

Modeles de scénario pour la gestion de crise

Modèles de scénarios de crise

10 scénarios prêts à l'emploi pour vos exercices de simulation

Introduction

Les exercices de simulation constituent un élément essentiel dans la préparation à la gestion de crise. Ils permettent de tester les procédures, d'entraîner les équipes et d'identifier les points d'amélioration de votre dispositif. Ce document vous propose 10 scénarios détaillés, adaptables à différents secteurs d'activité, pour organiser des exercices réalistes et formateurs.

Comment utiliser ce guide

Chaque scénario comprend :

- Une description générale de la situation
- Un déroulé chronologique avec des "injects" (informations nouvelles)
- Des éléments contextuels (communications externes, réactions des parties prenantes)
- Des variantes pour adapter le scénario à votre contexte
- Des points d'observation pour évaluer la réponse

Vous pouvez utiliser ces scénarios tels quels ou les adapter à votre organisation en modifiant les noms, les lieux et les spécificités techniques pour les rendre plus pertinents à votre contexte.

Sommaire des scénarios

1. **Cyberattaque par ransomware**
 2. **Incendie dans les locaux**
 3. **Scandale médiatique et crise de réputation**
 4. **Défaillance d'un fournisseur critique**
 5. **Accident grave impliquant des collaborateurs**
 6. **Contamination de produit/service**
 7. **Catastrophe naturelle impactant les opérations**
 8. **Crise sanitaire et pandémie**
 9. **Fraude interne et malveillance**
 10. **Panne majeure des systèmes d'information**
-

Scénario 1 : Cyberattaque par ransomware

Description générale

Votre organisation est victime d'une attaque par ransomware qui chiffre les données de votre système d'information. Les pirates demandent une rançon en cryptomonnaie pour débloquer vos données. L'incident affecte progressivement l'ensemble de vos services informatiques.

Public cible

- Comité de direction
- Équipe informatique
- Service juridique
- Communication
- Ressources humaines

Objectifs de l'exercice

- Tester la coordination entre IT et direction
- Évaluer la prise de décision concernant la rançon
- Vérifier les procédures de communication interne/externe
- Tester les procédures de restauration des données

Déroulé chronologique

Jour 1 - 8h30

Situation initiale : Un employé des services financiers signale qu'il ne peut plus accéder à ses fichiers. Un message s'affiche sur son écran indiquant que les fichiers ont été chiffrés et qu'une rançon de 50 000 € en Bitcoin doit être payée dans les 72 heures.

Inject 1 (J1 - 9h00) : Le service informatique confirme que plusieurs postes sont touchés. Les utilisateurs ne peuvent plus accéder à leurs documents.

Inject 2 (J1 - 10h30) : L'infection se propage rapidement. Le serveur de fichiers principal est désormais inaccessible.

Inject 3 (J1 - 11h30) : Les premiers clients signalent l'impossibilité d'accéder à votre portail en ligne.

Inject 4 (J1 - 14h00) : Un expert en cybersécurité externe est contacté. Il confirme un ransomware sophistiqué qui semble avoir été introduit il y a plusieurs semaines.

Inject 5 (J1 - 16h00) : Les hackers envoient un nouveau message, augmentant la rançon à 80 000 € si le paiement n'est pas effectué dans les 48 heures.

Jour 2

Inject 6 (J2 - 9h00) : Les équipes IT signalent que les sauvegardes récentes semblent également compromises. Seules les sauvegardes de plus de 3 mois sont potentiellement utilisables.

Inject 7 (J2 - 11h00) : Un journaliste local contacte le service communication pour un article sur "l'attaque informatique" dont vous êtes victime.

Inject 8 (J2 - 14h00) : Les analyses techniques révèlent que des données confidentielles ont probablement été exfiltrées avant le chiffrement.

Inject 9 (J2 - 17h00) : L'ANSSI vous contacte car d'autres entreprises de votre secteur sont touchées par la même attaque.

Éléments contextuels

Communications externes :

- Email de revendication des hackers
- Messages inquiets de clients sur les réseaux sociaux
- Demandes de précisions des partenaires commerciaux

Réactions des parties prenantes :

- Collaborateurs anxieux cherchant des informations
- Clients mécontents de l'interruption de service
- Fournisseurs inquiets pour leurs données

Variantes possibles

- Attaque pendant un week-end ou des congés
- Fuite dans la presse avec données sensibles publiées
- Attaque ciblant spécifiquement votre système de production/service critique

Points d'observation

- Délai de détection et d'alerte
- Efficacité de l'isolement des systèmes pour limiter la propagation
- Qualité de la communication interne et externe
- Processus de décision concernant le paiement de la rançon
- Capacité à maintenir les activités essentielles en mode dégradé
- Coordination avec les autorités compétentes (ANSSI, CNIL, police)

Scénario 2 : Incendie dans les locaux

Description générale

Un incendie se déclare dans vos locaux pendant les heures de travail, nécessitant une évacuation d'urgence et causant des dommages significatifs à

une partie de vos installations. L'incident provoque une interruption immédiate de vos activités et soulève des questions de sécurité, de continuité d'activité et de communication.

Public cible

- Comité de direction
- Équipe sécurité/services généraux
- Ressources humaines
- Communication
- Responsables opérationnels

Objectifs de l'exercice

- Évaluer l'efficacité des procédures d'évacuation et de mise en sécurité
- Tester l'activation du plan de continuité d'activité
- Vérifier la chaîne d'alerte et la mobilisation des équipes
- Évaluer la coordination avec les services d'urgence externes
- Tester les processus de communication de crise

Déroulé chronologique

Jour 1

Situation initiale (J1 - 10h30) : Une alarme incendie se déclenche dans le bâtiment principal. De la fumée est visible au deuxième étage, dans la zone des services administratifs.

