authority Root (CA Root) is a component which role is to represent the highest confidence point in a hierarchical structure denominated Public Key Infrastructure (PKI). A PKI provides people, IP addresses and Web domains with digital certificates under X.509 standard, offering logic security and legal entailment to transactions performed on the internet by the certificate's owner. Confidence resides in private key protection through strong physical and logical security schemes, so these schemes allow the certificate emission. This work shows the development process of a CA root management application. For this development it's used libraries, tools, compilers, operating systems and licenses compatible with the principles of free software. In first place, the requirements to satisfy are determined based on a general description of a CA's functions and characteristics; subsequently, functionalities are designed and requirements are specified in order to produce a formal vision of the processes to automate. A section is dedicated to the implementation, this consists on codification in a programming language of the processes forseen in the previous stages, like also, of the incorporation of strong mechanisms of validation of identity of users, registry of events, actions signature by application's administrators, and connections specification with specialized hardware, like smart cards. Finally, application display and configuration are shown, it involves its installation in a safe environment (vault or data center) and CA Root connection with other components of the infrastructure.

5.1 Introducción

La disponibilidad de Internet como medio digital seguro permite que cualquier persona, empresa, institución, o administración realice transacciones gubernamentales, comerciales o personales en la mayoría de los casos, tal cual, como se realizarían en una oficina o espacio físico de forma presencial. Dado este hecho, al utilizar Internet para establecer relaciones humanas, se está de acuerdo que es necesario trasladar el concepto de "identidad" al medio digital[**?**]. La criptografía provee algoritmos y mecanismos para construir este concepto en la red, ya que es posible utilizar herramientas que aporten elementos para definir la identidad de un usuario, entidad o institución, de la misma forma de la que se está familiarizado en el mundo real.

En muchas ocasiones para realizar actividades cotidianas personales o de trabajo, se debe establecer contacto con un individuo u organización que no se conoce o del cuál no se tiene ninguna referencia. Mediante un contacto personal o directo, los sentidos humanos permiten percibir un gran número de detalles que le caracterizan, y cuya combinación muy probablemente le hace irrepetible. Esta combinación permite

identificar al individuo de forma única y certera. Dicho esto, la identidad se define como el reconocimiento que se hace de las credenciales físicas o informativas, que ese individuo ofrece para que se le acepte como poseedor de una determinada individualidad [**?**]. Las credenciales físicas pueden ser documentos como la Cédula de Identidad, el Pasaporte, la Licencia de Conducir, entre otros. Todos los documentos citados generalmente incluyen una fotografía que permite la comparación con la apariencia del interlocutor; también usualmente se agrega otra característica informativa que puede ser un nombre, una firma manuscrita y posiblemente un número de referencia.

Cuando se traslada el concepto de identidad al medio informático, se habla de identidad digital, y se hace necesario contar credenciales traducibles a información binaria. Por otro lado, la criptografía, por sí misma no proporciona este concepto: es el uso de una infraestructura computacional que utiliza algoritmos criptográficos para representar credenciales digitales, como por ejemplo el certificado digital, y que son otorgados por terceros de confianza, denominados Autoridades de Certificación (AC), y que se describen como Raíz cuando son el punto inicial de una jerarquía, las que proveen a usuarios y organizaciones de identidad digital, y que cuenta con las mismas connotaciones que tiene este concepto en el ámbito personal y jurídico.
Uno de los problemas que aparece en este punto, en la disponibilidad de la infraestructura mencionada anteriormente, la cuál debe contar como un elemento obligatorio una aplicación que gestione, bajo un estándar aceptado, como lo es el estándar X.509[**?**], los certificados digitales que emite la AC. La discusión de importantes aspectos que surgen en las diferentes etapas del proceso desarrollo de la aplicación de gestión, y que están vinculados con los principios del software libre y los requisitos muy particulares del ambiente de despliegue, subrayan los objetivos de este trabajo.

5.2 Marco Teórico

Con el objetivo de contextualizar los términos “identidad”, “confianza”, o “transacción segura” y“AC Raíz” en el medio digital, y específicamente en relación con internet; es imprescindible en una primera aproximación, discutir sobre determinados temas y conceptos vinculados con la seguridad informática. En los párrafos siguientes se abordan brevemente algunos de los puntos más importantes relacionados con el tema.

5.2.1 Seguridad Informática

Se ha llegado a un consenso sobre lo que significa seguridad informática[**?**]. En general, se dice que un activo de información, (información digital con un valor real para una empresa o persona) está asegurado si cumple con niveles aceptables relativos a su valor potencial en los siguientes aspectos:

Disponibilidad: es el grado en que un dato está en el lugar, momento y forma en

que es requerido por uno o un conjunto de usuarios autorizados. Como premisa, un sistema seguro debe mantener la información disponible para los usuarios autorizados. Disponibilidad también significa que el sistema, debe mantenerse funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo.

Confidencialidad: es el aspecto de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. Igual que para la disponiblidad, los usuarios pueden ser personas, procesos o programas. Para evitar que nadie no autorizado pueda tener acceso a la información transferida y que recorre la Red se utilizan técnicas de cifrado 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: corresponde a garantizar que la información transmitida entre dos entidades autorizadas no sea modificada por un tercero no autorizado. Un mecanismo para lograrlo es 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 le a nade. La validación de la integridad del mensaje se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se a nadió al final cuando se calculo 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 ningún agente externo o extraño ha modificado el mensaje.

5.2.2 Criptografía

La criptografía es la ciencia o arte información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas o usuarios autorizados [**?**]. La criptografía ha tomado gran importancia en los últimos a nos, ya que es posible transformar las "técnicas matemáticas" en algoritmos que pueden ser comprendidos por una computadora. Se puede clasificar la criptografía en dos tipos, según el tipo de clave que se utilice:

Criptografía Simétrica: los sistemas de criptografía simétrica son aquellos que utilizan una única clave para cifrar y descifrar un texto claro. Este tipo de sistema conlleva una desventaja, que consiste en el conocimiento de las partes (emisor y receptor) de la clave única que les permite intercambiar información por un canal seguro. Como respuesta a ello, se hace necesario formalizar un procedimiento que muestre a las partes autorizadas la información sobre la clave, sin que sea develada a un tercero no autorizado.

Criptografía Asimétrica: también se conoce como Sistema de Cifrado de Clave Pública[**?**]. Usa dos claves diferentes, una de ellas es la Clave Pública que puede ser enviada a cualquier persona y otra, que se denomina Clave Privada que es secreta, y no debe ser revelada. A diferencia del sistema de cifrado simétrico donde las partes deben concertar un procedimiento para conocer la clave única, en este tipo de

sistema el remitente usa la clave pública del dest inatario para cifrar el documento. Una vez que el documento o mensaje ha sido cifrado, solamente con la clave privada del destinatario el mensaje puede ser descifrado.

5.2.3 Certificados digitales

Un certificado digital es un documento de acreditación que permite a las partes tener confianza en las transacciones que realicen en internet. Por tanto, garantiza la identidad de su poseedor mediante un sistema de claves administrado por una tercera parte de confianza. Para validar un certificado basta con conocer la clave pública de la tercera parte conocida como la Autoridad de Confianza (AC). Para cuidarnos de que piratas informáticos cambien su clave pública por la de la autoridad de confianza, la AC debe crear un certificado con su propia información de identidad y a la vez su clave pública y firmar el certificado, este certificado se le conoce como certificado autofirmado. Dado que los certificados son información pública y lo que se desea es que todos tengan acceso a ellos, pueden hacerse copias del certificado de acuerdo sea necesario. Los certificados digitales permiten varias cosas, entre ellas se pueden citar que los usuarios pueden a nadir firmas electrónicas a los formularios en línea; que los destinatarios pueden comprobar la autenticidad del correo electrónico confidencial; que los compradores pueden estar seguros de que un website es legítimo; y por último, controla el acceso a bancos y comercios online, así como los intranets y extranets.

5.2.4 Estándar X.509

X.509 y X.500 fueron originalmente diseñados a mediados de los años 80, antes del enorme crecimiento de usuarios en Internet. Es por esto por lo que se diseñaron para operar en un ambiente donde sólo los computadores se interconectaban intermitentemente entre ellos. En las versiones 1 y 2 de X.509 se utiliza una lista estandarizada denominada “CRL” (Certificate Revocation List) que contiene la información referente a clientes o certificados que han sido revocados.

La versión 3 introduce cambios significativos en el estándar. El cambio fundamental es el hacer el formato de los certificados y los CRLs extensible. Ahora los que implementen X.509 pueden definir el contenido de los certificados como crean conveniente. Además se han definido extensiones estándares para proveer una funcionalidad mejorada.

Con la utilización de la tecnología de certificados digitales se provee a los clientes (personas o programas) de un nivel más alto en los procesos de autenticación y autorización, ya que se le otorga al cliente algo que puede poseer, incluso incluir dentro de elemento físico, como una tarjeta inteligente. Los certificados en el formato X.509 v3 contienen datos del sujeto, como su nombre, dirección, correo electrónico, etc. (Ver Fig. 5.1)

En la versión 3 de X.509, no hace falta aplicar restricciones sobre la estructura del certificado, gracias a la definición de las extensiones de certificados. Se permite que una organización pueda definir sus propias extensiones para contener información

específica dentro de su entorno de operación. Este tipo de certificados es el que usa el protocolo de comercio electrónico SET (del inglés Secure Electronic Transaction, Transacción Electrónica Segura) [**?**].

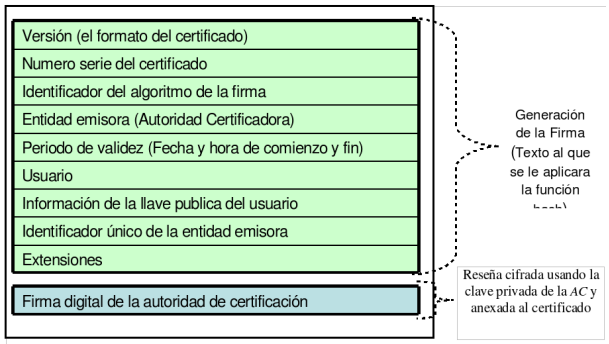

Figura 5.1 Especificación del estandar X.509

Los certificados digitales tienen multitud de usos, entre los tipos de certificados más utilizados están:

- **Certificado de Servidor SSL (del inglés Socket Secure Layer, Nivel de Conexión Segura):** Permite incorporar el protocolo SSL a un servidor web con el objetivo que toda la comunicación entre el cliente y el servidor permanezca segura, cifrando la información que envía cada parte. El certificado del servidor posibilita la autenticación fuerte, es decir, que el servidor puede exigir certificados personales de navegación a los usuarios para acceder a determinadas carpetas, lo que repercute en la seguridad y en la comodidad por la ausencia de cuentas y contraseñas para la identificación de los usuarios.
- **Certificados personales (Correo y navegación):** Un certificado digital personal es la herramienta necesaria para navegar, comprar y enviar/recibir correo a través de Internet, de una manera segura. Con el uso de este certificado se puede firmar o cifrar los mensajes de correo para tener la seguridad que el receptor será el único lector de nuestro mensaje. Se puede aumentar la seguridad y confianza entre el cliente y el servidor web, al autenticarse también al usuario, esto también va a permitir a las empresas la posibilidad de personalizar los contenidos a un usuario concreto, con la certeza que otros usuarios no podrán ver dicho contenido, tales como información confidencial, ofertas especiales, entre otros.
- **Certificado para firma de código:** El certificado para la firma de código permite a un administrador, desarrollador o empresa de software firmar su software y macros, y distribuirlo de una forma segura. Esta solución de Seguridad es el requisito mínimo que necesitan nuestros clientes o lista de correo, para confiar y tener la seguridad de que el fichero que reciben o se descargan, proviene exclusivamente de una empresa determinada. Con ello se evitan los problemas

causados por la suplantación de personalidad y la distribución de objetos dañinos o perjudiciales bajo esta supuesta identidad. Cualquier modificación (por ejemplo: inclusión de un troyano o infección de un virus) sobre el software original lo invalidará, con lo que el usuario tendrá la confirmación para rechazarlo al comprobar que la firma electrónica no corresponde con la del software modificado.

