# Modèle Post-Mortem – Réponse aux Incidents

## 1. Résumé de l'incident

... Rédigez un résumé de l'incident en quelques phrases. Décrivez ce qui s'est passé et pourquoi, la gravité de l'incident et la durée de son impact.

## 2. Chronologie des événements

... Détaillez la chronologie de l'incident. Nous vous recommandons d'utiliser UTC pour normaliser les fuseaux horaires.

Indiquez tous les événements antérieurs, tout début d'activité, le premier impact connu et les remontées. Notez les décisions prises ou les changements apportés, la date à laquelle l'incident a pris fin, ainsi que tout événement survenu après l'impact.

Identification de la cause profonde : les « Cinq pourquoi »

Les « Cinq pourquoi » constituent une technique d'identification de la cause profonde. Voici comment l'appliquer :

1. Commencez par décrire l'impact et demandez-vous pourquoi il s'est produit.
2. Notez l'impact de l'incident.
3. Demandez-vous pourquoi l'incident s'est produit et pourquoi il a eu l'impact qui en a résulté. Ensuite, continuez à vous demander « pourquoi » jusqu'à trouver une cause profonde.
4. Consignez les « pourquoi » dans votre documentation post mortem

## 3. Impact (opérationnel, financier, réputationnel)

... Décrivez comment les utilisateurs internes et externes ont été affectés au cours de l'incident. Incluez le nombre de dossiers de support créés.

## 4. Détection (qui, quoi, comment)

... Quand l'équipe a-t-elle détecté l'incident ? Comment a-t-elle pris conscience de sa survenue ? Comment améliorer le temps de détection ? Posez la question suivante : comment aurions-nous pu réduire ce temps de moitié ?

## 5. Réponse (actions entreprises)

... Qui a répondu à l'incident ? Quand la réponse a-t-elle eu lieu et en quoi consistait-elle ? Notez tout retard ou obstacle à la réponse.

## 6. Récupération (retour à la normale)

... Décrivez comment le service a été rétabli et pourquoi l'incident a été jugé terminé. Expliquez comment vous avez réussi à rétablir le service et comment vous connaissiez les mesures à prendre pour garantir la récupération.

Selon le scénario, posez-vous les questions suivantes : comment améliorer le temps d'atténuation ? Comment auriez-vous pu réduire ce temps de moitié ?

## 7. Analyse de la cause profonde (RCA)

... Notez la cause profonde définitive de l'incident, l'élément identifié à modifier afin d'éviter que cette catégorie d'incident ne se reproduise

## 8. Enseignements clés

... Discutez de ce qui s'est bien passé lors de la réponse aux incidents, de ce qui aurait pu être amélioré et des possibilités d'amélioration.

## 9. Actions correctives et préventives

... Décrivez les actions correctives ordonnées pour prévenir cette catégorie d'incident à l'avenir. Notez qui est responsable, quand il doit terminer le travail et à quel niveau ce dernier fait l'objet d'un suivi.