Medidas de Seguridad Informática - Guía Práctica

1. Control de acceso

- Contraseñas robustas y únicas.
- Doble factor de autenticación (2FA).
- Mínimo privilegio en accesos.
- Bloqueo automático por inactividad.
- Control de accesos físicos.

2. Protección de dispositivos y endpoints

- Antivirus/EDR actualizado.
- Cifrado de discos (BitLocker, FileVault).
- Restricción de USB y dispositivos externos.
- Política de uso seguro en móviles.

3. Seguridad en la red

- Firewall correctamente configurado.
- Segmentación de red por niveles.
- VPN para acceso remoto seguro.
- Escaneo de puertos y tráfico (IDS/IPS).

4. Gestión de actualizaciones y vulnerabilidades

- Actualizaciones automáticas o supervisadas.
- Inventario de activos actualizado.
- Plan de parcheo regular.

5. Copias de seguridad

- Copias diarias automatizadas.
- Versionado y retención segura.
- Almacenamiento aislado (offline o cloud).
- Pruebas regulares de restauración.

6. Formación del personal

- Formación en buenas prácticas.
- Simulacros de phishing.
- Procedimientos de reporte claro.

7. Seguridad en el software y servicios

- Desarrollo seguro (OWASP).
- HTTPS en todos los servicios.
- Gestor de contraseñas seguro.
- Validación de integridad y logs.

Medidas de Seguridad Informática - Guía Práctica

8. Auditoría y supervisión

- Registros de accesos y cambios.
- Logs de eventos críticos.
- Supervisión con herramientas SIEM (Wazuh, etc.).

9. Medidas organizativas y legales

- Registro de actividades de tratamiento.
- Evaluaciones de impacto (DPIA).
- Contratos con proveedores adecuados.
- Plan de respuesta ante incidentes.