5.2.5 Lenguaje Unificado de Modelado

UML (del inglés Unified Modeling Language, Lenguaje de Modelado Unificado) es un lenguaje que permite diseñar sistemas a través de modelos, que se componen de un conjunto de símbolos y diagramas en donde se plasma las ideas de funcionalidad. El UML fue creado por Grady Booch, James Rumbaugh e Ivar Jacobson en el a no 1997[**?**],[**?**] y [**?**]. Cada diagrama tiene fines distintos dentro del proceso de desarrollo, su finalidad es presentar diversas perspectivas de un sistema. La clave está en organizar el proceso de dise no de tal forma que los analistas, clientes, desarrolladores y otras personas involucradas en el desarrollo del modelo lo comprendan y convengan con él. Los diagramas que componen el lenguaje son:

- Diagramas de casos de uso
- Diagramas de estados
- Diagramas de secuencias
- Diagramas de colaboraciones
- Diagramas de distribución
- Diagramas de actividades
- Diagramas de componentes
- Diagrama de despliegue

En este trabajo se utilizaron esencialmente los diagramas de clases, los diagramas de casos de uso y los diagramas de actividades, que se describen brevemente a continuación:

Diagramas de clases: son representaciones gráficas de las categorías en que pueden clasificarse los objetos del mundo real. En general, se hace una descripción de las categorías que se utilizan en la aplicación a desarrollar. Los clases se dise nan en funcion de sus atributos y relaciones con otras clases.

Diagramas de casos de uso: son descripciones de las acciones que debe realizar el usuario en el sistema [**?**]. Por ejemplo: Usuario que tiene la necesidad de expedir un certificado digital a una AC de confianza.

Diagramas de actividades: muestran el flujo de actividades que ocurren dentro de un caso de uso o dentro de un comportamiento de un objeto[**?**]. Por ejemplo, las actividades que se realizan para expedir un certificado digital.

5.2.6 Software Libre

El software libre [**?**] es un asunto de libertad, no de precio. Para que un programa, aplicación o conjunto concreto se considere "software libre" debe cumplir con las siguientes libertades: 1) Libertad de ejecutar el programa en cualquier sitio, cualquier propósito, por siempre; 2) Libertad de estudiarlo y adaptarlo a nuestras necesidades; 3) Libertad de redistribuirlo a cualquiera, logrando ayudar a un amigo o vecino; y por último 4)la Libertad de mejorar el programa y publicar las mejoras.

Las libertades antes expuestas, proveen muchos beneficios a los usuarios finales. En particular, en el área de seguridad informática. Se pueden nombrar entre los beneficios más importantes: la no dependencia de un único fabricante, y la posibilidad de realizar auditorías y pruebas exhaustivas por parte de terceros, que pueden ser personas, empresas o instituciones diferentes responsables del proyecto de software. Los procesos de adaptación, mantenimiento, integración y auditorías son más transparentes y colaborativos.

5.3 Infraestructura de Clave Pública

Uno de los problemas del despliegue de la tecnologías basada en certificados y firmas digitales, es contar con un elemento que proporcione una relación fuerte de confianza entre dos o más sujetos que desean realizar una operación o transacción utilizando como medio Internet. Es por ello, que se recurre a establecer un tercero de confianza, que se define, como un actor encargado de brindar confianza basada en la disponibilidad de una infraestructura robusta que incluya el uso tecnologías basadas en algoritmos criptográficos estandarizados, y la aplicación estricta de políticas para los procesos de registro, publicación, firma, renovación y revocación de certificados. El tercero de confianza se denomina Infraestructura de Clave Pública (ICP)[**?**], y consiste en la combinación de hardware y software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía pública. Una ICP debe proporcionar los tres conceptos de seguridad mencionados anteriormente.

5.3.1 Componentes de la Infraestructura de Claves Pública (ICP)

Los componentes habituales que conforman la infraestructura son los siguientes (Ver Fig. 5.8):

- Autoridad de Registro (AR): es el nodo o conjunto de nodos responsables del registro y la autenticación inicial de los usuarios a quiénes se les expide un certificado, después de aprobada una solicitud de registro.
- Autoridad de Certificación (AC): es el nodo central de la infraestructura, se encarga de los procedimientos de firma, renovación y revocación de certificados digitales. El procedimiento de firma de certificados utiliza la clave privada de la AC.

- Interfaz con los clientes (PUB): es el nodo que brinda toda la información a las entidades finales (usuarios) sobre el estado de su certificado, además de ofrecer una información general al público en general sobre los aspectos y servicios relevantes de la ICP.

Los nodos de una ICP pueden ordenarse según diversos modelos. El más utilizado es el modelo jerárquico, que presenta una raíz y nodos hijos que distribuyen los certificados a los clientes o entidades finales (Ver Fig. 5.2). Se muestra un ejemplo de modelo de jerarquía de una ICP de cuatro niveles, que se encuentra en el tercer nivel del modelo, que certifica a los usuarios.

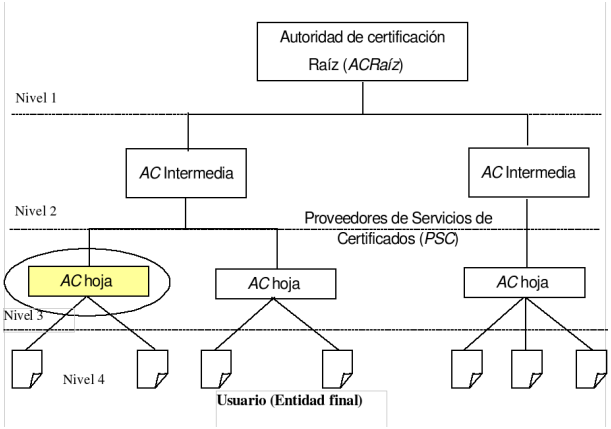

Figura 5.2 Modelo jerárquico de una ICP

Este modelo de establecimiento de relaciones de confianza, es necesaria entre múltiples autoridades de certificación para garantizar que los usuarios (entidades finales) no tengan que depender y confiar en una sola AC, algo que haría imposible el manejo de estabilidad, administración y protección. El objetivo es que las entidades finales que utilizan identidades creadas por una AC puedan confiar en ellas, aunque dichas partes tenga una autoridad expedidora diferente.

5.4 Desarrollo de la aplicación

En los párrafos siguientes se discute los aspectos, procesos y técnicas principales, que se siguen a lo largo del desarrollo de la aplicación (software) de gestión del componente Autoridad Certificadora Raíz.

5.4.1 Conceptualización

Uno de los objetivos de esta etapa es determinar el rol del componente AC Raíz en la ICP, con la finalidad de obtener los requisitos, procesos y funciones que deben

ser implementados por el software. Este rol tiene que ver con la definición de la AC Raíz como elemento central y de máximo resguardo de la infraestructura, ya que este nodo inicial o "Raíz" contiene la clave privada que valida todos los certificados de los otros nodos de la jerarquía.

Se considera como punto importante en esta etapa, distinguir las diferencias entre una AC Raíz y una AC de un Proveedor de Servicios de Certificación (PSC). La diferencia principal entre estos dos tipos de AC, es la cantidad de certificados que deben gestionar (firmar, renovar, revocar, etc) , en un determinado periodo cada uno de ellos. Esto es, una AC Raíz solo gestiona un número mínimo de certificados, los cuáles sirven para dar inicio a la jerarquía (certificados otorgados a los PSC), por el contrario, una AC de un PSC debe gestionar un número mucho mayor de certificados, ya que la función de este nodo es entregar certificados periódicamente a usuarios, también llamados entidades finales.

La diferencia de escala de los dos tipos de AC conlleva a que la AC Raíz tenga características particulares, que tienen que ver los niveles y elementos de seguridad tanto físicos como lógicos que deben considerarse en la gestión del componente. Por ejemplo, la desconexión de red del equipo donde se ejecuta la aplicación de gestión hace que la recepción y entrega de certificados se realice a través de unidades de memoria externas y portátiles, debidamente validadas, con las cuáles el software debe mantener una comunicación segura.

La conexión de la aplicación con hardware especializado, como el almacenador y generador de claves públicas/privadas (Hardware Security Module: HSM) o las tarjetas inteligentes, es un factor que debe considerarse en el momento de enumerar las funciones iniciales del software de gestión.

La selección del sistema operativo Linux[**?**] para desplegar la aplicación, ya que cumple con los principios del software libre, y cuenta con gran número de herramientas en el área de programación [**?**], es un requisito no funcional que se establece en esta etapa.

Considerando los aspectos nombrados anteriormente, en este punto se elabora una lista inicial de requisitos, con la cual debe cumplir la aplicación. Como técnicas utilizadas en ésta etapa están la realización de entrevistas a clientes, a posibles administradores y operadores; la elaboración de tablas comparativas entre diferentes aplicaciones que existen en las bibliotecas o portales de software libre, con la finalidad de evaluar las herramientas a utilizar en la elaboración de la aplicación.

5.4.2 Diseño

La etapa de diseño consiste en elaborar diagramas formales que permitan en la etapa de implementación representar requisitos y procesos de la gestión del componente AC Raíz en un lenguaje de programación. Para el diseño de requisitos se utilizan los diagramas de casos de uso del lenguaje UML, que muestran una primera aproximación las operaciones que se deben realizar en relación con las entradas dadas por los usuarios. Los actores (usuarios) del caso de uso principal que se muestra en la Fig. 5.3 son: el Administrador del componente AC, el Administrador del Compo-

nente AR, el Administrador del componente PUB, y el actor PSC, quiénes son los que interactúan con la aplicación.

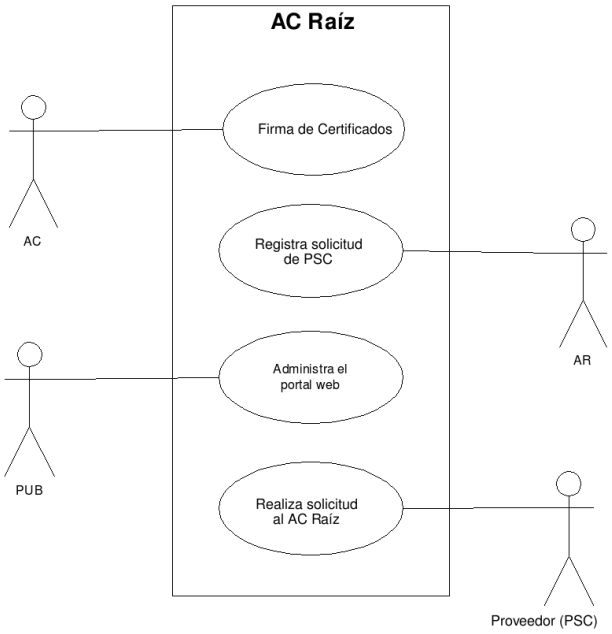

Figura 5.3 Caso de uso principal

Para el resto de la especificación de requisitos se elaboran casos de uso que modelan las funcionalidades con que debe contar la aplicación. Para cada actor, se especifican el correspondiente diagrama de caso de uso. En la Fig. 5.4 se muestra el caso de uso para el actor del componente AC. Las acciones que realiza este actor son emisión, renovación y revocación de certificados, que conlleva procesos de firma con la clave privada, modificación de los periodos de vigencia del certificado y elaboración de listas de certificados revocados respectivamente para casa caso de uso.

