**Pablo Andrés Suarez Murillo - 201632293**

**Valerie Parra Cortés- 201610703**

**Parte 1: Datos del sistema que deberían ser protegidos**

Datos que deben ser protegidos

* Directorio de usuarios
* Datos de contabilidad:
  + Ventas realizadas
  + Impuestos pagados
  + Compras a proveedores
  + Inventario
  + Remisiones
  + Cuentas por pagar
  + Cuentas por cobrar
* Datos de tesorería
* Facturación
* Compras

Básicamente todos los datos que soporta la aplicación.

**¿Qué sucede en caso de que un actor no autorizado consiguiese acceso a los datos?**

* Directorio de usuarios:
  + Se puede hacer pasar por un usuario (Suplantación).
  + Podría hacer cambios no deseados en los datos a los cuales el usuario puede acceder (Adulteración).
* Datos de contabilidad:
  + Puede adulterar la contabilidad de la empresa causando errores en los balances y reportes (Adulteración).
* Datos de tesorería:
  + El atacante podría conocer la situación económica de la empresa (Espionaje), información valiosa que puede llegar a ser vendida. Además, podría llegarse a dar un intento de robo directamente a las cuentas de la empresa
* Facturación
  + Si el atacante tiene acceso completo al área de facturación podría empezar a general facturas falsas con miras de favorecer los balances contables de otras compañías (Suplantación)
* Compras
  + Si se accede a esta área el atacante podría generar certificados de egreso falsos (Suplantación) .SI el atacante es un empleado de la misma empresa podría coger el dinero físico de los comprobantes de egreso falsos generados (Robo).

**Propuesta de soluciones**

* **Guardar cada uno de los datos en servidores diferentes:** Al distribuir la información, un ataque no llevará a una pérdida o adulteración masiva. Las desventajas de esta implementación es que es costosa ya que tanto los claustres como su mantenimiento requerirían una inversión considerable. Además, que se tendría buscar un espacio físico para mantener los servidores, sino se posee el alquiler o la compra de dicho espacio incurrirían en otro gasto.
* **Encriptar todos los datos:** El software podría guardar de manera cifrada sus datos para que así si son accedidos de manera irregular no podrán tener acceso a la información que guardan. El costo de esto se ve reflejado principalmente en el desempeño ya que dependiendo del algoritmo de cifrado se tardará más o menos tiempo en el almacenamiento de los datos. Entre más seguro sea el algoritmo más se verá un costo en tiempo de respuesta.
* **Crear códigos de autenticación:** Implementar las aplicaciones de tal forma que el usuario y el servidor puedan enviar un certificado de autenticación al inicio de sesión. Los certificados pueden ser generados localmente por un administrador o alguien que conozca el tema.
* **Notificaciones y alertas:** Si un canal envía un mayor flujo de lo habitual o si es reiterado que un usuario intente ingresar mostrando credenciales o un código de autenticación erróneo, el sistema puede generar alertas para ser revisadas por alguien especializado en el tema. Para la implementación de este sistema se utilizaría un Software configurado por un experto que además se encargue de revisar periódicamente las alertas generadas haciendo las veces de administrador.
* **Purgar las credenciales:** Cada cierto tiempo, verificar que las credenciales y los códigos de autenticación existentes en los servidores sean de empleados que efectivamente pertenezcan a la empresa y no existan puntos de acceso para personas que ya no estén autorizadas ni vinculadas con la empresa.