Infraestructura Computacional

Integrante 1: Lina Paola Cardozo Garzón **Código:** 201712455
Integrante 2: Andrés Ortiz Gómez **Código:** 201727662

Caso 2

A. Análisis y Entendimiento del Problema

1. Identifique los datos que maneja el sistema Time & Attendance y que deben ser protegidos.

   Los datos que maneja el sistema Time & Attendance son el identificador, la geolocalización de cada usuario (que en este caso es un agente de campo), así como su hora de llegada y salida.

   En cuanto a los datos que se deben proteger, es recomendable que se protejan todos. Por un lado, el identificador contiene la información de cada agente, por lo que solamente el supervisor que esté a cargo de determinado agente debe poder ser el único capaz de ver su información. La identificación del agente puede otorgarle al supervisor acceso a información confidencial, como la identidad del agente, las credenciales de la aplicación, etc. Es importante que la identificación esté protegida para garantizar que la información personal del agente se mantenga privada. De igual forma, la geolocalización, hora de llegada y hora de salida de los agentes son datos que también deben ser protegidos. Dado que la compañía se encarga de verificar que no se realicen actos ilícitos que interfieran con las operaciones de los clientes, es necesario que esta información se encuentre oculta para personas que no están autorizadas a acceder a ella.

2. Identifique los requerimientos de seguridad para cada uno de los datos del punto anterior. Explique su respuesta en cada caso y responda la pregunta: si no se garantiza ese requerimiento para ese dato ¿cómo podría afectar a la entidad?

   Para los datos del agente que se deben proteger (el identificador, la geolocalización y su hora de llegada y salida) se deben cumplir los siguientes requerimientos de seguridad:

   - **Confidencialidad:** Para cada agente, solamente su supervisor encargado debe ser autorizado para ver su información personal, esto es, su identificador, geolocalización, hora de llegada y hora de salida.

Integrante 1: Lina Paola Cardozo Garzón **Código:** 201712455
Integrante 2: Andrés Ortiz Gómez **Código:** 201727662

En caso de que la identificación, la geolocalización o la hora de llegada o salida de un agente se hicieran públicas debido a algún tipo de filtración de datos, potenciales secuestradores u otros terceros interesados en interferir con la seguridad de una operación podrían ser capaces de planear un ataque para robar mercancía, dañar productos o realizar cualquier otra actividad ilegal que pudiera causar una pérdida para los clientes o incluso un riesgo para su vida o la de los trabajadores de la empresa.

- **Integridad:** Para este sistema es importante garantizar que solo los usuarios autorizados puedan modificar información, pues de esta manera se puede asegurar que, por ejemplo, solamente los agentes (o sus supervisores si los agentes no poseen smartphone) puedan cambiar su información, es decir, registrar su turno en el sistema para así reportarse en el lugar de trabajo. Si no se garantiza este requerimiento, podría pasar que, por ejemplo, un agente altere datos como su geolocalización o su hora de llegada o salida para hacer creer a su supervisor que sí estuvo trabajando cuando en realidad no lo estaba haciendo.

- **Disponibilidad:** Es fundamental garantizar este requerimiento, dado que el sistema Time & Attendance debe estar disponible todo el tiempo para que los agentes de campo siempre puedan registrar su información relacionada con su geolocalización, hora de llegada y hora de salida del lugar de trabajo. De igual forma, los supervisores deben poder ver en tiempo real la información de los agentes que tienen a cargo.

  Si no se garantiza este requerimiento, los supervisores no podrían llevar un control adecuado de sus agentes a cargo, lo cual causaría posibles pérdidas para la empresa, en la medida en que los supervisores no sabrían si los agentes están cumpliendo a cabalidad con sus jornadas laborales y no se darían cuenta si, por ejemplo, algún agente no va a trabajar o no trabaja la cantidad de horas que debe.

- **Autenticación:** Este requerimiento es importante para el sistema Time & Attendance, en la medida en que se debe garantizar que cada agente que se reporte en el sistema sea realmente quien dice ser, es decir que se encuentre registrado. Además, de acuerdo con el enunciado del caso, los servidores solamente ejecutan transacciones para usuarios autenticados, de acuerdo con los permisos asignados, por lo que en este caso el solamente se almacenarán los datos

como geolocalización, hora de llegada y hora de salida de un agente si este está autenticado (lo cual significa que inició sesión) en el sistema. De igual forma, se debe verificar que los supervisores sean realmente quienes dicen ser, pues solamente ellos pueden ver la información de sus agentes a cargo, por lo que también deben estar autenticados en el sistema para poder acceder a esos datos. Si no se garantiza este requerimiento, cualquiera podría ver la información de los agentes o de los supervisores, rompiendo la confidencialidad del sistema.

