**UNIVERSIDAD DE LOS ANDES**

**DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN**

**Caso 2 ‐ ISIS 2203 ‐ Infraestructura Computacional 2015-20**

**Profesor**: Rafael Gómez

**Profesora**: Sandra Rueda

|  |  |  |  |
| --- | --- | --- | --- |
| **NOMBRE** | **CÓDIGO** | **LOGIN** | **ENTREGA SICUA** |
| Anamaría Irmgard Mojica Hanke | 201316580 | ai.mojica10 |  |
| Claudia Daniela Bedoya Motta | 201211241 | cd.bedoya212 |  |

Caso de Estudio – Canales Seguros

Sistema de Gestión Empresarial y Operativa de una Compañía Transportadora

Tabla de Contenidos

[Introducción 2](#_Toc432442255)

[Objetivos 2](#_Toc432442256)

[Análisis y Entendimiento del Problema 2](#_Toc432442257)

[Propuesta de Soluciones 3](#_Toc432442258)

[Implementación del Prototipo 3](#_Toc432442259)

[Referencias 3](#_Toc432442260)

[Imágenes 3](#_Toc432442261)

# Introducción

En este documento, se resolverá el literal A y B del enunciado del caso 2. Para esto se debe tener en cuenta que:

Las principales tareas del sistema son: la recepción de órdenes de recogida, gestión de rutas, rastreo de unidades de distribución y paquetes, y gestión administrativa contable de recursos y de clientes.

Con lo cual surgen distintos problemas de seguridad para ciertas transacciones a nivel de: transmisión, procesamiento y almacenaje de datos. Entonces, en consecuencia, es necesario evaluar los riesgos y determinar medidas para mitigar los problemas detectados.

