AI FRONT LAB

Checklist operativa per audit di workflow AI

Documento di supporto del portale Umanità Aumentata / AI Front Lab.

Questa checklist aiuta a fare una prima ricognizione su workflow AI gia in uso o in avvio, soprattutto quando entrano in gioco assistenti di coding, agenti, plugin, integrazioni o strumenti con accessi sensibili.

1. Strumenti e perimetro operativo

- Quali strumenti AI sono gia in uso nel team?
- Quali possono leggere, scrivere o modificare file, repository, configurazioni o sistemi esterni?
- Quali workflow sono solo consultivi e quali possono produrre effetti reali?

2. Account, credenziali e permessi

- Chi controlla gli account usati nei workflow?
- Esistono token, chiavi o profili condivisi senza ownership chiara?
- I permessi concessi sono proporzionati al compito reale?

3. Dati, codice e materiali sensibili

- Quali dati interni, documenti o repository possono transitare nel workflow?
- Quali contenuti non dovrebbero mai essere caricati o esposti agli strumenti?
- Esistono file o configurazioni che richiedono soglie di protezione piu alte?

4. Passaggi di controllo umano

- Dove un output AI puo diventare modifica reale, pubblicazione o decisione?
- Chi puo verificare, correggere o bloccare ogni passaggio critico?
- Esistono punti in cui la revisione umana e solo implicita ma non progettata?

5. Tracce, test e criteri di verifica

- Il workflow lascia log, cronologia o evidenze utili per ricostruire cosa e successo?
- Quali test o controlli minimi servono prima di considerare affidabile il flusso?

- E chiaro cosa conta come esito accettabile e cosa invece richiede stop o rollback?

6. Primo passo operativo

- Qual e il flusso piu utile da verificare per primo?
- Quale rischio o fragilita concreta conviene chiarire subito?
- Quale mini-audit o review circoscritta puo generare il massimo apprendimento con il minimo perimetro?

Domande finali

- Stiamo introducendo automazione piu velocemente dei controlli?
- Abbiamo visibilita sufficiente su permessi, dati e superfici di scrittura?
- Quale scelta renderebbe il workflow piu leggibile e difendibile gia questa settimana?

Fonte: www.aifrontlab.com

Uso consigliato: confronto interno, webinar, workshop, orientamento operativo.