**Caso de Estudio 2 – Canales Seguros**

*Sebastián Santos Bautista (201816848), Nicolás Urrego Sandoval (201815544)*

1. **Datos manejados por el sistema *Time & Attendance* que deben ser protegidos**
   1. Geolocalización de los agentes de campo
   2. Fecha y hora de llegada y de salida
   3. Lista de agentes de campo a cargo de cada supervisor
   4. Información de autenticación.
2. **Requerimientos de seguridad**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dato** | **Requerimiento de seguridad** | **Explicación** | **Efectos del no cumplimiento** |
| A | Confidencialidad | Es necesario para evitar que personal no autorizado o entes externos acceda a la información de los agentes. | Se compromete la privacidad y seguridad de los agentes de campo. |
| Disponibilidad | Es necesario ya que los supervisores deben poder acceder a la información de la ubicación de los agentes en tiempo real. | Se incumple una de las funcionalidades que debe prestar el sistema. Adicionalmente, no es posible cumplir con el requerimiento de confidencialidad. |
| Integridad | Es necesario debido a la importancia de verificar correctamente la ubicación del agente de campo al iniciar y terminar su turno. | Almacenamiento de información errónea sobre la ubicación de los agentes, hecho que puede generar repercusiones negativas en el funcionamiento del negocio. |
| B | Confidencialidad | Es necesario para no comprometer la privacidad los agentes de campo. | Personal no autorizado o entes externos pueden acceder a datos protegidos de los agentes. |
| Integridad | Es necesario para que la información recolectada por la aplicación pueda utilizarse de forma significativa para el negocio | Se recolecta información que no refleja el mundo real, por lo que ciertas operaciones (como el cálculo de las horas trabajadas) se realizarán de forma incoherente y el negocio se verá afectado. |
| C | Confidencialidad | Garantiza que solo el supervisor asignado pueda acceder a la información de algún agente de campo a su cargo. | Se compromete la información privada de los agentes de campo. Especialmente, la información a la que tenga acceso el supervisor. |
| Disponibilidad | Es necesario ya que el supervisor debe poder acceder a los datos de cualquiera de sus agentes en tiempo real. | No se cumple la funcionalidad de control en tiempo real de la aplicación. |
| Integridad | Es necesario para poder relacionar, guardar y acceder de forma adecuada a la información recolectada. | Puede haber perdida de datos, lo cual se traduce en modelamiento inadecuado del negocio. |
| D | Confidencialidad | Garantiza que la información de autenticación de cada usuario no se vea comprometida. | Usuarios internos o externos podrían tener acceso a datos o funcionalidades a los que no deberían tener acceso. |
| Disponibilidad | Es necesario para que los usuarios del sistema puedan autenticarse en todo momento. | Se afectaría la confidencialidad del sistema al comprometer el acceso de los supervisores a información protegida de los agentes de campo a su cargo. Adicionalmente, las perdidas de disponibilidad dificultan la identificación y corrección de ataques. |
| Integridad | Es de gran importancia que la información de autenticación no se vea alterada para garantizar el “inicio de sesión” de cada usuario. | Se comprometería el acceso que tienen los usuarios a la aplicación. Se podrán presentar situaciones de suplantación y/o acceso a información indebidamente. |

1. **Vulnerabilidades técnicas y de procesos**
   1. **Espionaje:** Teniendo en cuenta que el requerimiento de confidencialidad es clave en la protección de los datos identificados, una vulnerabilidad potencial es el espionaje de la información enviada y recibida por los usuarios del sistema. Luego, se identifica especialmente el impacto que podría tener el espionaje sobre datos como la geolocalización de los agentes de campo y la información de autenticación de los usuarios. Por ejemplo, la geolocalización de los agentes de campo podría dar lugar a uso indebido a esta información y comprometer su seguridad personal y la información de autenticación podría ser utilizada para perpetuar ataques a la organización.
   2. **Incoherencia:** Considerando la importancia del requerimiento de integridad se identifica que la falta de coherencia de los datos es una vulnerabilidad potencial. Uno de los impactos de esta se ve evidenciado al considerar un escenario donde la fecha de inicio de un agente no se guarde íntegramente, si el dato se utiliza para calcular las horas trabajadas para dicho agente se contará una cantidad diferente a la cantidad real, lo cual puede llevar a pérdidas económicas o demandas laborales.
   3. **Repudio:** El incumplimiento de la integridad de algunos datos (geolocalización, fecha y hora del inicio y fin del turno) puede permitir que se den situaciones de repudio, lo cual se debe considerar como vulnerabilidad debido a sus potenciales consecuencias. Por ejemplo, se podría presentar un caso en el que se modifique la hora de inicio de algún agente de campo y, posteriormente, dicho agente niegue haber realizado dicha acción. En este caso, esto podría dar lugar a accesos indebidos a funcionalidades y/o a información y a potenciales ataques al sistema.
   4. **Concurrencia:** A partir de la descripción de la aplicación es adecuado considerar la ejecución del sistema en un entorno deteriorado debido a problemas con el manejo de la concurrencia como una vulnerabilidad; como el sistema tiene un uso diario y es de prioridad alta, un rendimiento no optimo tiene serias implicaciones para el negocio
2. **Comentarios sobre la aplicación**

* Se utiliza el puerto 3400.
* Por consola se muestra los pasos que realiza el cliente.
* El idUsuario se solicita por consola y debe ser insertado por este medio en una única línea.