- **No repudio:** Este requerimiento es importante para el sistema, en la medida en que se debe garantizar que si llega a ocurrir algún suceso inusual durante una hora en la que un agente o supervisor se encontraba en su lugar de trabajo, este no pueda negar que efectivamente estuvo en el lugar y momento indicados. Si no se garantiza este requerimiento, podría pasar que en la empresa suceda algo peligroso o sospechoso (como lo puede ser un robo, por ejemplo), y que no se sepa quién ejecutó la acción, pues el culpable podría mentir sobre si estuvo o no en su lugar de trabajo en el momento en el que sucedieron los hechos. Al garantizar este requerimiento, se garantiza el cumplimiento de la misión de la empresa, que es prevenir actos de interferencia ilícita en la aviación civil.

3. Identifique cuatro vulnerabilidades de este sistema, teniendo en cuenta únicamente aspectos técnicos o de procesos (no organizacionales). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento y procesamiento de los datos. Explique su respuesta en cada caso.

   Las vulnerabilidades encontradas que podrían convertirse en puntos de ataque son las siguientes:

   a. **Falta de entrenamiento técnico a empleados:** Dado que los agentes al registrarse y los supervisores al registrar a sus agentes a cargo en el sistema usarán principalmente una aplicación que se encuentra en un smartphone, se podría asumir que los agentes y supervisores deben tener algún tipo de entrenamiento técnico para así registrarse o registrar a otros (según sea el caso) correctamente. Sin embargo, si los empleados no reciben el entrenamiento suficiente o no toman las precauciones de seguridad adecuadas, esto puede comprometer la seguridad de ellos mismos y de la empresa. Por ejemplo, si el smartphone que un agente está usando tiene el Bluetooth encendido, potenciales

atacantes podrían aprovecharse de esto para emplear una variedad de ataques. Algunas de estas vulnerabilidades podrían ser explotadas para obtener información sensible que el agente posea en su teléfono, o para hacer que la persona sea víctima de un ataques DDoS, causando que el agente no pueda actualizar su ubicación actual. La falta de entrenamiento técnico adecuado es una gran vulnerabilidad que podría tener la empresa, pues es la puerta de entrada a varias amenazas de seguridad. Para prevenir algunas de estas amenazas, la compañía debe tomar medidas para capacitar a sus agentes y supervisores en seguridad, especialmente en vulnerabilidades que deben evitar, amenazas y ciberataques.

b. **Elevación de privilegios de forma descuidada:** Es importante que existan diferentes tipos de cuentas en el sistema que permitan el monitoreo de los agentes y supervisores, y de las operaciones que realizan cada día. Si el sistema no asigna ciertos privilegios correctamente, esto generaría graves consecuencias que pueden llegar hasta permitir que alguien que no debe, por ejemplo un agente, posea permisos de superusuario, dándole la posibilidad de que ejecute comando a nivel de administrador. Esto puede ser un problema pues si se diera una situación en la que, por ejemplo, un agente perdiera su smartphone, cualquier persona sería capaz de acceder a la información de los demás agentes e incluso de los supervisores, poniendo la operación de la empresa en peligro ante posibles ataques maliciosos. Administrando de forma apropiada los privilegios de administrador (y en general, los privilegios asignados a cada usuario del sistema), esta vulnerabilidad puede ser mitigada.

c. **Uso de claves débiles para registrarse en el sistema por parte de agentes o supervisores:** Esta vulnerabilidad es grave pues si los usuarios poseen claves muy fáciles de descubrir, un atacante podría, por ejemplo, acceder a la cuenta de un supervisor y ver todos los agentes que tiene a cargo junto con su información (identificación, geolocalización, hora de llegada, hora de salida), lo cual podría utilizar para vulnerar la seguridad en los puntos donde se encuentren ubicados esos agentes y ejecutar actos de interferencia ilícita que perjudiquen a la empresa o a algunas de las empresas de sus clientes a los cuales les presta seguridad aérea tales como, transportistas, aeropuertos, empresas de servicios terrestres, entre otros.

Infraestructura Computacional

Integrante 1: Lina Paola Cardozo Garzón **Código:** 201712455
Integrante 2: Andrés Ortiz Gómez **Código:** 201727662

d. **Falta de actualización de la base de datos por parte de la empresa:** Es importante que la empresa se preocupe por actualizar con cierta regularidad la base de datos de Time & Attendance, no solamente con respecto a la información que contiene, que es la de todos los agentes y supervisores de la empresa, sino también con respecto al software que utiliza. En el caso de esta compañía, se utiliza para el sistema Time & Attendance la base de datos de Oracle. No actualizar continuamente la base de datos podría generar graves problemas de seguridad para el sistema, pues las actualizaciones generalmente corrigen errores o vulnerabilidades que las versiones previas de las bases de datos tenían, y usualmente los atacantes buscan aprovechar los huecos de seguridad de sistemas no actualizados para atacarlos. Esto sería muy grave para Time & Attendance, en la medida en que este es un sistema que guarda información sensible de muchas personas, como su identificación, geolocalización y hora de llegada y salida, por lo que si se tiene acceso a todos estos datos, se pondría en peligro no solo la integridad de los dueños de esos datos (que son los agentes y supervisores), sino también la de la empresa y sus clientes, pues alguien inescrupuloso podría aprovechar esta información para vulnerar la seguridad que presta la compañía y cometer algún acto ilegal.