Actividad integradora - Plan de seguridad

**GRUPO 1:** Micheli D. | Nuñez C. | Blanco M. | Santia G. | Dematei M. | Lamanna A.

**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.

**Plan de seguridad:**

Paso 1- Seguridad lógica

* Otorgar credenciales de acceso a los empleados, con contraseñas seguras.
* El acceso a los datos sensibles deben ser restringidos para que solo los usuarios autorizados puedan acceder.
* Así mismo, estos datos deberían encontrarse cifrados para evitar su divulgación.
* Los equipos de los empleados deben poseer instalados software antivirus y firewall.
* Los mismos deben estar correctamente configurados y se debe verificar su actualización.
* Las transacciones de los clientes se deben realizar a través de un canal encriptado, utilizando el protocolo HTTPS.
* Los datos sensibles de los usuarios se deben almacenar de forma encriptada en la base de datos.

Paso 2 - Seguridad física

* El acceso a las instalaciones de la empresa debe ser controlado con dispositivos de control de acceso físico, como tarjetas de proximidad.
* Los equipos imprescindibles para el funcionamiento del sistema deben contar con UPS para evitar la interrupción de la operación durante los cortes de energía eléctrica.\
* Se deben realizar backups de los datos completos e incrementales, los cuales deben estar físicamente alejados del servidor, y ser probados de forma periódica.
* Deberá contar con sistemas redundantes que permitan la disponibilidad de los servicios ofrecidos en caso de falla o ataque al servidor principal.

Paso 3 - Seguridad pasiva

* Deberían hacer copias de seguridad de los datos en diferentes dispositivos y también diferentes ubicaciones físicas
* Controlar el buen funcionamiento de los antivirus

Paso 4 - Seguridad activa

* Deberían incorporar autenticaciones tanto del personal en la red privada, como de los clientes en el ecommerce
* Hacer uso de software de seguridad informática, para prevenir ataques

Paso 5 - Controles de medidas de seguridad

* Definir medidas directivas sobre qué se puede hacer y qué no
* Generar advertencias que permitan desviar usos indebidos
* Realizar controles de los accesos a los sistemas.
* Verificar que el software antivirus y el sistema operativo de los equipos se encuentre actualizado.

Paso 6 - Controles de vulnerabilidades

* Evaluar cómo está constituida la red e infraestructura de la empresa.
* Delimitar quién puede y debe acceder a la información confidencial.
* Probar que las copias de seguridad realizadas funcionen.
* Identificar las partes más sensibles y esenciales del sistema
* Realizar auditorias del estado de la seguridad informática