Un título para el libro de seguridad

Araujo Antonio, Bravo Víctor, Mora Endira, Sumoza Rodolfo

2014

Índice general

Parte I

Seguridad en las TIC y la Identidad Digital. Fundamentos

Capítulo 1

Bases de la identidad digital

1.1. Conceptos básicos

test

1.2. Implicaciones

test

1.3. Identificación, autenticación

test

1.3.1. Técnicas de identificación y autenticación

test

Contraseñas

test

Certificados electrónicos

test

Firmas electrónicas

test

Dispositivos de usuario

test

Capítulo 2

Políticas de Seguridad

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 La Información

La definición de 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 brindar las características esenciales de la seguridad de la información. La seguridad de la información se define sobre tres conceptos: confidencialidad, integridad y disponibilidad; de esta manera, permitir la adaptación a nuevos paradigmas en seguridad de la información.

Sin embargo, es necesario dar una idea sólida respecto al concepto de *Seguridad* [**?**], en la cual puede mostrarse las siguientes características:

- **Confidenciabilidad**, que consiste en dar acceso a la información sólo a los usuarios autorizados.

- **Control de acceso**, que consiste en controlar el acceso a recursos de usuarios autorizados.

- **Disponibilidad**, que consiste en la posibilidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

- **No repudio**, que consiste en garantizar que una información o mensaje no han sido manipulado.

- **Integridad**, que consiste en garantizar que una información o mensaje no han sido manipulados.

Las políticas de seguridad de la información deben seguir un proceso de reflexión y actualización periódica sujeta a cambios relevantes en la institución, tales como: 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.

Las políticas de seguridad de la información no se deben convertir en una herramienta de restricciones ni de carga para los usuarios. Hay que tener en cuenta, desde el punto de vista de la seguridad informática, 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. 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 sensibles 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, 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, requisitos, limitaciones y nivel de confianza que existe en ella, de manera de concretar las ideas en documentos que orienten las acciones de la institución.

2.4. Importancia de la Seguridad de la Información

Las instituciones deben entender que la seguridad informática es un proceso que puede desarrollarse en ciclos iterativos, y no es un producto listo para ser usado. 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, 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 del sistema.
- Limitar las pérdidas y recuperar los 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:

- tanto a nivel físico como lógico.
- Selección, instalación, configuración y actualización de las soluciones de hardware y software.
- Criptografía.
- Desarrollo seguro de aplicaciones.

Humano:

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

Institucional:

- Definición e implementación de políticas y normas de procedimientos de seguridad de la información.
- Definición y aplicación de planes de contingencias en casos de desastres en contexto de los activos de información.
- Cultivo de buenas practicas de actuación ante la seguridad de la información.

2.5. Seguridad de la Información para Software Libre

En el ámbito de las tecnologías libres y específicamente en el software libre, la noción de seguridad es objeto de controversias. Entusiastas del software libre promueven las potencialidades de éste tipo de software en contraste con el software propietario. Asimismo, los partidarios del software propietario y las grandes corporaciones que están detrás de los desarrollos de este tipo, promueven sus aplicaciones y herramientas llegando, en algunos casos, hasta el desprestigio voluntario del software libre.

Las potencialidades intrínsecas del software libre permiten incorporar elementos de seguridad en sistemas informáticos de instituciones, organizaciones y hasta de 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. El apoyo de comunidades de usuarios y desarrolladores alrededor de las aplicaciones y herramientas
4. La frecuente corrección de errores y publicación de software comparada con otros modelos de desarrollo
5. El rompimiento del paradigma de la seguridad por obscuridad
6. Entre otras

La seguridad de la información en software libre no sólo incluye conocer y revisar cómo funcionan las aplicaciones de software; más allá de eso, se sigue un modelo de desarrollo de software con potencialidades para el surgimiento de valores como la 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.

La adopción de software libre como alternativa para la seguridad informática en organizaciones trasciende a un cambio de pensamiento; cambiar el modelo imperante basado en compras de soluciones, por un modelo que incorpore tecnologías abiertas en búsqueda de la soberanía e independencia tecnológica.

2.6. Principio de Defensa en profundidad

Esto es un concepto viejo, 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. 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 2.1 establece una sola línea de seguridad al rededor de las activos, que cubra la mayor área posible como por ejemplo: cortafuego, contraseñas, etc. Los problemas que presenta este enfoque, es que la línea de seguridad es susceptible a tener vulnerabilidades por diferentes razones como por ejemplo: una mala configuración de sistema de protección, fallas del sistemas, etc, una vez que es superada esta linea de seguridad, no hay forma de detener el ataque.

Mientras que el enfoque de defensa en profundidad (ver figura 2) establece múltiples lineas 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, en una de las lineas de seguridad, debería debilitar el

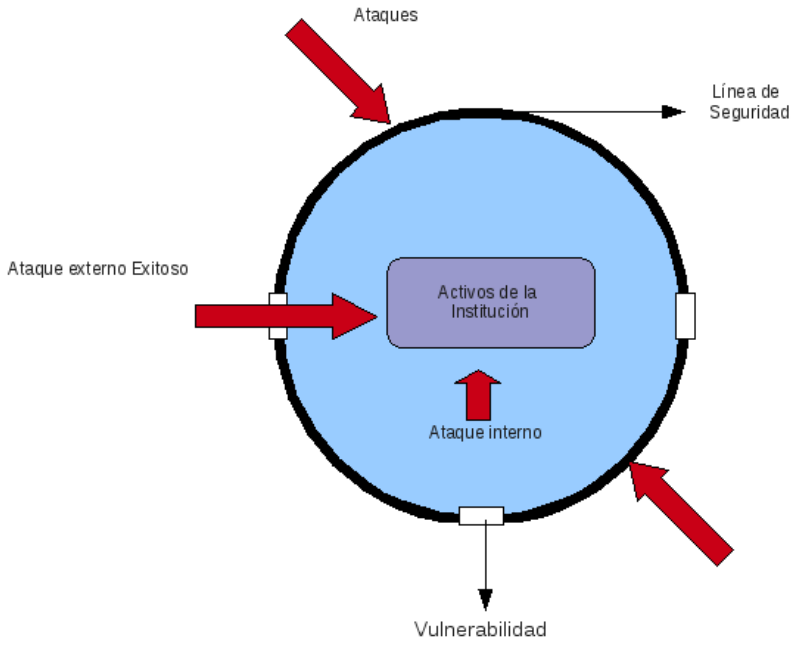

Figura 2.1: *Enfoque tradiconal de Seguridad.*

ataque, por que existe la posibilidad de que el ataque pueda ser detectado, recogiendo la mayor información sobre su origen, naturaleza, anomalías, trazas, y con esto se pueda reforzar las otras linea de seguridad, que puedan detener el ataque o que el mismo no genere perdidas mayores a la institución, ademas permite, corregir la(s) vulnerabilidad(es) de las lineas de seguridad que fueron traspasado.

Este enfoque permite cubrir todos los puntos de riesgos de un sistemas y dependiendo de la estructuración de las líneas de seguridad, lo protege de los ataques interno.

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

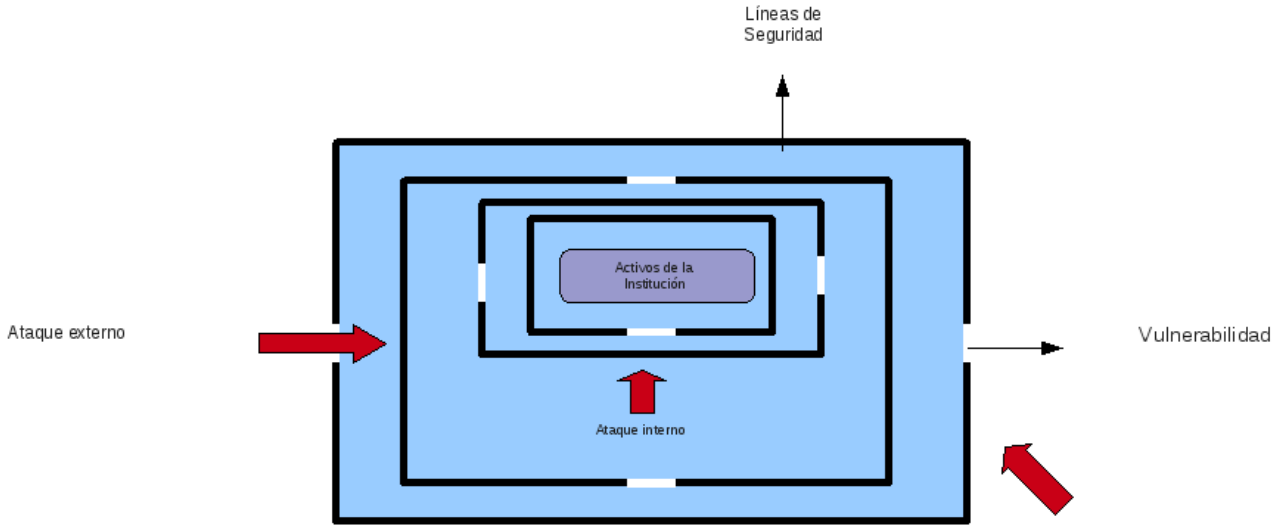

Figura 2.2: *Enfoque de defensa en profundidad.*

2.6.1. Los principios generales de la defensa en profundidad

- Debe ser global, lo que significa que se engloba todas las dimensiones del sistema de información como los aspectos organizacionales, técnicos, y de implementación.
- Deben estar coordinadas, lo que significa que los medios implementados actúen gracias a una capacidad de alerta y difusión, tras una correlación de los incidentes.
- Deben ser dinámicas, lo que significa que dispone de políticas de seguridad que identifica: capacidad de reacción y planificación de acción, ante incidentes.
- Debe ser suficientes, lo que significa que 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 lineas de seguridad.

2.7. Responsabilidad

Antes de que se aplique las políticas de seguridad en una institución, deben ser aprobadas, publicadas, documentadas, y comunicadas a todos sus miembros. Estos son los respons-

ables de la aplicación y cumplimiento de las políticas de seguridad dentro de cada una de sus áreas.