También en esta etapa se construye el modelo de datos de la aplicación. La Fig. 5.5 muestra de forma parcial, ya que no se incluyen los atributos, el diagrama de clases que explica el modelo de datos. Se consideran como objetos persistentes del sistema a elementos como usuarios, clientes, certificados, autoridades o proveedores de certificación, solicitudes de autoridad de certificación, solicitudes de entidad finales, y sus respectivas relaciones.

Para modelar la secuencia de acciones que se realizan para cada caso de uso se utilizan los diagramas de actividades. La Fig. 5.6 muestra el diagrama de actividades general para el caso de uso “Emisión de certificados”’ del actor Administrador del componente AC. Para este conjunto de actividades participan cuatro (4) actores: Administrador del PSC, quién entrega los recaudos necesarios para que se le firme su

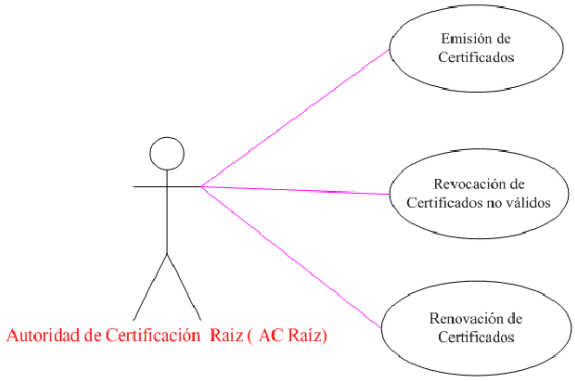

Figura 5.4 Caso de uso para el actor Administrador Autoridad de Certificación

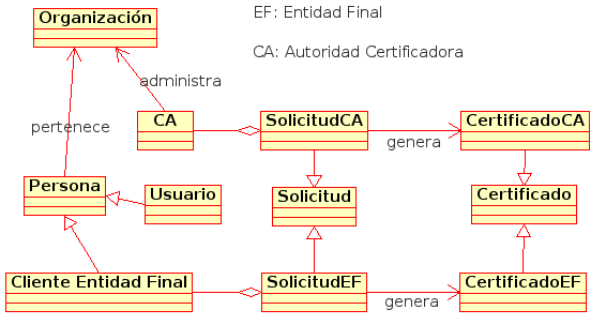

Figura 5.5 Diagrama de clases

solicitud, el Administrador de la AR, quién es el encargado de chequear los recaudos entregados por el PSC, el Administrador de la AC Raíz y el Administrador PUB, este último encargado de de publicar en los diferentes repositorios los certificados (claves públicas) para que sean visibles por el mayor número de usuarios interesados.

5.4.3 Implementación

En esta etapa se utiliza como insumo los diagramas de casos de uso, diagrama de clases y actividades, generados en la etapa de dise no. Se traduce el diagrama de clases al que se hace referencia en la Fig. 5.6 en un modelo de datos relacional, y se genera un script SQL que genera el mapa de tablas relacional, donde las tablas representan relaciones tales como usuarios, clientes, certificados, y las demás entidades que conforman el modelo de datos.

Se utilizan y validan los diagramas de casos de uso mediante la elaboración de interfaces gráficas de usuarios y funcionalidades de interacción con el usuario. Los

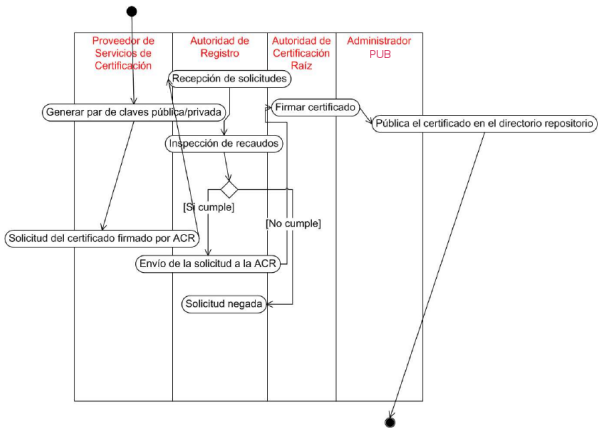

Figura 5.6 Diagrama de actividades

diagramas de actividades ayudan en el planteamiento de algoritmos que proveen funcionalidades o características con las cuáles debe contar la aplicación y que deben estar en coordinación con los respuestas y valores esperados.

Haciendo uso de las ventajas que trae el uso de software libre (Sección 5.2.6), se implementa la aplicación utilizando la mayor cantidad de líneas de códigos disponibles en los repositorios y proyectos de la comunidad, de tal manera que satisfagan los requisitos y funcionalidades planteadas en la etapa de dise no. En este sentido, se utiliza el código fuente del proyecto XCA [**?**], desarrollado por Christian Hohnstädt, que tiene como objetivo proveer una aplicación escrita en el lenguaje de programación C++[**?**] y la biblioteca Trolltech Qt[**?**], que cumpla con el estándar X.509. La aplicación satisface los requisitos básicos para la gestión del componente de gestión de AC Raíz, esto es, los diagramas UML de la etapa de dise no calzan con un gran conjunto de requisitos satisfechos en el proyecto XCA, esto ocurre debido a que este trabajo comparte objetivos con dicho proyecto; por ejemplo, para el caso de uso de la Fig. 5.4, donde el actor debe ejecutar tres acciones: emitir, renovar y revocar certificados, la aplicación XCA incorpora estas tres actividades, pero se hace necesario adaptar la interfaz de usuario y agregar características en función de los requisitos capturados.

Es importante recalcar, que XCA no sastiface todos los requisitos documentados en la etapa de dise no. En respuesta a este hecho, se realiza un proceso de completación de funcionalidades. En este sentido, se incorporan características a la aplicación acorde con la especificaciones de dise no, entre las cuáles se enumeran:

- La incorporación de un sub-sistema de seguridad para acceso a los activos de información que gestiona la aplicación, que incluya aspectos de autenticación y autorización de usuarios, como lo es la validación de credenciales a través del uso de tarjetas inteligentes, el registro y firma digital de las acciones realizadas por los usuarios dentro de la aplicación. En La fig 5.7 se muestra la caracterís-

tica de registro de acciones. La ventana a la derecha muestra los detalles de la acción seleccionada en la lista, se incluyen datos importantes como nombre de la cuenta de usuario, fecha, hora, y otros datos particulares relacionadas con la acción realizada por el correspondiente usuario.

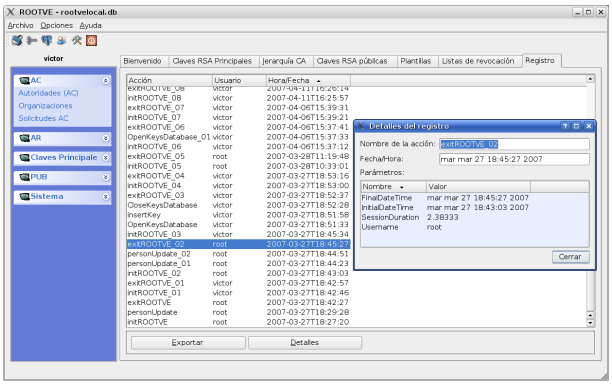

Figura 5.7 Sistema de registro de acciones

- Estandarización del sistema de gestión de documentos como solicitudes, plantillas de certificados y certificados.
- Conexión a través de una interfaz propia con el hardware donde se resguardan las claves privadas (HSM).

También en esta etapa se seleccionan e integran las tecnologías a utilizar para la codificación y creación de la aplicación de gestión del componente AC Raíz. Los tipos de tecnologías que deben seleccionarse son: bibliotecas para construir la interfaz hombre-máquina (HMI), motor criptográfico, conexiones con hardware, interfaces con repositorio de datos y algoritmos de cálculo criptográfico más utilizados.

Como criptosistema se utiliza OpenSSL version 0.9.8 [**?**], que provee de un conjunto de funciones criptográficas apegadas al estándar X.509. . Para la construcción de interfaces hombre-máquina y uso de algoritmos generales se selecciona la biblioteca Trolltech Qt. Como interfaz para el uso de tarjetas inteligentes se utilizo el estándar PKCS11, también conocido como Cryptoki, que especifica una forma para interactuar con este hardware criptográfico[**?**].

5.4.4 Pruebas

Esta etapa tiene dos objetivos. El primero de consiste en asegurar que la aplicación funcione correctamente, es decir, que se generen la menor cantidad de salidas inesperadas o fallas a entradas dadas. En relación al logro de este objetivo se utilizan un conjunto de técnicas aplicadas a lo largo del proceso de desarrollo, entre las cuáles se pueden citar la revisión en parejas[**?**], que consiste que la programación se realice en equipo de dos programadores por computador, uno de ellos se encarga de escribir

los algoritmos en un lenguaje de programación, y el segundo de ellos de revisarlo inmediatamente, después de periodo de unas horas, que debe ser definido con anticipación, se intercambian los roles. Otra de las técnicas utilizadas que es importante nombrar son las pruebas unitarias[**?**], las cuáles consisten en aplicar un número casos de pruebas a métodos o módulos peque nos de la aplicación (unidades), de tal manera que se asegura que funcionan correctamente de forma independiente. Seguidamente, se realizan pruebas de integración, que consisten en probar módulos más complejos formados por las unidades revisadas en las pruebas unitarias. Las pruebas unitarias y de integración presentan la ventajas que son automatizables, y por lo tanto, se cuenta como herramientas de software para llevarlas a cabo.

El segundo objetivo, es que se satisfagan los requisitos plasmados en la etapa de dise no, y que se extraen de los diagramas UML , es decir, la aplicación debe cumplir con las características necesarias para resolver el problema de gestión de una AC Raíz. En este sentido, se toma una estrategia basada en prototipos con liberaciones periódicas, que permite a los usuarios y desarrolladores de la comunidad chequear el progreso en el proyecto. Los prototipos son chequeados por los usuarios y la modificación de requisitos y notificación de errores son notificados en un sistema web de chequeo y seguimiento [**?**].

También se habilita un sistema de control de versiones de licencia libre llamado subversion [**?**], que permite a los programadores involucrados en el proyecto obtener en todo momento y de forma local o remota la última versión de los programas fuentes.

Debido a que la aplicación de gestión de AC Raiz debe ser parte de una infraestructura, es necesario realizar pruebas en condiciones similares a la configuración final de ésta; por ello se simula la configuración de producción que conlleva pruebas con el sistema operativo y el donde se instala la aplicación, conexión con tarjetas inteligentes y el módulo de seguridad en hardware, controles de acceso físico y lógico, y desconexión de red, ya que la autoridad debe operar fuera de línea.

5.4.5 Despliegue y configuración

El despliegue consiste en la instalación en condiciones reales de la aplicación de gestión de AC Raíz dentro de la infraestructura. La figura 5.8 muestra una propuesta para el despliegue de la infraestructura. La aplicación se instala en un computador desconectado de red que debe estar ubicado dentro de un lugar físico seguro, lo que significa que el acceso a personas deber estar restringuido por llaves y controles biométricos, y el flujo de información digital hacia adentro y afuera de la bóveda debe ser realizado a través de dispositivos de memoria secundaria con seguridad incorporada, tal como un lapiz usb (pendrive) con bloqueo por contrase na, como se muestra en la figura. También es necesario la habilitación de servidores para la validación de los periodos de vigencia de los certificados (OSCP), y para la generación de solicitudes de firma de certificados, donde las entidades finales o usuarios consignan los recaudos.