Inject 1 (J1 - 10h35) : Le responsable sécurité confirme un départ de feu dans une salle technique. L'évacuation du bâtiment est en cours.

Inject 2 (J1 - 10h45) : Les pompiers arrivent sur le site et prennent en charge la situation. Ils demandent des informations sur les matériaux dangereux potentiels et les personnes possiblement présentes dans le bâtiment.

Inject 3 (J1 - 11h15) : Un collaborateur est signalé manquant lors du comptage au point de rassemblement. Son badge indique qu'il était présent ce matin.

Inject 4 (J1 - 11h45) : Les pompiers confirment que l'incendie est circonscrit mais a causé des dégâts importants au deuxième étage et des dommages dus

à l'eau au premier étage. Le collaborateur manquant a été retrouvé (il avait quitté le site pour une réunion externe sans badger).

Inject 5 (J1 - 12h30) : Les autorités informent que le bâtiment ne pourra pas être réintégré avant plusieurs jours pour des raisons de sécurité. Une enquête sur l'origine du sinistre est ouverte.

Inject 6 (J1 - 14h00) : Plusieurs médias locaux sont présents aux abords du site et sollicitent des interviews. Des photos de l'incendie circulent déjà sur les réseaux sociaux.

Inject 7 (J1 - 16h00) : Les experts de l'assurance arrivent pour une première évaluation des dégâts. Ils estiment que les travaux de remise en état prendront au minimum 3 semaines.

Jour 2

Inject 8 (J2 - 9h00) : Une réunion de crise est organisée pour faire le point sur la situation. Les services IT signalent que le serveur local hébergeant des applications critiques a été endommagé.

Inject 9 (J2 - 11h00) : Plusieurs clients majeurs expriment leur inquiétude quant à votre capacité à honorer vos engagements dans les délais prévus.

Inject 10 (J2 - 14h00) : L'enquête préliminaire suggère qu'un défaut électrique serait à l'origine de l'incendie. Des questions se posent sur la maintenance préventive des installations.

Éléments contextuels

Communications externes :

- Questions des médias locaux
- Demandes d'informations des clients et fournisseurs
- Rapport préliminaire des pompiers
- Communication des assurances

Réactions des parties prenantes :

- Anxiété des collaborateurs concernant leur sécurité et leur poste de travail
- Préoccupations des clients quant aux délais de livraison
- Intérêt des concurrents pour récupérer des marchés

- Sollicitations de soutien des partenaires locaux

Variantes possibles

- Incendie se déclarant en dehors des heures de travail
- Origine criminelle suspectée
- Blessés graves nécessitant une hospitalisation
- Contamination environnementale due aux eaux d'extinction

Points d'observation

- Efficacité des procédures d'évacuation et du comptage
 - Rapidité de mobilisation de la cellule de crise
 - Qualité de la communication avec les parties prenantes
 - Mise en œuvre effective du plan de continuité d'activité
 - Gestion des aspects humains (soutien psychologique, réaffectation)
 - Coordination avec les services externes (pompiers, police, assurance)
-

Scénario 3 : Scandale médiatique et crise de réputation

Description générale

Votre organisation fait face à une crise de réputation suite à des accusations graves relayées par les médias et amplifiées sur les réseaux sociaux. La situation menace votre image de marque, la confiance de vos clients et partenaires, ainsi que le moral de vos équipes.

Public cible

- Direction générale
- Service communication
- Service juridique
- Ressources humaines
- Responsables métiers concernés

Objectifs de l'exercice

- Tester la réactivité de la communication de crise
- Évaluer la coordination entre communication et juridique
- Vérifier l'efficacité de la veille médiatique et du monitoring des réseaux sociaux
- Développer la capacité à formuler des messages adaptés aux différentes parties prenantes
- Tester la gestion des demandes médias sous pression

Déroulé chronologique

Jour 1

Situation initiale (J1 - 8h00) : Un média en ligne influent publie un article accusatoire concernant des pratiques douteuses au sein de votre organisation (options selon votre secteur : fraude, harcèlement, non-respect des normes environnementales, discrimination, défauts de sécurité cachés, etc.).

Inject 1 (J1 - 8h30) : L'article est partagé massivement sur les réseaux sociaux, avec plusieurs milliers de partages en quelques heures. Un hashtag critique envers votre entreprise commence à être tendance.

Inject 2 (J1 - 9h15) : Plusieurs médias nationaux contactent votre service communication pour obtenir votre réaction. Ils précisent qu'ils publieront leurs articles dans la journée, avec ou sans votre commentaire.

Inject 3 (J1 - 10h30) : Des collaborateurs signalent qu'ils sont contactés directement via LinkedIn par des journalistes. Certains messages internes commencent à fuiter sur les réseaux sociaux.

Inject 4 (J1 - 12h00) : Une ONG ou association professionnelle annonce qu'elle suspend sa collaboration avec votre organisation dans l'attente d'éclaircissements.

Inject 5 (J1 - 14h30) : Le service client est submergé d'appels et de messages de clients inquiets ou mécontents. Certains menacent d'annuler leurs commandes ou contrats.

Inject 6 (J1 - 16h00) : Une chaîne d'information en continu annonce un reportage spécial sur l'affaire pour le journal de 20h. Ils sollicitent une interview

en direct avec un représentant de votre organisation.

Jour 2

Inject 7 (J2 - 8h00) : De nouveaux témoignages aggravants sont publiés dans la presse. Un concurrent se positionne publiquement comme “l’alternative éthique” à votre organisation.

Inject 8 (J2 - 10h30) : Plusieurs clients importants vous contactent pour exiger des explications et des garanties formelles.

Inject 9 (J2 - 14h00) : Un groupe de collaborateurs exprime publiquement sa désapprobation des pratiques dénoncées et appelle à des changements internes.

