Caso 2

Infraestructura computacional.

Tabla de contenido

[1. Análisis y entendimiento del problema 1](#_Toc447924577)

[1.1. Amenazas 1](#_Toc447924578)

[1.1.1. Un empleado autorizado hace cambio de la información de Time & Attendance 1](#_Toc447924579)

[1.1.2. Una aplicación móvil envía datos falsos 1](#_Toc447924580)

[1.1.3. Un atacante utiliza Time & Attendance para modificar el código fuente del servidor dos 1](#_Toc447924581)

[1.1.4. Ataque DoS al servicio Time & Attendance 2](#_Toc447924582)

[1.2. Vulnerabilidades 2](#_Toc447924583)

[1.2.1. Supervisor de campo o agente no cambia la contraseña dada por defecto de su cuenta 2](#_Toc447924584)

[1.2.2. Un agente de campo recibe más privilegios de los necesarios 2](#_Toc447924585)

[1.2.3. Un supervisor recibe más privilegios de los necesarios 2](#_Toc447924586)

# Análisis y entendimiento del problema

# Amenazas

# Un empleado autorizado hace cambio de la información de Time & Attendance

Si un usuario autorizado cambia los datos que se encuentran en el segundo servidor especialmente los de time & Attendance podría eventualmente modificar las horas y coordenadas de los trabajadores haciendo que algunos sean despedidos injustamente u otros pagados sin hacer nada. Si esta amenaza de consolida el servicio de información de Time & Attendance no ofrecería ni integridad, ni confidencialidad ni no repudio ni autenticación de fuente ni destino. Es decir la aplicación de time & Attendance no serviria.

# Una aplicación móvil envía datos falsos

Un atacante es capaz de cambiar el código fuente de su aplicación móvil para que esta modifique los datos antes de ingresarlos a memoria. Si esta amenaza se consolida sería catastrófico para todo el sistema puesto que no se tendría confiabilidad en los datos reportados en la aplicación Time & Attendance

# Un atacante utiliza Time & Attendance para modificar el código fuente del servidor dos

Un atacante es capaz de modificar el código fuente de la aplicación time & Attendance para acceder al sistema operativo del servidor dos. Si esta amenaza se consolida todos los servicios provistos por el servidor no serían confiables y la empresa tendría problemas puesto que no sabrían si sus agentes y supervisores de campo están haciendo su trabajo

# Ataque DoS al servicio Time & Attendance

Un atacante podría hacer ataques de negación de servicio bloqueado los servicios de Time & Attendance. Si esta amenaza se consolida los agentes y supervisores de campo no tendrán forma de reportarse, además eventualmente el procesamiento en el servidor dos seria solo de peticiones de Time & Attendance por lo cual el servicio de correo electrónico también podria verse negado.

# Vulnerabilidades

# Supervisor de campo o agente no cambia la contraseña dada por defecto de su cuenta

Al recibir la aplicación móvil el agente o supervisor de campo no cambian su contraseña dada por defecto. Esto causa que

# Un agente de campo recibe más privilegios de los necesarios

Un agente de campo solo debe poder reportar su posición y no más. Si un agente de campo puede consultar las posiciones y horas de otros agentes y supervisores eventualmente podría hacer una negación de la consulta de estos servicios.

# Un supervisor recibe más privilegios de los necesarios

Un agente supervisor solo debe poder reportar la posición de sus subordinados y la propia. Si este puede consultar las posiciones y fechas de otros agentes y supervisores y modificarlos eventualmente podría hacer que la integridad del sistema se pierda además de poder hacer una negación de servicios.