Todas los roles y responsabilidades de la seguridad de la información debiera estar claramente definidas, y documentada y 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 las mayoría responsabilidades de la seguridad de la información y el manejo de las actividades criticas de la institución (Cuenta de usuario crítica, ver sección 14.1) sobre caiga en un grupo pequeño de persona, esto generaría una debilidad en la seguridad de la información, Ya que por ejemplo: se podría ver afectada el normal funcionamiento de la institución si este grupo pequeño de persona por alguna razón (viajes laboral, enfermeda, vacaciones, etc) no puedan asistir a la institución

2.8. Procesos para aumentar la percepción 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.

2.8.1. Identificación de los riesgos

Es una medida que busca rastrear vulnerabilidades en los activos que puedan ser explotados por amenazas. Es necesario la identificación de los riegos que puedan existir en la institución, para la misma es importante considerar los distintos ámbitos para 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 las configuración de los componentes de toda la infraestructura tecnológicos de respaldo, comunicación,

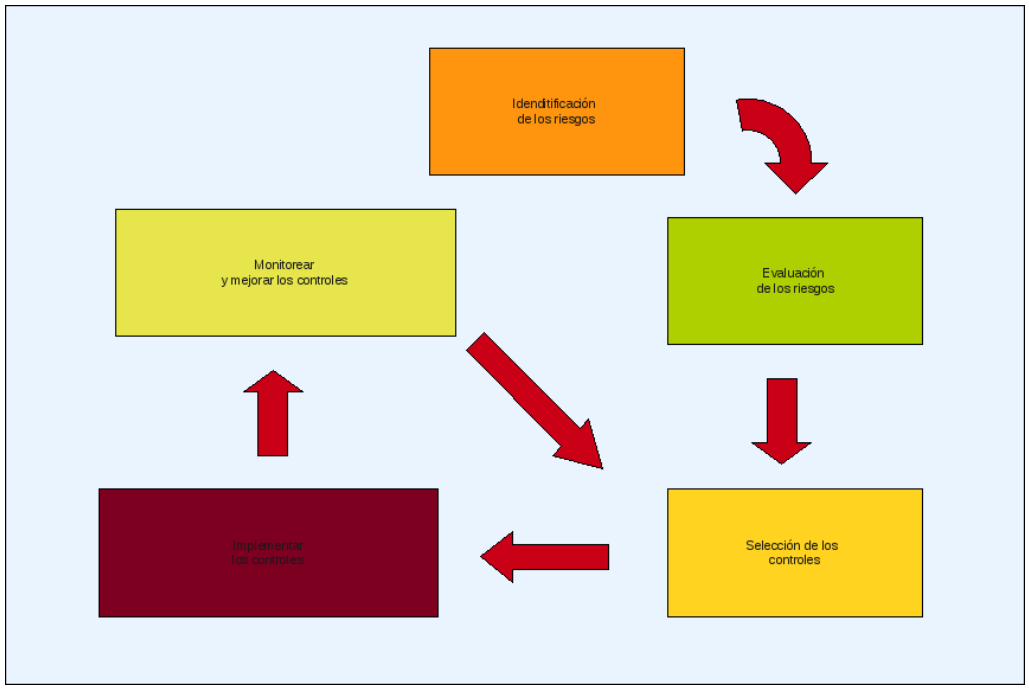

Figura 2.3: *Proceso de percepción de la Seguridad.*

procesamiento, tránsito y almacenamiento de la información. Los activos en este ámbito son de tipo 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 permitirá:

- Tener un registro actualizado de los activos de la institución.
- Facilitar el posterior 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 intento 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 relaciona 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 análisis pretende inicialmente identificar vulnerabilidades en los activos de tipo usuario y 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:** El análisis físico de seguridad de la información 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 encuentra los equipos computacionales de la institución.
- Investigar sobre los servicios requeridos como linea telefónica, antenas de comunicación, instalaciones eléctricas.
- 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 riesgo de la institución de acuerdos a los objetivos relevantes de la institución. La evaluación de los riesgos tiene como resultado un grupo de 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 bien claro y definido el alcance que va a tener para que la misma sea efectiva.

La evaluación de los riesgos se conforma por saber:

- La amenaza que representa el riesgo al normal funcionamiento de la institución.
- El impacto que tendría el riesgo en la institución si llegara a ocurrir,
- La posible frecuencia que podría ocurrir el riesgos.

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 tenga cambios significativos; nuevos requerimiento 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 riegos deben ser aceptados por toda la institución de manera objetiva y con conocimiento. De ser necesario hay que trasferir 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 funcione 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 la evaluaciones de la seguridad de los sistemas informáticos se realizan las pruebas de penetración internas y externas, que representa una valiosa herramienta metodológica. 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 tratamientos 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 existente para cada uno de los riesgos identificados de cada ámbito, por ejemplo, en el ámbito técnico se hace una investigación de la tecnología libres existentes 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, etr), 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 proporciona un punto de partida adecuada 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; como por ejemplos: charlas y/o cursos en materia de seguridad.
- Asignar las responsabilidades de seguridad a miembros de la institución, en concordancia con las políticas de seguridad.
- Identificar los procedimientos de seguridad asociados a cada activos de la institución.
- Definir y documentar los niveles de autorización.
- Registrar las incidencias y mejoras de seguridad.

- Desarrollar e Implementar procedimiento de gestión de continuidad de actividades para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de seguridad.

- Salvaguarda los registros de la organización. Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y/o falsificación.

- Sencibilización 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 técnicos de seguridad se implemente en un ambiente de pruebas antes de colocarlos en el ambiente de producción para no producir inconveniente 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 depende de la legislación aplicable en la institucion, como por ejemplo lo seria: la protección de datos y privacidad de la información personal.

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

- El correcto uso de los medios de procesamientos de la información.

- Actualización de nuevos controles y políticas de seguridad

- El conocimientos de las vulnerabilidades existente

Permitiendo aumentar la conciencia y conocimiento a los miembros de la institución con le 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 beberían ser revisado en periodos planificados o cuando ocurran cambios significativos que puedan afectar la eficiencia y efectividad de los controles.

Se recomienda la realización de pruebas y auditorias periódicas de seguridad 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:

- Pruebas de análisis de posibles vulnerabilidades del sistema informático, para localizar de forma automáticas 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.

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 funcione 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 la evaluaciones de la seguridad de los sistemas informáticos se realizan las pruebas de penetración internas y externas, que representa una valiosa herramienta metodológica.

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

2.9. 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 trabajos 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 de recuperación de datos en caso de fallas.
- Coordinación de la implementación de controles de seguridad.
- Promoción y difusión de herramientas y buenas practicas 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 la contraseñas en secreto o tener una contraseña lo suficientemente robusta es uno de los problemas que se presenta, es el mecanismo mas utilizado para la autenticación en los sistemas y que representa uno de los puntos mas débiles en la seguridad de

la información, ya que un atacante que obtenga la contraseña, ya sea por ejemplo: robo, espionaje, ingeniería social, engaño, extorsión, fuerza bruta, puede acceder a los sistemas y provocar daños o alteraciones a los sistemas e 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 seria imposible de adivinar pero también seria imposible de recordar para muchos usuarios.

Existes algunas recomendaciones para la gestión de las claves, entre las que tenemos:

(a). No solo se conforme con letras o números, sino que se de la combinación de ambas y que a demás incluyas mayúsculas, minúsculas y caracteres especiales

(b). No sean claves que puedan estar relacionado 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.

¿ Como se puede generar un clave que sea fácil de recordar, que cumpla las normas descritas en el sección anterior, que no pueda ser adivinada por cualquier infractor, y que ademas, no genere una carga para el usuario (en su generación, resguardo, utilización)?, es difícil, se han desarrollados sistemas que permite la generación y resguardo, algunos no cumple con todas las recomendaciones descritas en la sección anterior (no quiere decir que no sean seguras) pero presentan otros inconvenientes como por ejemplo: la portabilidad de las claves para ser usada desde otra máquina, ahora existe otros inconvenientes y tiene que ver con la responsabilidad de las personas para generar y resguardar las claves, que depende de las costumbres, el contexto social, uso consciente, tipo de información que resguarda y el nivel de riesgo que implica el que personas no autorizada conozca tu clave y acceda a la información.

2.10.1. Claves con menos de ocho dígitos

Existen 96 caracteres posibles de utilizar en una clave (letras minúsculas y mayúscula, números, símbolos), en una clave con 8 dígitos existe 96^8 (7.213.895.789.838.336) posibilidades para adivinar la clave y analizando 1.000.000 palabras por segundo tardaría 228 años.

No se dispone de esa cantidad de años para analizarlos por fuerza bruta, existen métodos que reduce el tiempo de análisis de las contraseñas, como por ejemplo: Probar primero con contraseñas posibles de adivinar utilizando palabras de diccionario, palabras que tenga relación con el usuario, ya que la mayoría de las contraseñas de los usuarios tienen o se conforman de esta manera.

Existe técnicas básicas para la selección de contraseñas como educar al usuario; Se les puede explicar la importancia de usar contraseñas difíciles de adivinar, sensibilizarlo en las posibles implicaciones de una mala gestión de la contraseñas, proporcionarles recomendaciones para la selección de las contraseña fuertes como por ejemplo:

Seleccione una oración que no se le vaya a olvidar y a partir de ella generar la contraseña, ejemplo:

- Oración 1, *Mi hermana Sofia me regalo 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 pueden notar, de esta manera se generaría una buena contraseñas, que es difícil de adivinar por un tercero, y fácil de recordar para la persona ya que son generadas de oraciones particulares que se puede recordar

2.11. ¿Qué se entiende por puesto de trabajo?

Se entiende por puesto de trabajo, al lugar físico y/o lógico donde al usuario se le asigna 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 computacional y de redes de comunicaciones, el cual tiene el objetivo de prestar la mayoría de los servicios informáticos 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 solo a personas autorizadas a los activos lógicos de la institución

2.14. ¿Qué es seguridad física?

Se refiere a los mecanismo de seguridad que generan barreras físicas y procedimientos de control sobre y alrededor de los equipos computacionales como medida de prevención y protección de los activos informáticos de la institución, al acceso no autorizado a los equipos y medio de almacenamiento de datos o de 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

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"), aplicaciones como cortafuego, administrativas, entre otros.

2.16. Vulnerabilidades de los sistemas de información

Se refiere a la debilidad que tiene los sistemas informáticos, que pueden ser afectados, violando 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 tenemos:

- Debilidad en el diseño de los protocolos utilizados en las redes, como por ejemplo los protocolos de intercambio de información en texto claro, algunos protocolos de Internet no contemplaron la seguridad en su diseño inicial.
- Fallos en los diseños y/o codificación de los programas. En algunos ocasiones los parches y actualizaciones de seguridad suministradas por los desarrolladores, no arreglan los problemas, o incluso pueden incluir nuevas vulnerabilidades.
- Configuración inadecuada de los sistemas informáticos ya sea por: la poco documentación que exista de sistema, por lo poco seguro del sistema o dispositivo.
- Políticas de seguridad deficientes o inexistente, en muchas instituciones no han definido e implementado de forma eficaz unas adecuadas políticas de seguridad de acuerdo a sus necesidades.
- 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

- Disponibilidad de herramientas, de fácil instalación , utilización, con detallada documentación que te permite encontrar agujeros de seguridad, ataques contra redes y sistemas informáticos.
- Existencia de puertas traseras (backdoors) en los sistemas informáticos que representa una vía de acceso no autorizada.
- La no correcta instalación, configuración y mantenimiento de los equipos
- El no contemplar la seguridad frente a las amenazas del interior de la institución

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

Dentro de la evaluación de la seguridad, que representa una valiosa herramienta metodología, son las pruebas de penetración que constan de las siguientes etapas:

Reconocimiento del sistema, para conocer que tipo de información se podría obtener un atacante o un usuario malicioso.