Inject 10 (J2 - 16h30) : Une autorité de régulation ou instance professionnelle annonce l’ouverture d’une enquête sur les faits allégués.

Éléments contextuels

Communications externes :

- Articles de presse de plus en plus nombreux
- Commentaires virulents sur les réseaux sociaux
- Demandes formelles d’explication des partenaires
- Communications opportunistes des concurrents

Réactions des parties prenantes :

- Baisse de moral des collaborateurs et questionnements internes
- Inquiétude des investisseurs et impact sur la valeur boursière (si applicable)
- Méfiance accrue des clients et prospects
- Pression des autorités de tutelle ou organismes professionnels

Variantes possibles

- Crise déclenchée par un lanceur d’alerte interne
- Accusations basées sur des informations partiellement fausses ou déformées
- Crise survenant juste avant un événement commercial important
- Implication de personnalités politiques ou médiatiques dans la dénonciation

Points d'observation

- Réactivité initiale et qualité de la première communication
 - Cohérence des messages entre les différents canaux
 - Gestion de la pression médiatique et des demandes d'interview
 - Équilibre entre reconnaissance des problèmes et défense de l'organisation
 - Capacité à mobiliser des soutiens et des témoignages positifs
 - Communication interne pour maintenir l'engagement des collaborateurs
-

Scénario 4 : Défaillance d'un fournisseur critique

Description générale

Un fournisseur essentiel à votre chaîne d'approvisionnement ou à la fourniture de vos services connaît une défaillance majeure qui impacte directement votre capacité à maintenir votre activité normale. Cette situation met en péril vos engagements envers vos clients et nécessite une réorganisation rapide de vos opérations.

Public cible

- Direction des opérations/production
- Achats et supply chain
- Service commercial et relation client
- Direction générale
- Service juridique

Objectifs de l'exercice

- Tester la résilience de la chaîne d'approvisionnement
- Évaluer la capacité à identifier rapidement des solutions alternatives
- Vérifier les procédures de priorisation des clients et activités
- Tester la coordination entre les fonctions opérationnelles et commerciales
- Évaluer les processus de communication avec les clients impactés

Déroulé chronologique

Jour 1

Situation initiale (J1 - 9h00) : Vous recevez une notification urgente d'un fournisseur stratégique vous informant qu'il fait face à une interruption majeure de ses activités (options selon contexte : faillite soudaine, incendie dans son usine, grève massive, problème qualité critique, cyberattaque paralysante, etc.).

Inject 1 (J1 - 9h30) : Votre service des achats confirme que les livraisons prévues pour la semaine sont annulées. Aucune date de reprise n'est communiquée.

Inject 2 (J1 - 10h15) : Un état des stocks révèle que vous disposez d'une autonomie limitée (selon votre activité : quelques jours à quelques semaines) avant impact critique sur votre production ou service.

Inject 3 (J1 - 11h30) : D'autres entreprises de votre secteur, également clientes de ce fournisseur, commencent à contacter les fournisseurs alternatifs, créant une forte tension sur le marché.

Inject 4 (J1 - 14h00) : Votre service commercial signale que plusieurs commandes importantes doivent être livrées dans les 15 jours, avec des pénalités contractuelles significatives en cas de retard.

Inject 5 (J1 - 16h30) : Un fournisseur alternatif est identifié mais avec des délais de livraison allongés, des prix supérieurs de 30% et une capacité limitée à 60% de vos besoins habituels.

Jour 2

Inject 6 (J2 - 8h30) : Les médias spécialisés de votre secteur commencent à relayer l'information sur les difficultés du fournisseur, générant des appels inquiets de vos clients.

Inject 7 (J2 - 10h00) : Votre service juridique analyse les contrats et confirme que la clause de force majeure pourrait être invoquée, mais avec un risque contentieux significatif.

Inject 8 (J2 - 11h30) : Une réunion technique avec le fournisseur défaillant révèle que son retour à la normale prendrait au minimum 4 semaines et qu'il

priorise ses plus gros clients.

Inject 9 (J2 - 14h00) : Votre plus gros client vous contacte pour exiger des garanties formelles sur ses livraisons à venir et menace de se tourner vers la concurrence.

Inject 10 (J2 - 16h00) : Les équipes opérationnelles proposent une solution de contournement partielle mais qui nécessiterait de modifier temporairement les spécifications de vos produits/services.

Éléments contextuels

Communications externes :

- Informations contradictoires du fournisseur défaillant
- Sollicitations multiples des clients préoccupés
- Démarches opportunistes des concurrents
- Propositions des fournisseurs alternatifs

Réactions des parties prenantes :

- Pression interne des équipes commerciales
- Tension entre les équipes achats et production
- Inquiétude des actionnaires sur l'impact financier
- Questionnements des collaborateurs sur l'organisation du travail

Variantes possibles

- Défaillance affectant simultanément plusieurs fournisseurs (crise sectorielle)
- Problème qualité critique nécessitant un rappel de produits
- Rupture d'approvisionnement liée à des restrictions internationales
- Découverte d'une fraude ou de pratiques non-éthiques chez le fournisseur

Points d'observation

- Rapidité de l'évaluation d'impact et de la prise de décision
- Efficacité de l'identification des solutions alternatives
- Pertinence des critères de priorisation des clients et activités
- Qualité de la communication vers les clients impactés
- Cohérence entre les aspects commerciaux, opérationnels et juridiques

- Capacité à négocier des arrangements avec les fournisseurs et clients
-

Scénario 5 : Accident grave impliquant des collaborateurs

Description générale

Un accident grave impliquant plusieurs de vos collaborateurs survient pendant les heures de travail, avec des blessés sérieux et potentiellement des victimes. Cette situation traumatisante nécessite une gestion humaine, juridique et médiatique immédiate, tout en maintenant la continuité des activités essentielles.

