CHECKLIST DE CIBERPROTECCIÓN PARA EMPRESAS

1. Identidades y accesos

☐ Autenticación multifactor (MFA) en correo, nube y accesos críticos

☐ Principio de mínimos privilegios aplicado a usuarios y proveedores

☐ Revisión periódica de cuentas activas e inactivas

2. Copias de seguridad

☐ Backups automáticos y cifrados

☐ Copias almacenadas fuera del entorno principal

☐ Pruebas periódicas de restauración

3. Actualizaciones y parches

☐ Sistemas operativos actualizados

☐ Aplicaciones críticas con parches al día

☐ Inventario básico de software y dispositivos

4. Concienciación del equipo

☐ Formación periódica en phishing e ingeniería social

☐ Protocolos claros ante correos o enlaces sospechosos

☐ Canal interno para reportar incidentes

5. Red y dispositivos

☐ Segmentación básica de red

☐ Protección de dispositivos móviles y portátiles

☐ Accesos WiFi separados (empresa / invitados)

6. Correo y navegación

☐ Filtros antiphishing y antimalware activos

☐ Configuración de

☐ Bloqueo de enlaces y archivos sospechosos

7. Monitorización

☐ Herramientas de detección de comportamientos anómalos

☐ Alertas ante accesos o actividades sospechosas

☐ Registro de eventos críticos

8. Entornos cloud

☐ Accesos protegidos con MFA

☐ Políticas claras de uso de la nube

☐ Revisión de permisos en servicios cloud

9. Evaluación y planificación

☐ Evaluación de riesgos periódica

☐ Auditorías básicas de seguridad

☐ Plan de respuesta ante incidentes documentado

10. Protección financiera

☐ Ciberseguro adaptado al tamaño del negocio

☐ Identificación de proveedores críticos

☐ Procedimientos de continuidad de negocio