Por otro lado, la configuración conlleva el establecimiento de parámetros para el funcionamiento la aplicación, tales como métodos de control y restricción de ac-

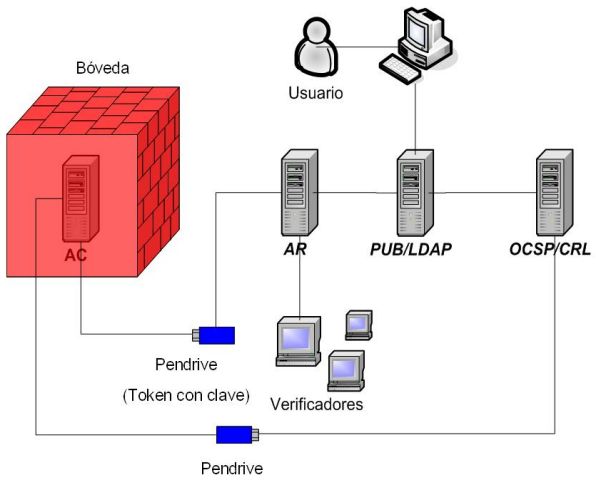

Figura 5.8 Configuración de los componentes del nodo raíz de una ICP

ceso, ubicación de archivos y directorios, rutas para importación e exportación de datos, perfiles de usuario, generación y nombres de claves, inicialización de tarjetas inteligentes, inicialización de HSM, y copias de seguridad.

5.5 Conclusiones

La puesta en marcha de una AC Raíz supone obligatoriamente contar con una aplicación que gestione este componente de la infraestructura. En este sentido, éste trabajo mostró el proceso de desarrollo de una aplicación que respondiera a los requisitos particulares de gestión, determinados por el rol de confianza raíz y última que debe representar la Autoridad. En función de ello, la aplicación tiene un alto grado de especialización, ya que cuenta con un mercado relativo de pocos usuarios, si se compara con el mercado de los sistemas de información o aplicaciones de ofimática, y su operación se realiza en condiciones estandándares y específicas. A pesar de este hecho, para la construcción de la aplicación se integraron varios proyectos disponibles en los repositorios de software libre, que permitió disponer de un criptosistema estándar y suficientemente completo para cumplir con los requisitos descritos en la etapa de dise no. La criptografía se utiliza como herramienta para otorgar las tres propiedades (Confidencialidad, Integridad y Disponibilidad) de la seguridad informática a los datos que gestiona la aplicación, y en virtud de ello el hardware criptográfico utilizado como las tarjetas inteligentes y el módulo de seguridad en hardware configuran un “mundo seguro” que cumple con los estándares aceptados a nivel mundial.

En la etapa de dise no, los diagramas de casos de uso y actividades sirvieron para obtener una visión formal de los requisitos y de los procesos con los que cumplir la

aplicación. Estos documentos de dise no en el lenguaje UML, permitieron alcanzar de manera más rápida y certera los objetivos que son coincidentes con la gestión real de una AC Raíz.

Al seguir el estándar X.509 se asegura que los certificados, solicitudes y claves gestionados por la aplicación sean compatibles con el esquema de seguridad basado en un tercero de confianza, y aceptado por gran cantidad de aplicaciones y sitios de comercio y transacciones seguras en internet.

Para la tarea de eliminación de fallas las técnicas como la colaboración utilizando herramientas web, la programación en equipos y las pruebas unitarias y de integración sirvieron para los procesos de prevención, notificación, búsqueda y arreglo de errores, permitiendo además guardar una bitácora del progreso a la solución a problemas. La implementación de características específicas en función de los requisitos cada vez más refinados y particulares que surgieron en las iteraciones de prototipos probados con usuarios y condiciones reales.

La combinación de diversos elementos como software, hardware y la configuración de un espacio físico adecuado, esto es, que cumpla determinadas reglas para el control de acceso, conforma la infraestructura necesaria para la operación de una AC, incluso que ésta no sea Raíz, y sea parte de otro nodo de la jerarquía. Las condiciones de seguridad lógica y física pueden reproducirse exactamente para los nodos intermedios y los nodos Proveedores de Servicios de Certificación de la ICP, tomando en cuenta el escalamiento.

5.6 Glosario

AC: Autoridad de Certificación; componente de la PKI encargada de guardar de firmar, renovar, revocar las claves de los usuarios o entidades finales.

AR: Autoridad de Registro; componente de la PKI encargada de validar los recaudos de un PSC o Entidad Final, es decir, su identidad, y generar la solicitud para una firma de Certificados.

Entidad Final: Persona natural o jurídica a la que un PSC le expide un certificado digital.

PSC: Proveedor de Servicios de Certificación Digital; Organización que mantiene la infraestructura de nodo de una ICP, y está autorizada a expedir certificados a las personas naturales y jurídicas que soliciten y reunan los recaudos necesarios para obtener un certificado digital.

PUB: Publicador; componente de la PKI encargada de mantener accesibles los certificados digitales emitidos por la PKI en medios como portales Web o directorios.

PKI: Public Key Infrastructure, Infraestructura de clave pública; es el conjunto formado por software, hardware, y políticas que asegura en la internet la propiedad de la claves públicas de los usuarios.

HSM: Hardware Security Module; módulo de seguridad en hardware, equipo físico computacional que contiene funciones criptográficas, en específico funciona para almacenar con un alto nivel de seguridad claves privadas.

CAP´TULO 6

FIRMAS ELECTRÓNICAS

V. Bravo y A. Araujo

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

A continuación el contenido del artículo de componente de firmas electrónicas

Automation is use the information technologies as a direct method for improvement. However, there are elements such as handwritten signature that have been taken of all the digital area, but which, when recurrent events in organizational processes stand as a critical factor in the flow of operations. In response to this situation have developed numerous standards and technologies grouped by Electronic Signature concepts and PKI, but that in turn have discovered new questions in this field, among them, those that have to do with the integration processes. In this paper we propose a software component and a method for connecting computer systems as essential technology using the Advanced Electronic Signature. In this sense addresses the document formats, validation infrastructure, and safety conditions that ensure legal support. The work has center, the details and problems of integration, and that have been grouped under "coupling joint" concept.

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

6.1 Introducción

La adopción de la tecnología de firma electrónica aún no está suficientemente extendida. Esta se utiliza en distintas áreas y en muchas instituciones o empresas alrededor del mundo pero no ha llegado a ser equivalente a la firma autógrafa en un sentido amplio. Vinculado a este hecho, surge la pregunta ¿Pueden converger estas dos tecnologías en un futuro próximo?. Con la finalidad de responder esta interrogante, se puede decir que la herramienta electrónica debe tener por lo menos tres características comunes a la autógrafa: identificar a la persona que la realiza; declarar la asunción u obligatoriedad de cumplimiento (contrato) del contenido de lo que se firma y por último, servir como prueba de autenticidad o no repudio del firmante. El modelo de firma electrónica basado en una infraestructura PKI (siglas en inglés de Infraestructura de Clave Pública), ha sido jurídicamente aceptado en muchos países, lo que equivale a decir que en estos casos se cumple con las características antes mencionadas.

La firma manuscrita se percibe como un elemento tecnológico desacoplado, esto es, no dependiente de otra tecnología o factor (solo se necesita papel y lápiz) que puede usarse casi en cualquier lugar y con aceptación universal. En cambio la firma electrónica requiere de elementos de software (manejadores de dispositivos, clientes de firma, etc) y hardware (lector de tarjetas, tarjeta inteligente, computador, tableta o móvil), adicionalmente y por lo general se debe contar con una conexión a internet para la validación. Otra ventaja importante de la firma manuscrita es la permanencia de factores biométricos que son fundamentales en la realización de auditorías confiables. A pesar de todas estas ventajas, en los últimos años ha crecido el uso de la firma electrónica, Gobiernos nacionales y locales de España[17]. Alemania[16] y Estonia[18] tienen disponibles plataformas para sus ciudadanos, y la popularización de la tarjeta inteligente (smartcard) como elemento de identificación personal ha apoyado este crecimiento.

En este punto se plantean nuevos problemas vinculados al hecho de introducir o sustituir el elemento físico o autógrafo por el elemento electrónico, entre estos podemos señalar: elección del formato o formatos de archivo de los documentos firmados; ubicuidad y ergonomía de la acción de firma; verificación de los documentos firmados; histórico o archivo de documentos firmados y finalmente la integración de la firma con sistemas de base de datos relacionales, mapeos objetos-relacionales, servicios web, entre otros elementos utilizados en sistemas informáticos actuales.

En este sentido, este trabajo plantea un método para integrar un componente[2] de Firma Electrónica Avanzada denominado ComponenteFEA a procesos de negocio, teniendo presente parámetros de seguridad, rapidez y auditabilidad.

6.2 El modelo actual de Firma Electrónica

Una de las acciones para dar soporte jurídico a la firma electrónica y lograr su equivalencia con la firma manuscrita es fijar unas condiciones iniciales que garanticen integridad y auditabilidad de los documentos firmados, y que puedan ser validada-

dos a través de un estándar. Bajo este enfoque, se ha creado el concepto de Firma Electrónica Avanzada, que por definición debe contar con las siguientes propiedades a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control y d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La formalización de esta idea ha sido llevado a cabo principalmente por el Parlamento Europeo, y se describe en la directiva 1999/93/EC [3]. .

Existen dos grandes dominios tecnológicos para el uso de la Firma Electrónica Avanzada: uno es el que tiene que ver con los procesos de identificación, registro, emisión y validación de certificados electrónicos. De este dominio se ocupan las organizaciones que están bajo el esquema PKI, que funcionan como terceros de confianza. Cada certificado brinda identidad a una persona o empresa en la internet, y se le otorga al ente bajo la aceptación de un contrato que especifica condiciones de uso. El certificado es un documento -un archivo- que autentifica la clave vinculada al ente. La clave secreta/privada se distribuye en una tarjeta inteligente o token criptográfico que funciona como un elemento de control de acceso de nivel 2. Los certificados electrónicos contienen información especificada bajo el formato X.509v3 [4], el cual incluye campos como fecha de expedición y vencimiento del certificado, Nombre único del propietario (conocido como Nombre Común), datos del Proveedor del certificado, datos criptográficos del certificado y datos del servidor de validación, conocido como OCSP (Online Certificate Status Protocol, por sus siglas en inglés).

El segundo dominio corresponde a las aplicaciones que usa el propietario del certificado para aplicar la firma electrónica, y que generan valor agregado. Las aplicaciones de este tipo más utilizadas cuentan con una interfaz basada en bibliotecas dinámicas (.dll o .so) para este fin, así como también tienen un archivo de certificados de autoridades de certificación para validar la vigencia y correctitud del certificado del firmante. Esta interfaz es básica, solo permite generar un archivo de firma en formato PKCS#7[10] separado del documento firmado, lo que conlleva a que las tareas de almacenamiento, validación y auditoría deben ser provistas adicionalmente a través de un programa o complemento de software. Las aplicaciones de este tipo más utilizadas son navegadores web y clientes de correo electrónico.

Por otro lado, se han especificados diferentes formatos estándares de archivo con firma autocontenida. Por ejemplo el formato PDF dada sus características de solo lectura y visualización en pantalla como documento impreso es uno de los más utilizados para este fin. El estándar PADES[13] basado en PDF es un ejemplo de ello, también existe el formato PDF nativo, y que es verificable por los visores más populares como el de *Adobe Reader*©.