Public cible

- Direction générale
- Ressources humaines
- Service sécurité/HSE
- Service juridique
- Communication
- Management opérationnel

Objectifs de l'exercice

- Tester les procédures d'urgence et de premiers secours
- Évaluer la prise en charge humaine et psychologique
- Vérifier la gestion des aspects juridiques et réglementaires
- Tester la communication de crise dans un contexte émotionnel fort
- Évaluer la capacité à maintenir l'activité dans un contexte traumatisant

Déroulé chronologique

Jour 1

Situation initiale (J1 - 9h15) : Un accident grave se produit sur un de vos sites (options selon votre activité : effondrement d'une structure, accident de

véhicule de service, explosion, chute de hauteur, accident avec machine, etc.). Plusieurs collaborateurs sont impliqués, dont certains gravement blessés.

Inject 1 (J1 - 9h20) : Les services d'urgence (pompiers, SAMU) sont appelés et arrivent sur les lieux. La zone est sécurisée et les premiers soins sont prodigués.

Inject 2 (J1 - 9h40) : Un premier bilan fait état de 3 blessés graves transportés à l'hôpital et 5 blessés légers pris en charge sur place. L'état d'un des blessés graves est critique.

Inject 3 (J1 - 10h30) : Les forces de l'ordre arrivent sur site pour procéder aux premières constatations. Elles demandent accès aux enregistrements de vidéosurveillance et aux documents relatifs à la sécurité.

Inject 4 (J1 - 11h15) : L'inspection du travail est notifiée et annonce son arrivée imminente. Des questions se posent sur le respect des procédures de sécurité.

Inject 5 (J1 - 12h00) : Les médias locaux sont présents aux abords du site et diffusent déjà des images et premières informations, parfois imprécises ou exagérées.

Inject 6 (J1 - 14h30) : L'hôpital informe que l'état d'un des blessés graves s'est détérioré. Sa famille est présente et très bouleversée, demandant des explications à l'entreprise.

Inject 7 (J1 - 16h00) : Les collaborateurs non impliqués sont profondément choqués. Certains refusent de reprendre le travail, estimant les conditions de sécurité insuffisantes.

Jour 2

Inject 8 (J2 - 8h00) : Vous êtes informés que l'un des collaborateurs gravement blessés est décédé dans la nuit, malgré les soins intensifs.

Inject 9 (J2 - 9h30) : Un syndicat appelle à l'exercice du droit de retrait et demande une réunion extraordinaire du CSE (Comité Social et Économique).

Inject 10 (J2 - 11h00) : L'inspection du travail remet un rapport préliminaire pointant des manquements potentiels aux procédures de sécurité.

Inject 11 (J2 - 14h00) : La famille du collaborateur décédé annonce son intention d'engager des poursuites judiciaires pour négligence.

Inject 12 (J2 - 16h30) : Une rumeur circule selon laquelle des alertes antérieures sur les risques auraient été ignorées par la direction.

Éléments contextuels

Communications externes :

- Communiqués officiels des autorités (police, pompiers)
- Articles et reportages des médias locaux et nationaux
- Notifications des autorités de contrôle (inspection du travail)
- Communications des syndicats et représentants du personnel

Réactions des parties prenantes :

- Choc et traumatisme des collaborateurs témoins et collègues
- Détresse et colère des familles des victimes
- Inquiétude des clients et partenaires sur la continuité d'activité
- Questionnements des autres sites/filiales sur leurs propres mesures de sécurité

Variantes possibles

- Accident impliquant également des sous-traitants présents sur site
- Accident survenant lors d'un déplacement professionnel à l'étranger
- Accident avec impact environnemental associé
- Accident touchant plusieurs sites simultanément

Points d'observation

- Efficacité des premiers secours et de la coordination avec les services d'urgence
- Qualité de la prise en charge des aspects humains (victimes, familles, collègues)
- Gestion des relations avec les autorités (police, inspection du travail)
- Communication interne et externe dans un contexte émotionnel
- Traitement des aspects juridiques et assurantiels
- Capacité à maintenir les activités essentielles tout en respectant l'impact émotionnel

Scénario 6 : Contamination de produit/service

Description générale

Une contamination ou un défaut grave est découvert dans l'un de vos produits ou services, créant un risque pour la santé ou la sécurité des utilisateurs. Cette situation nécessite une intervention rapide, potentiellement un rappel de produit, et une gestion de crise impliquant des aspects sanitaires, réglementaires et réputationnels.

Public cible

- Direction générale
- Qualité et production
- Service client
- Affaires réglementaires
- Communication
- Service juridique

Objectifs de l'exercice

- Tester les procédures de rappel de produit ou d'alerte de service
- Évaluer la capacité à identifier l'étendue précise du problème
- Vérifier la communication avec les autorités et instances réglementaires
- Tester la stratégie de communication avec les consommateurs/utilisateurs
- Évaluer la coordination entre les fonctions techniques, réglementaires et commerciales

Déroulé chronologique

Jour 1

Situation initiale (J1 - 8h00) : Vous êtes alertés d'un problème grave avec l'un de vos produits/services (options selon votre secteur : contamination bactérienne, substance toxique, défaut de sécurité, dysfonctionnement dangereux, allergie sévère, etc.).

Inject 1 (J1 - 8h30) : Une première analyse confirme la présence d'un problème potentiellement dangereux pour les utilisateurs/consommateurs. L'origine exacte et l'étendue restent à déterminer.

Inject 2 (J1 - 9h15) : Le service client signale la réception de plusieurs réclamations similaires mentionnant des effets indésirables chez des utilisateurs (maaises, réactions allergiques, blessures, etc.).

