**Documento de Análisis y Entendimiento del Problema**

**Integrantes: Luis Miguel Gómez Londoño – 201729597**

**Infraestructura Computacional**

**Profesora: Sandra Rueda**

1. El portal web descrito en el enunciado debe contar con un sistema de seguridad para la protección de los datos de la entidad Colpensiones. Algunos de estos datos, personales (Contraseña, cédula…), por el otro lado, existen los datos de los servicios de cada persona, como Recaudo, afiliación, historia laboral, nomina de los pensionados, y tutelas. En el caso de los **datos personales** existirían graves problemas si alguien sin autorización tuviera acceso tanto de lectura como de escritura. Para estas dos, los datos de las personas con pensiones en las plataformas se verían comprometidas, si se tiene acceso al perfil del afiliado, se tiene acceso al arduo trabajo que tienen los clientes de pensiones en la empresa. Además de eso, los problemas legales que enfrentaría la empresa serian gigantes, desde demandas hasta la posible quiebra. Por esto es por lo que la protección total de la empresa desde la red es de gran importancia.
2. **Primera vulnerabilidad:** Bajos niveles de defensa, la empresa en el enunciado dice que solo tiene un firewall para proteger las subredes internas y de servidor web. Para mantener un buen nivel de defensa se recomienda que además del firewall existan mas capas de protección como IDS, Antivirus y Antispam.

**Segunda vulnerabilidad:** Falta de verificación del cliente o servidor previo al intercambio de los certificados. Previo a este intercambio existiría la probabilidad de una suplantación de un hombre en el medio ya que luego de haberse entregado los certificados, se hacen verificaciones y envíos de llaves simétricas.

**Tercera vulnerabilidad:** Falta de verificación de cliente. Se propone una implementación en el protocolo para el uso de una firma digital para verificar al cliente.

**Cuarta vulnerabilidad:** Falta de aislamiento de las redes. Si, existe un aislamiento cuando se dividen las redes en interna y externa, sin embargo, a través del servidor del portal se tiene acceso a las dos. Se proponen mas capas de aislamiento para la red. Se propone aislar algunos servicios para que no estén conectados al internet (Cómo los backup de procesamiento y almacenamiento), la implementación de un proxy, y finalmente, el aislamiento de algunas unidades organizacionales…