II.

a. En términos de la transferencia de datos, a Novasoft: Proponemos, hacer una transición mucho más brusca, dado que la naturaleza paulatina actual de dicha transferencia es lo que la hace tan vulnerable a diferentes ataques. Esta medida de mitigación se haría por medio de un esfuerzo enfocado sobre la transferencia, para así hacerla de manera voluminosa y lo más rápido posible.
b. Por otro lado, para mitigar lo más posible ataque posibles sobre la transferencia a las 10pm entre las versiones online y offline de Novasoft, se debe poner en práctica un sistema de seguridad extremadamente robusto, así como flexibilizar las horas de integración, dada la naturaleza del internet, ya que esta restricción de tiempo podría llegar a ser nociva a la hora de hacer que la información sea congruente entre si a la hora de hacer una concatenación de la misma.
c. Ahora bien, para evitar la adulteración y suplantación a la hora de usar el sistema de time & attendance, recomendamos migrar de una aplicación de smartphone, a algún tipo de activo fijo que se mantenga en la compañía, para así mitigar la posibi9lidad de que alguien pueda adulterar la geo localización del sistema, ya que la responsabilidad de dicha seguridad pasaría a ser parte de la empresa. Por otro también deberían implementarse sistemas para evitar suplantación, siendo que algún individuo externo (o interno, mas no autorizado) marque su llegada en lugar del individuo en cuestión.
d. Finalmente para evitar casos de suplantación promovida por la empresa, hemos de propones seguir la solución anotada en el punto anterior, dado que esto también, por su propia naturaleza evitaría de manera absoluta la posibilidad de que algún individuo este incapacitado usar el sistema de la compañía, lo cual mejoraría substancialmente el mantenimiento del sistema de time & attendance.