AUDITORÍA GRUPO 8 A GRUPO 7

Damelio Agustín, Díaz Salvador, Gattás Martina, Ravina Rodrigo, Sánchez Antonella, Vitelli Daniela

Escenario:

Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site y están dispuestos a recibir capacitación. Poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa). No realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

Análisis de la situación actual de la empresa:

La seguridad informática de la empresa es débil dado que solo hay dos personas encargadas de la seguridad de la organización. La empresa no establece como prioridad el resguardo de información sensible de sus clientes ni la realización de copias de seguridad. Por último, se observa una insuficiente capacitación a sus empleados.

Plan de seguridad:

Para idear un plan de seguridad, se listan los bienes y patrimonios a resguardar. Entre ellos encontramos:

- Información y datos personales de los clientes y usuarios que utilizan la página web.
- Información del personal de la empresa.
- Servicios de conexión de red.
- Servidores.

En primer lugar, consideramos importante resguardar la información sensible, tanto los datos personales de la empresa como también la información de sus clientes. Estos aspectos podrían mejorarse mediante la encriptación de datos (seguridad activa) y copias de seguridad de los mismos tanto locales como en más de un dispositivo o ubicaciones físicas (seguridad pasiva y física).

Por otro lado, se recomienda aprovechar la buena predisposición del personal y realizar capacitaciones sobre phishing, spam, entre otros posibles ataques.

Se aconseja acotar los accesos a la red por horarios y permisos de usuario.

Se sugiere también la instalación y configuración de un firewall y antivirus con controles de seguridad automáticos periódicos.

Deberían hacer verificación de la contraseña todos los meses