- Detección y verificación de vulnerabilidades de los sistemas de la institución.
- Intentos de penetración en la vulnerabilidades detectadas
- Generación de informes, con el análisis de los resultados.
- Aplicación de mecanismos o medidas de seguridad de ser necesario (en caso de que la seguridad a sido comprometida).

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 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 de la institución de una red que no es confiable como Internet.

Hay cortafuego que esta constituido por hardware (Figura 2.4) maquina diseñadas, construidas y especializadas para esta función, en su configuración inicial ya viene con una serie de reglas de filtrado determinado, se instala por lo general, entre la red privada (Zona fiable) e Internet, puede ser un producto independiente o puede venir junto a los routers.

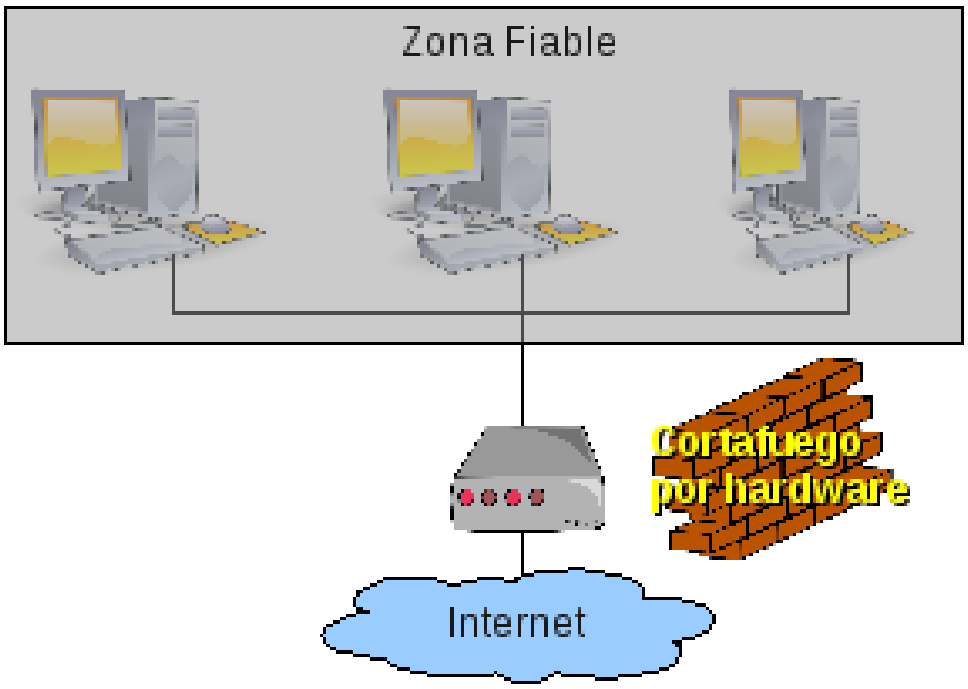

Figura 2.4: *Corta fuego por Hardware.*

Hay cortafuego de software (Figura 2.5) que por lo general son instalado en un computador que ofrecen red a la institución. Entre las diferencia que se tiene del cortafuego por hardware y el cortafuego por software, es que en el cortafuego de software, hay que definir y probar la mayoría de las reglas, ocupa espacio y procesamiento en el servidor donde esta instalado, son muchas mas barato, por lo general son utilizados en instituciones pequeñas.

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

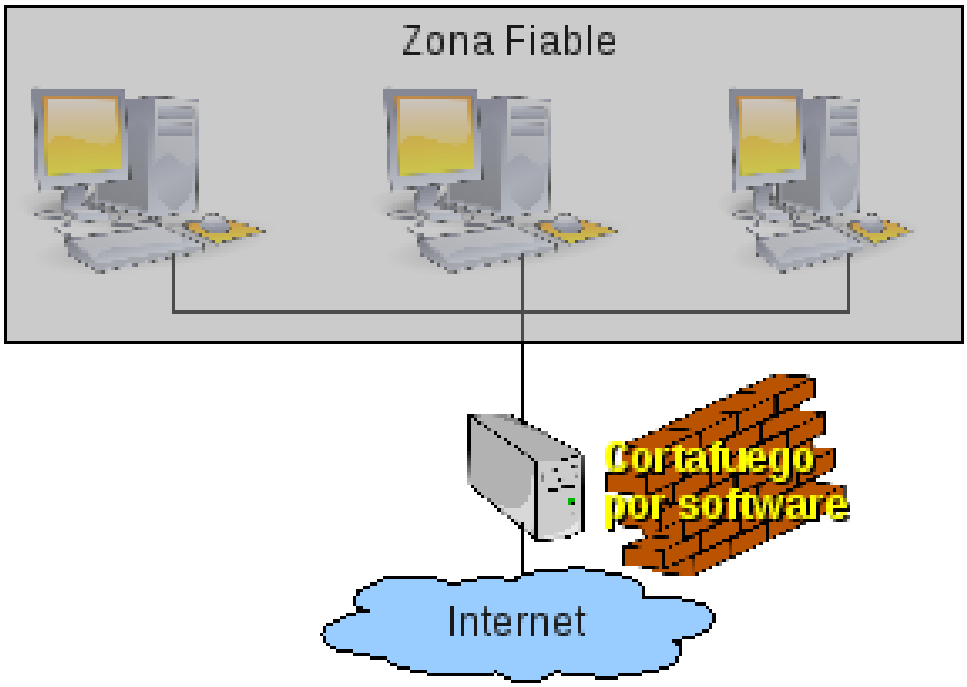

Figura 2.5: *Cortafuego por Software.*

También se puede instalar en un computador dentro de la red interna − *cortafuego personal* −, Figuras 2.6, 2.7) un cortafuego, que solo controlaría el trafico que entra y sale de esa computadora, de esta manera se puede agregar reglas de filtrados a esa computadora, de acuerdo a la necesidad del usuario, como por ejemplo: brindar protección adicional, (que no estén definidas o prohibidas en el cortafuego de la red) por tipo de información que se maneja.

Los cortafuego personales, es el termino utilizados para los casos donde el área protegida se limita solo al computador donde esta instalado el cortafuego.

2.17.2. ¿Para que sirve el cortafuego?

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

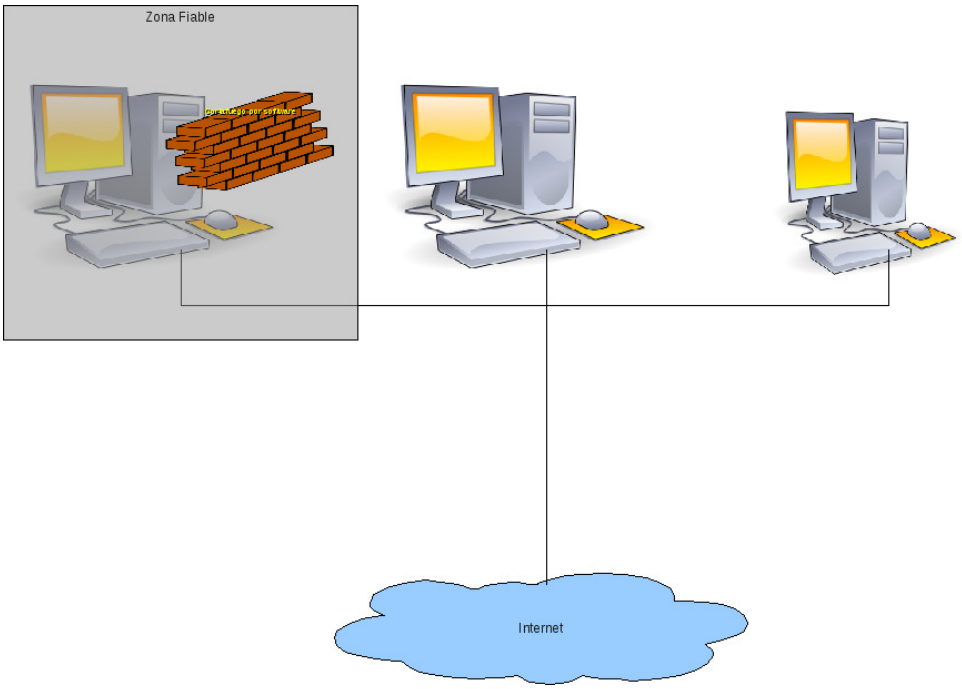

Figura 2.6: *Cortafuego personal.*

- Restringir el acceso a: determinados programas, segmento de red de la institución, servicios de Internet, ciertas paginas web, intruso, bloqueando el tráfico no autorizado por la organización y no permitir ataques a nuestras computadoras desde el exterior e interior de la red.

- Ocultación de los equipos internos de la institución, de forma que estos no puedan ser detectado antes 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.

- Auditoria y registro de uso, ya que puede recopilar información sobre el uso de la red

- Mejor aprovechamiento del ancho de banda utilizado en la institución

- Monitorización de los ataques o intentos de intrusión a la red de la institución.

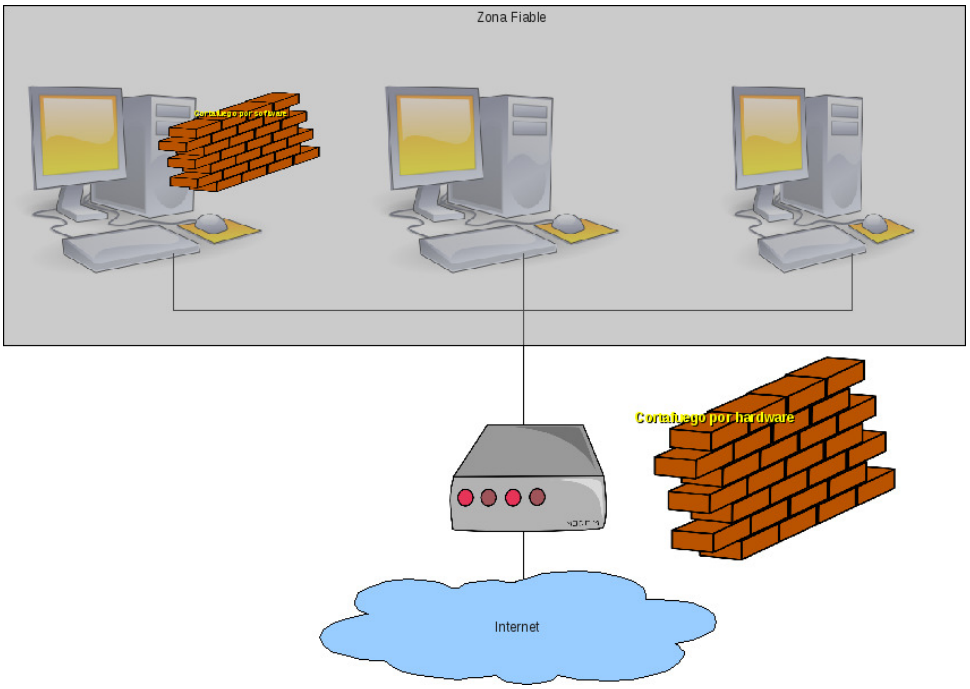

Figura 2.7: *Cortafuego personal combinado.*

2.17.3. Consideraciones para la instalación y configuración de un cortafuego

Dentro de las políticas de seguridad de la información se deben considerar el uso de cortafuego, donde se especifique a parte de la configuración, la persona responsable de la administración. Consideraciones para la Configuración de un cortafuego:

Conocer en profundidad los protocolos y servicios de Internet

- En el caso que utilice un cortafuego de software, el equipo debe encontrarse libres de virus, de programas espías (spyware), programas maligno (malware), para que no afecte o altere el funcionamiento del cortafuego.
- 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.