También existen estándares para archivos con firma electrónica basados en XML. La ventaja de estos formatos es que pueden integrar metadatos como la fecha y lugar de la(s) firma(s), y permiten incluir diferentes tipos de archivos como fotos, videos, documentos de texto u ofimáticos. Entre los estándares XML más conocidos está el XMLDsig [6]. Esta estándar cuenta con diferentes implementaciones y extensiones, entre ellas el formato creado por las repúblicas bálticas llamado BDOC[15], que

sigue a su vez el popular estándar OpenDocument, utilizado por el paquete ofimático OpenOffice como formato principal para sus archivos.

6.3 Antecedentes

La inclusión de la firma electrónica en un proceso de negocio tiene varios aspectos asociados. Se pueden señalar como los más relevantes la ergonomía de la firma (facilidad de uso), los formatos y visualización de documentos, la integración con plataformas de software y la arquitectura de la solución.

En relación con el tema de la ergonomía Xyzmo SIGNificant[1] es una novedosa propuesta. Xyzmo es una una aplicación comercial de código fuente propietario, que introduce elementos innovadores en el área de ergonomía y adaptación al cambio: no obliga a aprender una nueva técnica de firma sino que ofrece a los usuarios de esta tecnología el uso la firma manuscrita a través de una tableta electrónica o teléfono con interfaz multitoque (multitouch) bajo sistemas operativos Android© y iOS©, esto sin desvincularse del esquema PKI. Este modelo proporciona al usuario la metáfora de la firma manuscrita mostrando el documento tal cual como si fuese impreso, habilitando la firma electrónica avanzada a través del uso de los dedos o de un lápiz para pantalla táctiles. Para el proceso de validación se utilizan parámetros biométricos tales como ritmo, velocidad o características del trazo, y también técnicas criptográficas estandarizas vinculadas al esquema PKI.

Existen diferentes implementaciones de software para las gestión y visualización de los dos tipos de formatos principales: PDF y XML. Para el caso del formato PDF la visualización está automáticamente disponible ya que existen numerosos lectores para este tipo de archivo, por ejemplo, el Adobe Reader© visualiza la firma electrónica o digital como un sello (imagen) dentro del documento, y muestra también su contenido con características de forma (encabezado, líneas, tablas, logos, etc.) que pueden ser parte o no del documento firmado, pero que en muchos casos son necesarias para la elaboración de documentos formales o legales. En el caso de los formatos XML la visualización no es automática, por lo tanto si se requiere visualizar el contenido con elementos de forma se debe disponer de un software visualizador que formatee el contenido. En [1] se muestra una propuesta para documentos XML que necesitan por disposiciones legales o formales de gobierno aplicar forma a documentos firmados electrónicamente.

Una de las potencialidades de la firma electrónica es su integración con sistemas informáticos para la mejora de procesos mediante la eliminación de puntos lentos. Es por ello que los temas de integración y arquitectura juegan un papel preponderante. En esta tendencia se inscribe el proyecto @*firma*: una solución desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, que se plantea como una plataforma de firma electrónica orientada a brindar servicios de gobierno electrónico, y que está integrada con el sistema de identificación Español. Cuenta con una aplicación de escritorio que puede usarse en diversos sistemas operativos, y

[1] Para ver información completa sobre Xyzmo Significant visitar la dirección web: http://www.xyzmo.com

un *applet*[14] para usar la firma a través de la web. Estas características habilitan a *@firma* para el desarrollo de aplicaciones de gobierno electrónico, así como también para la integración con sistemas empresariales.

6.4 Acoplamiento de la Firma Electrónica Avanzada

La conexión entre un componente (software) y el sistema informático se denomina acoplamiento. Este procedimiento debe cumplir con un conjunto de requisitos que tienen que ver con características tales como reutilización, cohesión y la exportación de una interfaz definida. A continuación se describen los elementos desarrollados en este trabajo.

6.4.1 Componente de Firma Electrónica Avanzada

Se desarrolló un componente que permite realizar diferentes operaciones asociadas con la firma electrónica: subir un documento desde el computador cliente; realizar la firma utilizando una tarjeta inteligente con PIN (contraseña) desde el computador cliente y entregar un archivo firmado en formato XAdES[5] al programa servidor. El componente se ha denominado de Firma Electrónica Avanzada (ComponenteFEA), ya que cumple con las condiciones citadas en la sección 6.2 sobre este tipo de firma.

Las funcionalidades que implementa el ComponenteFEA son las siguientes:

(a). Firmar electrónicamente (para este caso se asume que lo electrónico está asociado un dispositivo en hardware como una tarjeta inteligente. y en relación a ello debe connotar vinculación jurídica, lo digital solo a una clave en software) un documento de tipo de archivo definido por especificación MIME[11].

(b). Firmar digitalmente (usando un archivo PKCS#12[12]) un documento de tipo de archivo definido por especificación MIME .

(c). Verificar un archivo firmado electrónicamente usando o no validación OCSP.

(d). Verificar un archivo firmado digitalmente usando o no validación OCSP.

(e). Mostrar propiedades como algoritmos utilizados, fecha y lugar de la firma de un archivo firmado

(f). Firmar electrónicamente utilizando un componente para el navegador un documento de tipo de archivo definido por especificación MIME.

```
class BDocDocument : QObject {
// *** Métodos para firma electrónica
    BDocDocument();
    void init();
    void create( const QString file );
```

```
    bool openBDocContainer(const QString path);
    void saveBDocContainer(const QString path);
    bool signWithP12(const QString  profile,...);
    void addDocument(const QString path);

// ** Mètodos de firma por navegador web
    bool presignWeb(const QString  profile, ...);
    bool postsignWeb(const QString  profile, ...);


// ** Métodos para validación
    QString signatureAlgorithm(int index );
    bool validateOffline() const ;

// ** Métodos para Gestión de archivos
    QString signatureFormat(int index );
    QString signatureDateTime(int index );
    QStringList signatureLocation(int index );
    QString signatureRol(int index );
    QString signatureDigestMethod(index )
    QString subjectCertificateCommonName(int i);
    QString documentName(int docId);
    int documentCount();
    int signatureCount();
    void saveDocument(int docId...);


}
```

Listado 1. API del ComponenteFEA en C++ accesible desde *python*

Bajo esta perspectiva se propone tratar las funcionalidades asociadas a la Firma Electrónica Avanzada, es decir, empaquetar las funcionalidades exportando una API (por su siglas en inglés Interfaz de Programación de Aplicaciones) que puede ser utilizada de forma encapsulada y separada por una aplicación anfitrión, escrita teóricamente en cualquier lenguaje de programación. Uno de las aplicaciones que trabaja bajo este esquema de complementos o componentes es el navegador web, este diseño ha permitido contar con grandes repositorios que extienden las funcionalidades del navegador casi para cualquier uso.

La figura 6.1 muestra un diagrama en lenguaje UML del componente y su conexión con un sistema informático. Existen tres tipos de funcionalidades que exporta el ComponenteFEA: ”Firmar”, interfaces para firma electrónica y digital, ”Validar“, interfaces para validación fuera de línea y en línea de certificados electrónicos, y ”Gestionar“, interfaces para la almacenamiento y búsqueda de archivos firmados.

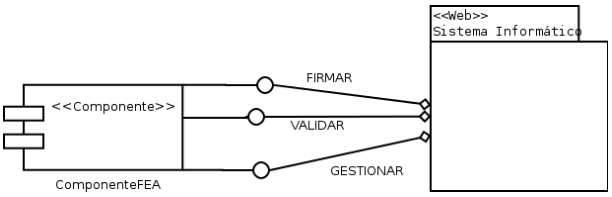

Figura 6.1 Diagrama UML de acoplamiento

A nivel de lenguaje de programación se provee un paquete o *package* para *python* que está construido envolviendo una librería de firma electrónica avanzada escrita en lenguaje *C/C++*. El listado **1** muestra los métodos que son accesibles desde *python*.

6.4.2 Método de conexíón

El diagrama de flujo de la figura 6.2 muestra los pasos a seguir para incorporar el ComponenteFEA dentro de un proceso de una organización. Los primeros dos pasos de este diagrama corresponden a la identificación de los puntos de firma y validación dentro del proceso de negocio, para luego conectar los métodos (mensajes) correspondientes del ComponenteFEA en dichos puntos.

En un siguiente paso y dependiendo del tipo de proceso a automatizar se adoptará un esquema de conexión para el servidor. En esta fase se establecen algunos aspectos importantes relativos al sistema informático a colocar en funcionamiento, entre estos están la existencia de un sistema automatizado, el tipo de lenguaje de programación y sistemas operativos a utilizar, el soporte de la PKI, la asignación de las tarjetas inteligentes, entre otros.

En este punto el desarrollador tiene la libertad de utilizar el componente de firma según su criterio, sin embargo, puede seguir algunas pautas relacionadas con el proceso a automatizar. Si el proceso no se encuentra automatizado se recomienda seleccionar para el desarrollo de software el lenguaje *python*. Para el caso anterior o si el sistema se implementó utilizando este lenguaje se sigue el paso 7.1 de la figura 6.2 que corresponde con la instalación del componente ”servidor“ para la Firma Electrónica Avanzada.

En el caso de que los procesos de negocio se encuentren automatizados bajo un lenguaje diferente a *python*, se utilizan la interfaz de servicios web[2] que provee del ComponenteFEA (Paso 8.1 de la figura 6.2).

Un tema a tomar en cuenta es el relativo al tipo de repositorio donde se almacenan los archivos firmados. El ComponenteFEA genera archivos tipo XAdES con extensión *.bdoc*. Para este fin puede utilizarse un directorio en el sistema de archivos o un gestor de base de datos relacional. En este punto también hay que trabajar sobre el nombramiento, es decir la forma como se identifican unívocamente los archivos para que puedan ser encontrados. Para ello se puede utilizar la vinculación de metadatos

[2]La interfaz de servicios web está disponible en: http://bazaar.launchpad.net/~esignature/esignature/bdoc/files/head:/server/

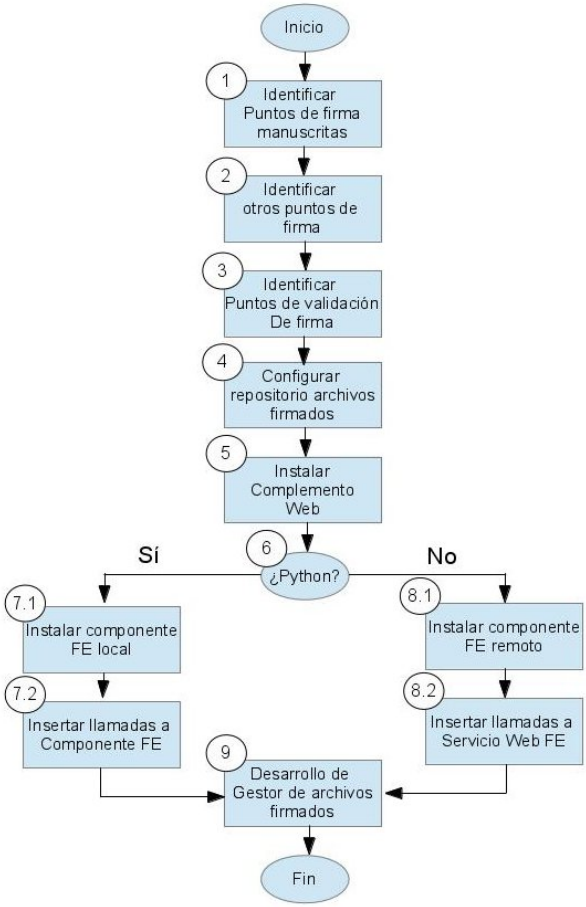

Figura 6.2 Diagrama de flujo para el acoplamiento del ComponenteFEA

en los registros de las tablas de la base de datos relacional, o simplemente asignar un nombre como clave única a los archivos firmados.

