MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET DE LA COHÉSION
DES TERRITOIRES

Liberté
Égalité
Fraternité

dgac direction générale de l'Aviation civile
DSAC

Plan de gestion de crise
Emergency response plan

Synthèse sur les bonnes pratiques

Direction de la sécurité de l'Aviation civile
Mission évaluation et amélioration de la sécurité
Version nº 1
Publiée le jeudi 13 juillet 2023

Gestion documentaire

Historique des révisions

Edition et version	Date	Modifications
Ed1v1	01/07/2023	

Approbation du document

Nom	Responsabilité	Date	Visa
André VERNAY DSAC/MEAS	Rédacteur	01/07/2023	
Antoine LELERRE DSAC/MEAS/APPS	Vérificateur	03/07/2023	
Stéphane CORCOS Chef DSAC/MEAS	Approbateur	06/07/2023	

Pour tout commentaire ou suggestion à propos de ce guide, veuillez contacter la direction de la sécurité de l'aviation civile à l'adresse suivante : rex@aviation-civile.gouv.fr

Sommaire

Avertissement

Les membres du groupe de travail ayant produit ce document appartiennent au Réseaux Sécurité Aérienne France Maintenance et Hélicoptères. Ils ont contribué de manière collective à des fins de publication de bonnes pratiques et points d'intérêts dans le domaine organisationnel, dans le cadre de la gestion de crise, de situations d'urgence ou d'évènements graves dans le seul but d'améliorer la sécurité. Cette réflexion a pour but de proposer des éléments présentés à titre informatif et provenant d'analyses de crises ou problématiques récentes ou historiques dans le domaine aéronautique.

Les éléments mentionnés ne sauraient remplacer les règlements nationaux et internationaux liés au travail et actions prévues par les acteurs au sein des organisations ; ce document ne dispose en aucun cas d'une force contraignante : il s'agit de lignes directrices ayant pour objectif de constituer un guide de bonnes pratiques tirées de conclusions positives lors de crises dans le management d'entreprises du domaine aérien. Tout ce travail s'inscrit dans le cadre de la promotion des Facteurs Organisationnels et Humains (FOH) en lien avec le Programme de Sécurité de l'Etat (PSE) et plus particulièrement avec le plan national pour la sécurité aérienne « Horizon 2023 ».

Ce guide ne se substitue pas à la réglementation et aux standards en vigueur. Il ne constitue pas une étude de sécurité. Il est de la responsabilité des utilisateurs de l'utiliser dans le domaine concerné.

Aucun processus de mise à jour n'est prévu sur ce document informatif.

Introduction

Les organisations mettent en place des ERP (Emergency Response Plan ou plan de gestion de crise) qui suivent une logique très solide de gestion d'une crise ou situation d'urgence. Pourtant, en analysant les dernières crises passées ou en cours, l'intérêt de fournir des pistes pour les compléter dans les domaines de l'anticipation, de la gestion et des suites, paraît opportun. Les éléments mentionnés ou développés dans ce document sont utilisables librement, tels quels ou comme base de travail au sein de toute organisation en amont, pendant ou après actions de la cellule de crise.

Définition générale de l'Emergency Response Plan : Un ERP correspond à une liste d'actions les plus immédiates à déclencher et qui requièrent d'être lancées sans délai au moment où une situation d'urgence est identifiée. Le constat plus global d'entrer en situation de crise et la décision consécutive d'installer une cellule de crise afin de manager les actions au-delà de la réaction immédiate représente une deuxième étape d'une situation d'urgence. Ces deux phases ou étapes chronologiques sont prises en compte dans les réflexions collectives qui suivent dans ce document.

générale de la résilience : la résilience définit la capacité d'une personne ou d'un groupe à revenir à un état stable après une déstabilisation ou une crise. Le niveau de résilience peut être traduit comme la capacité à prendre en compte l'imprévu et gérer les marges qui permettent de contenir ou d'éviter l'évolution négative d'un évènement majeur.

Objectifs

Ce guide s'adresse à l'ensemble des organismes du secteur aérien. Il s'applique à toute situation d'urgence nécessitant la mise en œuvre d'un plan de gestion de crise.

Devraient être intégrées dans la conception de l'ERP les notions suivantes :

- Sécurité aérienne (Aviation Safety) ;
- Management et gestion organisationnelle ;
- Facteurs humains ;
- Aide aux victimes.

Comment se préparer au mieux ? Cette question doit couvrir le scope complet d'un ERP depuis la création de la documentation jusqu'à l'entraînement des différentes parties de l'entreprise.

Les 5 objectifs mis en évidence par le Groupe de Travail sont organisés dans les 5 sous-parties du document.

- Préparation à une crise éventuelle ;
- L'entrée dans la crise ;
- La gestion de la crise ;

- La sortie de crise ;
- L'intégration du retour d'expérience.

Comme le montrent ces sous-parties, l'ERP dans son ensemble comprend : une phase de préparation, des actions adaptées pendant la gestion de crise et une utilisation de l'expérience après l'évènement.

