1. Análisis del Cliente: Gestoría "Trámites Fáciles"

La Gestoría "Trámites Fáciles" es un claro ejemplo de una PYME que ha realizado una importante transición digital pero sin una estrategia de seguridad y gobernanza paralela que mitigue los nuevos riesgos asociados. Maneja información altamente sensible: nóminas, contratos laborales, y datos fiscales de cientos de clientes. Actualmente, la infraestructura se basa en un servidor local sin medidas de redundancia ni accesos securizados.

Situación Actual y Riesgos Identificados:

- **Activo Crítico:** Gestiona información altamente sensible (nóminas, contratos, datos fiscales) de cientos de clientes.
- **Infraestructura:** Servidor local sin detalles sobre su gestión de seguridad (parches, backups, acceso).
- **Riesgo Alto (BYOD):** Los empleados utilizan dispositivos personales para acceder y almacenar información confidencial sin un estándar de seguridad definido. Estos dispositivos probablemente carecen de controles de seguridad básicos (antivirus actualizado, cifrado).
- **Riesgo Alto (Acceso Remoto):** Las conexiones desde domicilios se realizan sin una VPN segura, exponiendo las credenciales y los datos transmitidos a posibles interceptaciones.
- **Falta de Procedimientos:** No existe un protocolo definido para incidentes de seguridad, como la pérdida o robo de un dispositivo.
- **Riesgo Legal:** La falta de medidas técnicas organizativas adecuadas supone un incumplimiento directo del RGPD y la LOPDGDD, con el riesgo de cuantiosas sanciones.

2. Propuesta de Seguridad (Basada en ISO/IEC 27002:2022)

Proponemos la implementación prioritaria de los siguientes controles para establecer una base sólida de seguridad de la información.

Control 1: Políticas de trabajo a distancia (Alineado con ISO 27002 - 6.7)

- **Riesgo detectado:** El uso de portátiles personales no securizados para conectarse a la red corporativa.

- **Objetivo:** Garantizar que el acceso remoto a los sistemas y datos de la empresa se realice de forma segura, protegiendo la confidencialidad e integridad de la información.
- **Propuesta de Acción:**
    1. Establecer una política formal de trabajo a distancia que defina los requisitos de seguridad.
    2. Prohibir el uso de dispositivos personales (BYOD) para el almacenamiento de datos de clientes hasta que se implementen controles MDM. Mientras tanto, proporcionar equipos corporativos seguros.
    3. Implementar el acceso remoto exclusivamente a través de una Red Privada Virtual (VPN) segura.
- **Herramientas Recomendadas:**

  OpenVPN o **Cisco Secure Client**. Son soluciones robustas y escalables que cifran toda la comunicación entre el dispositivo del empleado y la red de la oficina, protegiendo los datos en tránsito.

Control 2: Clasificación de la información (Alineado con ISO 27002 - 5.12)

- **Riesgo detectado:** No existe control sobre la sensibilidad y el etiquetado de la información de clientes.
- **Objetivo:** Identificar la información crítica de la empresa para aplicar los niveles de protección adecuados en función de su sensibilidad.
- **Propuesta de Acción:**
    1. Desarrollar una política de clasificación de datos que categorice la información (e.g., Pública, Uso Interno, Confidencial, Restringida).
    2. Los datos de clientes (nóminas, contratos) deben etiquetarse como "Restringido" o "Confidencial".
    3. Formar a los empleados para que identifiquen y traten cada categoría de datos según las políticas establecidas.
- **Herramientas Recomendadas:**

  Microsoft Purview Information Protection (antes Azure Information Protection). Permite etiquetar documentos y correos electrónicos de forma manual o automática. La etiqueta aplica metadatos y, lo que es más

importante, puede obligar al cifrado del documento, restringiendo su acceso sólo a personas autorizadas, incluso si sale del perímetro de la empresa.

Alternativa: VeraCrypt para cifrado local de ficheros sensibles

Control 3: Concienciación y formación en seguridad (Uso aceptable de los activos de información - Alineado con ISO 27002 - 6.3)

- **Riesgo detectado:** Los empleados no cuentan con capacitación sobre riesgos de seguridad (pérdida de portátiles, phishing, contraseñas inseguras).
- **Objetivo:** Establecer las reglas claras para el uso correcto y seguro de los dispositivos, sistemas e información de la empresa.
- **Propuesta de Acción:**
    1. Redactar y hacer firmar a todos los empleados una política de uso aceptable de los activos.
    2. Implementar un programa de formación continua en ciberseguridad.
    3. Realizar simulaciones de ataques de phishing.
    4. La política debe prohibir explícitamente el almacenamiento de datos de clientes en dispositivos personales sin cifrar y definir las consecuencias por su incumplimiento.
    5. Esta política es el paraguas legal y organizativo que sustenta técnicamente los otros dos controles.
- **Herramientas Recomendadas:**

  Herramienta de firma digital como **Adobe Sign** o **DocuSign** para obtener el acuse de recibo y aceptación de la política por parte de cada empleado, dejando una evidencia auditada.