- Contar con los últimos parches y actualizaciones de seguridad del cortafuego.

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 encarga de detectar y reaccionar de forma automática antes los incidentes de seguridad que tiene lugar en las redes y computadoras, que de acuerdos a unos patrones (patrones de comportamiento de actividades sospechosas) establecidos por defecto (hay algunos programas viene con ellos) y los definidos por el administrador del sistema (de acuerdo a las políticas de seguridad), detectan y permite prevenir la intrusión. Un incidente de seguridad podría ser una intrusión, que se define como un intento de comprometer la confidencialidad, la integridad, la disponibilidad de los mecanismos de seguridad de un ordenador o red, que valiéndose de la existencia de vulnerabilidades accede a los sistemas sin autorización.

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.

El funcionamiento básico de los IDS tenemos:

- Una fuente de eventos del sistema.
- Una base de datos con los patrones de comportamiento que se considera como normal, así como los perfiles de posibles ataque.
- Motor de análisis de los eventos quien es el que detecta las evidencias de intento de intrusión.
- Módulo de respuesta, que de acuerdo al análisis de los eventos, realiza determinada acción

Los IDS pueden presentar problemas y limitaciones, como por ejemplo, podría generar falsas alarmas, ya sean estas falsos negativos, que se produce cuando el IDS no puede detectar algunas actividades relacionadas con incidentes de seguridad que esta ocurriendo en la red o en los equipos informáticos, o bien falsos positivos, que se presenta cuando IDS registra y genera alertas sobre determinada actividad que no resultan problemáticas, ya que se consideran con el funcionamiento normal del sistema o red.

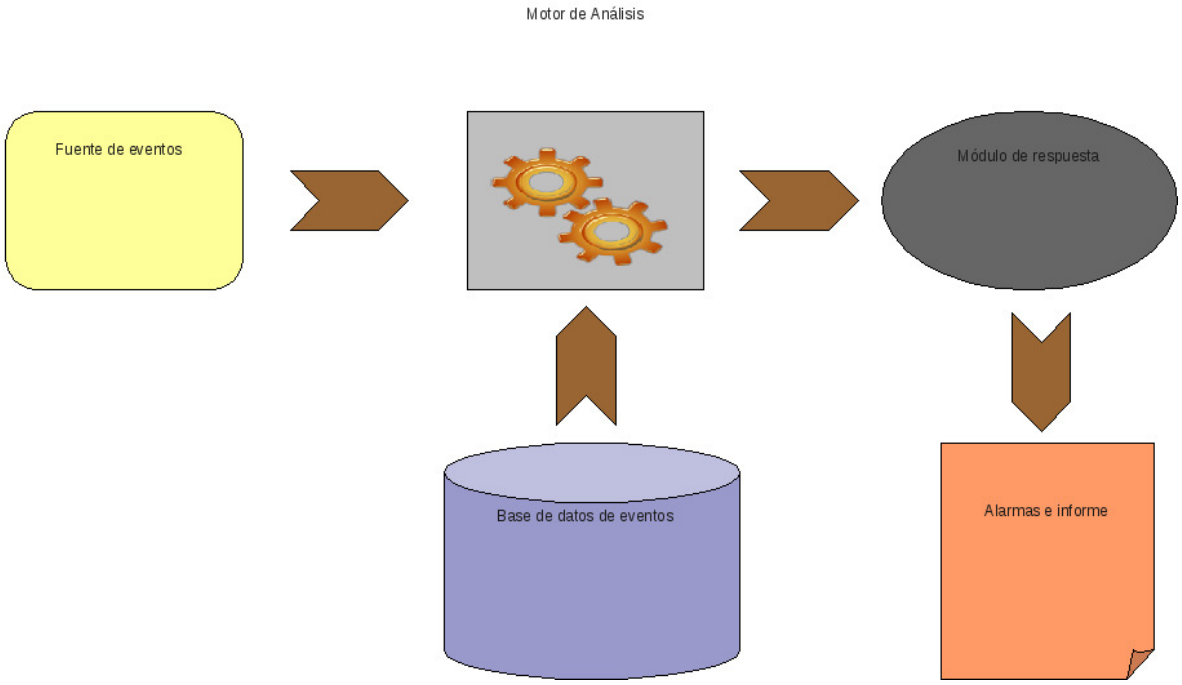

Figura 2.8: *Estructura funcional básica del IDS.*

2.18. Identificación de los riesgos a terceros

Cuando exista la necesidad de otorgar acceso a terceras personas (entre los que se podría identificar como visitantes, becarios, pasantes, mantenimiento, etc.), ésta puede representar una vulnerabilidad; ya que se pueden presentarse posibles ataques a la seguridad de la información y los servicios que la institución maneje (internos y externos).

Se debe llevar acabo una evaluación de los riesgos que representan en acceso a terceros 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, a qué recursos y servicios); de acuerdo a las actividades que va a realizar en institución, va a requerir del uso de activos lógicos de la institución, y/o acceso a determinadas áreas, que pueden ser vitales a la institución, como por ejemplo: acceso al centro de datos, y de acuerdo a esto, tener la certeza de permitir o no, el acceso a tercero, para la misma se debe:

- Los medios de procesamientos de información a las cuales necesita tener acceso (equipos muy especializados, delicados, sensibles, costosos).
- Evaluar el valor de la información a la que accede, medido en diferentes aspectos (Económicos, sociales, morales, entre otra).
- Las costumbres de la institución y de la 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.
- Configuración de recursos informáticos requeridos.
- La carga de procesos en la realización de la actividades para el cumplimientos de las políticas de seguridad.
- 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.
- Responsabilidades de la institución por actos de las personas que utilicen recursos de la institución como correo institucional, enviar spam, información confidencial de la institución a terceros sin autorización, ataques o intento de intrusión contra equipos utilizando la red de la institución.

Las consideraciones anteriores, deben ser tomadas en cuenta en la políticas de seguridad de la institución y los mas importante en las formas culturales de ella.

2.19. Seguridad lógica en los puestos de trabajo

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

- Determinar y clasificar el grado de sensibilidad y criticidad de la información que maneja en las memorias persistentes ubicadas en los puestos de trabajo.
- La contraseña de administración de los equipos de computación (que en algunos sistemas se denomina “root”), solo debe ser conocida por la persona responsable del puesto de trabajo; debe ser seleccionada de manera robusta.
- Se debe realizar cambio de la contraseñas cuando se tenga en menor indicio de vulnerabilidad o que personas no autorizadas tenga el acceso o conocimiento de la misma
- No utilizar la misma claves 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 los paquetes actualizados en relación a los parches de seguridad en los sistemas ubicados en los puestos de trabajo.
- Utilizar herramientas y procedimiento que verifique la integridad y fuente de los paquetes a instalar (mecanismos de verificación de integridad y autoría).
- Utilizar el correo institucional con métodos criptográficos, previa clasificación de la información, para proteger la confidencialidad e integridad de los mensajes.
- Considerar políticas referentes al bloqueo automáticamente de todas las sesiones de trabajo cuando no se encuentre el responsable del puesto de trabajo.
- De acuerdo a la sensibiliad de la información y a configuracion de la red, se puede utilizar instalar y configurar cortafuegos de software persona para incrementar la seguridad en el puesto de trabajo

2.20. Seguridad lógica en el centro de dato

- Investigar los diferentes protocolos de comunicación, y seleccionarlo en función a las necesidades de la institución.
- Segmentación de 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 autorizados a los activos de la institución
- Respaldar la información de los servidores de forma periódica, haciendo un compromiso entre los recursos de la institución, el valor de la información y tasa de cambio de la información
- Cerrar todas las sesiones de red después de ser utilizadas, para mayor seguridad de la información.
- Controlar el acceso remoto a los equipos de la red institucional a través de herramientas seguras.
- Utilizar sistema de control de cambio que tiene como objetivo verificar las modificaciones realizadas en los equipos de computación como configuración, modificación, etc.
- Realizar buenas prácticas de seguridad en el uso y selección de las contraseñas.
- Utilizar contraseña a nivel de BIOS para proteger el acceso a este elemento que registra la configuración básica de los equipos.
- Utilizar contraseña para el encendido de los equipos.
- Configurar los servidores de manera robusta como por ejemplo:
  - Desactivación de servicios y cuentas que no vayan a ser utilizadas
  - Instalación de los últimos parches de seguridad y actualizaciones (updates) publicados por el fabricante, pero convendría comprobar su correcto funcionamiento en otra maquina de pruebas antes de la máquina de producción
  - Enlazar sólo los protocolos y servicios necesarios a la tarjeta de red
  - Activar los registro de actividades de los servidores (logs)
  - Disponer de una copia de seguridad completa del sistema operativo de cada servidor tras una configuración correcta y robusta.
  - Instalar herramientas que permita comprobar la integridad de los ficheros 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 proponen:

- De acuerdo a la información que se maneje y la confianza existente, se determinará la ubicación y seguridad física de los puestos de trabajo:
  - Por ejemplo, para la información que es confidencial y con un limitado acceso de personas no autorizadas, se recomienda que los puestos de trabajo deben estar ubicados en locales cerrados, utilizando con perimetro de seguridad (barreras tales como: paredes, rejas de entrada controladas por tarjetas o recepcionista), ventilados, con medidas de control de acceso, siempre tomando en cuenta la ergonomía, para prevenir el acceso no autorizado
- Los equipos deben contar con fuentes o suministro de poder (UPS), para regular la corriente y proporcionar energía eléctrica continua, ya que un pico de tensión alta puede ocasionar que se queme algún componente eléctrico de la computadora, o los pequeños y repetidos picos de voltajes le acorte la vida útil de los componentes de la computadoras.
- Los equipos debe estar ubicados en ambiente de trabajo adecuados (temperatura, humedad, polvo, según las características de las computadoras).
- Las ubicación de las equipos (cpu, ups) y el cableado no puedan ser golpeados, los cables no puedan ser pisados y pinchados o que se le coloque otros objetos encimas o contra ellos.
- Mientras se este trabajando en el puesto de trabajo, se debe tener cuidado al consumir alimentos y/o ingerir líquidos.
- Contar con planes de mantenimientos de los equipos de los puestos de trabajos, según o 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 detectar a tiempos posibles fallas