Inject 3 (J1 - 10h30) : Les analyses préliminaires suggèrent que le problème pourrait concerner plusieurs lots/versions du produit distribués ces dernières semaines.

Inject 4 (J1 - 11h45) : Un client mécontent publie son expérience négative sur les réseaux sociaux, avec photos à l'appui. La publication commence à être largement partagée.

Inject 5 (J1 - 14h00) : Les autorités réglementaires (selon secteur : DGCCRF, ANSM, etc.) vous contactent suite à des signalements et demandent des informations détaillées sous 24h.

Inject 6 (J1 - 16h30) : Un média spécialisé publie un article sur le problème et sollicite votre réaction officielle.

Jour 2

Inject 7 (J2 - 8h30) : Une réunion de crise est convoquée pour décider de la stratégie à adopter. Les équipes techniques confirment que le risque est significatif.

Inject 8 (J2 - 10h00) : Le service juridique présente les risques légaux et réglementaires. Une décision doit être prise rapidement sur un éventuel rappel de produit.

Inject 9 (J2 - 11h30) : Un cas médical grave potentiellement lié à votre produit/service est signalé. La personne a été hospitalisée.

Inject 10 (J2 - 14h00) : Les autorités réglementaires exigent un plan d'action immédiat et envisagent d'émettre elles-mêmes une alerte publique.

Inject 11 (J2 - 16h00) : L'analyse approfondie révèle que le problème provient d'un changement récent dans le processus de production/fourniture de service ou d'un composant provenant d'un nouveau fournisseur.

Jour 3

Inject 12 (J3 - 9h00) : Suite à votre communication ou celle des autorités, les médias grand public s'emparent de l'affaire. Les demandes d'interview se multiplient.

Inject 13 (J3 - 11h00) : Les distributeurs/partenaires demandent des instructions claires pour la gestion des produits concernés et l'information des clients.

Inject 14 (J3 - 14h30) : Une association de consommateurs annonce qu'elle envisage une action collective contre votre entreprise.

Éléments contextuels

Communications externes :

- Signalements des clients/utilisateurs
- Communications des autorités réglementaires
- Articles de presse et reportages
- Publications sur les réseaux sociaux
- Informations des professionnels de santé (si applicable)

Réactions des parties prenantes :

- Inquiétude des consommateurs/utilisateurs
- Pression des distributeurs/revendeurs
- Questions des investisseurs sur l'impact financier
- Interrogations des collaborateurs sur les procédures internes
- Opportunisme des concurrents

Variantes possibles

- Contamination intentionnelle (malveillance)
- Problème affectant un produit phare ou récemment lancé
- Incident survenant dans un contexte réglementaire en évolution
- Problème similaire ayant déjà touché un concurrent récemment

Points d'observation

- Rapidité et qualité de l'évaluation technique du problème
 - Décision concernant le rappel/l'alerte et son ampleur
 - Coordination avec les autorités réglementaires
 - Efficacité de la communication vers les différentes parties prenantes
 - Traçabilité et gestion logistique du rappel
 - Équilibre entre transparence et protection de l'image de marque
-

Scénario 7 : Catastrophe naturelle impactant les opérations

Description générale

Une catastrophe naturelle (inondation, tempête, séisme, etc.) frappe la région où se trouve l'un de vos sites principaux, perturbant gravement vos opérations et affectant potentiellement vos collaborateurs. Cette situation crée des défis logistiques, humains et opérationnels nécessitant une réponse coordonnée et une adaptation rapide.

Public cible

- Direction générale
- Services généraux/sécurité
- Ressources humaines
- Opérations/production
- IT et systèmes d'information
- Communication

Objectifs de l'exercice

- Tester l'activation du plan de continuité d'activité
- Évaluer la capacité à localiser et soutenir les collaborateurs affectés
- Vérifier les procédures de bascule vers des sites alternatifs
- Tester la coordination avec les autorités locales et services de secours
- Évaluer la résilience logistique et informatique

Déroulé chronologique

Jour 1

Situation initiale (J1 - 6h00) : Une catastrophe naturelle majeure (inondation, tempête, séisme, etc.) touche la région où se trouve l'un de vos sites principaux. Les alertes météo ou sismiques sont au niveau maximal.

Inject 1 (J1 - 6h30) : Les autorités locales émettent des consignes d'évacuation ou de confinement pour certains quartiers, incluant la zone de votre site.

Inject 2 (J1 - 7h15) : Plusieurs collaborateurs signalent qu'ils sont bloqués chez eux ou en cours d'évacuation. Certains sont injoignables.

Inject 3 (J1 - 8h00) : Une évaluation préliminaire indique que votre site est inaccessible et potentiellement endommagé. Les réseaux électriques et télécom sont perturbés dans toute la zone.

Inject 4 (J1 - 10h30) : Les autorités annoncent que l'accès à la zone sinistrée sera restreint pendant au moins 72 heures pour permettre les secours et évaluations de sécurité.

Inject 5 (J1 - 12h00) : Vos systèmes de sauvegarde informatique signalent une perturbation de la réplication des données due aux coupures électriques.

Inject 6 (J1 - 14h30) : Des clients et fournisseurs commencent à vous contacter pour s'enquérir de la situation et de votre capacité à maintenir vos engagements.

Inject 7 (J1 - 16h00) : Un bilan initial de vos équipes RH indique que 15% des collaborateurs sont directement affectés par la catastrophe, certains ayant subi des dommages personnels significatifs.

Jour 2

Inject 8 (J2 - 8h00) : Un accès limité au site est organisé pour une équipe d'évaluation. Les premiers rapports font état de dégâts significatifs sur l'infrastructure et les équipements.

Inject 9 (J2 - 10h30) : Les experts en assurance estiment que la remise en état complète du site pourrait prendre plusieurs semaines, voire plusieurs mois.

