

Checklist Operative per AI Crisis Response Team

Guide Procedurali per la Gestione Operativa degli Incidenti AI

Versione: 1.0

Data di Pubblicazione: 2025

Classificazione: Documento Operativo Riservato

Utilizzo: Esclusivamente per membri dell'AI Crisis Response Team

Sommario Esecutivo

Il presente documento fornisce checklist operative dettagliate per ogni ruolo all'interno dell'AI Crisis Response Team (A-CRT). Ogni checklist è progettata per garantire che tutte le azioni critiche vengano eseguite tempestivamente e in modo coordinato durante la gestione di incidenti AI.

Le checklist sono organizzate per ruolo specifico e fase temporale, consentendo una gestione strutturata e verificabile delle attività di risposta alla crisi.

1. Checklist del Crisis Leader

1.1 Attivazione Immediata (T+0 - T+15 minuti)

Ricezione della Segnalazione:

- ☐ Confermare ricezione della segnalazione di incidente Al critico
- ☐ Registrare timestamp esatto della segnalazione
- ☐ Identificare la fonte della segnalazione e verificare credibilità
- ☐ Effettuare valutazione preliminare della gravità

Attivazione del Team:

- ☐ Convocare immediatamente tutti i membri dell'A-CRT
- ☐ Inviare notifica di attivazione P.R.I.A. con codice "PRIA ACTIVATION"
- ☐ Verificare disponibilità di tutti i membri del team entro 10 minuti
- ☐ Attivare backup per membri non disponibili
- ☐ Stabilire canale di comunicazione prioritario per il team

Preparazione Operativa:

- ☐ Attivare war room fisica o virtuale
- ☐ Verificare funzionamento di tutti i sistemi di comunicazione
- ☐ Preparare documentazione di base (template, procedure, contatti)
- ☐ Informare il Consiglio di Amministrazione dell'attivazione del protocollo

1.2 Coordinamento Iniziale (T+15 - T+60 minuti)

Briefing del Team:

- ☐ Condurre briefing iniziale con tutti i membri dell'A-CRT
- ☐ Presentare informazioni disponibili sull'incidente
- ☐ Assegnare responsabilità specifiche a ogni membro del team
- ☐ Stabilire timeline per le prime azioni critiche
- ☐ Definire frequenza e modalità degli aggiornamenti interni

Valutazione della Gravità:

- ☐ Applicare la scala DEFCON-AI per classificare l'incidente
- ☐ Documentare la classificazione e le motivazioni
- ☐ Adeguare le procedure operative al livello di gravità identificato
- ☐ Comunicare la classificazione a tutto il team

Decisioni Strategiche Iniziali:

- ☐ Decidere se attivare consulenti esterni
- ☐ Determinare necessità di comunicazioni pubbliche immediate
- ☐ Autorizzare azioni di contenimento tecnico
- ☐ Stabilire budget di emergenza per la gestione della crisi

1.3 Gestione Continuativa (T+1 ora in poi)

Supervisione Operativa:

- ☐ Condurre briefing del team ogni 2 ore nelle prime 24 ore
- ☐ Monitorare progressi di tutte le workstream
- ☐ Prendere decisioni su escalation e de-escalation
- ☐ Approvare tutte le comunicazioni esterne

Comunicazioni Strategiche:

- ☐ Mantenere aggiornato il Consiglio di Amministrazione
- ☐ Gestire comunicazioni con investitori e partner strategici
- ☐ Coordinare con ufficio legale per aspetti normativi
- ☐ Supervisionare comunicazioni con autorità competenti

Documentazione e Controllo:

- ☐ Garantire documentazione completa di tutte le decisioni
 - ☐ Monitorare rispetto delle timeline stabilite
 - ☐ Autorizzare modifiche alle procedure standard quando necessario
 - ☐ Preparare report periodici per stakeholder interni
-

2. Checklist dell'AI Ethics Advisor

2.1 Analisi Tecnica Immediata (T+0 - T+30 minuti)

Valutazione Tecnica Preliminare:

- ☐ Accedere ai sistemi AI coinvolti nell'incidente
- ☐ Identificare il tipo di malfunzionamento (bias, allucinazione, errore logico, etc.)
- ☐ Valutare la portata tecnica del problema
- ☐ Stimare il numero potenziale di output problematici generati

