Práctica Equipo 3

Escenarios para grupos 1, 3, 5, 7, 9, 11

● 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.

Seguridad lógica: Antivirus Windows Defender
Seguridad física: UPS para prevenir cortes o fallas eléctricas y dar tiempo de guardado y correcto apagado de equipos.
Seguridad activa: usuario y contraseña para cada empleado de la empresa.
Seguridad pasiva: realización de backups en cortos plazos para resguardo de datos.
Control de vulnerabilidad: encriptación de datos personales para clientes que compran en la página web.
Control de medida de seguridad:Crear particiones en el disco duro para almacenar archivos y backups en una unidad distinta a donde tienen el sistema operativo.

AUDITORÍA EQUIPO 4

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

   Dado que la información confidencial de la empresa no tiene mucha seguridad física, debe mejorarse ese aspecto. También debe asegurarse el acceso a intranet para aquellos usuarios que acceden remoto lo hagan mediante una VPN.

   La resistencia a cambios por parte de los usuarios amerita una capacitación para toma de conciencia de las amenazas existentes.

2. **Para cada escenario planteado, crear un plan de seguridad**

   → 2FA para logins, contraseñas que caducan cada 45 días y no pueden ser reutilizadas las ya usadas anteriormente, con un mínimo de complejidad aceptable
   → Laptops proporcionadas por la empresa a los empleados
   → Uso obligatorio de una VPN para poder conectarse a intranet
   → Política estricta de candados para laptops para los empleados onsite
   → Bitlocker por default en todas las laptops
   → Cámaras de seguridad y tokens de acceso en la empresa para toda persona que ingrese/salga
   → Deshabilitar los puertos USB de las laptops
   → Modificar las políticas de Windows para que los usuarios no puedan instalar programas no habilitados expresamente por el administrador del sistema (whitelist)
   → Monitoreo de tráfico saliente para detectar posibles fraudes/fuga de información confidencial
   → Encriptación de discos duros por default
   → En caso de estar inactivo por 15 minutos, se bloqueará la pantalla
   → Curso de capacitación para concientizar de riesgos y amenazas que se encuentran en el mercado

→ Test de pishing

3. 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.

   Esta serie de pasos y sugerencias debe ser presentada en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

El resultado de la auditoría es favorable, ya que cumple con la mayoría de los protocolos de seguridad.
solo recomendamos el uso de antivirus en cada una de las computadoras del trabajo.