Inject 10 (J2 - 13h00) : Les systèmes informatiques centraux sont partiellement opérationnels mais avec des performances dégradées. Certaines applications critiques restent inaccessibles.

Inject 11 (J2 - 15h30) : Des problèmes logistiques majeurs sont signalés dans toute la région, affectant l'approvisionnement et les expéditions. Plusieurs routes et infrastructures de transport sont hors service.

Jour 3

Inject 12 (J3 - 9h00) : Une cellule de soutien psychologique est mise en place pour les collaborateurs affectés. Plusieurs cas de détresse importante sont signalés.

Inject 13 (J3 - 11h30) : Les médias locaux sollicitent votre contribution à l'effort de solidarité régional, questionnant votre engagement communautaire.

Inject 14 (J3 - 14h00) : Un point complet avec les managers révèle des capacités de travail à distance très variables selon les équipes et fonctions.

Éléments contextuels

Communications externes :

- Bulletins d'alerte des autorités
- Communications des services de secours
- Couverture médiatique de la catastrophe
- Informations des services publics (électricité, eau, télécommunications)
- Annonces des compagnies d'assurance

Réactions des parties prenantes :

- Préoccupation des familles des collaborateurs
- Inquiétude des clients sur les délais et engagements
- Sollicitations des communautés locales pour assistance
- Offres de soutien d'autres entités du groupe ou de partenaires
- Questions des actionnaires sur l'impact financier

Variantes possibles

- Événement touchant simultanément plusieurs de vos sites

- Catastrophe dans un pays étranger où vous avez des opérations significatives
- Événement survenant pendant une période critique (lancement produit, fin d'année fiscale)
- Catastrophe avec contamination environnementale associée

Points d'observation

- Efficacité du recensement et du soutien aux collaborateurs affectés
 - Rapidité d'activation des solutions de continuité
 - Qualité de la communication interne dans un contexte dégradé
 - Coordination avec les autorités et services de secours
 - Flexibilité dans la réorganisation des opérations
 - Équilibre entre impératifs business et considérations humaines et sociétales
-

Scénario 8 : Crise sanitaire et pandémie

Description générale

Une crise sanitaire majeure de type pandémie se développe, affectant progressivement vos opérations, la disponibilité de votre personnel et votre environnement économique global. Cette situation évolutive et prolongée nécessite une adaptation constante, une gestion des ressources humaines complexe et une révision des priorités opérationnelles.

Public cible

- Direction générale
- Ressources humaines
- Opérations/production
- Santé et sécurité au travail
- IT et digital
- Communication

Objectifs de l'exercice

- Tester les procédures de continuité face à un absentéisme massif
- Évaluer la capacité à mettre en place des mesures sanitaires adaptées
- Vérifier l'adaptabilité de l'organisation au travail à distance généralisé
- Tester la communication de crise dans un contexte d'incertitude prolongée
- Évaluer les processus de priorisation des activités sur une longue période

Déroulé chronologique

Phase 1 : Émergence (Semaine 1)

Situation initiale : Des alertes sanitaires signalent l'émergence d'une nouvelle maladie contagieuse dans plusieurs pays. Les autorités sanitaires mondiales élèvent progressivement leur niveau d'alerte.

Inject 1 : Les autorités nationales émettent des recommandations préliminaires concernant les voyages internationaux et les rassemblements.

Inject 2 : Les premiers cas sont signalés dans votre pays. Des mesures préventives sont suggérées pour les entreprises.

Inject 3 : Certains collaborateurs revenant de zones touchées présentent des symptômes suspects. Des questions émergent sur la politique à adopter.

Phase 2 : Intensification (Semaine 2-3)

Inject 4 : Le nombre de cas augmente significativement. Les autorités imposent des restrictions de déplacement et des mesures de distanciation sociale.

Inject 5 : Le taux d'absentéisme atteint 15% et continue d'augmenter, combinant malades, cas contacts et garde d'enfants (écoles fermées).

Inject 6 : Des contraintes logistiques apparaissent, certains fournisseurs commençant à rencontrer des difficultés d'approvisionnement.

Inject 7 : Les autorités annoncent un renforcement des mesures, incluant potentiellement des restrictions d'activités non essentielles.

Phase 3 : Pic de crise (Semaine 4-5)

Inject 8 : Un confinement partiel ou total est imposé, limitant strictement les déplacements et activités professionnelles.

Inject 9 : Le taux d'absentéisme atteint 30-40%. Certaines fonctions critiques sont sous tension maximale.

Inject 10 : Des difficultés techniques émergent liées à la généralisation du télétravail (capacité réseau, accès VPN, sécurité informatique).

Inject 11 : Des tensions apparaissent entre collaborateurs concernant l'inégalité des situations (personnel terrain vs télétravail, charge familiale).

Phase 4 : Adaptation (Semaine 6-8)

Inject 12 : Les autorités annoncent un plan de sortie progressive étalé sur plusieurs mois avec des critères évolutifs.

Inject 13 : Certains collaborateurs expriment des réticences à revenir sur site malgré l'assouplissement des mesures.

Inject 14 : Un foyer de contamination est détecté au sein de l'un de vos services, nécessitant des mesures d'isolement immédiates.

Inject 15 : Des discussions s'engagent sur les adaptations à long terme de l'organisation du travail et des espaces.