2.22. Seguridad física en el centro de dato

Para establecer la seguridad física se debe tener en consideración varios aspectos (físico, lógico y ambiental) que permitirá una configuración apropiada y segura para el centro de dato. Esta área es delicada y por lo general se encuentra un alto porcentaje de los activos de la institución, en él concentra y procesa todos los recursos lógicos con que opera la institución. Para configurar un buen centro de datos debemos considerar:

2.22.1. Servicios que presta o prestara el centro de datos:

requerido para conocer las necesidades en infraestructura física (equipos computacionales, espacio físico, etc)

- Tipos de servicios a prestar tanto a los usuarios internos como externos.
- Cantidad de usuarios que requiere ingresar y permanecer en el centro de dato, como los usuarios que se beneficiara de los servicios prestados por el centro de dato
- Escala de crecimientos que se tiene al futuro (incluir nuevos servicios internos, externos que requiera la instalación de nuevos equipos computaciones en el centro de dato)
- Características y especificaciones técnica de los equipos

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

2.22.2. Ubicación y condición física del centro de dato

La selección del lugar de ubicación de un centro de procesamiento 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 debe considerar que:

- Se encuentre alejado de instalaciones eléctricas como Radares, microondas, entre otros para que no influya las señales o rayos de estas estaciones, en el funcionamiento de los equipos de computación del centro de dato

- Lejos de estaciones de materiales volátiles, gasolinera, por que representa un latente peligro para incidentes intencionado o fortuitos,
- En lugares no desolados o desprotegidos por se puede convertir en una blanco fácil para incidentes intencionados

Entre los factores inherentes a la localidad hay que considerar

- Si el terreno donde se encuentra ubicado presenta problemas de hundimiento
- si existen condiciones climatológica adversa (áreas de constantes lluvias y descargas eléctricas, altas temperaturas, etc) para el correcto funcionamiento de los equipos de computación del centro de dato
- Ubicada en área con constantes actividades de sismo, ya que el local del centro de datos pueda presentar destrucción parcial o total
- En áreas de inundaciones que afecte al local del centro de dato

Ademas se debe contar con todos los servicios que requiere el centro de datos para su funcionamiento de comunicación y de procesamiento de datos y que debe ser proporciona el lugar donde esta ubicado

- Línea telefónica
- Instalaciones eléctricas
- Antenas de comunicación

2.22.3. Especificaciones técnicas del centro de dato

Se refiere a las disposiciones del local del centro de dato que se debe considerar, entre las que tenemos:

- Espacio amplio disponible por la institución con todos los servicios que requiere el centro de dato
- El acceso de los equipos de computación y del personal al centro de datos, debe ser lo mas cómodo y seguro posible, para evitar que se presente incidente, como por ejemplo: en los traslados de los equipos de computación

- Buen diseño de las Instalaciones de suministro eléctrico, que garantice el suministre y la disponibilidad de la energía eléctrica estable, y ademas sea independiente del resto de la instalaciones del edificio del la institución.
- Se debe contar con un acondicionamiento térmico del local que controles la humedad, temperatura requerida por los equipos computacionales del centro de datos
- Áreas adyacentes para el almacenamiento
- Instalación de pisos falso, evita que las descargas eléctricas afecten a los equipos por su característica conductiva, y representa una optima razón para la distribución de cableado, canaletas, aire acondicionado del centro de datos
- 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
- Sellado hermético 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, por ejemplo: la contaminación del ambiente que afecte a los operadores del centro de dato, o produzca corto circuitos en los equipos, etc
- contar con sistemas de aterramiento, que permite la absorber descargas eléctricas, que minimiza la diferencia de potencial entre los equipos metálicos y las personas
- Para las paredes y techos del centro de dato se recomienda usar pintura plásticas lavable para poderlos limpiarlos fácilmente y evitar las erosión, la altura del techo este entre los 2,70 y 3,30 mts para permitir la movilidad del aire dentro del centro de dato
- 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, ubicados de forma separada en función al tipo de cables (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 o fase de la instalaciones electricas del centro de dato.
- 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 y tener disponibles los servicios, procesamientos de datos, etc, 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 dato

- Fuentes o suministro de poder (UPS) para proteger a los equipos electrónicos por fluctuaciones de poder.

2.22.4. Control de acceso físico

Los sistema de control de acceso debe ser un sistemas flexible y confiable para el control, monitoreo de accesos, registro de datos de los usuarios, verificación de los datos para permitir el acceso solo al personal autorizado a las instalaciones o áreas restringidas de la institución, los sistema de control de acceso, involucra personal de seguridad, políticas de seguridad, hardware y software.

- Identificación del personal que entra y sale del centro de datos bajo estricto control

- Asegurar que durante la noche, el fin de semana, los descansos o cambios de turnos sean tan estricto como durante el día.

- Se debe identificar, controlar y vigilar las actividades que realizan las terceras persona durante su estadía en el centro de datos, entre las personas que se considera como terceras personas están, los visitantes, personal de limpieza, personal de mantenimiento de los diferentes equipos.

- Instalación de Torniquetes.

- Cerraduras electromagnéticas.

- Circuitos cerrados de televisión

- Detectores de movimiento.

- Tarjetas de identificación.

- Control de aperturas de puertas

- 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 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 requiere
- Se debe contar con aire acondicionado de respaldo, en el caso que el principal presente problemas, con esto evitamos que se tenga que apagar los equipos computacionales y se aseguraría por ese lado, la disponibilidad de los servicios que presta en centro de datos ya si e
- Controles y alarmas de temperatura y humedad que permita 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
- 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
- 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 incombustible
- Techo resistente al fuego
- Canales y aislante resistente al fuego
- Sala y área de almacenamiento impermeables
- Sistema de drenaje en el piso firme
- Detectores de fuego alejado del aire acondicionado
- Alarmas de fuego conectado al general

  vSistemas de detección temprana de humo

2.23. Definición de las Políticas de seguridad de la información en el centro de datos

En el momento de definir las políticas de seguridad de los sistemas informático frente al personal de la institución requiere contemplar los siguientes aspectos:

- Definir los procedimientos para la creación de nuevas cuentas críticas.
- Definir 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.
- Definir los procedimientos para eliminar/bloquear las cuentas y los posibles escenario para incurrir a la medida.
- Delegación de confianza, definir la persona que delegará la responsabilidad de la información tales como usuarios, claves, entre otros, en el momentos cuando no este el responsable principal.
- Definir políticas de respaldo y recuperación antes incidentes para garantizar el continuo funcionamiento de los sistemas de las institución.
- Definir los procedimientos para respaldar o eliminar información o sistemas de los equipos de computación. [ver sección 11, Políticas de respaldo y recuperación]
- Definir las posibles violaciones y consecuencias derivadas del incumplimiento de las políticas de seguridad.
- Definir las sanciones a los responsables por la violación de las políticas de seguridad.
- Clasificar la información e identificar los activos de la institución

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

- Mantener en óptimas condiciones la red para garantizar su disponibilidad.
- Revisar el estado físico del cableado horizontal y vertical de la red de la institución.

- Realizar mantenimiento preventivo 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.
- Asignar las direcciones IP a los equipos de computación; ya sea por direccionamiento dinámico o estático.
- Crear mapas de IP.
- 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.
- Administrar las contraseñas críticas como por ejemplo: administrador (root), aplicaciones como cortafuego, servidores, entre otros.
- Ubicar los equipos en salas (centro de datos) con acceso restringido y medidas de seguridad física, utilizando estándares o certificación

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 naturales o accidentales como incendios, mal funcionamientos de los sistemas, errores humanos, entre otros, resulta necesario, requiriendo de una acción rápida para poner disponibles el servicio y de esta manera brindar unas de las características requerida para garantizar la seguridad de la información como es la disponibilidad.

Para garantizar la rápida disponibilidad de los servicios es necesario contar con planes de contingencias ante desastres y políticas de respaldo y recuperación.

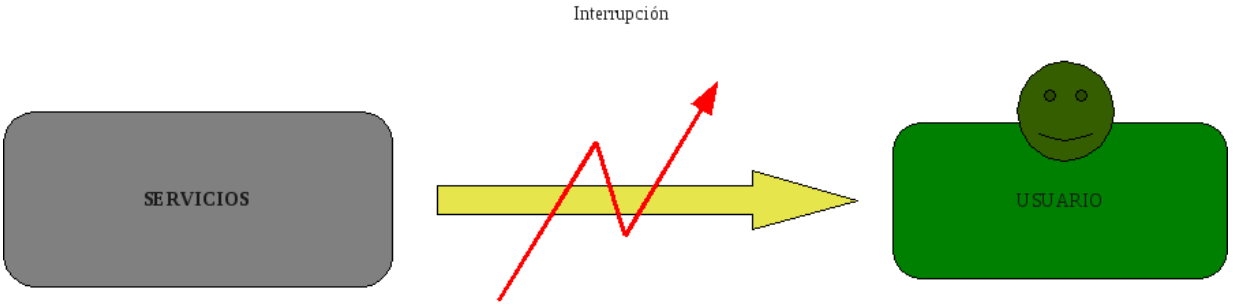

Figura 2.9: *Interrupción de los servicios.*

2.24.1. Normas para las políticas de respaldo y recuperación

- Las copias de respaldo de datos y ficheros de servidores deberían 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, debe contar con información, tales como: la configuración de equipos, paquetes de software necesarios, archivos y/o bases de datos, cronograma de ejecución del respaldo del activo.
- Planificar las copias de respaldo que debería realizar en función del volumen y del tipo de información generara por los sistemas informáticos
- Todas las copias de respaldo y medios de almacenamiento utilizado, deberían estar bien identificadas con información tales 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 utilizado, identificación de la persona que ejecuta el respaldo, ubicación asignada para su almacenamiento, persona responsables del almacenamiento.
- Establecer los sistemas o técnicas (algoritmo criptográfico como por ejemplo) 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 respaldo, físicamente seguro y poseer controles de acceso al lugar.
- Generar en un tiempo determinado dos copias de los respaldo, 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. Ademas el acceso y traslado de las copias debe ser realizados por personal debidamente identificado y autorizado para ejecutar el procedimiento.

- Efectuar 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 casos de aplicaciones críticas se recomienda implementar técnicas de replicación 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 Incidente de seguridad

Cualquier evento que pueda ocasionar la interrupción o degradación de los servicios de los sistemas, estos incidentes pueden ser por causas: intencionado, de error, de infringir accidental o deliberado 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 las 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 considera los servicios, equipos, aplicaciones, infraestructura, existente dentro de la institución

- 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 incidente de seguridad que pueda ocurrir en cada área crítica identifica, las misma deben estar bien documentadas
- Descripción clara y detallada de los planes de contingencia de todos los posibles escenarios de incidentes de seguridad, donde indique 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 un incidente de seguridad, la institución debería prestar con especial atención a los posibles indicadores de un incidente de seguridad, como una actividad a contemplar dentro del plan de respuesta a incidentes, entre 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 inusual en algunas cuentas como: conexión de usuarios en horarios extraños.

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 permita establecer prioridades en las actividades que debería llevar a cabo
- 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 el posterior estudio del incidente. 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 del o 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 más que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operativa mínima luego de una contingencia, en donde se vean afectados los procesos y recursos informáticos que sostienen a la Institución.

