Caso de estudio (Canales seguros)

# Objetivos

* Identificar los requerimientos de seguridad de los canales usados para transmisión de la información en el sistema de apoyo a las aplicaciones de la entidad administradora de pensiones.
* Construir un prototipo a escala del sistema que permita satisfacer algunos de los requerimientos de seguridad identificados. Entendiendo las garantías de seguridad y las limitaciones de la implementación propuesta.

# Descripción General

En esta segunda parte, su tarea es determinar los requerimientos de seguridad para la construcción de algunos componentes del sistema de tecnologías de información que soporta las operaciones de la entidad administradora de pensiones.

# Problemática

Como se indicó en el enunciado del caso, las principales tareas del sistema son el manejo de afiliaciones, recaudos, AFE, historia laboral, reconocimiento, nómina de pensionados, tutelas y portal web.

En este contexto, surgen diversos problemas de seguridad para algunas de las transacciones que el sistema soporta, tanto a nivel de transmisión como a nivel de almacenaje de datos. Como consecuencia, es necesario evaluar riesgos y vulnerabilidades y determinar medidas para mitigar los riesgos detectados.

Su tarea en este caso es actuar como consultor y analizar, desde el punto de vista de la seguridad, las tareas relacionadas con el proceso de afiliación.

# Tareas

Suponga que la arquitectura del sistema incluye un cliente en la empresa que maneja las afiliaciones y un servidor en la oficina principal de la entidad de manejo de pensiones. En este servidor se corre el front-end de la aplicación que se encarga de procesar las afiliaciones. El cliente se comunica con el servidor vía internet.

Los desktops de los empleados que trabajan en la oficina central de la entidad de manejo de pensiones están conectados a una subred privada y aislada de la subred en la que correo el servidor. El servidor maneja dos interfaces de red, una para conexiones con los clientes externos, entre los que se cuenta el servidor de la empresa que maneja las afiliaciones, y una para conexiones con los computadores de la red privada interna.

# Análisis y entendimiento del problema

## Amenazas

1. **Espionaje:** Dado que las oficinas tienen que reportar al servidor las actividades diarias, es necesario enviar la información por la red y al realizar esta acción es posible sufrir de espionaje.

En el proceso de Afiliaciones se subcontrata un tercero, quien además es el encargado de realizar los back up. Esta transferencia de información permite problemas como Man-in-the-Middle (si no manejan autentificación) donde un tercero revisa la información enviada.

Si se llega a sufrir de espionaje es posible poner en riego a los funcionarios, afiliados y a los aportantes ya que cualquier persona podría adquirir la información de las afiliaciones. Además, se podría filtrar información de los procesos y empleados de la empresa. Recordemos que la información es lo más importante para tomar decisiones y ser competitivo, por eso la necesidad de ocultarla de la competencia y de peligros potenciales. Así mismo, la información de los afiliados podría caer en manos de terceros y esa información es privada, lo cual requiere altos niveles de protección.

1. **Modificación no autorizada de datos:** Al igual que en el punto anterior, el envió de la información vía red desde las sucursales y la comunicación con el tercero permiten la interferencia de un intermediario. En el caso anterior este únicamente revisaba el contenido de los archivos o transacciones, sin embargo es posible que este intermediario genere modificaciones a la información que se almacena en la base de datos de la sucursal central. Lo anterior debido a que no se usan mecanismos de seguridad para el envío de la información.

Al sufrir de la modificación no autorizada de datos se presentan inconsistencias en el sistema de pagos de pensiones y se podría beneficiar a personas que no están afiliadas.

1. **Fraude:** Esta amenaza no se aplica directamente a la arquitectura de la empresa. Esta amenaza es posible si el fraude se realiza sobre el tercero encargado de las afiliaciones. Para explicar lo mencionado anteriormente se debe definir que se toma como fraude. En este contexto fraude es introducir información, de forma no autorizada, en el software. Ahora bien, es posible agregar información en el tercero para verse beneficiado de las afiliaciones aun si estas no son reales.

Si se sufre esta amenaza habría datos basura y pérdidas monetarias. No habría consistencia en los datos ya que la cantidad de afiliados por empresa variaría y los aportantes no tendrían información de esto.

1. **Filtración de información:** En la oficina central y en las sucursales es posible que se filtre información. Esta amenaza se puede dar de manera intencional y no intencional. A continuación se explicara cada una de ellas.
   1. **Intencional:** Se da cuando un funcionario realiza una copia de la información a parte de ella para sacarlo de la empresa.
   2. **No intencional:** Se da cuando un usuario conecta un equipo propio a alguna de las redes y este equipo tiene algún malware que filtre información.

