Andrea Navas 201125090
Diego Rodríguez Baquero 201223538

Repositorio Git: https://github.com/DiegoRBaquero/IC-CASO2

**Caso 2 Infraestructura Computacional**

A.

1 .Todos los datos del sistema de manejo de órdenes deben ser protegidos y confidenciales ya que ponen en juego la reputación de la organización. Estos datos incluyen:

a. Contrato de transporte
    i. Datos del remitente
        1. Lectura: Se deben proteger los datos privados del cliente (Persona/Empresa) ya que incluye su dirección e identidad. Lo que puede resultar en fraude con la identidad del cliente.
        2. Escritura: Se deben prevenir suplantación de remitente para una orden dada y evitar el repudio. Además no recogerían el paquete original lo que causaría disgusto por parte del cliente.
    ii. Datos del destinatario
        1. Lectura: Además de tener la información del individuo, si un tercero no autorizado tiene acceso a los datos del destinatario, podría enviar un paquete al tener conocimiento de que este está a la espera de uno.
        2. Escritura: Se podría cambiar el destinatario y que un tercero reciba el paquete lo que causaría inconformidad por parte del remitente y destinatario. Además se podría cambiar el tiempo de entrega para recibir un mejor servicio.
    iii. Descripción de las unidades
        1. Lectura: Si un tercero tiene la oportunidad de conocer los contenidos puede realizar acciones criminales para adquirir de manera ilegal el paquete atacando al destinatario o a la organización y su infraestructura. Además no habría confidencialidad de los contenidos de los paquetes.
        2. Escritura: Se podrían hacer cambios en cuanto al trato que se le da al paquete (Paquetes frágiles) dañando su contenido y dejando inconformes a los clientes. Por otro lado, se podrían evitar impuestos, retenciones y chequeos que se realizan dependiendo del contenido transportado.
b. Tipo de cliente
    i. Lectura: No hay efectos negativos a la organización en caso de lectura

ii. Escritura: Una empresa podría cambiar el tipo de cliente a persona natural para evitar la facturación a fin de mes del paquete. Igualmente, una persona natural podría cambiar el tipo de cliente a empresa para recibir una factura a fin de mes como si fuera una.

c. Factura de la orden
   i. Lectura: Ya que incluye todos los datos del cliente, se deben proteger para prevenir fraude con la identidad del cliente y mantener confidencialidad de los paquetes. Si no se realiza esta protección, la anteriores serían en vano.
   ii. Escritura: Se puede cambiar el valor de la orden o peor aún, marcar como ya pago, generando pérdidas a la organización.

2. a. Comunicación entre puntos de atención y el servidor de órdenes en la oficina central. Esto es una vulnerabilidad porque porque puede haber espionaje, suplantación y alteración de la información de la comunicación HTTP/TCP entre los puntos de atención y el servidor de órdenes.
b. Comunicación entre clientes finales y el servidores de órdenes en la oficina central. Esto es una vulnerabilidad porque porque puede haber espionaje, suplantación y alteración de la información de la comunicación HTTP/TCP entre el navegador web del cliente y el servidor de órdenes.
c. Almacenamiento de los datos de las órdenes en la bases de datos. Esto es una vulnerabilidad porque en caso de que se roben el servidor de órdenes de la oficina, se debe asegurar que el ladrón no tenga acceso a los datos.
d. Control de acceso, autenticación y autorización a la información. Esto es una vulnerabilidad porque si no se realiza autenticación, cualquier persona tendría acceso a las funciones que tienen un operador de un punto de atención y tener permisos de lectura/escritura que no le corresponden. No se garantiza el no repudio.

B. Para las vulnerabilidades presentadas anteriormente se proponen los siguientes mecanismos de resolución:

1. Para la vulnerabilidad a y b de la comunicación entre puntos de atención y clientes y el servidor de órdenes, se propone cifrar el canal de comunicación con SSL/TLS sobre HTTP utilizando un certificado emitido por una entidad certificadora usando una llave privada RSA de 4096 bits. Esta cifrado es simétrico en un inicio y pasa a ser asimétrico por sesión después del *handshake*. Ya que el canal es HTTP, proponemos esta solución porque tiene un costo muy bajo (USD$10/año) y es de fácil implementación en cualquier servidor web utilizando la llave privada y el certificado dado por la EC. La eficiencia no disminuye de manera considerable por implementar este tipo de solución que resulta eficaz.
2. Para la vulnerabilidad c de almacenamiento de las órdenes, se propone encriptar toda la información de los discos del servidor. En caso de que el servidor sea Linux, se utilizaría TrueCrypt; para Windows se utilizaría Bitlocker; para Mac se utilizaría FileVault. Esto no

tendría un costo monetario alguno pero sí un decremento del desempeño, aún así, se considera necesario para resolver la vulnerabilidad que se tiene.

3. Para la vulnerabilidad d, se propone utilizar un sistema de control de acceso definiendo los roles, dando permisos y asignando propiedad sobre los objetos. Esto tendría un efecto en el desempeño para cada pedido ya que se tiene que verificar de parte de quién viene. Ya que el canal está cifrado, no toca preocuparse por la transmisión de los datos de autenticación del usuario. Se propone utilizar un servidor LDAP corriendo en el servidor de órdenes con la información y rol de los clientes y empleados.