Los eventos de desastres pueden ser naturales o accidentales como incendios, inundaciones, corte en el suministro de energía eléctrica. En este plan de recuperación antes desastres se deben 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 del sistema informática de la institución, así de la recuperación de los datos, aplicaciones y servicios básicos: La practica de recuperación que se acostumbra a realizar según los especialista es por ejemplo:

- Disponibilidad de un centro alternativo para la ubicación de los principales recursos informáticos (servidores, aplicaciones, bases de datos, entre otros), este centro debería contar con las mismas medidas de seguridad que las instalaciones principales de la institución. Entre los diferentes alternativas de centro alterno tenemos:
  - Centro alterno “Frió”, se tiene un equipamiento suficiente de hardware, software y de comunicación para mantener los servicios críticos de la institución, en este centro se cuenta con las copias de seguridad de los datos y aplicaciones de la instalación.
  - Centro alterno “Caliente”, se tiene un equipamiento suficiente de hardware, software y de comunicación para mantener los servicios críticos de la institución, estos equipos se encuentra en funcionamiento y disponen de una replica de todos los datos y aplicaciones del sistemas que se realizan de formas diaria o incluso cada hora.
  - Centro alterno “Caliente” en una configuración en “espejos”. Se trata de un centro con el mismo equipamiento que el centro principal y que trabajo de modo paralelo a este, pudiendo entrar en acción inmediatamente a la caída del centro principal.
- Existencia de políticas de respaldo y recuperación.
- Herramientas para llevar a cabo una replicación de los documentos y las base de datos.

- Detección y respuesta al desastre en el centro principal, adoptando las medidas de contención prevista dependiendo del tipo de desastre: incendio, inundación, explosión, entre otros.
- Traslado de las actividades al centro alternativo, como por ejemplo al personal necesario para la puesta en marcha de los servicios, equipos informáticos, copias de seguridad mas reciente y con las medidas de seguridad que corresponda, entre otros.
- Es posible otra solución como la recuperación con capacidades limitadas del centro principal.

2.27. Seguridad en redes

después de includes

Capítulo 3

Privacidad

test

3.1. Definición y políticas de privacidad

test

3.2. Técnicas para proporcionar privacidad

test

3.2.1. Anonimato

test

Redes de mezcla

test

Enrutamiento cebolla

test

Capítulo 4

Fundamentos Jurídicos

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

Parte II

Aportes de CENDITEL en la Seguridad vinculada a la Identidad Digital en las TIC

Capítulo 5

Certificación Electrónica

A continuación el contenido del artículo de ROOTVE

Una Autoridad de Certificaci'on Ra'iz (AC Ra'iz) es un componente que tiene el rol de ser el punto m'as alto de confianza en una estructura jer'arquica denominada Infraestructura de Clave P'ublica (ICP). Una ICP provee de certificados digitales bajo est'andar X.509 a personas, direcciones IP y direcciones en la Web; proporcionando seguridad l'ogica, y vinculaci'on legal a las transacciones que realiza el propietario del certificado en la Internet. La confianza reside en la protecci'on a trav'es de esquemas fuertes de seguridad f'isica y l'ogica de la clave privada que permite la emisi'on de estos certificados. Este trabajo muestra el proceso de desarrollo de una aplicaci'on 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 funci'on de una descripci'on general de las funciones y caracter'isticas de una Autoridad de Certificaci'on; posteriormente, se dise nan funcionalidades y se especifican requisitos, con el objetivo de producir una visi'on formal de los procesos a automatizar. Se dedica una secci'on a la implementaci'on que consiste, en la codificaci'on en un lenguaje de programaci'on, de los procesos previstos en las etapas anteriores, como tambi'en, de la incorporaci'on de mecanismos fuertes de validaci'on de identidad de usuarios, registro de eventos, firma de acciones por parte de los administradores de la aplicaci'on, y especificaci'on de conexiones con hardware especializado, como tarjetas inteligentes. Finalmente, se muestra el despliegue y configuraci'on de la aplicaci'on, que involucra la instalaci'on en un ambiente seguro (b'oveda o centro de datos) y el enlace de la AC Ra'iz con los dem'as 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 cer-

tificates 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, instituci'on, o administración realice transacciones gubernamentales, comerciales o personales en la mayor'ia de los casos, tal cual, como se realizar'ian en una oficina o espacio f'isico 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 instituci'on, 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 organizaci'on que no se conoce o del cu'al no se tiene ninguna referencia. Mediante un contacto personal o directo, los sentidos humanos permiten percibir un gran n'umero de detalles que le caracterizan, y cuya combinación muy probablemente le hace irrepetible. Esta combinaci'on permite identificar al individuo de forma 'unica 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 f'isicas pueden ser documentos como la C'edula de Identidad, el Pasaporte, la Licencia de Con-

ducir, entre otros. Todos los documentos citados generalmente incluyen una fotograf'ia que permite la comparaci'on con la apariencia del interlocutor; tambi'en usualmente se agrega otra característica informativa que puede ser un nombre, una firma manuscrita y posiblemente un n'umero de referencia.

Cuando se traslada el concepto de identidad al medio inform'atico, se habla de identidad digital, y se hace necesario contar credenciales traducibles a informaci'on binaria. Por otro lado, la criptograf'ia, por s'i misma no proporciona este concepto: es el uso de una infraestructura computacional que utiliza algoritmos criptogr'aficos para representar credenciales digitales, como por ejemplo el certificado digital, y que son otorgados por terceros de confianza, denominados Autoridades de Certificaci'on (AC), y que se describen como Ra'iz cuando son el punto inicial de una jerarqu'ia, las que proveen a usuarios y organizaciones de identidad digital, y que cuenta con las mismas connotaciones que tiene este concepto en el 'ambito personal y jur'idico.
Uno de los problemas que aparece en este punto, en la disponibilidad de la infraestructura mencionada anteriormente, la cu'al debe contar como un elemento obligatorio una aplicaci'on que gestione, bajo un est'andar aceptado, como lo es el est'andar X.509[**?**], los certificados digitales que emite la AC. La discusi'on de importantes aspectos que surgen en las diferentes etapas del proceso desarrollo de la aplicaci'on de gesti'on, y que est'an 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 Te'orico

Con el objetivo de contextualizar los t'erminos "identidad", "confianza", o "transacci'on segura" y"AC Ra'iz" en el medio digital, y espec'ificamente en relaci'on con internet; es imprescindible en una primera aproximaci'on, discutir sobre determinados temas y conceptos vinculados con la seguridad inform'atica. En los p'arrafos siguientes se abordan brevemente algunos de los puntos m'as importantes relacionados con el tema.

5.2.1. Seguridad Informática

Se ha llegado a un consenso sobre lo que significa seguridad inform'atica[**?**]. En general, se dice que un activo de informaci'on, (informaci'on digital con un valor real para una empresa o persona) est'a 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 tambi'en 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 aplic'andole 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 criptograf'ia es la ciencia o arte informaci'on utilizando t'ecnicas matem'aticas que hagan posible el intercambio de mensajes de manera que s'olo puedan ser le'idos por las personas o usuarios autorizados [**?**]. La criptograf'ia ha tomado gran importancia en los 'ultimos a nos, ya que es posible transformar las "t'ecnicas matem'aticas" en algoritmos que pueden ser comprendidos por una computadora. Se puede clasificar la criptograf'ia en dos tipos, según el tipo de clave que se utilice:

Criptografía Simétrica: los sistemas de criptografía simétrica son aquellos que utilizan una 'unica 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 'unica 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 informaci'on sobre la clave, sin que sea develada a un tercero no autorizado.

Criptografía Asimétrica: tambi'en se conoce como Sistema de Cifrado de Clave Pública[**?**]. Usa dos claves diferentes, una de ellas es la Clave P'ublica 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 sim'etrico donde las partes deben concertar un procedimiento para conocer la clave 'unica, 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 'ultimo, 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 informaci'on 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 m'as alto en los procesos de autenticación y autorización, ya que se le otorga al cliente algo que puede poseer, incluso incluir dentro de elemento f'isico, 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 ingl'es Secure Electronic Transaction, Transacci'on Electr'onica Segura) [**?**].

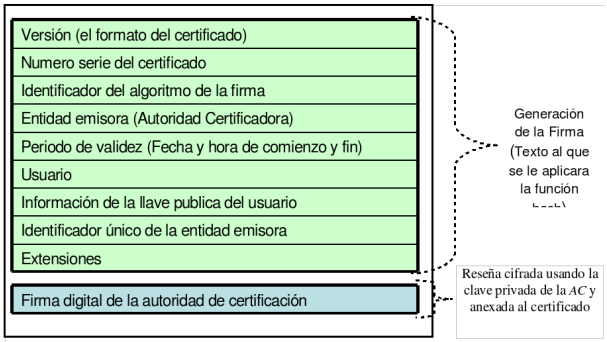

Figura 5.1: Especificaci'on del estandar X.509

Los certificados digitales tienen multitud de usos, entre los tipos de certificados m'as utilizados est'an:

- **Certificado de Servidor SSL (del ingl'es Socket Secure Layer, Nivel de Conexi'on 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 informaci'on que env'ia cada parte. El certificado del servidor posibilita la autenticaci'on 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 trav'es 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 ingl'es Unified Modeling Language, Lenguaje de Modelado Unificado) es un lenguaje que permite diseñar sistemas a trav'es de modelos, que se componen de un conjunto de s'imbolos 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 'el. Los diagramas que componen el lenguaje son:

- Diagramas de casos de uso
- Diagramas de estados
- Diagramas de secuencias
- Diagramas de colaboraciones

- Diagramas de distribuci'on
- 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 continuaci'on:

Diagramas de clases: son representaciones gr'aficas de las categor'ias en que pueden clasificarse los objetos del mundo real. En general, se hace una descripci'on de las categor'ias que se utilizan en la aplicaci'on 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 en-

tre 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 informaci'on general al público en general sobre los aspectos y servicios relevantes de la ICP.

Los nodos de una ICP pueden ordenarse seg'un diversos modelos. El m'as utilizado es el modelo jer'arquico, que presenta una ra'iz y nodos hijos que distribuyen los certificados a los clientes o entidades finales (Ver Fig. 5.2). Se muestra un ejemplo de modelo de jerarqu'ia de una ICP de cuatro niveles, que se encuentra en el tercer nivel del modelo, que certifica a los usuarios.

Este modelo de establecimiento de relaciones de confianza, es necesaria entre m'ultiples autoridades de certificaci'on para garantizar que los usuarios (entidades finales) no tengan que depender y confiar en una sola AC, algo que har'ia imposible el manejo de estabilidad, administraci'on y protecci'on. 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.