Éléments contextuels

Communications externes :

- Bulletins réguliers des autorités sanitaires
- Évolutions réglementaires fréquentes
- Recommandations des organisations professionnelles
- Couverture médiatique intense et parfois contradictoire
- Partage d'expériences d'autres entreprises

Réactions des parties prenantes :

- Inquiétudes variables des collaborateurs selon leur profil de risque
- Tensions potentielles concernant les mesures de protection
- Adaptabilité différenciée au travail à distance selon les fonctions
- Préoccupations des clients sur la continuité de service
- Pression économique croissante avec l'extension de la crise

Variantes possibles

- Contamination massive au sein d'un site ou service critique
- Divergences entre exigences sanitaires et impératifs économiques
- Crise survenant dans un contexte social déjà tendu
- Développements inégaux selon les pays pour une entreprise internationale

Points d'observation

- Réactivité de mise en place des mesures sanitaires adaptées
 - Efficacité du déploiement des solutions de travail à distance
 - Qualité de la communication et du soutien aux collaborateurs
 - Pertinence des critères de priorisation des activités
 - Équilibre entre protection de la santé et continuité économique
 - Capacité à maintenir la cohésion d'équipe dans un contexte prolongé
-

Scénario 9 : Fraude interne et malveillance

Description générale

Votre organisation découvre une fraude ou un acte de malveillance significatif commis par un ou plusieurs collaborateurs internes. Cette situation crée un choc dans l'organisation et nécessite une gestion complexe alliant enquête interne, aspects juridiques, communication sensible et préservation de la confiance des parties prenantes.

Public cible

- Direction générale
- Service juridique
- Ressources humaines
- Finance/audit interne
- Sécurité/IT
- Communication

Objectifs de l'exercice

- Tester les procédures d'investigation interne
- Évaluer la gestion des aspects juridiques et réglementaires
- Vérifier l'équilibre entre transparence et confidentialité
- Tester la communication interne dans un contexte de crise de confiance
- Évaluer la capacité à renforcer les contrôles tout en maintenant l'activité

Déroulé chronologique

Jour 1

Situation initiale (J1 - 9h00) : Une anomalie significative est détectée, suggérant une possible fraude ou malveillance interne (options selon contexte : détournement de fonds, corruption, sabotage, vol de données sensibles, falsification de documents, etc.).

Inject 1 (J1 - 10h30) : Une vérification préliminaire confirme la réalité du problème et son caractère intentionnel. Les premières estimations indiquent un impact potentiellement important.

Inject 2 (J1 - 11h30) : Des éléments suggèrent l'implication d'un cadre ou collaborateur ayant des responsabilités significatives dans l'organisation.

Inject 3 (J1 - 14h00) : Le service juridique présente les implications légales potentielles, incluant l'obligation de signalement aux autorités dans certains cas.

Inject 4 (J1 - 16h00) : Des rumeurs commencent à circuler en interne, créant un climat d'incertitude et de suspicion.

Jour 2

Inject 5 (J2 - 8h30) : L'enquête interne identifie clairement le(s) responsable(s) et révèle que les actes frauduleux durent depuis plusieurs mois, voire années.

Inject 6 (J2 - 10h00) : Une décision doit être prise concernant la mise à pied immédiate des personnes impliquées et les mesures conservatoires.

Inject 7 (J2 - 11h30) : Des failles dans les procédures de contrôle interne sont identifiées, soulevant des questions sur la responsabilité de l'encadrement et la gouvernance.

Inject 8 (J2 - 14h00) : Un client ou partenaire commercial signale avoir reçu des informations troublantes suggérant qu'il pourrait être indirectement impliqué ou impacté.

Inject 9 (J2 - 15h30) : Le service informatique découvre que des données confidentielles ont potentiellement été compromises ou extraites.

Jour 3

Inject 10 (J3 - 9h00) : Les autorités (selon le cas : police, parquet financier, CNIL, etc.) contactent votre organisation suite à un signalement externe ou à votre propre déclaration.

Inject 11 (J3 - 11h00) : Un média économique ou local vous contacte, indiquant détenir des informations sur l'affaire et préparant un article.

Inject 12 (J3 - 14h30) : L'évaluation complète de l'impact révèle des conséquences plus étendues que prévu initialement (financières, opérationnelles, réputationnelles, etc.).

Inject 13 (J3 - 16h00) : Une réunion extraordinaire des instances de gouvernance (conseil d'administration, comité d'audit) est convoquée pour faire le point sur la situation.

Éléments contextuels

Communications externes :

- Demandes d'information des autorités réglementaires ou judiciaires
- Sollicitations des médias pour commentaires
- Questions des auditeurs externes ou commissaires aux comptes
- Inquiétudes exprimées par clients ou partenaires alertés

Réactions des parties prenantes :

- Choc et perte de confiance au sein des équipes
- Questionnements sur les systèmes de contrôle et la gouvernance
- Préoccupation des clients concernant la fiabilité des opérations
- Inquiétude des investisseurs et actionnaires
- Vigilance accrue des régulateurs sectoriels

Variantes possibles

- Fraude impliquant un dirigeant ou membre du comité de direction
- Collusion avec des parties externes (fournisseurs, clients)
- Lanceur d'alerte ayant tenté de signaler la situation auparavant
- Impacts réglementaires spécifiques selon secteur (finance, santé, etc.)

Points d'observation

- Réactivité et méthode d'investigation interne
 - Équilibre entre procédure disciplinaire et présomption d'innocence
 - Qualité de la communication interne dans un contexte sensible
 - Gestion des aspects juridiques et réglementaires
 - Mesures correctives mises en place pour les contrôles
 - Préservation de la confiance des parties prenantes externes
-

Scénario 10 : Panne majeure des systèmes d'information

Description générale

Une panne majeure affecte l'ensemble ou une partie critique de vos systèmes d'information, perturbant gravement vos opérations et services. Cette situation technique crée des impacts en cascade sur l'ensemble des activités et nécessite une coordination entre équipes IT, métiers et communication.

