**Grupo 1**

Para realizar la auditoría necesitamos de 4 empleados de diferentes áreas, con el fin de hacerles una serie de preguntas (**encuesta**), para tener un panorama claro del estado de la empresa. Al igual se analizarán los procesos mediante la documentación para verificar que se cumplen con los estándares pautados.

En la auditoría se evidenciaron las siguientes fallas en los siguientes niveles de seguridad:

1. **Seguridad lógica.**Es importante contar con un sistema de cifrado de datos, ya que es una página, mediante la cuál los clientes de la empresa de fertilizantes hacen las compras, sus datos podrían quedar expuestos a ataques, de igual forma se debe tener un control de accesos tanto para clientes como para trabajadores de la empresa.
2. **Física.**No realizan respaldo de sus copias de seguridad, lo cual puede traerles pérdida de información importante. La información no debería estar al alcance de todos los empleados de la compañía, se debería tener implementado un sistema de seguridad, que le permita a la empresa controlar, quién, cómo cuándo y dónde se revisa la información.
3. **Pasiva.**

Al contar con una página web, es necesario que los servidores, así como los equipos y dispositivos que reciben y almacenan la información, no tengan ningún tipo de malware o spyware, por tanto, se debe manejar:

* Copias de seguridad en caso de un secuestro de datos.
* Escaneo y limpieza de los equipos.
* Mantener en condiciones óptimas los antivirus.

1. **Activa.**

* En este tipo de seguridad, los usuarios deberían tener claves de acceso, con contraseñas en minúsculas y mayúsculas para evitar el robo o pérdida de información de manera fácil.
* Contar con antivirus auténticos para el trabajo requerido.
* Encriptar los datos.
* Se deben manejar listas de control de acceso.

1. **Controles de medida de seguridad.**

* Implementación de antivirus.
* Implementación de cifrado de datos.
* Implementación de políticas para la confidencialidad de la información (listas de control de acceso).
* Implementación de Backups.

1. **Vulnerabilidades.**

* Una de las vulnerabilidades halladas, es que todos los empleados tienen acceso a la información, así sea solo a la visualización, esto puede traer fuga de información, robo de información, etc.   
  **Solución:** Es necesario implementar políticas para controlar el acceso a la información ya que toda la información no es concerniente a todos los empleados.
* La información puede perderse debido a que no realizan backups.  
  **Solución:** Se deben contar con servidores de respaldo, o copias de seguridad para tener la información de respaldo para que no se pierda la información.