1) **Análisis de la empresa:**

-Tienen empleados dispuestos a capacitarse en informática.

-Poseen solamente dos personas que manejan la información sensible de la empresa.

Sugerimos elevar esa cantidad a 3 para cubrir posibles problemáticas o ataques informáticos por si alguna de las dos personas no está disponible.

-Tener un control con el tipo de información que se maneja, al ser información sensible no es conveniente que esté a disposición de todos.

2)

Seguridad Lógica:

-Poner un control de acceso para que solamente las personas que manejan la información sensible sean las que tienen acceso a ella.

-Proteger la información de cada venta a los clientes mediante un cifrado de datos para que los mismos no sean vulnerados.

-Contratar un Firewall y Antivirus de alto rendimiento, tales como bitDefender, Norton o McAfee.

Seguridad Física:

-Como nombramos anteriormente, Hacer copias de seguridad o backUps para respaldar los datos.

-Contar con un UPS para que los dispositivos no queden inutilizados en caso de un apagón y se puedan seguir realizando operaciones.

Seguridad Pasiva:

-El uso de hardware adecuado frente a accidentes o averías, como conexiones eléctricas adecuadas, refrigeración del sistema.

- La realización de copias de seguridad de los datos y el sistema operativo en más de un soporte y en distintas ubicaciones físicas.

- Creaciones de particiones lógicas en el disco duro para poder almacenar archivos y copias de seguridad si es posible en una unidad distinta al sistema operativo.

Seguridad Activa:

- Que solo el personal autorizado tenga acceso a las contraseñas alfanuméricas, para así proteger los equipos y los datos que contienen.

-Encriptar los datos más importantes y que puedan acceder a ellos solo por las contraseñas.

- El uso de antivirus para cada computadora y demás software que nos ayude a proteger nuestra información.

Controles de medida de seguridad:

Implementar periódicamente medidas reactivas, para Detectar y Corregir las fallas de seguridad encontradas en el sistema (por ejemplo la nula ocultación de datos) y sumar medidas Proactivas para complementar (Capacitación de los empleados, una restricción de permisos sobre los usuarios, tanto clientes como trabajadores de la empresa)

Vulnerabilidades:

Como vulnerabilidades el sistema posee varias, una nula capacitación de los empleados, la misma puede resolverse fácilmente educando a dichas personas. No existen datos de respaldo, esto se corregirá con la implementación de las medidas de seguridad fìsicas. Lo mismo ocurre con los datos del sistema, una vez que esté debidamente protegida con las medidas de seguridad lógica.

Una vez todo se haya cumplido se recomienda realizar una segunda auditoría para testear y buscar las nuevas posibles vulnerabilidades.

Feedback grupo 4:

Consideramos que las medidas que se tomaron podrían resolver algunos de los problemas. Sin embargo, encontramos ciertas falencias que se pueden mejorar:

-Se menciona que la seguridad lógica de los dispositivos de la empresa es buena, pero se desconoce la situación particular de cada empleado, ya que la mayoría trabajan en remoto.

-Se recomienda una segunda auditoría una vez cumplidas las condiciones expresadas aquí

-A pesar de que los empleados se resisten a las nuevas capacitaciones, es crucial hacerles comprender la importancia de la seguridad informática y los riesgos que se corren. La capacitación particular **debe** estar.