Si se evidencia esta amenaza, se está vulnerando la privacidad y confidencialidad de la información. Para la empresa es un riesgo muy alto ya que la información robada puede ser usada en contra de los afiliados, aportadores y los demás funcionarios. También se pueden divulgar secretos empresariales de la empresa, como la arquitectura de software, claves e información de las dos redes que se utilizan (local y externa).

1. **Denegación del Servicio**: Cada vez es más común este tipo de ataques a través de Internet. Terceros a la organización pueden desarrollar un ataque de denegación del servicio ya sea para perjudicar a la organización o para perjudicar a alguno de los clientes, o simplemente para demostrar algún tipo de habilidad frente a un grupo particular. Puede ocurrir este tipo de ataques también sin estar dirigidos a la organización, por el simple hecho de estar conectado a Internet.

## Vulnerabilidades

1. **Disponibilidad de comunicaciones**: Puesto que el cliente se comunica con el servidor a través de Internet, es posible que se presenten fallas en las comunicaciones, ya sea en el proveedor de servicios de Internet del cliente o en el proveedor de servicios de Internet del servidor. En este caso, aunque las aplicaciones estén operativas, no será posible realizar las transacciones por lo que el servicio no estaría disponible todo el momento requerido.
2. **Fallas de servidor**: El servidor puede presentar fallas de hardware o de software, lo que representa que el servicio no estaría operativo el tiempo que se requiere, ni para los empleados locales ni para los usuarios remotos.
3. **Autenticación**: Los clientes que se comunican a través de Internet deben poder asegurar que el “interlocutor” es en realidad el servidor “front-end” que se encarga de procesar las afiliaciones. De no ser posible esta autenticación, se puede presentar una sustitución del servidor y por ende la información privada y confidencial de los afiliados podría estarse entregando a un tercero.
4. **Confidencialidad**: La información hacia el servidor fluye a través de Internet, en el caso de los usuarios remotos o clientes externos, o a través de una red privada interna, en el caso de los empleados. Si la información no se transmite con mecanismos seguros, es posible que ésta sea “capturada” por agentes externos a l organización.
5. **Cortez de luz:** En Bogotá y en la ciudad donde se encuentra el servidos, es común verse afectado por cortes de luz. Algunos son por razones de mantenimiento de la infraestructura física, otros por daños en la red eléctrica o en las cajas de energía. Por otro lado, los robos de cable no son ajenos a la ciudad ya que la venta de cobre es un buen negocio en el mercado negro.

De llegar a ocurrir, implicaría que las aplicaciones ofrecidas a los afiliados no estarían disponibles todo el tiempo, como se desea. Además, si la falla se diese en horario laboral, ninguno de los funcionarios podría cumplir con sus deberes hasta que se solucione el origen del corte de luz.

## Propuestas de soluciones

Se sugieren las siguientes medidas para manejar los riesgos presentados por las amenazas y vulnerabilidades descritas:

1. Contratar los servicios de Internet para el servidor con redundancia y preferiblemente contratar un doble servicio con otro proveedor. Lo primero permite que el nivel de disponibilidad se incremente para un mismo proveedor de servicios de internet (ISP, por sus siglas en inglés de *Internet Service Provider*). Lo segundo permitiría, además, que si se presenta una falla en uno de los ISP, se cuenta con el otro servicio.

La disponibilidad paralela, esto es cuando se tienen enlaces redundantes, se calcula mediante la siguiente ecuación[[1]](#footnote-1)

Disponibilidad = 1 -

Donde n es el número de enlaces disponibles.

De esta forma, si se tienen dos (2) enlaces con disponibilidad cada uno de 99.9%, la disponibilidad real para la conectividad es de 99.9999% resultante de la operación [1 – (1-0.999)\*(1-0.999)]

1. Implementar servidores seguros: Al implementar servidores seguros se manejan dos temas simultáneamente. El primero corresponde a la autenticación, pues el servidor seguro debe tener un certificado digital que permite su identificación unívoca. Lo segundo corresponde a la protección de la información que fluye a través de las redes, pues la comunicación con los servidores seguros se realiza con mecanismos de ciframiento o encripción de datos y ello garantiza que si esta información cae en manos de terceros ésta no podrá ser interpretada. Esto incrementa la confidencialidad y disminuye tanto la posibilidad de fraude como de filtración de información.

El servidor seguro requiere el uso de un certificado digital que es expedido por una Entidad de Certificación (Certicámaras, por ejemplo en Colombia). Cuando el cliente se conecta con el servidor seguro, se establece un mecanismo de autenticación con llave pública o asimétrica, en el cual el cliente realiza las validaciones correspondientes del certificado digital y por ende puede validar o verificar la autenticidad del servidor. Para esto se utilizan algoritmos como el de RSA.