Public cible

- Direction des systèmes d'information
- Direction des opérations
- Service client
- Communication
- Direction générale
- Ressources humaines

Objectifs de l'exercice

- Tester les procédures de gestion des incidents IT majeurs
- Évaluer la capacité à maintenir l'activité en mode dégradé
- Vérifier la coordination entre équipes techniques et opérationnelles
- Tester la communication avec les utilisateurs internes et externes
- Évaluer les procédures de restauration et de retour à la normale

Déroulé chronologique

Jour 1

Situation initiale (J1 - 8h00) : Une panne majeure est détectée, affectant des systèmes critiques de l'entreprise (options selon contexte : ERP, CRM, infrastructure réseau, serveurs de production, systèmes de paiement, etc.).

Inject 1 (J1 - 8h15) : Les premiers diagnostics confirment qu'il s'agit d'un incident grave dont la résolution pourrait prendre plusieurs heures ou jours. L'origine reste à déterminer.

Inject 2 (J1 - 8h45) : Les équipes métiers commencent à signaler des impacts opérationnels significatifs. Certains services sont totalement à l'arrêt.

Inject 3 (J1 - 9h30) : Les clients externes signalent des dysfonctionnements dans les services ou produits. Le centre de service est submergé d'appels.

Inject 4 (J1 - 10h30) : Une première investigation suggère que la panne pourrait être liée à (selon contexte : mise à jour défectueuse, problème d'infrastructure, défaillance matérielle, erreur de configuration, attaque externe, etc.).

Inject 5 (J1 - 12h00) : Les équipes IT estiment un délai initial de résolution de 24 à 48 heures pour un retour à la normale complet. Des solutions temporaires sont à l'étude.

Inject 6 (J1 - 14h30) : Certains collaborateurs expriment leur frustration face à l'impossibilité de travailler normalement et au manque d'informations précises.

Inject 7 (J1 - 16h00) : Les premières estimations d'impact financier et opérationnel sont alarmantes. Des engagements clients critiques sont menacés.

Jour 2

Inject 8 (J2 - 8h00) : Après une nuit de travail, les équipes techniques ont identifié précisément l'origine du problème mais la résolution complète reste complexe.

Inject 9 (J2 - 9h30) : Une solution de contournement partielle est proposée pour les fonctions les plus critiques, mais avec des limitations importantes.

Inject 10 (J2 - 11h00) : Des questions émergent sur la prévention de ce type d'incident et sur le niveau de préparation de l'organisation.

Inject 11 (J2 - 14h00) : Un plan de reprise progressif est élaboré, nécessitant une priorisation des applications et services à restaurer.

Inject 12 (J2 - 16h30) : Un dysfonctionnement secondaire est détecté lors des opérations de restauration, complexifiant le processus.

Jour 3

Inject 13 (J3 - 9h00) : Les systèmes commencent à être restaurés progressivement. Un plan de vérification est mis en place pour s'assurer de l'intégrité des données.

Inject 14 (J3 - 11h30) : Des discussions s'engagent sur les compensations éventuelles pour les clients impactés et sur la communication de reprise.

Inject 15 (J3 - 14h00) : Une analyse préliminaire des causes profondes révèle des vulnérabilités structurelles dans l'architecture des systèmes.

Éléments contextuels

Communications externes :

- Sollicitations des clients et utilisateurs externes
- Questions des fournisseurs de solutions IT impliqués
- Demandes d'information des partenaires connectés à vos systèmes
- Intérêt des médias spécialisés (selon l'ampleur et la visibilité)

Réactions des parties prenantes :

- Frustration des collaborateurs face aux perturbations
- Pression des équipes commerciales concernant les impacts clients

- Stress des équipes techniques travaillant sur la résolution
- Questionnements de la direction sur la robustesse des systèmes
- Préoccupations sur les conséquences à moyen terme

Variantes possibles

- Panne survenant pendant une période critique (clôture comptable, pic d'activité)
- Indisponibilité prolongée nécessitant des semaines de reconstruction
- Suspicion d'action malveillante externe (cyberattaque) ou interne
- Perte de données nécessitant des procédures de réconciliation complexes

Points d'observation

- Efficacité des procédures d'escalade et de gestion d'incident
 - Qualité de la communication vers les différentes parties prenantes
 - Capacité à mettre en place des solutions de contournement
 - Pertinence des critères de priorisation pour la restauration
 - Maintien de la sécurité des données durant la résolution
 - Documentation et suivi des actions pour analyse ultérieure
-

Conseils pour l'animation des exercices

Préparation

- Désignez un animateur principal et des observateurs
- Préparez les "injects" sous forme de messages, emails, appels téléphoniques
- Définissez clairement les règles de l'exercice (timing, communication, documentation)
- Prévoyez une salle dédiée pour la cellule de crise

Animation

- Respectez le timing prévu mais adaptez-vous aux réactions des participants
- Utilisez des canaux de communication réalistes (emails, appels)

- Jouez le rôle des parties prenantes externes
- Maintenez une pression réaliste sans surcharger les participants

Débriefing

- Organisez un retour à chaud immédiatement après l'exercice
- Recueillez les impressions des participants
- Partagez les observations des observateurs
- Identifiez les points forts et les axes d'amélioration
- Élaborez un plan d'action concret

Amélioration continue

- Documentez chaque exercice et ses enseignements
- Suivez la mise en œuvre des actions correctives
- Variez les scénarios et niveaux de complexité
- Alternez exercices sur table et simulations complètes
- Augmentez progressivement le niveau de difficulté

Création d'une culture de résilience

- Valorisez la participation aux exercices
- Partagez les bonnes pratiques identifiées
- Intégrez les nouveaux collaborateurs dans les exercices
- Communiquez sur les progrès réalisés
- Connectez les exercices aux incidents réels vécus

© 2025 Pulse - Tous droits réservés

© 2025 Pulse-Crisis - Tous droits réservés