**Práctica integradora**

Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. La información confidencial de la empresa tiene buena seguridad lógica, pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica. No tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

**Microdesafío**

La empresa que se les haya asignado los contrata como asesores de seguridad, ya que creen que es una parte fundamental para resguardar sus activos. En base a lo visto en clase y clases anteriores deben hacer:

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.