I. Phase 1 : préparation à une crise éventuelle

1.1 Existence d'une politique de culture juste comme pré-requis

La culture juste est un prérequis dans cette gestion de l'incertitude et permet aux membres de l'équipe de gestion de crise d'obtenir l'assurance de l'application d'une politique « Just and Fair » au niveau de l'organisation.

Objectif : Nécessaire pour ne pas entraver la phase d'alerte, la culture juste reste un pilier indispensable de la Sécurité Aérienne pour permettre la remontée d'information en vue de son analyse et s'applique aussi bien aux directeurs qu'aux membres de la cellule de crise, sur leur comportement et les décisions qu'ils pourraient prendre.

https://www.ecologie.gouv.fr/observatoire-culture-juste-laviation-civile

Le guide DSAC culture juste

1.2 Gestion de l'effet de surprise

L'annonce d'un évènement ou d'une crise peut amener une réaction très différente d'une personne à l'autre. Notre métabolisme tente ainsi de se protéger dans un premier temps puis de s'adapter. Trois postures existent et peuvent se mettre en place d'une manière dissociée ou chronologiquement avec des statuts tels que sidération, suractivité ou tunnelisation…)

https://riojeanluc.com/2018/01/31/la-surprise-a-telle-des-effets/

Question : Faut-il préparer des plans d'actions types suivant la typologie d'événement, un peu comme un catalogue ?

Le REX, l'expérience de l'entreprise et des acteurs (par exemple) font que les plans d'actions peuvent changer d'une crise à l'autre et il paraît difficile voire impossible de créer un catalogue exhaustif de toutes les situations critiques que l'organisation pourra rencontrer. A titre indicatif, les entités présentes dans le groupe de travail ont connu des situations aussi diverses que des inondations stoppant toute activité opérationnelle, un accident grave avec décès, la gestion COVID, un incendie...

1.3 Composition de la cellule de crise

Directeur de crise : ne pas le confondre avec le dirigeant de l'entreprise

Missions :

- Animer l'équipe de crise ;
- Veiller à l'exécution du plan de crise ;
- Prendre les dispositions en matière de communication ;
- Assurer la liaison avec les autres cellules de crise (Autorités, etc.) ;
- Informer la direction générale et la cellule stratégique ;
- Prendre la décision finale.

Modes opératoires :

- Organiser des points d'échanges fixes à intervalles réguliers toutes les heures avec les équipes ;
- Neutraliser toute communication avec l'extérieur et s'assurer de la bonne coordination et du bon fonctionnement de l'équipe ;
- S'assurer de la rédaction des compte rendus et de l'enregistrement des relevés de décision ;
- Communiquer aux dirigeants les informations essentielles, les enjeux, les difficultés, l'état du dispositif, le respect et le niveau d'avancement du Plan de crise.

Directeur Adjoint de crise

- Identique aux pré requis du directeur de crise, il est prêt à prendre sa relève à tout moment.

Coordinateur ou Assistant (Responsable de la main courante / Journal de bord)

Missions :

- Collecter les informations utiles relatives à :
  - Situation et évolution de l'événement ;
  - Situation des secours ;
  - Statut et état des victimes ;
  - Données connues relatives au vol, à l'avion, à l'équipage, à la structure impliquée ou affectée;
  - La gestion du déroulement du plan de crise
- Structurer l'information ;
- Identifier l'information manquante par secteur opérationnel ;

- Rédiger les comptes rendus de point d'étape.

Modes opératoires :
- Porter assistance aux membres de l'équipe ;
- Structurer et harmoniser les modes de rédaction des membres de la cellule de crise :

  • Formatage des notes ;

  • Identification des documents et pièces jointes et des blocages rencontrés par les équipes ;

  • Authentification des informations et précisions des commentaires ;

  • Alerte au directeur de crise en cas de difficultés ou de fonctions vacantes.

Agents opérationnels :
- Identifier les informations disponibles sur la crise, les fonctions dont chaque acteur impliqué est titulaire, les tâches qu'il faudra accomplir ;
- Procéder dans l'ordre et avec rigueur ;
- Vérifier **Qui fait quoi ? Qui est disponible ? Qui ne l'est pas ?** et se coordonner avec les autres membres de son équipe ou de la cellule de crise nécessitant de la coactivité ;
- Exécuter ou faire exécuter les tâches de sa fonction ;
- S'assurer du statut des tâches et documents requis.

Missions :
- Exécuter la check-list, lorsqu'elle existe, en y ajoutant les informations utiles qui parviennent ou qui sont demandées en fonction de l'évolution de la crise ;
- Ajouter les documents et toutes les informations considérées comme utiles
  - qui ont un réel degré d'importance ;
  - qui concernent l'accident ou la gestion de crise ;
  - qui est associée à la fonction attribuée ;
  - qui doit être accessible à l'équipe de crise, et en particulier aux dirigeants.
- Trouver l'information requise par le plan de crise ;
- Organiser le travail des collaborateurs ;
- Organiser une rotation des équipes afin de ne pas rester titulaire trop longtemps (deux heures maximum) et tenir son équipe en permanence informée.