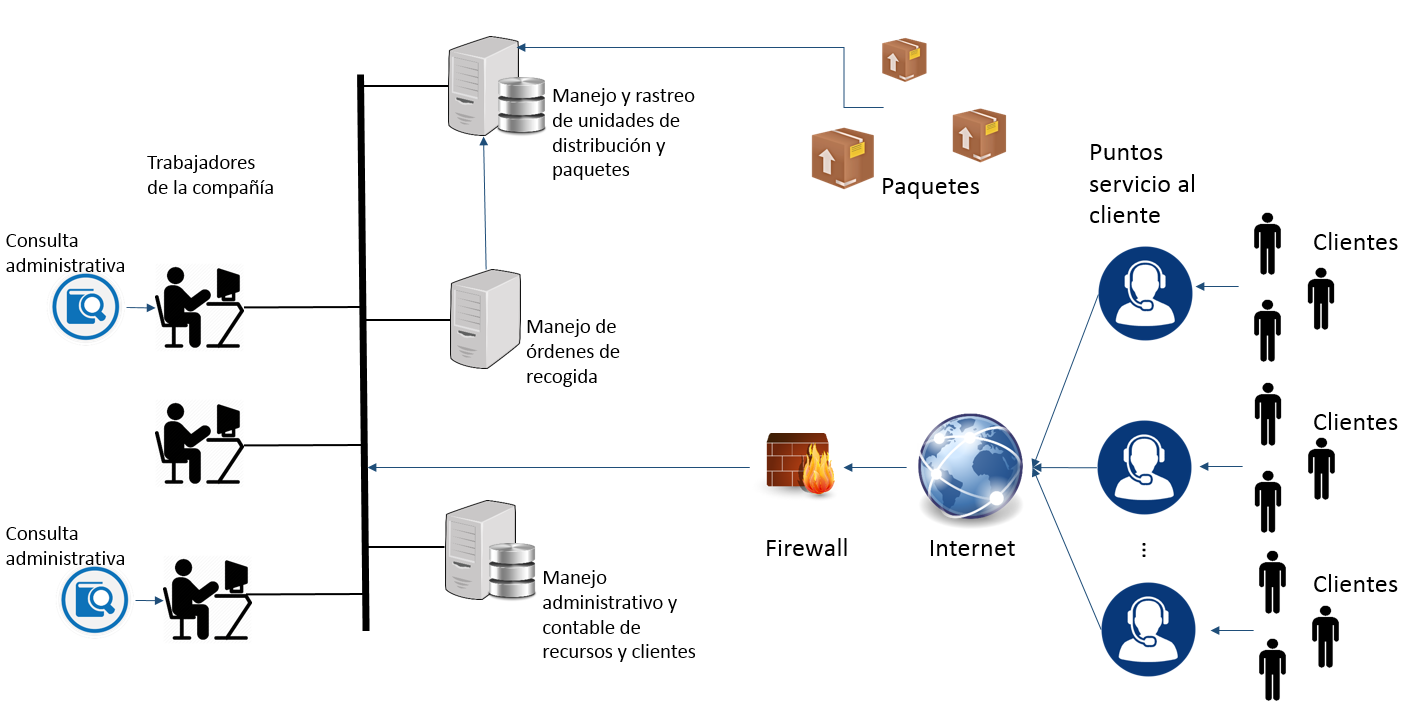
# Objetivos

* Identificar los requerimientos de seguridad de los canales usados para transmisión de la información en el sistema de gestión empresarial y operativa de una compañía transportadora.
* Construir un prototipo a escala del sistema que permita satisfacer algunos de los requerimientos de seguridad identificados. Entendiendo las garantías de seguridad y las limitaciones de la implementación propuesta.
* Practicar los conceptos vistos en clase.

# Análisis y Entendimiento del Problema

*Suponiendo que el sistema descrito en el párrafo anterior implementa control de acceso a nivel de sistema operativo en todos los servidores, y cuenta con un firewall que filtra paquetes a la entrada de la red.*

Para entender mejor el problema, en la *Figura 1* se plantea un diagrama de contexto, con el cual se pretende mostrar cómo fue entendido el sistema.



*Figura 1*

1. *Identifique y describa los datos que deben ser protegidos en el sistema de manejo de órdenes. Explique su respuesta en cada caso(\*) y responda la pregunta ¿Si un actor no autorizado consigue acceso al dato mencionado, ya sea en modo lectura o escritura, cómo podría afectar la empresa?*

A continuación se presentan los datos que deben ser protegidos en el sistema de manejo de órdenes:

1. **Datos recibidos sobre el estado de los puntos de atención al cliente**: estos son los datos que son recibidos desde los puntos de atención al cliente sobre su estado, por el servidor de manejo de órdenes de recogida.

Estos datos deben ser protegidos, ya que indican las nuevas órdenes solicitadas por los clientes. Lo cual, afecta directamente la operación de la compañía. Estos datos se usan para calcular las rutas óptimas del día.

Si un actor no autorizado consigue acceso a la información de los puntos de atención al cliente podría:

* Tener información sobre los diferentes clientes de la compañía y que tipo de paquetes envían. Esto puede perjudicar a la compañía ya que se puede estar manejando información personal de los clientes, los cuales probablemente no quieren que se sepa (esto puede traer demandas a la empresa) o si este actor hace parte de la competencia, esta puede aprovechar la información de los clientes para ofrecer sus servicios personalizados, y así quitarle clientes a esta compañía.
* Alterar los datos sobre el estado de los puntos de atención agregando información. Esto último provocaría que la empresa tuviera información adicional errada, lo cual provocaría que se calcularan rutas de los paquetes que no son las óptimas, y esto puede ocasionar retrasos, y desmejorar el servicio prestado por la empresa.
* Alterar los datos sobre el estado de los puntos de atención editando información. Esto provocaría que la información de los paquetes ya no fuera la correcta, por lo tanto se enviarían paquetes a destinos que no son. Esto haría quedar mal a la empresa, produciría demoras grandes para los clientes, y gastos de reenvió de los paquetes a los destinos correctos. Se perderían clientes por mal servicio.
* Alterar los datos sobre el estado de los puntos de atención eliminando información. Esto genera que no se procesen algunos paquetes. Lo cual retrasa la atención recibida por estos usuarios.

1. **Datos recibidos de las unidades o paquetes cada 60 segundos:** estos son los datos que son enviados por cada una de las unidades que están siendo transportadas a sus destinos. Las que se están comunicando con el servidor de manejo y rastreo de unidades de distribución de paquetes. Estos datos deben ser protegidos ya que representan los reportes del servicio que está prestando la compañía, además del estado continuo de los paquetes. Estos datos son usados para calcular las rutas de cada día, y para saber qué tantas órdenes han sido satisfechas.

Si un actor no autorizado consigue acceso a la información de los datos recibidos de las unidades o paquetes, podría:

* + - * Alterar los datos antes de la 1 am. Al cambiar los datos antes de la 1 am se pueden calcular rutas falsas, las cuales no sean necesariamente recurrentes, seguras ni efectivas.
      * Al tener acceso de este tipo de datos, se puede rastrear a la unidad que transporta los paquetes y llegado el caso en que haya un paquete de valor, puede ser robado.
      * Al tener acceso a esta información, se tiene acceso a la información de los clientes respecto a su vivienda y con ello, estos se convierten en sujetos vulnerables.

