Empresa Asignada

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.

A. Un análisis de la situación actual de cada empresa que se les haya asignado.

La empresa se dedica a la venta de productos por internet, por lo tanto, se hace necesaria una intranet segura, la información confidencial de ésta cuenta con poca seguridad física.

Como los empleados trabajan onsite sería necesario reforzar los procesos de respaldos de información, para que no haya pérdida de datos al estar trabajando desde dentro y fuera de la red.

Se requiere capacitación a los empleados de implementación de medidas de seguridad, pero estos están dispuestos a recibirla que hace más fácil la implementación de cambios.

B. Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

1. Seguridad lógica:

- Control de acceso, para identificar y autentificar la información para acceder a datos o recursos.

- Cifrado de datos,para proteger los datos confidenciales en sus servidores y bases de datos.

- Antivirus, para la protección de la información que se genere.

- Firewalls, para que bloquee el acceso no autorizado.

2. **Seguridad física: son las medidas para resguardar cualquier tipo de daños a los equipos.**

    - Dispositivos físicos de protección: detectores de humo.

    - UPS: Para que almacene los datos si se va la electricidad, y almacene los datos por un tiempo determinado.

    - Respaldo de datos: realizar copias de seguridad o backups de los datos completos e incrementales, para manejar y cuidar la información y evitar cualquier tipo de hurto, alteración o virus.

    - Sistemas redundantes: realizar la copia de los datos de mayor importancia, así en caso de fallas no se pierde la información.

3. **Seguridad pasiva.**

La realización de copias de seguridad de los datos en más de un dispositivo en distintas ubicaciones físicas.

Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.

Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.

Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.

Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.

4. **Seguridad activa.**

Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres.

Heisenbug No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.

Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.

Encriptar los datos importantes. La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información sólo pueda ser leído si se conoce la clave de cifrado.

5. Controles de medida de seguridad.

Para que los controles de seguridad sean integrales no solo hay que implementar controles técnicos sino también algunos controles administrativos y físicos.

Algunos controles que se podrían incluir son:

Controles proactivos

- Directivas, para que nos diga qué podemos hacer o no.
- Disuasivas, para darnos una advertencia si algo estamos haciendo mal, e incluso desviar la intención de un atacante
- Preventivas, para que busque y prevenga una acción indebida.

Controles reactivos

- Detectivas, para que busque potenciales atacantes.
- Correctivas, para que encuentre el riesgo y solucione el sistema.

6. Vulnerabilidades que podrían explotar los atacantes.

Heisenbug: bugs que alteran o desaparecen su comportamiento al tratar de depurarlos.

El cifrado de datos, debido a que quieran obtener algún tipo de información confidencial.