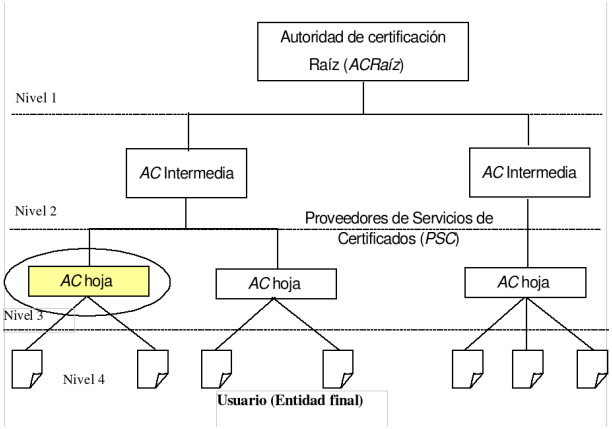

Figura 5.2: Modelo jer'arquico de una ICP

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 conexi'on 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 selecci'on del sistema operativo Linux[**?**] para desplegar la aplicaci'on, ya que cumple con los principios del software libre, y cuenta con gran n'umero de herramientas en el 'area de programaci'on [**?**], 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 elaboraci'on de la aplicaci'on.

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 programaci'on. 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 relaci'on 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 Componente AR, el Administrador del componente PUB, y el actor PSC, qui'enes son los que interactúan con la aplicación.

Para el resto de la especificación de requisitos se elaboran casos de uso que modelan las funcionalidades con que debe contar la aplicaci'on. 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 emisi'on, renovaci'on y revocaci'on de certificados, que conlleva procesos de firma con la clave privada, modificaci'on de los periodos de vigencia del certificado y elaboraci'on 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

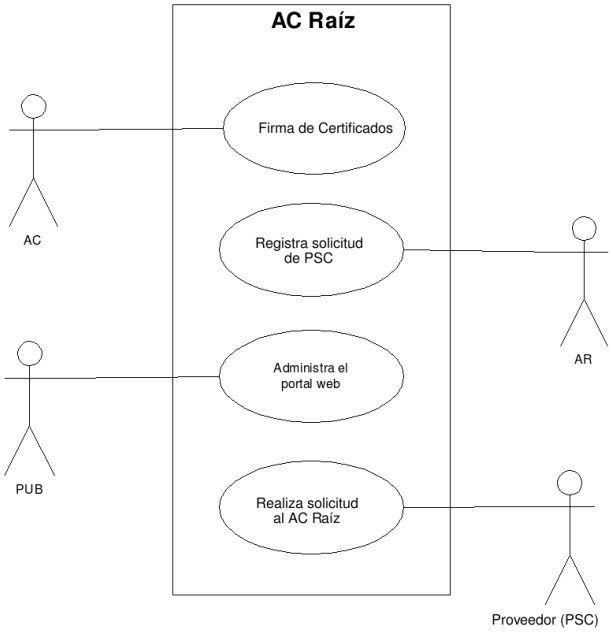

Figura 5.3: Caso de uso principal

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 certificaci'on, 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 "Emisi'on de certificados"' del actor Administrador del componente AC. Para este conjunto de actividades participan cuatro (4) actores: Administrador del PSC, qui'en entrega los recaudos necesarios para que se le firme su solicitud, el Administrador de la AR, qui'en es el encargado de chequear los recaudos entregados por el PSC, el Administrador de la AC Ra'iz y el Administrador PUB, este 'ultimo encargado de de publicar en los diferentes repositorios los certificados (claves p'ublicas) para que sean visibles por el mayor n'umero de usuarios interesados.

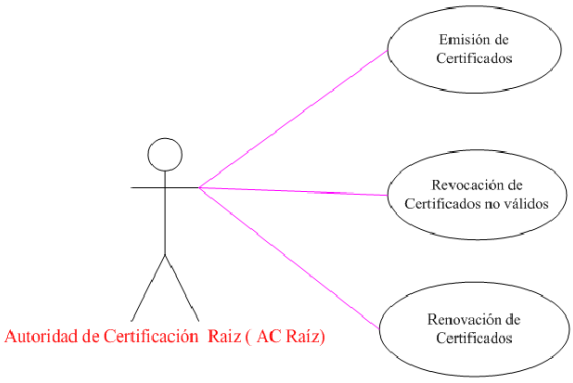

Figura 5.4: Caso de uso para el actor Administrador Autoridad de Certificaci'on

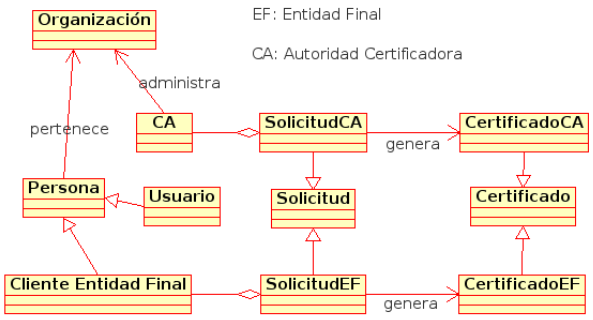

Figura 5.5: Diagrama de clases

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 dem'as entidades que conforman el modelo de datos.

Se utilizan y validan los diagramas de casos de uso mediante la elaboraci'on de interfaces gr'aficas de usuarios y funcionalidades de interacci'on con el usuario. Los diagramas de actividades ayudan en el planteamiento de algoritmos que proveen funcionalidades o caracter'isticas con las cu'ales debe contar la aplicaci'on y que deben estar en coordinaci'on con los respuestas y valores esperados.

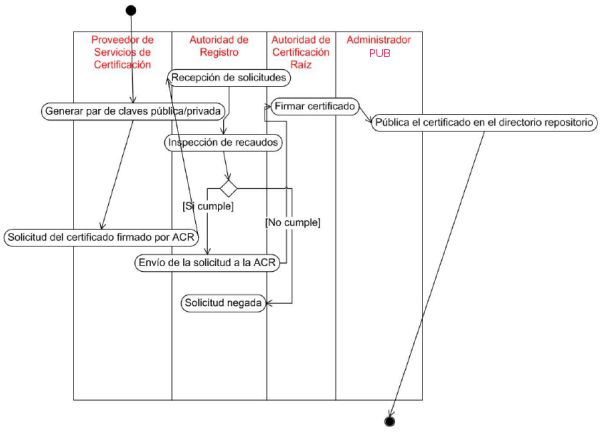

Figura 5.6: Diagrama de actividades

Haciendo uso de las ventajas que trae el uso de software libre (Secci'on 5.2.6), se implementa la aplicaci'on utilizando la mayor cantidad de l'ineas de c'odigos 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 c'odigo fuente del proyecto XCA [**?**], desarrollado por Christian Hohnstädt, que tiene como objetivo proveer una aplicaci'on escrita en el lenguaje de programaci'on C++[**?**] y la biblioteca Trolltech Qt[**?**], que cumpla con el est'andar X.509. La aplicaci'on satisface los requisitos b'asicos para la gesti'on del componente de gesti'on de AC Ra'iz, 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 aplicaci'on XCA incorpora estas tres actividades, pero se hace necesario adaptar la interfaz de usuario y agregar caracter'isticas en funci'on 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 completaci'on de funcionalidades. En este sentido, se incorporan caracter'isticas a la aplicaci'on acorde con la especificaciones de dise no, entre las cu'ales se enumeran:

- La incorporaci'on de un sub-sistema de seguridad para acceso a los activos de informaci'on que gestiona la aplicaci'on, que incluya aspectos de autenticaci'on y autorizaci'on de usuarios, como lo es la validaci'on de credenciales a trav'es del uso de tarjetas inteligentes, el registro y firma digital de las acciones realizadas por los usuarios dentro de la aplicaci'on. En La fig 5.7 se muestra la caracter'istica de

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

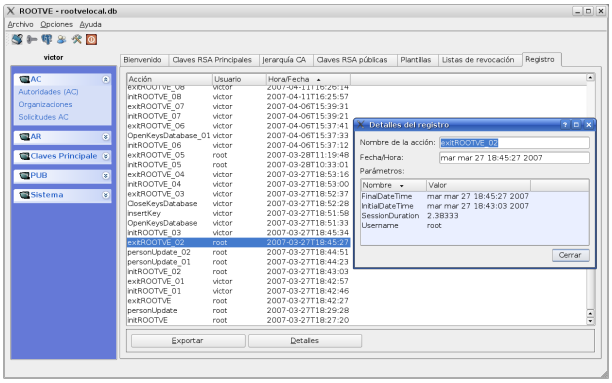

Figura 5.7: Sistema de registro de acciones

- Estandarizaci'on del sistema de gesti'on de documentos como solicitudes, plantillas de certificados y certificados.
- Conexi'on a trav'es de una interfaz propia con el hardware donde se resguardan las claves privadas (HSM).

Tambi'en en esta etapa se seleccionan e integran las tecnolog'ias a utilizar para la codificaci'on y creaci'on de la aplicaci'on de gesti'on del componente AC Ra'iz. Los tipos de tecnolog'ias que deben seleccionarse son: bibliotecas para construir la interfaz hombre-m'aquina (HMI), motor criptogr'afico, conexiones con hardware, interfaces con repositorio de datos y algoritmos de c'alculo criptogr'afico m'as utilizados.

Como criptosistema se utiliza OpenSSL version 0.9.8 [**?**], que provee de un conjunto de funciones criptogr'aficas apegadas al est'andar X.509. . Para la construcci'on de interfaces hombre-m'aquina y uso de algoritmos generales se selecciona la biblioteca Trolltech Qt. Como interfaz para el uso de tarjetas inteligentes se utilizo el est'andar PKCS11, tambi'en conocido como Cryptoki, que especifica una forma para interactuar con este hardware criptogr'afico[**?**].

5.4.4. Pruebas

Esta etapa tiene dos objetivos. El primero de consiste en asegurar que la aplicaci'on funcione correctamente, es decir, que se generen la menor cantidad de salidas inesperadas

o fallas a entradas dadas. En relaci'on al logro de este objetivo se utilizan un conjunto de t'ecnicas aplicadas a lo largo del proceso de desarrollo, entre las cu'ales se pueden citar la revisi'on en parejas[**?**], que consiste que la programaci'on se realice en equipo de dos programadores por computador, uno de ellos se encarga de escribir los algoritmos en un lenguaje de programaci'on, y el segundo de ellos de revisarlo inmediatamente, despu'es de periodo de unas horas, que debe ser definido con anticipaci'on, se intercambian los roles. Otra de las t'ecnicas utilizadas que es importante nombrar son las pruebas unitarias[**?**], las cu'ales consisten en aplicar un n'umero casos de pruebas a m'etodos o m'odulos peque nos de la aplicaci'on (unidades), de tal manera que se asegura que funcionan correctamente de forma independiente. Seguidamente, se realizan pruebas de integraci'on, que consisten en probar m'odulos m'as complejos formados por las unidades revisadas en las pruebas unitarias. Las pruebas unitarias y de integraci'on 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 aplicaci'on debe cumplir con las caracter'isticas necesarias para resolver el problema de gesti'on de una AC Ra'iz. En este sentido, se toma una estrategia basada en prototipos con liberaciones peri'odicas, 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 modificaci'on de requisitos y notificaci'on de errores son notificados en un sistema web de chequeo y seguimiento [**?**].