1. **Datos de las consultas contables:** hacen referencia a los aspectos contables y administrativos de la compañía, tanto de sus recursos como de sus clientes. Esta información es muy importante ya que es la constancia del capital de la empresa. Esta información debe ser protegida ya que la empresa debe tener registro de todos sus ingresos y gastos, para poder operar correctamente y rendir cuentas ante la ley.

Si un actor no autorizado consigue acceso a la información de los datos recibidos de las unidades o paquetes, podría:

* Conocer los montos de dinero que maneja la empresa u su ubicación. Esto puede llevar a robos muy bien planeados por la información a la que los atacantes tienen acceso.
* Debido a que esta información solo lo conocen las personas que tienen acceso al intranet de la compañía. Esta información podría ser vendida a la competencia para generar una ganancia personal y afectar a la compañía.
* Al mismo tiempo se puede modificar la contabilidad de la empresa y así generar un desfalco interno.

1. *Identifique cuatro vulnerabilidades del sistema de manejo de órdenes, teniendo en cuenta únicamente aspectos técnicos (no organizacionales o de procesos). 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 (\*).*

A continuación se presentan 4 vulnerabilidades del sistema:

1. **La información almacenada por el servidor de manejo y rastreo de unidades y paquetes esta desprotegida:** Esta información almacenada no cuenta con mecanismos de protección, lo cual puede llevar a que algún intruso pueda leer o editar los datos. Se puede perder información, generar inconsistencias, generar adulteración en la información, y espionaje.
2. **El servidor de manejo y rastreo de unidades y paquetes es un cuello de botella:** El servidor de manejo y rastreo de unidades y paquetes está encargado de muchas tareas. Cada 60 segundos todas las unidades reportan su estado, y por otro lado, este servidor también se encarga de recibir información del servidor de manejo de órdenes de recogida y calcular las rutas óptimas. Si este servidor falla, sería crítico para la empresa. Se perdería disponibilidad.
3. **La comunicación entre los paquetes y el servidor de manejo y rastreo de unidades esta desprotegida:** No se cuentan con mecanismos de protección a la hora en la que los paquetes se comunican con el servidor, para informar sobre su estado. Esto produce que la información pueda ser leída o alterada. Se puede perder información, se pueden generar inconsistencias, se puede generar adulteración en la información, y espionaje.
4. **La información manipulada por el servidor de manejo administrativo y contable está desprotegida:** Este servidor manipula información importante de la empresa, la cual hace referencia a los asuntos contables y administrativos. Este servidor no se encuentra protegido lo cual lo hace susceptible a ataques. Se puede perder información, se pueden generar inconsistencias, se puede generar adulteración en la información, y espionaje.

# Propuesta de Soluciones

*Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución. Los mecanismos propuestos deben ser explicados, por ejemplo, si se habla de cifrado sobre un canal de comunicaciones, debe identificar los participantes en la comunicación, y si es cifrado simétrico o asimétrico (y justificar la decisión). Además, debe justificar los mecanismos propuestos. Es decir, identifique explícitamente qué vulnerabilidad resuelve y justifique.*

*En sus justificaciones tenga en cuenta aspectos relacionados con eficacia, costo, eficiencia, flexibilidad, aspectos de implementación, y otros aspectos técnicos que considere convenientes.*

1. *Vulnerabilidad: La información almacenada por el servidor de manejo y rastreo de unidades y paquetes esta desprotegida*

**Mecanismos de Solución**

**Solución:** Para que la información almacenada por el servidor de manejo y rastreo de unidades y paquetes no se encuentre desprotegida, se puede guardar la información encriptada simétricamente y con una estampilla de tiempo para garantizar así su integridad.

Al mismo tiempo para asegurar la integridad de los datos se puede generar una estampilla de tiempo, con esto se verifica que la información permanezca constante a medida que

**Justificación:** De esta manera se provee un nivel más de seguridad en la que se tendría acceso si y solo si se conoce las llaves para descifrar la información, se cifraría simétricamente ya que sería más eficiente que un cifrado asimétrico y es un proceso que se debe realizar con cierta frecuencia. Además de esto se plantea el uso de una estampilla de tiempo, dado que así se puede garantizar la integridad de los datos una vez guardados en la base de datos. Estas dos soluciones bajan el desempeño, ya que en primer lugar se debe descifrar la información y en segundo lugar verificar la veracidad de la información con la estampilla de tiempo.

