Caso 2

**Amenazas:**

1. Suplantación de usuarios. Si esta amenaza se concreta, se podría acceder a la información privada del usuario y/o a la información sensible de la empresa dependiendo de los permisos del usuario.
2. Robo de datos almacenaos en el sistema. De nuevo si esta amenaza se concreta un usuario malicioso tendría acceso a la información sensible de la empresa.
3. Destrucción de la infraestructura de almacenamiento o borrado de datos. Si esta amenaza se concreta, se perdería información.
4. Caída de la conexión del servidor principal. Si esto pasa no se puede prestar el servicio.
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.

**Vulnerabilidades:**

1. Contraseñas débiles y fáciles de encontrar con un “password-craker”.
2. Algoritmos de cifrado vulnerables.
3. La información es guardada en un único servidor, lo que deja el sistema vulnerable a perdida de información.
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.

**Soluciones:**

1. Se podría implementar campañas de sensibilización acerca de la importancia de guardar de manera correcta las contraseñas, como hacerlo y como se puede ver afectado 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 deben saber 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.
2. Se pueden implementar algoritmos de cifrado un poco más pesados pero que son 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.
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.

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 cifrado 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.