Punto 3. Análisis de las necesidades.

Empresa de ciberseguridad Redex.

**Análisis de Necesidades – Empresa de Ciberseguridad "Redex"**

**1. Definición de la empresa**

* **Nombre**: Redex
* **Actividad principal**: Prestación de servicios de ciberseguridad (auditorías, pentesting, consultoría en seguridad, respuesta ante incidentes, formación).
* **Tamaño**: Mediana empresa con aproximadamente 50 empleados.
* **Ubicación**: Madrid, con una oficina central y posibilidad de trabajo remoto.
* **Modalidad de trabajo**: Híbrida (30% presencial – 70% remoto).
* **Infraestructura**: Oficina con centro de datos interno reducido y servidores en la nube.

**2. Estructura de personal**

* **Dirección**: 1 CEO, 1 CTO, 1 CFO
* **Administración y RRHH**: 3 personas
* **Departamento Técnico**:
  + 10 analistas de ciberseguridad
  + 10 especialistas en pruebas de penetración (pentesters)
  + 6 ingenieros de sistemas y redes
  + 4 desarrolladores de herramientas de ciberseguridad
  + 3 expertos en respuesta a incidentes
  + 2 analistas de malware
* **Departamento de soporte y operaciones**: 5 técnicos
* **Departamento comercial y atención al cliente**: 5 personas

**3. Servicios ofrecidos**

* Auditorías de seguridad (internas y externas)
* Pruebas de penetración
* Hardening de sistemas y redes
* Consultoría en cumplimiento normativo (ISO 27001, ENS, RGPD)
* Formación en ciberseguridad
* Servicios gestionados (MDR, SOC as a Service)
* Respuesta a incidentes y análisis forense

**4. Infraestructura tecnológica requerida**

* **Puestos de trabajo**:
  + Estaciones de trabajo de alto rendimiento para pentesters y analistas (Linux preferente)
  + Portátiles seguros y cifrados para directivos y empleados móviles (Linux/Windows según perfil)
  + Equipos con Windows para departamentos administrativos y comerciales
* **Servidores**:
  + Servidores Linux para gestión de logs, SIEM, IDS/IPS, honeypots y VPNs
  + Servidores Windows para compatibilidad con algunos clientes y uso de Active Directory
* **Redes**:
  + Segmentación de red para aumentar la seguridad
  + Accesos VPN con doble autenticación
* **Software**:
  + Herramientas de pentesting (Kali Linux, Burp Suite, Metasploit, etc.)
  + Plataformas de gestión de vulnerabilidades
  + Herramientas de ticketing y colaboración (Redmine, Mattermost, etc.)
  + Ofimática (LibreOffice y Microsoft Office)

**5. Requisitos de seguridad**

* Autenticación multifactor para todos los accesos
* Encriptación de datos en tránsito y en reposo
* Sistemas de monitorización y detección de intrusiones
* Políticas estrictas de control de acceso y gestión de contraseñas
* Backups automatizados y verificados

**6. Necesidades futuras**

* Escalabilidad en infraestructura cloud
* Formación continua del personal
* Certificación en normas ISO/ENS
* Alianzas estratégicas con fabricantes de seguridad