1. *Vulnerabilidad: El servidor de manejo y rastreo de unidades y paquetes es un cuello de botella*

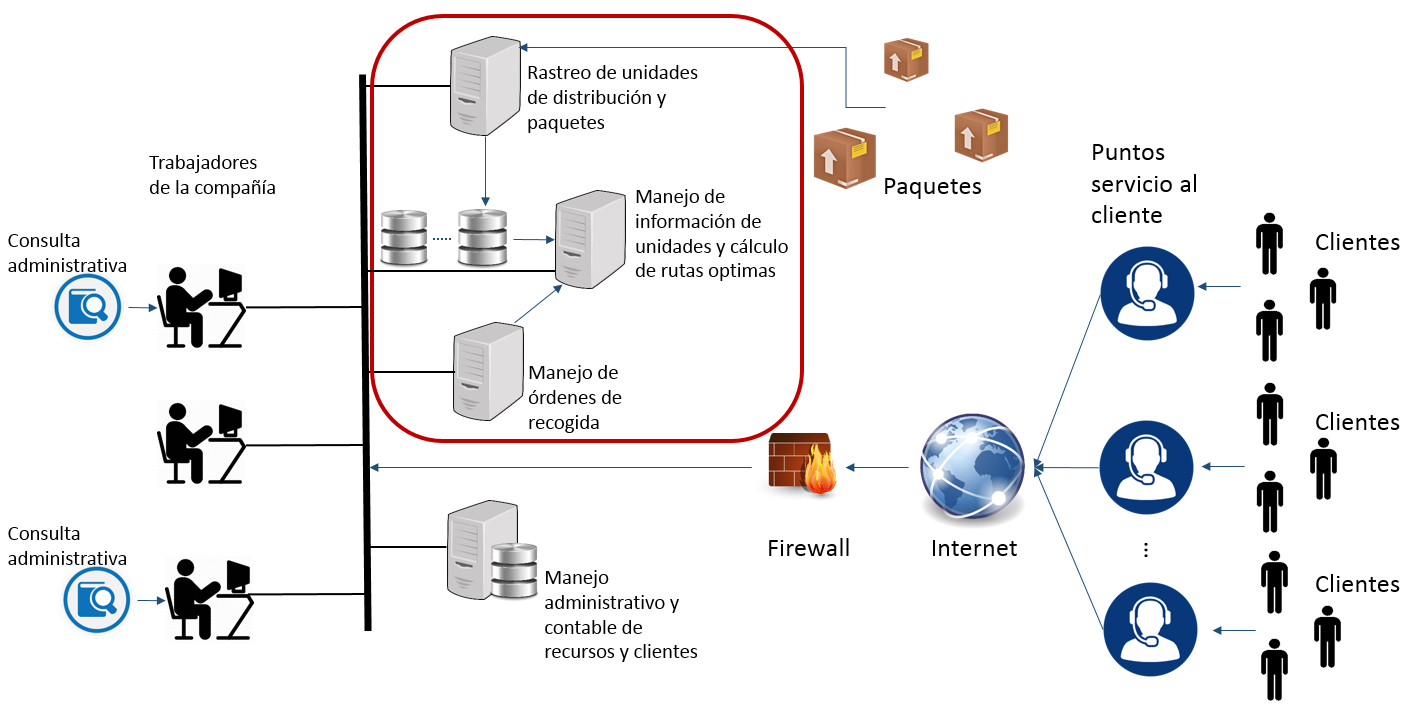
**Mecanismos de Solución**

**Solución:** Adicionar infraestructura. Es conveniente tener varios servidores que hagan el papel del servidor de manejo y rastreo de unidades y paquetes.

Este servidor de manejo y rastreo de unidades y paquetes se encarga de las siguientes actividades:

* Recibir los reportes de cada unidad, cada 60 segundos.
* Recibir la información del servidor de manejo de órdenes de recogida sobre las nuevas solicitudes.
* Calcular las rutas óptimas cada día.

Se propone tener 2 servidores. Uno que se encargue de recibir la información de las nuevas órdenes y de procesar las rutas óptimas tomando información de una base de datos. Y otro que solo se encargue de recibir información de los paquetes y almacenarla en una base de datos. La *Figura x* muestra la solución propuesta.



Como se puede ver en la *Figura ,* en el cuadrado rojo se encuentran los cambios con respecto a la *Figura 1* con la arquitectura original. En esta propuesta el servidor de rastreo de unidades y distribución de paquetes solo se encarga de recibir la información por parte de los paquetes, y almacenarla en la base de datos. El servidor de manejo de información de unidades y cálculo de rutas óptimas es el encargado de recibir la información de nuevas órdenes por parte del servidor de manejo de órdenes de recogida, y calcular las rutas del día con base en esa información, y la información del reporte de las unidades almacenado en la base de datos. La base de datos tiene una réplica, la cual se sincroniza cada cierto tiempo con la original, con el fin de garantizar disponibilidad en caso de algún problema con la base de datos original.