Como último paso se debe habilitar un módulo para gestionar los archivos firmados (paso 9 de la figura 6.2), es decir, proveer una interfaz de usuario para las acciones de visualización de propiedades de archivos, validación de firmas electrónica, búsqueda, entre otras. Estas funcionalidades las provee el ComponenteFEA mediante los métodos que se nombran en la sección ”Métodos para Gestión de archivos“ del Listado **1**, y pueden ser extendidas utilizando algunas de las funcionalidades del gestor de datos que se utilice.

6.5 Casos de estudio

A continuación se muestran tres casos de integración utilizando un mismo proceso con diversos sistemas informáticos. El proceso tratado es el conocido como ”Orden de compra“, el cuál está presente en muchas organizaciones. Consiste en realizar un proceso de negocio con la finalidad de obtener un conjunto de productos o servicios necesarios para la organización a través de una búsqueda y evaluación de un cierto número de cotizaciones y que siguen una serie de criterios, como por ejemplo, las características de calidad y precio. El proceso en pasos se puede describir así:

(a). Generar una requisición o documento de solicitud para el conjunto de productos o servicios

- Firma del solicitante

(b). Obtener por los menos n $(n \geq 2)$ cotizaciones para el conjunto de productos o servicios

(c). Seleccionar una cotización y generar un acta

- Firma del analista de compras

(d). Generar una orden de compra

- Firma del gerente del departamento

Generalmente este proceso se lleva a cabo utilizando firmas manuscritas en coordinación con un sistema informático: se imprime desde el sistema el documento (requisición, acta u orden de compra), se firma, y luego se actualiza la información en el sistema informático.

Para el caso de estudio planteado se puede sustituir la primera, la segunda o las tres firmas manuscritas por sus respectivas firmas electrónicas. También es posible agregar firmas electrónicas en puntos donde no existen firmas manuscritas.

La segunda funcionalidad a conectar del ComponenteFEA es la validación de los documentos firmados electrónicamente. Para ello se identifican los puntos donde se actualiza la información sobre la firma manuscrita. Una tercera funcionalidad es la que tiene que ver con la visualización de los atributos de los documentos firmados electrónicamente.

Después del proceso de identificación, para cada punto que se determinó en la fase anterior, se incorporan los métodos del ComponenteFEA con llamadas locales o remotas según sea el caso. A continuación se presenta tres implementaciones del proceso ”Orden de compra“ para tres sistemas informáticos diferentes.

6.5.1 Caso OpenERP

OpenERP[3] es un software de Planificación de Recursos Empresariales (ERP, por sus siglas en inglés), software libre, que tiene un gran número de instalaciones. En su

[3]Ver la dirección web: http://www.openerp.com

base incluye el proceso de ”Orden de compra“. Para realizar el acoplamiento se creó un nuevo módulo de OpenERP. Se identificaron los puntos de firma y validación y se sustituyeron por las llamadas respectivas al ComponenteFEA. Como elemento agregado, se creó un nuevo módulo basado en bandejas de documentos -archivos generados por OpenERP- (similar a las usadas en los clientes de correo electrónico) asociadas a los documentos a ser firmados electrónicamente.

La figura 6.3 muestra la interfaz de usuario para gestionar los archivos firmados electrónicamente. Los usuarios autorizados pueden utilizar una tarjeta inteligente para firmar los documentos correspondientes al proceso de ”Orden de compra“, teniendo la misma validez legal (especificado por las políticas de la PKI y la legislación del país) que la firma manuscrita. Primero el solicitante firma la requisición, y este documento se envía a la bandeja del analista de compra, quién busca las cotizaciones correspondientes y selecciona el conjunto de productos a comprar. Se generan los documentos ”Acta” y “Orden de compra”, este último es enviado a la bandeja del gerente quién lo firma para aprobar la compra del conjunto de productos o servicios seleccionados.

OpenERP provee al desarrollador patrones Modelo-Vista-Controlador (MVC) y un motor de flujo de trabajos o *Workflow* para implementar nuevas funcionalidades. Usando estas herramientas los documentos firmados se vinculan al modelo de datos y las validaciones de firma electrónica se realizan extendiendo el flujo de trabajo relacionado con el proceso “Orden de compra” base de OpenERP.

La última captura de pantalla de la figura 6.3 muestra un cuadro de diálogo que pide un PIN o contraseña al usuario. Esta interfaz forma parte del complemento Web que debe ser instalado en el cliente (navegador) y que tiene interacción con el certificado firmante contenido en una tarjeta inteligente.

6.5.2 Caso SAID

SAID[4] es un sistema administrativo que incluye procesos contables y administrativos para instituciones que operen en el sector público venezolano. Entre los procesos que implementa SAID está el de ‘Orden de compra“, que incluye entre sus capacidades la posibilidad de utilizar firmas digitales basadas en el formato PKCS#7.

El sistema fue escrito en PHP Versión 4.X, y es de código libre. Los puntos de firma y validación están claramente identificados, ya que son los indicados por las firmas digitales, en este caso solo se sustituyen las llamadas a la API del motor criptográfico local, por llamados a los servicios web del ComponenteFEA. El listado **2** muestra las llamadas que se insertaron en el código fuente para extender el sistema de tal manera que funcione con firmas electrónicas avanzadas. El repositorio de archivos firmados a utilizar es PostgreSql Version 8.4 (El mismo que utiliza SAID). El listado **2** muestra el código en PHP para validar una firma electrónica y mostrar los firmantes de un documento del proceso de Orden de compra: requisición, acta u orden. Después de realizar la conexión al servidor *localhost* por el puerto 4242, se

[4]Ver la dirección web: http://said.cenditel.gob.ve/wiki

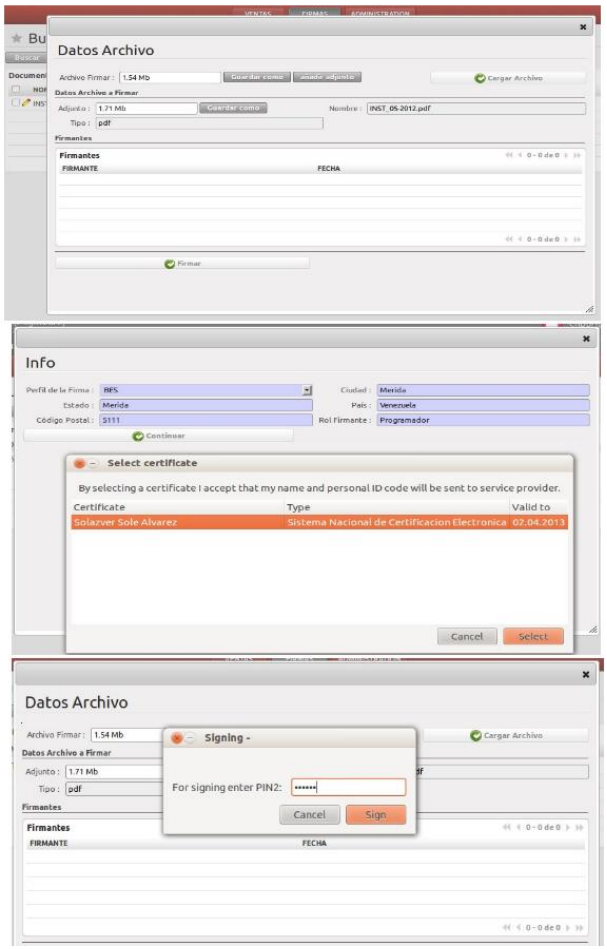

Figura 6.3 Interfaz de usuario OpenERP para el ComponenteFEA

procede a abrir un archivo firmado el método ”openBDocContainer“ a través de una llamada remota, luego se utiliza el método ”validateSignature“ para validar la firma, y finalmente se listan todos los firmantes utilizando el método ”subjectCertificate-CommonName“.

```
 <?php

include('xmlrpc.php');

$connec = new XMLRPCClient('localhost:4242');
$identificador = 'prueba1';
$connec->__call('init', array($identificador));
```

```
$connec->__call('openBDocContainer',
array($identificador,
'detalle_curso.odt.bdoc'));
$resp = $connec->__call('signatureCount',
array($identificador));
$firmantes = Array();
for($pos=0; $pos<$resp; $pos++)
{
$datos = Array();
$valida = 'No válido';
if($connec->__call('validateSignature',
array($identificador,$pos)))
{
   $valida = 'Válido';
   $nombre =
 $connec->
   __call('subjectCertificateCommonName',
array($identificador,$pos));
   $firmantes[] = array('nombre'=> $nombre,
'valida'=>$valida);
}
}

for($i=0;$i<count($firmantes);$i++)
{
echo "{$firmantes[$i]['nombre']}
{$firmantes[$i]['valida']}\n";
}
?>
```

Listado 2. Conexión mediante servicios web-rpc desde SAID al ComponenteFEA

De forma similar al caso OpenERP, se provee un complemento para el navegador de tal manera que los usuarios puedan realizar la firma de forma remota, utilizando una tarjeta inteligente desde su estación de trabajo. Luego el documento se procesa por el sistema SAID, y se almacena en la base de datos del servidor.

6.5.3 Caso Flujos de Trabajo

El proceso especificado en esta sección puede modelarse usando un motor de flujo de trabajo. Los flujos de trabajo son ampliamente utilizados para modelar procesos a través de un lenguaje descriptivo como BPM o BPEL[8]. Para implementar el proceso de ”Orden de compra“ se utilizó el motor SAFET[9], ya que incorpora el ComponenteFEA nativamente, solo se necesitan especificar los puntos en el proceso donde se requiere la firma electrónica. La validación la realiza el motor de forma

automática. Para este caso los pasos 1 y 2 del Diagrama de flujo para el acoplamiento del ComponenteFEA, se realizan sin la necesidad de agregar o modificar código fuente, solo se especifica en el archivo de definición de flujo.

```
<task id="Requisicion"
 title="Acción de solicitud de bien o servicio" >
<port side="forward" type="split" >
<connection source="Cotización"
query="vRequisicion SIGN NombreComunUsuario"
options="" >
</connection>
</port>
<variable id="vRequisicion" scope="task"
tokenlink=""
documentsource="select  id,
nombre,descripcion,
fechageneracion
from requisiciones" >
</variable>
</task>
```

Listado 3. Tarea de firma de requisición usando SAFET (XML)

El listado **3** muestra la definición de la acción de firma electrónica en un flujo de trabajo (SAFET). El usuario definido por el *NombreComunUsuario* debe firmar electrónicamente el documento de requisición para pasar a la siguiente actividad que en este caso se denominada *Cotización*. La sentencia *vRequisicion* ***SIGN*** *NombreComunUsuario* indica al motor de flujo de trabajo lo descrito anteriormente.

6.6 Conclusiones

En un mediano plazo la Firma Electrónica Avanzada puede consolidarse como una tecnología fundamental en los procesos de negocio ya que propone la digitalización de un elemento imprescindible en este contexto como lo es la firma manuscrita. Los retos de la digitalización son diversos y complejos, y tienen que ver con aspectos disímiles como lo son por ejemplo los formatos de archivo de firma electrónica y la ergonomía para el uso de esta tecnología.