Una vez validada la autenticidad del servidor, éste establece una clave simétrica que se establece para las comunicaciones seguras con el cliente y por lo tanto, desde ese momento, todo intercambio de información entre el cliente y el servidor se cifra o encripta a través de mecanismos de llave simétrica.

1. Para controlar los ataques de denegación de servicio, es recomendable colocar un equipo entre el servidor y la conexión a internet que incluya características técnicas para evitar o controlar este tipo de ataques. En el mercado es posible adquirir estos equipos, pero debe tenerse en cuenta que no basta con adquirirlo e instalarlos, sino que es necesario realizar permanentemente la administración del dispositivo.
2. Para la modificación no autorizada de datos se requiere implementar mecanismos de autenticación de usuarios, a través de identificación y contraseña como mínimo. Acompañando esta medida debe también activarse en el sistema de afiliaciones los mecanismos que generan las bitácoras de las transacciones, para poder tener trazabilidad de todos los cambios ocurridos. Esto desmotiva la intensión de fraude. Por obvias razones, es necesario implementar procesos o procedimientos dentro de la organización para estar verificando periódicamente el contenido de las bitácoras y detectar posibles problemas de fraude. No se gana nada recopilando información en las bitácoras si la empresa no los revisa.
3. Con el fin de atender las posibles fallas del servidor, es necesario contar con servidores de alta disponibilidad en los cuales muchas de sus partes son redundantes; de esta forma si alguno delos componentes falla, entra a funcionar su respaldo (en la parte de conectividad se señaló el beneficio de la redundancia). También es necesario contemplar un estricto programa de mantenimiento del servidor, tanto para los componentes de hardware como de software.
4. El servidor debe colocarse en un espacio con condiciones ambientales contraladas. Así mismo, dadas las condiciones de estabilidad de energía, es necesario implementar sistemas ininterrumpidos de potencia (UPS) y posiblemente una planta eléctrica complementaria. Para decidir la configuración del sistema de energía alterno será necesario analizar la información sobre cortes de luz (frecuencia y duración) de un periodo de tiempo anterior.
5. Nunca sobra contratar un servicio alterno para disponer de servidores de contingencia en caso de fallas graves en el sitio donde reside el servidor principal.

# Implementación del prototipo

## Algoritmo Simétrico

Para la implementación del prototipo escogimos el algoritmo simétrico AES. Éste es el sucesor de DES como algoritmo de cifrado simétrico estándar para EE.UU. AES acepta claves de 128, 192 o 256 bits, donde las llaves de 128 bits ya son bastante seguras. Utiliza bloques de 128 bits, por lo que no se requiere ninguna operación adicional, además es eficiente tanto en software y hardware.

Para dar veracidad de la seguridad citamos esta frase de Starkoverflow.com: “Fue seleccionado a través de un concurso abierto que involucra a cientos de criptógrafos durante varios años. Básicamente, usted no puede tener más que eso”.

Ya explicado el algoritmo explicaremos porque se escogió este en lugar de los otros candidatos. No se escoge el algoritmo DES ya que ya ha sido violado y no se considera seguro; Blowfish de 128 bits es un buen candidato para usar, sin embargo usa bloques de 64 bits lo que indica que incurriría en demoras al dividir los bloques de información; RC4 es el único cifrado por flujo permitido en este proyecto y es más rápido en operación que los demás, por otro lado este algoritmo es poco eficaz y se considera débil, por esta razón no se recomiendo usarlo en software.

Ahora bien hablemos de las razones del contexto por las cuales se decidió usar AES. Ya que Colpensiones cuenta con 1.900.000 de afiliados y 78 oficinas distribuidas por varios municipios del país es necesario transmitir cantidades bastante altas de información que no se quiere que cualquiera conozca, descartamos DES, además con esta cantidad tan alta de información la diferencia de tiempo en ejecución entre el cifrado con AES y Blowfish se vuelve considerable, descartamos blowfish. Por otra parte la información que se envía entre las oficinas contiene información de los afiliados, aportantes (relaciones entre afiliados y aportantes) y de los funcionarios (datos laborales como el sueldo) por lo cual las debilidades conocidas de RC4 se convertirían en una vulnerabilidad demasiado riesgosa.

## Algoritmo Asimétrico

Para el algoritmo asimétrico se usara el RCA. Éste funciona por medio de la operación modulo y sus propiedades. Funciona con números muy grandes y soporta números hasta de . Para que el método funcione se realizan los siguientes pasos:

1. Escoja 2 números primos grandes ().
2. Ahora calcular n, donde .
3. Ahora escoja un número tal que sea un primo relativo de . Este número lo llamaremos
   1. ó

## HMAC

1. Oggerino, Chris, High Availability Network Fundamentals, Cisco Press, 2001, page 26. [↑](#footnote-ref-1)