**Caso de Estudio 2 – Canales Seguros**

**Logística y Seguridad Aeroportuaria**

Felipe Guzmán Avendaño – 201813791 y Nicolás Munar González - 201814383

**A. Análisis y Entendimiento del Problema**

1. Primero hay que identificar los usuarios que están en el sistema los cuales son Agente y Supervisor en campo. De estos usuarios, se pide la geolocalización del agente, la hora de llegada y la hora de salida del lugar de trabajo. Además, los usuarios deben estar autenticados dentro del sistema con sus credenciales del negocio sin embargo de esta autenticación es encargado otro sistema. Por lo tanto, para este sistema deben ser protegidos todos los datos pues son sensibles para el funcionamiento del negocio y para la información personal de los usuarios.

2. -Los requerimientos de seguridad que necesita la geolocalización es confidencialidad, para que los datos solo puedan ser leídos por el supervisor previsto, integridad pues solo el agente debe escribir o modificar su localización, y disponibilidad para que tanto el agente pueda enviar su geolocalización como el Supervisor para verla y registrar el ingreso correctamente. En caso de no implementar estos confidencialidad, la geolocalización del agente se vería vulnerada y por ello su ubicación y privacidad; si no se garantiza la integridad otros agentes podrían modificar la localización y no garantiza la verdadera ubicación del agente deseado; y finalmente la disponibilidad para que en cualquier momento pueda ser accedida esa información como comprobante del trabajo y ubicación real del agente por parte del supervisor.

-En el caso de la hora de llegada y salida, debe tener los requerimientos de integridad para que nadie sea capaz de modificar la hora de llegada o salida, solo el supervisor, así como debe tener disponibilidad para poder acceder a la hora y entregar resultados de acuerdo al tiempo adecuado cuando sea necesario. Si no fuera garantizada la integridad, un agente u otro supervisor puede modificar alguna de las horas de llegadas o salidas y provocar un problema con el agente o los datos registrados; asimismo debe tener disponibilidad pues la hora de llegada debe ser registrada de acuerdo con la hora en el momento, así como poder registrar un agente correctamente en el instante que sea necesario.

3. a. Una de las principales vulnerabilidades es cuando se presente un acceso para registrar el geolocalización la red, el punto de acceso, puede no ser seguro, y por tanto al tener acceso a los datos de entrada a la empresa y brindar información confidencial a través de la red.

b. Una vulnerabilidad en estos sistemas es el almacenamiento de la información, ya que en esta, al usar Oracle DB, puede estar vulnerable a una inyección SQL directamente en la base de datos y robar la información tanto corporativa como de los individuos relacionados con la empresa.

c. En el caso de cada usuario, se tiene la vulnerabilidad que las cuentas puedan ser accedidas al tener una contraseña reutilizada, sencilla o fácilmente adivinable por cada trabajador, especialmente los que tengan acceso a información más sensible que ponen en peligro la seguridad de los servidores.

d. Ya que el sistema implementa el control de acceso al sistema operativo puede tener la vulnerabilidad de desbordamiento de buffer al tener el peligro de almacenar bytes sobrantes en otras zonas de memoria, por lo cual pueden acceder a código con permisos de administrador. Esto puede pasar si no se controla la cantidad de datos en el buffer en el sistema de Time & Attendance