  KnowBe4 Security Awareness Training

3. Propuesta de Servicios (Basada en ITIL 4)

Práctica ITIL 4 Recomendada: Gestión de Incidencias (Incident Management)

- **Situación:** Los empleados no tienen un procedimiento claro si pierden un portátil con información sensible.

- **Desarrollo:** La duda de los empleados sobre qué hacer ante la pérdida de un portátil es un síntoma claro de la falta de un procedimiento de gestión de incidencias. La práctica de Gestión de Incidencias de ITIL 4 se define como el proceso para restaurar un servicio interrumpido lo más rápido posible. Un incidente de seguridad de este calibre debe tener una vía de comunicación urgente y un flujo de trabajo definido.
- **Propuesta de Acción:**
    1. Establecer un Único Punto de Comunicación (Service Desk) para reportar incidentes (un teléfono y email dedicados).
    2. Documentar un procedimiento específico para "Pérdida/Robo de Dispositivos". Este procedimiento debe activar de inmediato la notificación al responsable, la invalidez de credenciales y el borrado remoto del dispositivo.

       Notificación inmediata→bloqueo del dispositivo→borrado remoto→reporte a la autoridad competente (si aplica RGPD)

    3. Comunicar y formar a todos los empleados en este nuevo procedimiento.

Herramientas Recomendadas:

Mobile Device Management (MDM) / Microsoft Intune

- **Justificación:** Para poder ejecutar el procedimiento de borrado remoto, es necesario tener una herramienta que gestione centralizadamente los dispositivos.
- **Propuesta: Microsoft Intune** (incluido en licencias Microsoft 365 Business Premium) o **Miradore**. Estas herramientas permiten:
    - **Gobernanza de dispositivos:** Inscribir los portátiles corporativos y, en políticas BYOD controladas, los personales.

- **Aplicación de políticas de seguridad:** Forzar el cifrado del disco, exigir una contraseña robusta, etc.
- **Borrado Remoto:** La función crítica para este caso. Permite borrar de forma remota todos los datos del dispositivo en caso de pérdida o robo, mitigando instantáneamente la brecha de seguridad.

Alternativa gratuita para PYMEs: Miradore MDM

4. Propuesta de Cumplimiento (RGPD y LOPDGDD)

Figura Legal en el Tratamiento de Datos:
La gestoría "Trámites Fáciles" actúa como RESPONSABLE DEL TRATAMIENTO. Esto se debe a que decide sobre la finalidad (gestión de nóminas, impuestos) y los medios del tratamiento de los datos personales de sus clientes. Sus clientes son los "interesados" a los que se refiere el RGPD. La gestoría debe cumplir con todas las obligaciones que el Reglamento impone al responsable (registro de actividades de tratamiento, notificación de brechas, etc.).

Medidas recomendadas:

- Firmar contratos de encargo de tratamiento con cada cliente (art. 28 RGPD).
- Garantizar medidas técnicas y organizativas adecuadas (cifrado, control de accesos, copias de seguridad).
- Documentar un Registro de Actividades de Tratamiento (RAT).

Herramientas para el Cumplimiento de Medidas de Seguridad:

Cifrado de Dispositivos

- **Justificación Legal:** El Artículo 32 del RGPD exige la implementación de "medidas técnicas y organizativas apropiadas" para garantizar un nivel de seguridad adecuado. El cifrado del disco duro es una medida técnica fundamental y básica para proteger los datos en caso de acceso físico no autorizado al dispositivo (como en un robo).
- **Herramientas Recomendadas:**
  - **Para dispositivos Windows (Corporativos): BitLocker**. Está integrado en Windows 10/11 Pro y Enterprise. Es transparente para el usuario y muy robusto. Su gestión se puede centralizar con Intune.

- **Para dispositivos macOS (Corporativos): FileVault 2**. La solución nativa de Apple, igualmente robusta y gestionable.
- **Opción Multiplataforma y de Código Abierto (para casos muy específicos): VeraCrypt**. Es una excelente herramienta, pero requiere una configuración más manual y no es tan fácil de gestionar centralizadamente para una PYME. La recomendación principal es BitLocker/FileVault.

5. Fuentes Consultadas

- ISO/IEC 27002:2022 – Controles de seguridad de la información
- AXELOS (2021). ITIL® 4: Guía de prácticas directivas, estratégicas y de mejora.
- Reglamento (UE) 2016/679 (RGPD) - Reglamento General de Protección de Datos.
- Ley Orgánica 3/2018 (LOPDGDD) - Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- Agencia española de protección de datos
- Documentación oficial de Microsoft: Microsoft Purview, Microsoft Intune, BitLocker.
- Documentación oficial de OpenVPN.