Caso 2

Como todo sistema, la mayor debilidad del mismo está en su eslabón más débil. En este caso, como en muchos otros su eslabón débil está en los usuarios, quienes seguramente no serán cuidadosos con sus contraseñas de acceso o protección de los equipos donde acceden. Esto daría accesos indebidos a personas maliciosas.

Para el sistema de apoyo a Colpensiones se instauraron muchos diferentes algoritmos de encriptamiento para probar los mismos. Se sabe que algunos de ellos ya han sido vulnerados y están fuera de uso, como el DES y RC4, por ende, su fiabilidad es dudosa. Esto permitiría que un atacante por fuerza bruta entrara con relativa facilidad.

Dentro de las amenazas que se encuentran en el sistema están las comunicaciones inseguras en las que se comunican los clientes con el servidor en las cuáles se podría presentar *spoofing* o suplantación y espionaje para robo de los datos transmitidos. Este caso no está considerado dentro del alcance del proyecto, pero es recomendable que Colpensiones evalúe sus sistemas de conexión.

Otra amenaza posible se halla en el almacenamiento de datos del sistema. En este caso no se conoce cómo está montado el servidor de Colpensiones, por ende, no se puede saber si los datos están protegidos contra amenazas o encriptados adecuadamente. Se confía que dentro del diseño del servidor haya sido tenido en cuenta. En caso de no estarlo, se expone toda la información sensible de los usuarios, sus ahorros y pensiones.

Además, se desconoce si se generan *logs* (registros) adecuados de las actividades en el sistema, sin embargo, se sabe que el cliente no lo hace. Esto no permitiría que, en caso de una intrusión, se supiese de dónde vino el ataque o cómo sucedió.

Por otro lado, no se han hecho pruebas de penetración, carga o y rendimiento, por ende, si se libera a producción se podrían explotar vulnerabilidades no revisadas. Esto es especialmente peligroso ya que se maneja información sensible de los usuarios que podría ser usada para suplantarlos.

Para solucionar todas estas debilidades del sistema Colpensiones debe extender el alcance del proyecto. Entre las cosas que se deben hacer es incluir el VPN a todos los clientes, el aislamiento del servidor, la administración de cuentas de usuarios tanto de acceso a equipos como de acceso a red y sistema, eliminar los algoritmos inseguros con consultoría sobre seguridad. Además, se debe dar tiempo a pruebas de penetración, ojalá con acceso a código del servidor, exigir logs de servidor, réplicas del mismo y balanceadores de carga detrás de un firewall para proteger las máquinas. Todas estas soluciones deben ser implementadas en simultáneo ya que no se hace seguro un sistema con una puerta trasera obvia.