El **proyecto es de manera individual o en pareja**, se elegirá una empresa que vosotros queráis, puede ser real o inventada, si es inventada que se parezca a la realidad.

Vamos a realizar una **auditoría de seguridad** de dicha empresa, se va a seguir el siguiente plan de seguridad:

1. **Seguridad física** (acceso físico al equipo, biometría, control de temperatura, otras medidas de prevención, incendios, inundaciones…)
2. **Seguridad lógica** (acceso al sistema, contraseña de BIOS y sistema operativo, opciones posibles sobre archivos y carpetas…)
3. **Análisis de malware** (virus, espías, troyanos…)
4. **Gestión de almacenamiento, copias de seguridad y restauración**. Periodicidad y gestión de copias de directorios, archivos, drivers, configuraciones del sistema y aplicaciones.
5. **Seguridad en redes**. Conexión inalámbrica, encriptación y política de filtrado mediante cortafuegos.
6. **Grado de cumplimiento LOPD-GDD y LSSI**.

Documentar los resultados. Medidas dispuestas actualmente y vulnerabilidades posibles.

Documentar las acciones realizadas en el equipo para ver disponibilidades y técnicas empleadas de seguridad, y resaltar las deficiencias.

Propuesta **de plan de mejora y recomendaciones** de uso de equipo (contraseñas, copias de seguridad, periodicidad de cambios y análisis del sistema)

**El proyecto se entregará como último día el 14 de Febrero a las 23h59. Si se entregará después de la fecha la penalización de la nota sería de un 40%.**

**Conceptos a tener en cuenta:**

**Palabras clave:**

* Malware
* Ingeniería social
* Scam
* Spam
* Sniffing
* Spoofing
* Pharming
* Phising
* Password cracking
* Botnet
* Denegación de servicio (DoS)
* Tabnabbing

**Objetivos seguridad:**

* Confidencialidad
* Integridad
* Disponibilidad
* Autenticidad y control de acceso
* Fiabilidad
* No repudio
  + En origen
  + En destino
* Auditabilidad

**Plan de Seguridad**

* Plan de respuesta

**Amenazas, riesgos y ataques**

* Amenazas
  + Internas
  + Externas
* Física o ambientales
  + Personal, empleados, hackers
  + Robos, sabotajes, suministro eléctrico, condiciones atmosféricas, catástrofes naturales (incendios)
* Lógicas
  + SW Malicioso, backdoors, virus, troyanos, gusanos
* Vulnerabilidades o brechas
  + HW, SW, DATOS
* Contramedidas
* Atacantes
* Riesgo

**Estándares y Normas ISO**

**Seguridad física y ambiental**

* Control de acceso físico
* Personal de seguridad, detector de metales, biometría, protección electrónica, etc…

**Seguridad lógica**

**NIST**

* Identificación y Autenticación
* Roles
* Transacciones
* Limitaciones a los servicios
* Modalidad de acceso
* Ubicación y horario
* Control de acceso interno (ACL)
* Control de acceso externo
* Administración

**Niveles de seguridad para sistemas operativos**

* Nivel A1 (TCSEC Orange Book)
* Nivel EAL4 (Common Criteria)

**Análisis forense**

**Criptografía**

* Hash
* Clave pública/clave digital
* Firma digital
* Certificados digitales (PKI)
* SSL/TSL
* SHH (Túneles)
* Cifrar ficheros

**Contraseñas**

* Claves de gran longitud
* Cambiar regularmente de clave y no utilizar una previa
* Utilizar todos los caracteres posibles
* No utilizar palabras fácilmente identificables
* Detectar repetidos intentos fallidos

Seguridad física

* Rack
* Biometría
* Protección electrónica
* Condiciones ambientales

CPD

* Centralizado
* Fiabilidad infalibre 99,999%
* Documentación de HW, SW, Datos
* Baja probabilidad de accidentes, edificios pelibrosos, primeras plantas…
* Aislamiento (Temperatura, Humedad, Interferencias, ruido)
* Ventilación (pasillos calientes, fríos)
* Suministro eléctrico y comunicaciones
* Centro de respaldo
* SAI (monitorización, triggers, mantenimiento)
* RAID
* Modelos arquitectónicos (DAS, NAS, SAN)
* Copias de seguridad (normal, incremental, diferencial)

**Legislación**

LOPD

* Datos persoanles, fichero, tratamiento
* Comunidcar a la AEPD

LSSI

* Ingresos?

LOPD-GBB

* Derechos digitales

**Tipos de atacantes**

* Sniffers
* Spammers
* Programadores de malware
* Personal interno
* Antiguos empleados
* Intrusos remunerados

**Tipos de ataques**

* Escaneres de puertos
* Sniffers
* Exploits
* Backdoors
* Rootkits
* Auto-rooters
* Password-crackers
* Generadores de malware

**Defensa en profundidad**

* Políticas, procedimientos, concienciación
* Seguridad físisca
* Perímetro
* Red Interna
* Host
* Aplicación
* Datos

**IDS**

**NAC**

**Seguridad en la BIOS**

* Denegación de servicio
* Ataques de suplantación
* Pérdidas o fugas de información

**Actualizaciones de SO y apps**

**Honeypots (pruebas falsas)**