En este trabajo se detalla un método para la integración de un componente de software con sistemas informáticos que automatizan procesos de negocio. En la fase de acoplamiento se define la identificación de puntos de firma electrónica, se especifica la validación de los certificados firmantes por una PKI, se muestra la habilitación del navegador web para la firma electrónica (basada en tarjetas inteligentes) a través de un complemento y se discute sobre los parámetros de seguridad de los formatos de firma electrónica. Las tareas como la construcción de un gestor de archivos firmados se proponen como una actividad complementaria.

Con la finalidad de mostrar la aplicación del método propuesto en sistemas en situaciones reales se mostraron tres casos de estudio, cada uno con sus particularidades. El acoplamiento del ComponenteFEA con los sistemas informáticos OpenERP, SAID y SAFET siguen el método descrito en el trabajo, evaluando para todos los casos especialmente el tipo de conexión a utilizar (local o remota), el tipo de almacenamiento y el procedimiento para la conexión en los puntos de firma electrónica y validación.

El análisis de vulnerabilidades es un tema omnipresente en el área de seguridad informática, y está relacionado con este trabajo a través del análisis de los formatos, protocolos y tecnologías utilizados en el proceso de integración.

Existen otros aspectos que no se discuten en este trabajo pero que se consideran importantes para la aprehensión de la tecnología de firma electrónica. Entre ellos se pueden señalar la mejora de la experiencia del usuario y la visualización de los archivos de formato XML firmados electrónicamente.

En el tema específico de integración, en [16] se discute sobre la necesidad de abrir el compás de aplicaciones compatibles con la tecnología de Firma Electrónica Avanzada, y en general, sobre la asunción de un nuevo paradigma en el despliegue de procesos de negocio.

REFERENCIAS

1. Neubauer, T.; Weippl, E.; Biffl, S., "Digital signatures with familiar appearance for e-government documents: authentic PDF," Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on , vol., no., pp.8 pp.,, 20-22 April 2006
2. Campderrich Falgueras, Benet. Ingeniería del Software. Editorial UOC. Barcelona, España. 2003.
3. DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO. Diciembre 1999. Disponible en: http://www.cert.fnmt.es/legsoporte/D_1999_93_CE.pdf
4. Cooper D., Santesson S., y otros. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Request for Comments (RFC) 5280. May 2008. Disponible en: http://www.ietf.org/rfc/rfc5280.txt. Febrero 2013.
5. Cruellas, J. Karlinger G., y otros. XML Advanced Electronic Signatures (XAdES). W3C Note 20 February 2003.
6. Bartel M., Boyer J., y otros. XML Signature Syntax and Processing (Second Edition). W3C Recommendation 10 June 2008. Disponible en: http://www.w3.org/TR/xmldsig-core/. Febrero 2013.
7. Duane. N. Brink, J. PKI: Infraestructura de Clave Pública. McGrawHill 2002.
8. Matjaz Juric, Mathew Benny. Business Process Execution for Web Services BPEL and BPEL4WS. 2 Ed. Packt Publishing. 2006.
9. Bravo, V. Araujo A., SAFET: Sistema para la generación de aplicaciones de firma electrónica. Revista Puente. Vol 6. Número 1. Bucaramanga, Colombia. 2011.

10. PKCS#7.Cryptographic Message Syntax. Disponible en: https://tools.ietf.org/html/rfc2315. Febrero 2013.
11. Security Multiparts for MIME. Multipart/Signed and Multipart/Encrypted. Disponible en: http://tools.ietf.org/html/rfc1847. Febrero 2013.
12. PKCS#12.Personal Information Exchange Syntax Standard. RSA Laboratories. Disponible en: https://www.rsa.com/rsalabs/node.asp?id=2138. Febrero 2013.
13. PAdES. PDF Advance Electronic Signatures. Disponible en: http://www.etsi.org/deliver/etsi_ts/ 102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf. Febrero 2013.
14. Richardson Clay, Avondolio Donald, others. Professional Java, JDK. 5th Edition. Wrox. February. 2005.
15. Formato para firmas electrónicas. Disponible en: http://www.signature.it/-TOOLS/Bdoc-1.0.pdf. Febrero 2013.
16. Andreas Poller, Ulrich Waldmann, Sven Vowe, Sven Turpe, Electronic Identity Cards for User Authentication Promise and Practice, IEEE Security & Privacy, vol. 10, no. 1, pp. 46-54, January/February, 2012
17. Portal del DNI Electrónico Español. Disponible en: http://www.dnielectronico.es/. Febrero 2013.
18. Oficial Gateway to Estonia. Disponible en: http://estonia.eu/about-estonia/economy-a-it/e-estonia.html. Febrero 2013.

Víctor Bravo nació en Maracaibo, Venezuela. Es Ingeniero de Sistemas y tiene una maestría en Computación de la Universidad de los Andes (ULA),Venezuela. Ha trabajado como director en importantes proyectos vinculados a procesos de Certificación Electrónica masiva tal como ”Software de Gestión Autoridad Raíz de la PKI Pública Nacional“. Ha dictado conferencias sobre temas de certificación electrónica en varios países. Actualmente está adscrito como Investigador a la Fundación CENDITEL, y ha sido profesor desde el año 2005 de la cátedra de Matemáticas Discretas del Departamento de Computación de la ULA.

Antonio Araujo es Ingeniero de Sistemas, egresado de la Universidad de Los Andes, en Mérida, Venezuela. Actualmente cursa estudios de Maestría en Computación de la Facultad de Ingeniería de la Universidad de Los Andes. Ha asesorado proyectos de certificación electrónica y participado como ponente en varias jornadas y congresos de certificación electrónica y firmas electrónicas en el país. Se desempeña desde el año 2007 como Analista de la gestión de desarrollado en Tecnologías Libres de la Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres – CENDITEL Nodo Mérida.

Joger Quintero es Técnico Superior en Informática, egresado del Instituto Universitario Tecnológico de Ejido, en Ejido, Venezuela. Se desempeña como Analista Desarrollador en CENDITEL(Nodo Mérida) desde el año 2011.

CAP´TULO 7

ANONIMATO

R. SUMOZA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

test

7.1 Modelo de protocolo para un sistema anónimo basado en estrategias bio-inspiradas

Resumen

In this paper we propose to use some of the tools provided by the Distributed Artificial Intelligence (DAI), in particular Artificial Ant Colony Systems, building anonymous systems that have the virtue of having acceptable levels of Anonymity at a low cost. This cost refers to the performance criteria typically used in the process of routing telecommunications systems, such as response times (latency), the consumption of network resources, among others.

Seguridad en las TIC: Identidad Digital, Primera Edición.
By Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza

7.1.1 Introduction

To preserve privacy on each person's data who participate in interaction network, such as the Internet, we must to use tools that are capable of providing protection against some types of attack. The attacks in this particular study case are intended to get (without authorization) users' "private information", including their own identity. For this type of attack have been proposed several ideas to help establish certain levels of Anonymity, which in most cases have tended to undermine the communications' performance. This still is an open problem: the anonymous systems still need to ensure the Anonymity at low cost (low response times, low resources consumption, usability of the system, etc.), this is to have *efficient Anonymity*. This paper presents a first approach to Distributed Artificial Intelligence to this branch of Information Technologies Security, that is, it intends to delegate the responsibility to achieve efficient Anonymity levels to the Distributed Artificial Intelligence, we propose to use Artificial Ant Colony systems.

7.1.2 Artificial Systems Ant Colony in Anonymity

Considering the ideas proposed for probabilistic Anonymity systems [4][6][5][7], and Artificial Ant Colony Systems' features used in telecommunications networks [8][9][10], this proposal is based on select messages' routes in a probabilistic way, using the probabilities set by mobile adaptive agents (the ants). These routes, having probabilistic components may include, depending the network parameters' configuration, certain controlled levels of Anonymity, in this way, we could have "intelligent control" on generated response times and we could have "intelligent control" on another indexes that they can be incorporated, such as resource consumption (load balancing).

We propose *mimic* real messages to agents, that is, each message has the same structure as the ants, and the only difference between them lies in the message payload, these mimic messages are encrypted with the destination node's public key. To match their sizes, we propose to use a single size for each agent, including the data structure to stores information to update the tables at each node, plus useless filler and the destination's public key encryption. Each message has the same size as the agents, each one is fractionated or filled, and the the message's payload is sent encrypted with the the destination node's public key. Each message is re-assembled at the destination node, using a numbering sequence established in the sending node. To have the messages the same structure that ants, they also contribute to the routing tables update, thus the attackers can't distinguish between the ants and the real messages. In this way, we can compare the messages with the ants having the task of loading the food into the nest, for this reason there are two types of ants in our system, *the scouts and the load* both without apparent differences.

We use an encryption layers strategy, so each node that an ant visits encrypts information related to the previous node with a symmetric encryption technique involves only each previously node key and to reach each destinations, including the final, we can log only the previous node, and not the entire sequence to the origin.

To do the reverse route, the node sends final response to the previous node, and it decrypts the layer that contains the node information before him, and so on until the initial node (the sender).

To optimize the performance criteria typically used in routing systems, while achieving increased levels of Anonymity, we must to set properly the update routing tables' rules. To do this, every time an ant moves from one place to another, update the routing table. To enhance the route's probability, it's selected based in performance criteria.

The following steps show the process:

A. We consider a system of N nodes forming a P2P network (such as Gnutella or other with similar characteristics), along with their servers (bootstrap).

B. Sets the parameters' values used, like uniformity index. In cases where you consider other performance criteria involved in the calculation, are initialized in this step.

C. Each participating node requests the list of other nodes to one or more servers in the P2P network. This list contains their public key.

D. The routes tables are initialized with probability $1/M$. M depends on the number of neighbors each node has.

E. The system is represented by a graph forming the solution space that will be traveled by the ants.

F. The following procedure is repeated on the graph until reach a stable solution:

1. Is placed m scout ants in each node.
2. For each $N - 1$ places from every node in particular, are sent m scout ants that choose the next hop (neighbor node) using the transition probabilities of the routing table.
3. Routing tables are updated.

G. When a node sends a message anonymously, it encrypts that with the recipient's public key and place a data structure similar to the scout ants, ie, creates a *load ant*. Each one carries a message part, which is split in order to match its size with the scout ant. Each fragment of the message contains a sequence number.

H. For each ant's jump, the intermediate node encrypt the previous node's identity with its private key.

I. When a load ant reaches the end node, and all the others load ants have reached, it is possible to complete the original message is decrypted with its private key, and re-assembled it using the corresponding sequence numbers.

J. To send the reply message, the end node uses the return path encrypted in layers.

7.1.3 Conclusion

It is proposed to implement in a distributed P2P System based probabilistic Anonymous Artificial Ant Colony Systems. To do that we can use a set of participating nodes as potential routers of anonymous messages. The routes for sending messages are constructed based on the strategies proposed for telecommunications systems that optimize performance criteria through the use of *Artificial Ant Colony Systems*. Once routes are created, Anonymity is achieved by selecting a probabilistic message routes and through the use of encryption in layers down the route of return or response.

Acknowledgements

This work was supported by the Ministerio de Industria, Turismo y Comercio (MITyC, Spain) through the Project Avanza Competitividad I+D+I TSI-020100-2010-482 and the Ministerio de Ciencia e Innovación (MICINN, Spain) through the Project TEC2010-18894/TCM. Rodolfo Leonardo Sumoza Matos is also supported by the Programme Alβan, the European Union Programme of High Level Scholarships for Latin America, scholarship No. E07D401826VE. We must to thank to José Lisandro Aguilar Castro for his revision, advices and recomendations about the whole content of this paper.