Con esta propuesta se pierde un poco de desempeño, ya que ahora la base de datos esta aparte del servidor y se separaron las tareas en dos servidores, por lo tanto se manejan más transacciones, lo cual hace que duren un poco más los procesos. Al tener que incluir nuevos servidores, implica que se incurre en el costo de comprar estas máquinas, costos monetarios altos. Por otro lado, la sincronización entre estos dos servidores y el acceso a la base de datos debe hacerse de manera cuidadosa.

**Justificación:** la razón de esta propuesta es evitar que por alguna catástrofe natural se pierda disponibilidad, y se pierda la información.

1. *Vulnerabilidad: La comunicación entre los paquetes y el servidor de manejo y rastreo de unidades esta desprotegida*

**Mecanismos de Solución**

**Solución:** Se debe establecer un canal seguro, con cifrado asimétrico entre el servidor de manejo y rastreo de unidades y las unidades, además de esto se debe establecer un protocolo de autentificación..

**Justificación:** Se debe establecer un cifrado asimétrico debido a que de esta manera se puede asegurar que a la información no se pueda acceder de una manera fácil, debe ser asimétrica ya que es información que viaja por una red externa a la compañía, lo cual implicaría más riesgos y la información que se maneja debe ser privada y confidencial de la empresa. Se debe manejar un protocolo de autenticación por parte de las unidades debido a que, como estas son móviles, y no se encuentran en un solo lugar o se puede verificar presencialmente, se debe poder asegurar que la persona que este descifrando la información con la llave publica sea quien dice ser.

1. *Vulnerabilidad: La información manipulada por el servidor de manejo administrativo y contable está desprotegida*

**Mecanismos de Solución**

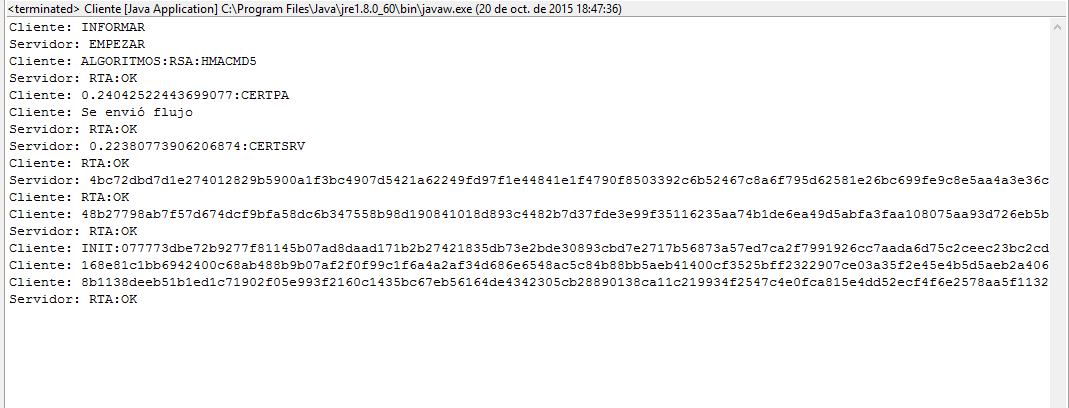
**Solución:** Se debe establecer un canal seguro por medio del uso de cifrado asimétrico, entre el servidor de manejo administrativo y los empleados que estén conectados a la intranet de la compañía. Además de esto se debe manejar una autentificación de usuarios.

**Justificación:** Debido a que se trata de información sensible para la empresa, como lo es la información contable, y a pesar de ser información que solo se trata en le empresa, esta información debe ser cifrado con un cifrado asimétrico, que a pesar de comprometer el desempeño, garantiza un mayor nivel de seguridad que el cifrado simétrico. Se debe manejar al mismo tiempo una autenticación de usuario debido a que se debe garantizar que las personas que tengan acceso a esta información tengan los permisos necesarios.

# Implementación del Prototipo

En el .zip del proyecto se puede ver implementado la parte del sistema de manejo de órdenes.

En la implementación se realizaron sysouts, para comprobar que lo que se mande es lo que llega.





# Referencias

## Imágenes

<http://www.macworld.com/article/2454226/parcel-122-review-where-in-the-world-is-your-package-use-this-mac-app-to-find-out.html>

<http://www.subaru.es/servicios>

<https://pixabay.com/es/servidor-web-red-computadora-567943/>

<http://eucinesis.com/centro-de-formacion/icono-busqueda/>

<http://appzsite.com/>

<http://about-animals.website/uVgU198iIopn/internet-icon.html>

<https://commons.wikimedia.org/wiki/File:Person_icon_BLACK-01.svg>