Mesa 1 - Adrian Gamarra - Nixon Angulo - Augusto Landra - Emanuel Centurión - Luciana Zaragoz

Empresa: emergente dedicada a la venta de fertilizantes.

1) Análisis de la situación actual

Es una empresa pequeña, con poca estructura organizacional, que es muy flexible con el manejo de la información y no posee controles ni restricciones sobre la misma.
Su personal en sistemas está orientado a la operatividad del negocio, y no tiene roles definidos para la seguridad informática.
No tiene controles de seguridad, ni de restricciones al acceso de la información, no realiza backup's de sus datos y por lo tanto tiene un riesgo enorme de padecer algún daño por alguna intervención externa o por ejemplo, contra daños físicos (descargas atmosféricas, incendios, robos, inspecciones de AFIP).
La empresa presenta un alto riesgo de vulnerabilidad en la gestión de su información. expuestas a factores internos y externos, humanos y físicos.

2) Plan de Auditoría

Se propone el siguiente plan de auditoría, basado en 6 puntos:

1) **Seguridad lógica**

- ➔ Control de acceso: implementar niveles de acceso y de uso de contraseñas personales y con resguardo legal sobre la responsabilidad en el uso de las mismas. Criticidad Alta.
- ➔ Antivirus: verificar si posee licencia de antivirus actualizada. Criticidad Alta
- ➔ Firewalls: verificar el nivel de seguridad de configuración del Firewalls. Además instalar un software dedicado sobre este aspecto. Criticidad Baja

2) **Seguridad física:**

Verificar las instalaciones donde se encuentra el servidor, cumpla con los estándares de Seguridad e Higiene y Buenas Prácticas: Extintores adecuados para equipos electrónicos y en cantidad suficiente, Sistema de alarma contra incendios (detectores de humo), sistema de alarma contra intrusos. Verificar el cumplimiento de sistema pararrayos y de puesta a tierra. Utilización de UPS y estabilizador de tensión eléctrica. La ventilación del cuarto de servidor debe ser adecuada y preferentemente refrigerada por sistema de enfriamiento (ej: Aire Acondicionado). Verificar que la instalación eléctrica cumpla con la normativa correspondiente y que los tableros eléctricos se encuentren fuera del cuarto de servidor.

3) **Seguridad pasiva:**

Como buenas prácticas se deberá implementar:

- ➔ La realización de copias de seguridad de los datos en más de un dispositivo o 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:**

Como buenas prácticas se deberá implementar:

- ➔ 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. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público. Firma legal de documento sobre cada usuario sobre la responsabilidad en el uso de la contraseña.
- ➔ 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 solo pueda ser leído si se conoce la clave de cifrado.

5) **Controles de seguridad:**

Proactivas:

☐ Directivas:

Nos dicen qué podemos o no hacer. Intentan que las actividades de los sistemas se realicen de una manera específica con el fin de que se produzcan ciertos resultados esperados.

Implementar procedimiento sobre política de seguridad informática que contemple las responsabilidades de cada puesto de trabajo.

☐ Preventivas:

Implementar procedimiento de verificaciones periódicas en el cumplimiento de las acciones involucradas en este plan.

Reactivas:

☐ Detectivas:

Se basan en la búsqueda de potenciales ataques o peligros a los que puede estar expuesto un sistema informático.

Implementar auditorías internas y externas de seguridad informática de forma periódica.

☐ Correctivas:

Una vez se ha encontrado el riesgo o ha sucedido un incidente que ha puesto en peligro a los datos o información, se activan estas medidas de seguridad. Su objetivo es solucionar el sistema luego que ha sucedido el desvío.

Implementar plan de contingencia, que contenga copias de backups o de sistemas redundantes.

Se recomienda la implementación de un Business Continuity Plan (BCP).

6) **<u>Vulnerabilidades que podrían explotar los atacantes:</u>**

➔ Falta de cifrado de datos sensibles.

➔ Falta de backup de la información.

➔ Antivirus desactualizados.