Tambi'en 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 'ultima versi'on de los programas fuentes.

Debido a que la aplicaci'on de gesti'on de AC Raiz debe ser parte de una infraestructura, es necesario realizar pruebas en condiciones similares a la configuraci'on final de 'esta; por ello se simula la configuraci'on de producci'on que conlleva pruebas con el sistema operativo y el donde se instala la aplicaci'on, conexi'on con tarjetas inteligentes y el m'odulo de seguridad en hardware, controles de acceso f'isico y l'ogico, y desconexi'on de red, ya que la autoridad debe operar fuera de l'inea.

5.4.5. Despliegue y configuración

El despliegue consiste en la instalaci'on en condiciones reales de la aplicaci'on de gesti'on de AC Ra'iz dentro de la infraestructura. La figura 5.8 muestra una propuesta para el despliegue de la infraestructura. La aplicaci'on se instala en un computador desconectado de red que debe estar ubicado dentro de un lugar f'isico seguro, lo que significa que el acceso a personas deber estar restringuido por llaves y controles biom'etricos, y el flujo de informaci'on digital hacia adentro y afuera de la b'oveda debe ser realizado a trav'es

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. Tambi'en es necesario la habilitaci'on de servidores para la validaci'on de los periodos de vigencia de los certificados (OSCP), y para la generaci'on de solicitudes de firma de certificados, donde las entidades finales o usuarios consignan los recaudos.

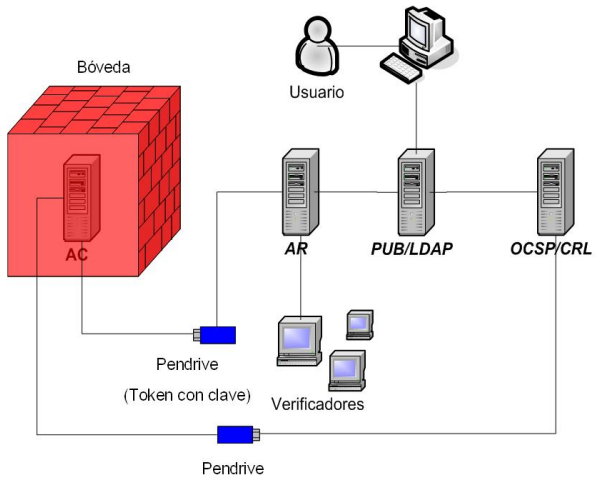

Figura 5.8: Configuraci'on de los componentes del nodo ra'iz de una ICP

Por otro lado, la configuraci'on conlleva el establecimiento de par'ametros para el funcionamiento la aplicaci'on, tales como m'etodos de control y restricci'on de acceso, ubicaci'on de archivos y directorios, rutas para importaci'on e exportaci'on de datos, perfiles de usuario, generaci'on y nombres de claves, inicializaci'on de tarjetas inteligentes, inicializaci'on de HSM, y copias de seguridad.

5.5. Conclusiones

La puesta en marcha de una AC Ra'iz supone obligatoriamente contar con una aplicaci'on que gestione este componente de la infraestructura. En este sentido, 'este trabajo mostr'o el proceso de desarrollo de una aplicaci'on que respondiera a los requisitos particulares de gesti'on, determinados por el rol de confianza ra'iz y 'ultima que debe representar la Autoridad. En funci'on de ello, la aplicaci'on tiene un alto grado de especializaci'on, ya que cuenta con un mercado relativo de pocos usuarios, si se compara con el mercado de los sistemas de informaci'on o aplicaciones de ofim'atica, y su operaci'on se realiza en condiciones estand'andares y espec'ificas. A pesar de este hecho, para la construcci'on de

la aplicaci'on se integraron varios proyectos disponibles en los repositorios de software libre, que permiti'o disponer de un criptosistema est'andar y suficientemente completo para cumplir con los requisitos descritos en la etapa de dise no. La criptograf'ia se utiliza como herramienta para otorgar las tres propiedades (Confidencialidad, Integridad y Disponibilidad) de la seguridad inform'atica a los datos que gestiona la aplicaci'on, y en virtud de ello el hardware criptogr'afico utilizado como las tarjetas inteligentes y el m'odulo de seguridad en hardware configuran un "mundo seguro" que cumple con los est'andares aceptados a nivel mundial.

En la etapa de dise no, los diagramas de casos de uso y actividades sirvieron para obtener una visi'on formal de los requisitos y de los procesos con los que cumplir la aplicaci'on. Estos documentos de dise no en el lenguaje UML, permitieron alcanzar de manera m'as r'apida y certera los objetivos que son coincidentes con la gesti'on real de una AC Ra'iz.

Al seguir el est'andar X.509 se asegura que los certificados, solicitudes y claves gestionados por la aplicaci'on 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 eliminaci'on de fallas las t'ecnicas como la colaboraci'on utilizando herramientas web, la programaci'on en equipos y las pruebas unitarias y de integraci'on sirvieron para los procesos de prevenci'on, notificaci'on, b'usqueda y arreglo de errores, permitiendo adem'as guardar una bit'acora del progreso a la soluci'on a problemas. La implementaci'on de caracter'isticas espec'ificas en funci'on de los requisitos cada vez m'as refinados y particulares que surgieron en las iteraciones de prototipos probados con usuarios y condiciones reales.

La combinaci'on de diversos elementos como software, hardware y la configuraci'on de un espacio f'isico adecuado, esto es, que cumpla determinadas reglas para el control de acceso, conforma la infraestructura necesaria para la operaci'on de una AC, incluso que 'esta no sea Ra'iz, y sea parte de otro nodo de la jerarqu'ia. Las condiciones de seguridad l'ogica y f'isica pueden reproducirse exactamente para los nodos intermedios y los nodos Proveedores de Servicios de Certificaci'on 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 jur'idica a la que un PSC le expide un certificado digital.

PSC: Proveedor de Servicios de Certificaci'on Digital; Organizaci'on que mantiene la infraestructura de nodo de una ICP, y est'a autorizada a expedir certificados a las personas naturales y jur'idicas 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.

Capítulo 6

Firmas Electrónicas

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.

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 jurídica-

mente 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 validadados 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

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

puede usarse en diversos sistemas operativos, y 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.

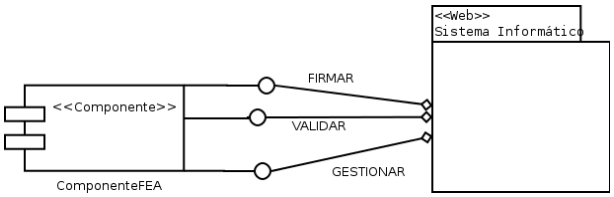

Figura 6.1: Diagrama UML de acoplamiento

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.

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 au-

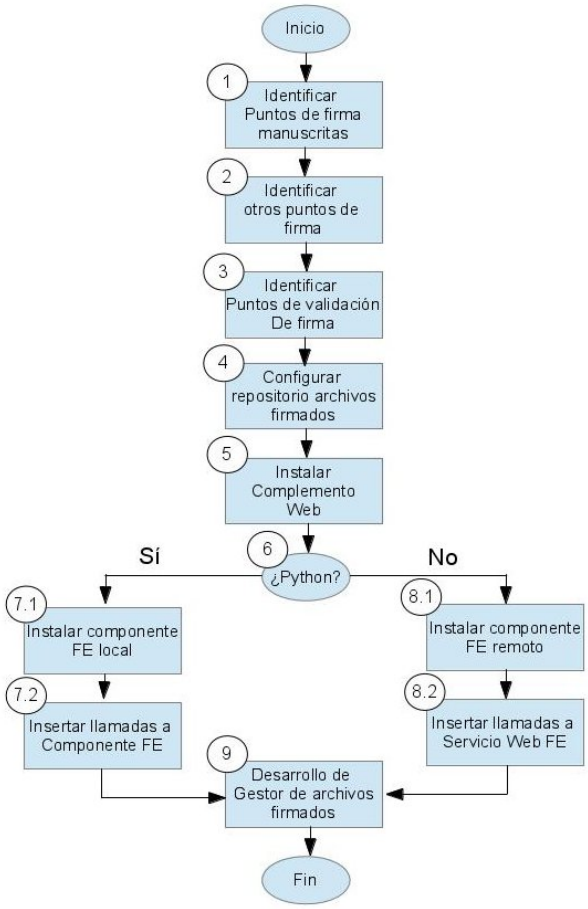

Figura 6.2: Diagrama de flujo para el acoplamiento del ComponenteFEA

tomatizar. 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*.

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

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 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 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

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

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.

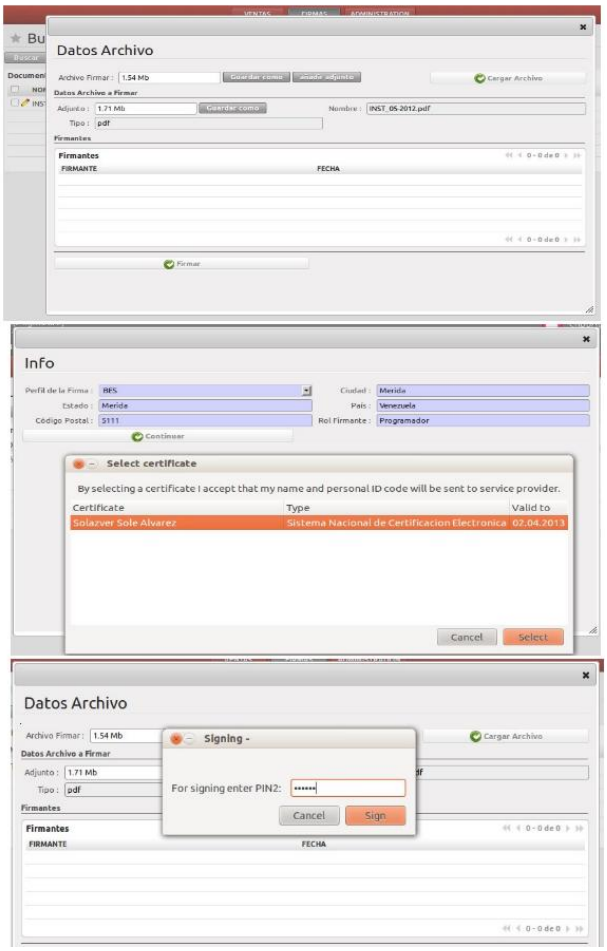

Figura 6.3: Interfaz de usuario OpenERP para el ComponenteFEA

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 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 "subjectCertificateCommonName".

```
 <?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';
```

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

```
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.

Bibliografía

[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.

Capítulo 7

Anonimato

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.

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 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. We must to thank to José Lisandro Aguilar Castro for his revision, advices and recomendations about the whole content of this paper.

Bibliografía

[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.

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.

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.

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.

Bibliografía

[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 Technologies 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 #1014. http://www.vernier.com/ (2011)

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