Santiago Cala Gómez – 201729218

Sergio Canales Martínez – 201729241

**Caso 2: Análisis y Entendimiento del Problema**

1. De acuerdo con el enunciado, “el portal web permite a los afiliados consultar su información en línea y solicitar reportes de su estado de cuenta” y con esta información es posible tener en cuenta los datos que posiblemente son importantes en este proceso. Los clientes que acceden al sistema desde un navegador instalado en sus computadores ingresan los datos de su cuenta (como la cédula y contraseña) que deben ser protegidos en el canal de comunicación con el servidor. Cuando un usuario usa a Colpensiones, espera que su información esté guardada de manera segura y por eso cuando alguien obtiene acceso a la cédula y la contraseña puede también ver toda la información y solicitar reportes del estado de cuenta. Ya en términos de los servidores de la empresa, es fundamental que estos estén bien protegidos porque de estos dependen los últimos años de vida de miles de personas. Si alguien accede a esta información en modo lectura puede usarla para fines delincuenciales y puede poner en riesgo la vida del cliente y aún peor, si alguien lograra acceder a los datos en modo escritura puede confundir a la empresa en términos de cuánto es el valor real de la pensión del cliente.
2. Cuatro posibles vulnerabilidades que tiene el sistema de Colpensiones podrían ser:   
   1. Dado que los empleados que trabajan en la oficina principal de la entidad están conectados a una subred interna de la organización, esta seguramente no tiene todos los mecanismos de protección que tiene la parte que se conecta con las entidades externas. Esto puede ser una vulnerabilidad ya que muchas veces se asume la buena fe y la responsabilidad de las personas que trabajan en una empresa, pero si alguien de la red interna quisiera acceder a la información importante le puede quedar más fácil.
   2. Gracias a que los usuarios pueden acceder a su información simplemente con su cédula y con su contraseña, también puede ser un riesgo ya que muchas personas que son usuarias de la plataforma no necesariamente son tan cuidadosas con ese tipo de información. Adicionalmente la cédula es un documento público al que en realidad mucha gente puede acceder, entonces para una persona con malas intenciones, lo único que tiene que hacer es conseguirse la contraseña del usuario y ya casi que automáticamente tiene acceso a toda la información y se le abre la posibilidad de solicitar reportes del estado de la cuenta. Para esta parte también es importante entender que muchos usuarios reutilizan sus contraseñas y si alguien consiguiera acceso a la contraseña de un usuario de otra plataforma es más propenso a poder acceder a este sistema.
   3. Como se había mencionado en el numeral anterior, el hecho de que la empresa cuente con múltiples servidores que almacenan la misma información y que cuente con un *backup* de procesamiento y almacenamiento ayuda mucho a distribuir el riesgo de pérdida de la información. Sin embargo, si se realizan ataques exitosos al servidor principal y al respaldo corren un riesgo muy alto ya que es información fundamental para la empresa y de esta depende el funcionamiento de ella. Para esta vulnerabilidad es importante también entender que por más de que los datos tengan un *firewall* adecuadamente configurado, no es 100% efectivo en el control de ataques ya que un ataque fuerte puede conseguir sobrepasarlo.
   4. Finalmente los *backups* de la empresa tienen que estar almacenados en algún lugar en físico. Gracias a esto, es importante entender que cualquier ataque netamente físico al sitio donde se esté almacenando esta información puede resultar en la pérdida de la información. Desastres naturales, incendios y otros factores externos pueden jugar un rol en esta vulnerabilidad. Inclusive si los datos están almacenados en “la nube”, los servidores de los prestadores de este servicio también pueden correr este riesgo, que a pesar de ser considerado bajo, es real y existe.