Caso 2

**Amenazas:**

1. Suplantación de usuarios en el sistema. Un atacante versado podría generar combinaciones de identificación hasta lograr emular lo que sabe el dueño real de la cuenta, accediendo con sus permisos al sistema. De concretarse esta amenaza, el atacante tendrá tantos permisos como el usuario, y si llegase a hacerlo para un *super user* (administrador) podría significar la pérdida de mucha información del fondo de pensiones.
2. Robo de datos almacenados en el sistema. Un atacante podría llegar a acceder a la base de datos sin necesidad de cuenta violando los sistemas de seguridad de la misma. En este caso, toda la información almacenada estaría comprometida para copiar. En este caso, los datos sensibles almacenados permitirían suplantaciones, chantajes y demás, dejando a los pensionados sin sustento.
3. Destrucción de la infraestructura de almacenamiento o borrado de datos. Si esta amenaza se concreta, se perdería información y se tendrá un sistema caído hasta la recuperación. En caso de no poder recuperarlos, el negocio está en riesgo por las cláusulas de cumplimiento que el gobierno impone a las compañías de pensiones.
4. Caída de la conexión del servidor principal. Si esto pasa no se puede prestar el servicio por el tiempo de recuperación, dejando el negocio de pensiones en pérdidas.
5. Interceptar las comunicaciones entre el servidor y un cliente. Si alguien intercepta las comunicaciones podría tener acceso a la información privada de un cliente, además de que hace decaer los tiempos de respuesta para las oficinas de pensiones.

**Vulnerabilidades:**

1. Contraseñas débiles y fáciles de encontrar con un *password-cracker* (ataque de fuerza bruta). Si no se implementan políticas estrictas con respecto a el espacio usable, se da pie a contraseñas fáciles como juan1 por la fácil recordación.
2. Algoritmos de cifrado vulnerables. En este caso se usan algoritmos DES y RC4 que ya no son considerados en la industria como seguros, por ende, una entidad gubernamental no debería usarlos
3. La información es guardada en un único servidor, lo que deja el sistema vulnerable a perdida de información. Sin réplicas, una caída del servidor principal inhabilita el sistema completo, dejando las consultas sin respuestas y las oficinas con la conocida respuesta de ¨no hay sistema¨.
4. No se implementa ningún control sobre la cantidad de peticiones hechas por un cliente lo que deja el servidor vulnerable a un ataque DOS. Sin un balanceador de carga configurado apropiadamente, un usuario con tiempo podría hacer peticiones hasta hacer caer el sistema.
5. Comunicaciones inseguras a través de internet. En ningún caso se enuncia si las comunicaciones van protegidas por HTTPS o a través de un VPN, por ende son susceptibles de ser interceptadas.

**Soluciones:**

1. Se podría implementar campañas de sensibilización acerca de la importancia de guardar de manera correcta las contraseñas, cómo hacerlo y como se puede ver afectado el sistema si hay incluso solo un usuario que no haga esto de manera correcta. Esto es importante ya que la mayoría de los usuarios no son conscientes de lo importante que puede llegar a ser mantener sus contraseñas secretas, ni de todo lo que pueden llegar a perder si alguien que sabe usarla la conoce. Así mismo, se les podría enseñar a los usuarios a generar contraseñas de buena calidad que sean difíciles de encontrar. Esto iría de la mano con la propuesta anterior, y se debe a que los usuarios del común no entienden cómo funcionan las contraseñas ni los *password-crackers* y no conocen qué es una buena contraseña y qué no. De nada sirve que los usuarios quieran tener buenas contraseñas y las guarden bien si no se les da el conocimiento necesario para generar buenas contraseñas. Además, no es un conocimiento complicado y les sirve en varios aspectos de su vida.
2. Se pueden implementar algoritmos de cifrado un poco más pesados en tiempo de computación pero más seguros. En este punto valdría la pena hacer un análisis detallado sobre la importancia de la confidencialidad de cada tramo de la comunicación y la importancia de una respuesta rápida. Ya que, algoritmos más seguros implican más tiempo de cálculo lo que vuelve al sistema más lento.
3. Se podría implementar un sistema de redundancia de información de tipo *back-up* que permita recuperar la información en caso de falla. De nuevo, esta estrategia requiere de un análisis profundo de la importancia de los datos. No necesariamente se quiere poder recuperar todos los datos en caso de falla y, además, hay que determinar qué tipos de fallas se van a considerar. Por ejemplo, ¿los datos son tan esenciales que se tendrán planes de contingencia ante fallas tan graves como la destrucción de toda la sede de la entidad? O, ¿solo tendremos en cuenta la posibilidad de que el servidor se dañe? Esto implica medidas muy diferentes y también costos muy diferentes. La primera opción requiere tener un respaldo constante en otra sede y la segunda solo tener un servidor de respaldo, lo cuál sería mucho más viable en términos monetarios (en especial para una entidad gubernamental cuyo presupuesto es controlado).
4. Se debería implementar en el protocolo de conexión un control sobre el número de peticiones hechas por un mismo usuario para evitar ataques DOS. Esto se puede hacer directamente en el código del protocolo al leer la IP del cliente y contar el número de peticiones hechas. Se debe establecer lo que es un número de peticiones normal y máximo. Al establecer esto el sistema quedaría protegido ante ataques DOS. Cabe resaltar que en una oficina con 10 equipos y 10 empleados atendiendo personas sobre sus pensiones, el máximo posible son 10 peticiones en 1 segundo.
5. Para resolver el problema de la conexión insegura entre las oficinas se puede montar un VPN sencillo que requiera autenticación del gerente de la oficina. Esto solo requiere configurar el *router* de cada oficina para conectarse al servidor principal.

Además, el sistema debería apegarse al estándar HTTPS que, hoy en día, cuesta muy poco implementar y mantener y le da bastante seguridad al sistema. Esta certificación podría incluso ser interna para que la entidad no tenga que pagar a terceros.