Analisi dell'Impatto:

- ☐ Identificare categorie di utenti potenzialmente impattati
- ☐ Valutare gravità dell'impatto per categoria di utente
- ☐ Identificare potenziali violazioni etiche (discriminazione, privacy, etc.)
- ☐ Stimare rischi di propagazione del problema

Raccomandazioni Immediate:

- ☐ Fornire raccomandazioni per il contenimento tecnico
- ☐ Suggestire priorità nelle azioni di rimedio
- ☐ Identificare necessità di expertise tecnica aggiuntiva

- ☐ Comunicare valutazione preliminare al Crisis Leader

2.2 Analisi Approfondita (T+30 minuti - T+4 ore)

Investigazione delle Cause Radice:

- ☐ Analizzare log di sistema per identificare sequenza di eventi
- ☐ Esaminare dati di training per identificare potenziali bias
- ☐ Verificare configurazioni e parametri del sistema
- ☐ Identificare eventuali modifiche recenti ai sistemi

Valutazione Etica Completa:

- ☐ Applicare framework etico aziendale per valutare l'incidente
- ☐ Identificare principi etici violati (fairness, transparency, accountability)
- ☐ Valutare conformità con linee guida AI etiche settoriali
- ☐ Documentare implicazioni etiche per diverse categorie di stakeholder

Sviluppo di Raccomandazioni:

- ☐ Formulare raccomandazioni tecniche per la risoluzione
- ☐ Proporre miglioramenti ai sistemi di controllo etico
- ☐ Suggerire modifiche ai processi di sviluppo AI
- ☐ Preparare briefing tecnico per comunicazioni esterne

2.3 Supporto Continuativo

Monitoraggio Tecnico:

- ☐ Supervisionare implementazione delle soluzioni tecniche
- ☐ Verificare efficacia delle misure di contenimento
- ☐ Monitorare per eventuali effetti collaterali delle correzioni

- ☐ Validare testing delle soluzioni implementate

Supporto alle Comunicazioni:

- ☐ Fornire spiegazioni tecniche comprensibili per comunicazioni clienti
 - ☐ Preparare FAQ tecniche per il team di customer support
 - ☐ Supportare preparazione di materiali per autorità normative
 - ☐ Contribuire alla preparazione del report post-mortem
-

3. Checklist del Chief Legal Officer

3.1 Valutazione Legale Immediata (T+0 - T+45 minuti)

Analisi dei Rischi Legali:

- ☐ Identificare potenziali violazioni contrattuali
- ☐ Valutare rischi di violazioni normative (GDPR, AI Act, etc.)
- ☐ Stimare esposizione a azioni legali da parte di clienti
- ☐ Identificare obblighi di notifica alle autorità

Obblighi Normativi Immediati:

- ☐ Verificare necessità di notifica entro 72 ore (GDPR)
- ☐ Identificare altre autorità da notificare
- ☐ Preparare timeline per adempimenti normativi obbligatori
- ☐ Attivare consulenti legali esterni se necessario

Protezione Legale:

- ☐ Implementare legal hold su documenti rilevanti

- ☐ Preparare comunicazioni coperte da privilegio legale
- ☐ Contattare compagnie assicurative per potenziali claim
- ☐ Preparare strategia difensiva preliminare

3.2 Gestione Compliance (T+45 minuti - T+4 ore)

Notifiche Normative:

- ☐ Preparare notifica formale al Garante Privacy (se applicabile)
- ☐ Compilare moduli richiesti dalle autorità competenti
- ☐ Coordinare invio delle notifiche entro i termini previsti
- ☐ Preparare documentazione di supporto per le autorità

Gestione Contrattuale:

- ☐ Rivedere contratti clienti per clausole di limitazione responsabilità
- ☐ Identificare obblighi specifici verso clienti enterprise
- ☐ Preparare comunicazioni contrattuali formali quando richieste
- ☐ Valutare necessità di modifiche contrattuali future

Coordinamento con Assicurazioni:

- ☐ Notificare incidente alle compagnie assicurative
- ☐ Preparare documentazione richiesta per claim
- ☐ Coordinare con adjuster assicurativi
- ☐ Monitorare coperture applicabili

3.3 Supporto Legale Continuativo

Gestione Litigation:

- ☐ Monitorare per potenziali azioni legali

- ☐ Preparare strategie difensive
- ☐ Coordinare con studi legali esterni
- ☐ Gestire discovery e produzione documentale

Compliance Monitoring:

- ☐ Monitorare risposta delle autorità alle notifiche
 - ☐ Gestire eventuali richieste di informazioni aggiuntive
 - ☐ Coordinare con audit esterni se richiesti
 - ☐ Preparare report di compliance per il management
-

4. Checklist del Head of Communications

4.1 Preparazione Comunicativa Immediata (T+0 - T+30 minuti)

Valutazione della Situazione Comunicativa:

- ☐ Valutare potenziale impatto reputazionale
- ☐ Identificare stakeholder chiave da informare
- ☐ Monitorare menzioni sui social media e news
- ☐ Preparare holding statement preliminare

Attivazione Canali di Comunicazione:

- ☐ Attivare hotline dedicata per media
- ☐ Preparare social media team per monitoraggio intensivo
- ☐ Contattare agenzia PR esterna se necessario
- ☐ Preparare canali di comunicazione interna

Preparazione Materiali Base:

- ☐ Adattare template di comunicazione alla situazione specifica
- ☐ Preparare FAQ preliminari
- ☐ Raccogliere informazioni aziendali standard
- ☐ Preparare lista contatti media prioritari

4.2 Gestione Comunicazioni Esterne (T+30 minuti - T+2 ore)

Holding Statement:

- ☐ Finalizzare holding statement con Crisis Leader
- ☐ Ottenere approvazione legale per il contenuto
- ☐ Distribuire holding statement ai media principali
- ☐ Pubblicare su canali aziendali ufficiali

Gestione Media:

- ☐ Rispondere a richieste immediate dei giornalisti
- ☐ Programmare interviste se appropriate
- ☐ Monitorare copertura mediatica in tempo reale
- ☐ Preparare correzioni per eventuali inesattezze

Comunicazioni Digital:

- ☐ Pubblicare aggiornamenti sui social media aziendali
- ☐ Monitorare sentiment sui social media
- ☐ Rispondere a commenti e domande appropriate
- ☐ Gestire crisis hashtag se emergenti

4.3 Comunicazioni Continuative

Aggiornamenti Regolari:

- ☐ Preparare aggiornamenti ogni 24-48 ore
- ☐ Coordinare messaggi coerenti su tutti i canali
- ☐ Monitorare efficacia delle comunicazioni
- ☐ Adattare strategia comunicativa basata su feedback

Gestione Stakeholder:

- ☐ Preparare comunicazioni specifiche per investitori
 - ☐ Coordinare con partner commerciali
 - ☐ Gestire comunicazioni con dipendenti
 - ☐ Mantenere dialogo con clienti chiave
-

5. Checklist del Chief Technology Officer

5.1 Contenimento Tecnico Immediato (T+0 - T+30 minuti)

Isolamento del Sistema:

- ☐ Identificare tutti i sistemi AI coinvolti
- ☐ Implementare shutdown controllato dei sistemi problematici
- ☐ Verificare che l'isolamento sia completo
- ☐ Documentare timestamp e procedure di isolamento

Preservazione delle Evidenze:

- ☐ Creare backup completi di log di sistema
- ☐ Preservare stati delle applicazioni al momento dell'incidente

- ☐ Salvare configurazioni attive
- ☐ Implementare chain of custody per evidenze digitali

Valutazione dell'Infrastruttura:

- ☐ Verificare integrità dei sistemi non coinvolti
- ☐ Identificare potenziali punti di propagazione
- ☐ Valutare impatto su sistemi dipendenti
- ☐ Implementare monitoraggio intensivo

5.2 Analisi Tecnica (T+30 minuti - T+4 ore)

Analisi Forense Preliminare:

- ☐ Analizzare log per ricostruire sequenza di eventi
- ☐ Identificare input che hanno causato l'output problematico
- ☐ Verificare integrità dei modelli AI
- ☐ Analizzare performance dei sistemi di controllo

Sviluppo di Soluzioni:

- ☐ Identificare cause radice tecniche
- ☐ Sviluppare patch temporanee se possibili
- ☐ Progettare soluzioni permanenti
- ☐ Stimare tempi di implementazione

Testing e Validazione:

- ☐ Testare soluzioni in ambiente isolato
- ☐ Validare efficacia delle correzioni
- ☐ Verificare assenza di effetti collaterali

- ☐ Preparare piano di rollback se necessario

5.3 Implementazione e Monitoraggio

Implementazione Soluzioni:

- ☐ Implementare correzioni in ambiente di produzione
- ☐ Monitorare sistemi durante il rollout
- ☐ Verificare ripristino delle funzionalità
- ☐ Documentare tutte le modifiche implementate

Monitoraggio Post-Implementazione:

- ☐ Implementare monitoraggio intensivo per 48 ore
 - ☐ Verificare stabilità dei sistemi corretti
 - ☐ Monitorare per ricorrenze del problema
 - ☐ Preparare report tecnico per il team
-

6. Checklist del Customer Success Leader

6.1 Identificazione Clienti Impattati (T+0 - T+1 ora)

Mappatura dell'Impatto:

- ☐ Identificare tutti i clienti potenzialmente impattati
- ☐ Categorizzare clienti per livello di impatto
- ☐ Prioritizzare clienti enterprise e strategici
- ☐ Preparare liste di contatto aggiornate

Valutazione dell'Impatto per Cliente:

- ☐ Quantificare impatto specifico per ogni cliente
- ☐ Identificare dati o servizi coinvolti
- ☐ Valutare urgenza delle comunicazioni
- ☐ Preparare informazioni personalizzate

Preparazione del Team:

- ☐ Briefing del team customer success sull'incidente
- ☐ Distribuzione di script e FAQ per il supporto
- ☐ Attivazione di risorse aggiuntive se necessario
- ☐ Preparazione di canali di comunicazione dedicati

6.2 Comunicazioni ai Clienti (T+1 - T+4 ore)

Notifiche Dirette:

- ☐ Inviare notifiche personalizzate ai clienti impattati
- ☐ Utilizzare canali di comunicazione preferiti per ogni cliente
- ☐ Fornire informazioni specifiche sull'impatto
- ☐ Offrire canali di supporto dedicati

Gestione delle Richieste:

- ☐ Rispondere a tutte le richieste clienti entro 2 ore
- ☐ Escalation immediata per clienti enterprise
- ☐ Documentare tutte le interazioni
- ☐ Fornire aggiornamenti regolari

Coordinamento Interno:

- ☐ Aggiornare team tecnico su feedback clienti

- ☐ Coordinare con team legale per questioni contrattuali
- ☐ Supportare team comunicazioni con insight clienti
- ☐ Monitorare sentiment generale dei clienti

6.3 Gestione Continuativa

Supporto Clienti:

- ☐ Mantenere canali di supporto dedicati attivi
- ☐ Fornire aggiornamenti regolari sui progressi
- ☐ Gestire richieste di compensazione
- ☐ Monitorare soddisfazione clienti post-incidente

Retention e Recovery:

- ☐ Implementare misure di retention per clienti a rischio
 - ☐ Preparare offerte di compensazione appropriate
 - ☐ Pianificare attività di relationship recovery
 - ☐ Monitorare churn rate post-incidente
-

7. Checklist di Coordinamento Inter-Team

7.1 Sincronizzazione delle Attività

Briefing Coordinati:

- ☐ Briefing generale ogni 2 ore nelle prime 24 ore
- ☐ Aggiornamenti specifici per workstream ogni ora
- ☐ Escalation immediata per decisioni critiche

- ☐ Documentazione di tutte le decisioni prese

Condivisione Informazioni:

- ☐ Database condiviso per tracking delle attività
- ☐ Canale di comunicazione dedicato sempre attivo
- ☐ Condivisione immediata di sviluppi critici
- ☐ Backup documentation per tutte le attività

7.2 Quality Control

Verifica delle Attività:

- ☐ Controllo completamento checklist per ogni ruolo
- ☐ Verifica coerenza delle comunicazioni esterne
- ☐ Validazione delle decisioni tecniche
- ☐ Controllo compliance delle azioni intraprese

Documentazione Completa:

- ☐ Registrazione di tutte le timeline
- ☐ Documentazione delle decisioni e motivazioni
- ☐ Conservazione di tutte le comunicazioni
- ☐ Preparazione materiali per post-mortem

Checklist sviluppate secondo standard operativi per la gestione professionale delle crisi AI aziendali.