# Infracomp Caso II

I.

1. En términos de Novasoft Online, es menester proteger ciertos grupos de datos sensibles de la compañía:

a. En primer lugar, dada su naturaleza financiera, la aplicación Novasoft online debe proteger los datos financieros de la compañía, esta protección debe ser enfocada a evitar suplantación y la adulteración, y dependiendo de determinada información incluso llegando a proteger del espionaje (dicha dependencia se debe a que gran parte de la información financiera de una compañía es conocimiento público.

b. Más allá de esto, la aplicación de be ser capaz de proteger las credenciales y la información de sus usuarios, dada la alta categoría jerárquica que estos demuestran dentro de la compañía. Esta información podría llegar a ser extremadamente sensible, dependiendo de la estructura interna de la compañía, aunque aún en el mejor de los casos es un escenario, cuando menos, indeseable. Esta información debe ser protegida del espionaje, ya que tanto el repudio como la adulteración y la suplantación tendrían consecuencias comparativamente mínimas sobre la infraestructura de la empresa.

En caso de que algún agente externo logre accede a los datos, las consecuencias serían las siguientes:

a. Dado que algún agente externo lograra accede a la información financiera de la compañía, podría alterar a voluntad la información financiera de la misma, indicando así indicadores y medidores erróneos a la organización. Esta información errónea seria entonces tomada en cuenta a la hora de hacer decisiones, las cuales estarían, por su misma naturaleza, alteradas.
Por otro lado, si cierta información financiera confidencial estuviera en manos de algún agente externo, este podría enterarse de esta información para hacer con ella, lo que su voluntad dictase, lo cual sería un escenario no muy cómodo para la compañía dada la naturaleza de esta información.

b. En caso de que algún agente externo lograra adquirir las credenciales de alguno de los usuarios, este podrían ingresar libremente al sistema financiero de la empresa, aun mas, si las credenciales son las mismas a través de todos los servidores de la compañía el daño seria aun de mayores proporciones. Aun en el mejor de los casos sin embargo, se repiten todos los riesgos asociados a la información financiera de la empresa recién presentados. Más seria aún más complicado de rastrear.

II. Hemos encontrado además, ciertas vulnerabilidades dentro del sistema descrito:

a. En términos del primer Servidor, se nos ha informado que la compañía está en medio de un proceso de migración de las bases de datos en Novasoft a las bases de datos de Open ERP. Dada la naturaleza de esta migración se espera una gran transferencia de datos entre estas dos bases, las cuales deben tener infraestructuras de seguridad extremadamente robustas, para evitar los problemas relacionados ya explicados en el primer punto, con relación a Novasoft Online. Esta línea de comunicación sin embargo, no tiene un esquema de seguridad explicito descrito, y dada la existencia de dos bases de datos en proceso de replicarse, debemos entender que esta línea de transferencia está expuesta a potenciales ataques de espionajes, y adulteración. En términos de almacenamiento, debemos también entender que al duplicar el número de bases de datos que reciben la información, así mismo se duplica cualquier riesgo asociado a la misma.

b. Por otro lado también hemos notado que en el primer servidor se halla una línea de transferencia policefálica la cual existe en la conexión que se establece entre los Novasoft Offline y Novasoft Online. Esta transferencia es vulnerable dada su naturaleza masiva, gracias a lo cual, la infraestructura de seguridad se verá ligada a extender su alcance a varias líneas de comunicación. Dada esta vulnerabilidad, hemos de asumir un posible ataque de naturaleza de repudio, adulteración o suplantación.

c. También hemos analizado el segundo servidor, desde el cual hemos podido derivar varias vulnerabilidades. Siendo una de los problemas más evidentes, la posibilidad de suplantación a la hora de utilizar el sistema de time & attendance. Dado que el sistema utiliza una aplicación de smartphone, es fácil imaginar algún tipo de adulteración sobre la geo localización del celular, lo cual llevaría a un caso de adulteración de la información desde el puesto interior de la compañía.

d. Por otro lado, aun no se ha mencionado el elefante blanco, que resulta ser la mecánica sobre el uso de la aplicación por quienes no pueden acceder, o no poseen un Smartphone, dado que este paso en la operación, promueve la suplantación, puesto que soluciona el problema por medio de la misma, lo cual abre la puertas a una gran cantidad de riesgos asociados con la confiabilidad de los “jefes” en la empresa.

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.