REFERENCIAS

1. Pfitzmann, A., Hansen, M.: Anonymity, Unobservability, and Pseudonymity: A Consolidated Proposal for Terminology. In: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, (2000)
2. Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring Anonymity. In: Designing Privacy Enhancing Technologies (PET'02). Springer LNCS 2482, pp. 54-68, (2002)
3. Serjantov, A., Danezis, G.: Towards an Information Theoretic Metric for Anonymity. In: Proceedings of Privacy Enhancing Technologies Workshop, (2002)
4. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. In: Communications of the ACM, Vol. 4, No. 2, (1981)
5. Díaz, C., Serjantov, A.: Generalising Mixes. In: Proceedings of Privacy Enhancing Technologies workshop (PET 2003), pp. 18-31, (2003)
6. Danezis, G., Dingledine, R., Mathewson, N.: Mixminion: Design of a Type III Anonymous Remailer Protocol. In: Proceedings of the 2003 IEEE Symposium on Security and Privacy, pp. 2-15, (2003)
7. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. In: Proceedings of the 13th USENIX Security Symposium, (2004)
8. Caro, G.D., Dorigo, M.: AntNet: Distributed Stigmergetic Control for Communications Networks. In: Journal of Artificial Intelligence Research, (1998)
9. White, T., Pagurek, B.: Connection Management using Adaptive Mobile Agents. In: Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, pp. 802-809, (1998)

10. Schoonderwoerd, R.: Ant-Based Load Balancing in Telecommunications Networks. In: Adaptive Behavior, Vol. 5, pp. 169-207, (1997)

7.2 Sistema de medición alternativo

Resumen This paper proposes the use of a system of measures for Anonymity based on the characteristics that define their main properties: the index of uniformity of the probability distribution and size of all anonymous. In previous proposals, the most widely used is based on the entropy, an index used in information theory, which has several drawbacks with respect to representation of the properties mentioned in the first place does not represent them explicitly and being a logarithmic index does not represent Anonymity levels or degrees that require linear behavior. To measure the uniformity index is proposed to use the Root Mean Square Error criterion or the Jensen-Shannon divergence. For anonymous set size proposes the use of a function of N. Claves(metrics, Anonymity, Root Squared Mean Error, Jensen-Shannon Divergence).

7.2.1 Introduction

The measures used to quantify levels of Anonymity achieved by the systems, mechanisms and tools in general is still considered an open problem. Several alternatives have been proposed for this purpose, and used more widely accepted so far is based on a type of measurement based on the Information Theory: Entropy, however, does not explicitly consider the fundamental characteristics of Anonymity: anonymous set size and uniformity index of the probability distribution. In this paper, we propose two indices explicitly representing both indicators. On one hand the anonymous set size would be represented by a function of N and uniformity index would be represented using one of these indicators: the Root Mean Square Error (RMSE) or the criteria of Jensen-Shannon divergence (CDJs .)

Pfiztmann et al. [1] established terminology to standardize the terms used in the context of Anonymity, in which it was determined that a subject is anonymous when it can not be differentiated from other subjects belonging to the same set. This set is called the Anonymous Set. In describing the Anonymity in these terms, states that its levels increase as you grow the size of that set and when the probability distribution assigned by the attacker to the members of that group tends to be uniform. The proximity of a probability distribution to any uniform probability distribution is what we call uniformity index of the probability distribution.

The latest proposals and the most widely used so far are those based on a measurement used in the context of Information Theory: Entropy, as defined Shannon [4]. This proposal was discussed in the work Díaz et al. [2] and Serjantov et al. [3], then there have been several streams that use the same basis, such as those proposed by Deng et al. [5], Edman et al. [6] and Gierlichs et al. [7]. However, not explicitly shown in the two aforementioned Anonymity characteristics, in particular the uniformity index.

Section 2 provides a theoretical review of the entropy and specific problems are shown in relation to its use as a measure of Anonymity, in sections 3 and 4 show the basic concepts necessary for the use of the measures proposed in section 5, establishing the uniformity index measurements of the probability distribution.

7.2.2 Related work

There have been several proposals to quantify the degree or level of Anonymity provided by any anonymous system. In [9] define the degree of Anonymity as $1 - p$, where p is the probability assigned to a particular user by the attacker. In [8] define the degree of Anonymity as $A = \log_2(N)$, where N is the number of users of the system. This degree only depends on the number of users of the system, and does not take into account the information the attacker may obtain by observing the system. In [2] and [3] propose to measure the information the attacker gets, taking into account the whole set of users and the probability information the attacker obtains about them, to do that they propose to use Information Theory Entropy to measure the degree of Anonymity (using Shannon's entropy definition [4]). None of them takes explicitly in consideration the anonymous set size and its uniformity index of probability distribution function like separated indexes to be measures, and these are the most important Anonymity's descriptors. Besides, in [2] proposed to use a normalized degree, but this measures could reach its maximal level with $N = 2$ (anonymous set size), contradicting the Anonymity's fundamental characteristics described in [1]: Anonymity level increases by increasing the size of the anonymous set and by increasing the uniformity index of probability distribution function. In [5], [6], [7] use Shannon's entropy with different focus but with the same problems. When they use Entropy, are using the logarithmic function, that mean to have no linear degrees to compare systems. For example, if we have four (4) systems, and the attackers don't have any information about them, that mean the attackers assigned the uniformity distribution function for all of them, and, if the first set has $N = 100$, the second one has $N = 200$, the third one has $N = 400$ and the fourth one has $N = 800$, the Anonymity degrees using Entropy are: 6.6438, 7.6438, 8.6438, 9.6438, respectively. These scenarios with the same probability distribution and different N (twice between each one) must to have twice the Anonymity degree comparing each one with the next one, but it is not happening because entropy's logarithmic function is not linear.

7.2.3 Proposal

We propose to use two indexes to measure Anonymity, each one to establish the levels of Anonymity's characteristics: One to measure the anonymous set size(we can use N or $1/N$, where N is the number of the elements), and one to measure uniformity index of probability distribution function assigned by the attacker. To measure the uniformity index we propose to use two metrics: the MSE - Mean Square Error and/or the JSD - Jennsen-Shannon Divergence.

7.2.3.1 Root Squared Mean Error - RSME

This term is used to estimate variance's error, this error is the residual sum of squares divided by the number of degrees of freedom. In regression analysis, it's an observed quantity given a particular sample, it's sample-dependent. Besides, this term is often referred to as "out-of-sample mean squared error": the mean value of the squared deviations of the predictions from the true values, over an out-of-sample test space, generated by a model estimated over a particular sample space. This also is an observed quantity, and it varies by sample and by out-of-sample test space.

$$RSME = \frac{\sqrt{(\bar{X} - X)^2}}{n(n-1)} \tag{7.1}$$

In our case, we can use $p_i = \frac{1}{N}$ (probabilities in a uniform distribution) to represent $\bar{X}$, and p_i is the probability assigned to the attacker to represent X. This measure permit to establish how far is the attacker's probability distribution from the uniform distribution.

$$RSME_a = \frac{\sqrt{\sum_{i=1}^{N}(\frac{1}{N} - p_i)^2}}{N(N-1)} \tag{7.2}$$

If one system has a $RSME_a \approxeq 1$ that mean it provides bad Anonymity protection. If another system has a $RSME_a \approxeq 0$ that mean it provides good Anonymity protection. But we have to look the set size to definitively take a real perspective of the Anonymity degree.

7.2.3.2 Jennesen-Shannon divergence

The Jensen-Shannon divergence is a popular method of measuring the similarity between two or more probability distributions. It is based on the Kullback-Leibler divergence, with the notable (and useful) difference that it is always a finite value. The square root of the Jensen-Shannon divergence is a metric to measure one Anonymity index: uniformity index of probability distribution function.

$$JSD(P_1, P_2) = H\left(\sum_{i=1}^{2} \pi_i P_i\right) - \sum_{i=1}^{2} \pi_i P_i \tag{7.3}$$

$$JSD_a(P_1, P_2) = \sqrt{JSD(P_1, P_2)} \tag{7.4}$$

where π_i are the weights for the probability distributions P_1, P_2, in this case $\pi_i = 1, \nabla i = \{1, 2\}$, and $H(P)$ is the Shannon entropy for distribution P. In this case, P_1 is a uniform distribution and P_2 is attacker's probability distribution.

With this result we can use both indexes to represent anonymity level o degree.

7.2.3.3 Results

Option 1: Anonymity degree (AD)using MSE to measure uniformity index of probability distribution function and $1/N$ to measure anonymity set size.

$$AD = 1/N \pm MSE_a$$

Option 2: Anonymity degree using JSD to measure uniformity index of probability distribution and $1/N$ to measure anonymity set size.

$$AD = 1/N \pm JSD_a$$

In both cases, the uniformity index and the set size are expressed separately and don't have the linearity problem.

Acknowledgments. This work was supported by the Ministerio de Industria, Turismo y Comercio (MITyC, Spain) through the Project Avanza Competitividad I+D+I TSI-020100-2010-482 and the Ministerio de Ciencia e Innovaci?n (MICINN, Spain) through the Project TEC2010-18894/TCM. Rodolfo Leonardo Sumoza Matos is also supported by the Programme Alβan, the European Union Programme of High Level Scholarships for Latin America, scholarship No. E07D401826VE.

REFERENCIAS

1. Pfitzmann, A., Hansen, M.: Anonymity, Unobservability, and Pseudonymity: A Consolidated Proposal for Terminology. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, (2000)
2. Diaz, C., Seys, S., Claessens J., Preneel, B.: Towards measuring anonymity. In: Proceedings of Privacy Enhancing Technologies Workshop (PET'02) - Springer LNCS 2482. pp. 54-68, (2002)
3. Serjantov, A., Danezis, G.: Towards an Information Theoretic Metric for Anonymity. In: Proceedings of Privacy Enhancing Technologies Workshop (PET'02) - Springer LNCS 2482. (2002)
4. Shannon, C.: The mathematical theory for communicactions. In: Bell Systems Technical Journal. pp. 30:50-64, (1948)
5. Deng, Y., Pang, J., Wu, P.: Measuring Anonymity with Relative Entropy. In: Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST'06), Lecture Notes in Computer Science 4691. pp. 65-79, Springer, (2007)
6. Edman, M., Sivrikaya, F., Yener, B.: A Combinatorial Approach to Measuring Anonymity. In: In Intelligence and Security Informatics. pp. 356-363, (2007)
7. Gierlichs, B., Troncoso, C., Diaz, C., Preneel, B., Verbauwhede, I.: Revisiting A Combinatorial Approach Toward Measuring Anonymity. In: Workshop on Privacy in the Electronic Society (WPES 2008), V. Atluri and M. Winslett (Eds.), pp. 111-116, ACM Press, (2008)
8. Berthold, O., Pfitzmann, A., Standtke, R.: The Disavantages of Free Mix Routes and How to overcome them. In: Hannes Federath (Ed.), Proceedings of Privacy Enhancing Technolo-

gies Workshop (PET'01), Lecture Notes in Computer Science. pp. 30-45, Springer-Verlag, (2001)

9. Reiter, M., Rubin, A.: Crowds: Anonymity for Web Transactions. In: ACM Transactions on Information and System Security. vol. 1, no. 1, (1998)

10. Vernier, D., and Gastineau, J.: What are Mean Squared Error and Root Mean Squared Error?. Article #104. http://www.vernier.com/ (2011)

11. Jianhua, L.: Divergences Measures Based in Shannon Entropy. IEEE Transactions on Information Theory. vol. 37, no. 1 (1991)