1. Mappatura dei sistemi AI in uso nell'organizzazione

Azione concreta: creare un inventario completo di tutti gli strumenti AI utilizzati.

Checklist operativa:

- Elencare tutti i software AI utilizzati (ChatGPT, Claude, Gemini, Copilot, etc.)
- Identificare strumenti AI "nascosti" nei software già in uso (es. funzioni AI in Excel, Word, CRM).
- Documentare chi li usa e per quali attività.
- Verificare se processano dati personali o prendono decisioni automatizzate.

Esempio pratico per uno studio di consulenza del lavoro:

- ChatGPT: ricerca giurisprudenziale, bozze contratti.
- AI nel gestionale: classificazione documenti.
- Software predittivo: valutazione rischi contenziosi.
- Trascrizione AI: sbobinatura riunioni.

2. Classificazione del rischio

Azione concreta: valutare il livello di rischio di ogni sistema AI secondo i criteri dell'AI Act.

Sistemi a RISCHIO LIMITATO (la maggioranza):

- Chatbot per assistenza clienti.
- AI per redazione testi.
- Traduttori automatici.
- Strumenti di analisi dati generale.

Obblighi: informare gli utenti che stanno interagendo con un sistema AI.

Sistemi potenzialmente ad ALTO RISCHIO:

- AI per selezione del personale.
- Sistemi di scoring creditizio.
- AI per valutazioni legali con impatto sui diritti.
- Sistemi biometrici per controllo accessi.

Obblighi: requisiti stringenti di documentazione e supervisione.

3. Implementare la trasparenza

Azione concreta: informare sempre quando si usa l'AI.

Template di informativa base:

"Il presente [documento/analisi/risposta] è stato elaborato con il supporto di sistemi di intelligenza artificiale. Il contenuto è stato verificato e validato da un professionista qualificato."

Dove inserire l'informativa:

- Footer delle e-mail quando si usa AI per rispondere.



- Note nei documenti generati o assistiti da AI.
- Disclaimer nei report analitici.
- Informativa privacy aggiornata.

4. Garantire la supervisione umana

Azione concreta: stabilire procedure di controllo umano.

Procedura minima:

1. Mai delegare completamente decisioni critiche all'AI.
2. Verificare sempre output prima di utilizzarli con clienti.
3. Documentare le verifiche effettuate.
4. Formare il personale sul controllo critico degli output AI.

Esempio di checklist di verifica:

- L'output è fattualmente corretto?
- Ci sono bias o discriminazioni?
- È conforme alla normativa di settore?
- Rispetta la privacy dei dati utilizzati?

5. Gestione dei dati

Azione concreta: proteggere i dati inseriti nei sistemi AI.

Regole base:

- **MAI inserire** dati personali sensibili in AI pubbliche.
- **Anonimizzare** sempre i dati dei clienti.
- **Verificare** le policy privacy del fornitore AI.
- **Preferire** soluzioni AI enterprise con garanzie privacy.

Cosa NON fare:

- Caricare un contratto con nomi reali su ChatGPT.
- Inserire codici fiscali o dati sanitari.
- Condividere informazioni riservate dei clienti.

Cosa fare invece:

- Sostituire nomi con [CLIENTE A], [CONTROPARTE B]
- Usare dati fittizi per esempi.
- Verificare che il fornitore sia GDPR compliant.



6. Documentazione e registro

Azione concreta: tenere traccia dell'uso di AI.

Registro minimo da mantenere:

Data	Sistema AI	Uso	Dati processati	Supervisore	Note
2/08/2025	ChatGPT	**Ricerca normativa**	Nessun dato personale	Avv. Rossi	Verificato output
3/08/2025	Claude	**Bozza contratto**	Dati anonimizzati	Dr. Bianchi	Revisionato completamente

7. Formazione del personale

Azione concreta: organizzare formazione specifica.

Programma formativo minimo:

1. **Rischi dell'AI** (2 ore)
   - Allucinazioni e errori
   - Bias e discriminazioni
   - Rischi privacy
2. **Uso responsabile** (2 ore)
   - Quando usare/non usare AI.
   - Come verificare gli output.
   - Procedure interne.
3. **Obblighi normativi** (1 ora)
   - Trasparenza.
   - Documentazione.
   - Responsabilità.

8. Policy aziendale AI

Azione concreta: redigere una policy interna.

Contenuti essenziali:

1. Sistemi AI autorizzati (lista approvata).
2. Usi consentiti e vietati.
3. Procedure di controllo.
4. Responsabilità e ruoli.
5. Gestione incidenti.



9. Contratti e termini di servizio

Azione concreta: rivedere accordi con fornitori AI.

Verificare presenza di:

- Clausole su conformità AI Act.
- Garanzie su protezione dati.
- Responsabilità per malfunzionamenti.
- Diritti di audit.
- Procedure di notifica modifiche.

10. Piano di risposta agli incidenti

Azione concreta: preparare procedure per gestire problemi.

Scenari da prevedere:

- Output AI errato causa danno a cliente.
- Violazione privacy per uso improprio AI.
- Discriminazione algoritmica segnalata.
- Richiesta di spiegazioni da autorità.

Procedura base:

1. **Bloccare** immediatamente l'uso del sistema.
2. **Documentare** l'incidente.
3. **Notificare** responsabili interni.
4. **Valutare** impatti su clienti/terzi.
5. **Rimediate** e implementare correzioni.

