**Caso 2**

**Logística y Seguridad Aeroportuaria**

**Nombres:**

Juan Camilo Sanguino P.

Amilkar Eslava G.

Juan Camilo Bojaca.

Contenido

[Novasoft financiero en línea: 1](#_Toc528257871)

[Login del usuario: 2](#_Toc528257872)

[Datos del cliente: 2](#_Toc528257873)

[Información bancaria: 2](#_Toc528257874)

[Vulnerabilidades y posibles soluciones: 2](#_Toc528257875)

[Uso de algoritmos propios de cifrado: 2](#_Toc528257876)

[Pasar los algoritmos de cifrado a usar: 2](#_Toc528257877)

[Seguridad en a la hora de integración 3](#_Toc528257878)

[Copias o servidores de respaldo 3](#_Toc528257879)

# Novasoft financiero en línea:

Según las funciones financieras que suple Navasoft hay ciertos datos que se deben mantener seguros ya que su mal uso el ser expuestos a terceros podría llevar graves consecuencias tanto económicas como legales para la empresa. Teniendo en cuenta lo anterior se definieron como los datos más importantes o relevantes a la hora de asegurar los siguientes:

## Login del usuario:

Debido a que una persona que posea la cuenta de un usuario administrador poseerá la autentificación y, por tanto, los permisos para ejecutar diferentes transacciones. Lo cual, le permite modificar y alterar el estado financiero de la empresa.

## Datos del cliente:

Si una persona es capaz de intervenir la comunicación entre Navasoft y los clientes pondrá apoderarse de la identidad del cliente frente al sistema. Por lo cual, podrá pedir diferentes tipos de transacciones haciéndose pasar el cliente. Este problema puede acarrear consecuencias legales para Navasoft.

## Información bancaria:

Exponer la información bancaria como cuentas y contraseñas respectivamente, podría tener un gran impacto en la liquidez de la empresa, proporcionando perdidas en estas. Por otro lado, estas podrían ser usadas para actividades ilícitas como lavado de activos, entre otros.

# Vulnerabilidades y posibles soluciones:

Teniendo en cuenta el contexto dado del caso y el algoritmo implementado se fijaron ciertas vulnerabilidades que el sistema posee, junto con ellas se ha planteado su respectiva solución

## Uso de algoritmos propios de cifrado:

Al ser usar algoritmos de cifrados propios no se puede tener confianza de ellos, ya que no han sido puestos a prueba en la vida real y no se conoce el grado de seguridad que estos proporcionan.

Por ello, es aconsejable usar algoritmos de cifrado ya probados y actualmente utilizados. Ya que estos a diferencia de los algoritmos propios ya han sido probados en ejecución

## Pasar los algoritmos de cifrado a usar:

Al transportar los algoritmos de cifrados a usar sin ningún tipo de protección, el mensaje puede ser interceptado y la persona que realizó dicha intercepción podrá posteriormente cifrar y descifrar la información que el cliente y el servidor se envían.

Por ello, es aconsejable bien sea acordar previamente que algoritmos usar y que estos sean estándar o en el momento de mandar dichos algoritmos cifrarlos con las llaves respectivamente.

## Seguridad en a la hora de integración

Como se debe realizar una integración de los datos, la cual consiste en enviar la información a un servidor centralizado, la información que viaja es sensible a que se vea afectada su integración y seguridad de estos. Ya que, en el transcurso de la información esta puede ser objetivo de ataques. Como consecuencia, al momento de integrar la información esta puede tener errores o registros falsos, lo cual puede impactar el reporte de finanzas de la empresa y con ellos puede acarrear problemas como fallos a la hora de realzar cálculos, como el del impuesto, o perdidas debido a ingresos que nunca fueron efectivos.

Por ello, se recomienda que la información al ser integrada se vea sumergida en un proceso de cifrado, posiblemente pasándola por unos algoritmos como el hash y luego usando las llaves públicas del receptor para cifrarlas.

## Copias o servidores de respaldo

Al ser el destino final un servidor centralizado, este podría ser objeto de un ataque de carga, en el cual se busca mandar solicitudes al servidor hasta que este caiga. La caída de este podría causar la perdía del sistema.

Por ello, es necesario tener un servidor de respaldo o copias de seguridad con el fin que dado un ataque en el que toque desmontar el servidor, inmediatamente se pueda subir uno nuevo que contenga la información y las instrucciones para el funcionamiento adecuado del sistema. Esto con el fin de perder la disponibilidad de 24 hora a la cual debe estar sometido