Nota : Un personnel formé à la gestion des actions favorables pour la mise en place de la gestion de crise à suivre peut apporter des connaissances majeures lors de la déclaration de l'évènement afin de gérer au mieux les points d'intérêt à préserver ou noter.

Qui constitue la cellule de crise ? « Un chef d'orchestre et des experts en regard » est une bonne image à avoir en tête pour comprendre comment fonctionnent les structures qui ont montré leurs qualités en période de crise.

Il peut être nécessaire dans les grandes structures d'établir un planning ou de définir une liste de fonctions : ainsi, le premier répondant est sélectionné.

La chaine d'alerte doit être définie et se doit d'être la plus courte possible. Elle peut s'organiser par effet domino ou rester déclenchée par une seule personne en charge.

Toute organisation se doit de prendre en compte la gestion des personnes qui « ne veulent **PAS** participer à la cellule de crise » (quelle qu'en soit la raison) ou qui seront mises à l'écart de cette même

cellule en cas de comportement inadapté. Il est important de préciser que le directeur de crise a toute autorité pour prendre la décision de retirer quelqu'un de la cellule de crise.

Les membres de la cellule de crise sont prédéfinis dans des check-lists en fonction de l'importance de leur rôle et de leur responsabilité dans la gestion d'un événement. Les événements pouvant survenir à des moments inopportuns, il convient de désigner également des suppléants. Un personnel d'astreinte est désigné selon un planning établi. Il a la responsabilité de convoquer l'ensemble de la cellule de crise lorsqu'une alerte est donnée.

Pour chaque membre de l'équipe, des fiches de rôles sont à établir afin de bien préciser leurs fonctions génériques, depuis l'activation de la cellule de crise jusqu'à la sortie de crise, ainsi que toutes les instructions spécifiques dont ils doivent avoir connaissance.

Chaque membre de la cellule de crise se doit de respecter un devoir de confidentialité sur les informations disponibles dans le cadre de sa fonction. De manière générale, un strict devoir de réserve doit être observé par l'ensemble des membres de la cellule de crise aussi bien à l'oral que par écrit ou tout autre support ou vecteur (y compris e-mail, photo, film, médias sociaux, etc.). En cas de sollicitation de la part des médias, décliner toute invitation et orienter les interlocuteurs vers le service de communication doivent être les bons réflexes à appliquer.

1.4 Définition de la structure hébergeant la cellule de crise

Lors de la définition de l'ERP, il est essentiel de définir le lieu d'accueil de la cellule de crise, en prenant en compte les aspects suivants :

- L'accès doit être restreint et sécurisé ; pour autant, il doit être garanti en tout temps. Par exemple,
  - Attention aux accès électroniques (badge, boîte à clefs électronique etc. en cas de panne de courant) ;
  - Prévoir une boîte à clefs à code pour éviter oubli / perte des clefs par le personnel etc.

    - Prévoir l'intervention de vigiles pour sécuriser les locaux.
- Prendre en compte les besoins logistiques : point d'eau, sanitaires, salle de repos, restauration, etc.
- Prévoir un lieu « back-up », même légèrement moins équipé si le lieu prédéfini était indisponible le jour de la crise (invasion, inondations, coupure électrique, etc.)

Par ailleurs, il est essentiel de prévoir d'autres salles de crise permettant, selon les cas, l'accueil des familles, des médias, la coordination avec une autre cellule de crise... En effet, il est préférable que les médias et les familles soient accueillis dans des lieux distincts de la cellule de crise (cela évitera les éventuelles intrusions ou rencontres fortuites entres les acteurs de la gestion de crise et les médias / familles).

1.5 Matériel et équipements obligatoires

La définition des fournitures essentielles est également nécessaire :

- Fournitures à prévoir dans la cellule de crise : tableau blanc, feutres, rétroprojecteurs, alimentation des différents ports pour connections des ordinateurs, piles, stylos, casques, multiprises, bouteilles d'eau, ordinateur, téléphone, système de Visio conférence... Cela permet d'avoir un minimum d'équipement au cas où, dans la précipitation, un ou des membres de la cellule de crise aurait oublié le matériel nécessaire. Il est également important de prévoir des versions supplémentaires des check-lists pour les personnes qui n'y ont pas accès (oubli dans lapanique, mauvaise version etc.)
- Dotation personnelle des membres de la cellule de crise :
    - Ordinateur et téléphones portables
    - Prévoir des sacoches ERP adaptées à chaque rôle est une bonne pratique reconnue par beaucoup d'organisations. Par exemple, la personne en charge de la sûreté pourrait avoir dans sa sacoche de la rubalise, des pastilles sûreté, jeu de clefs…
- Moyen d'identification des membres de la cellule de crise et des autres personnes interagissant dans la crise. Par exemple, une bonne pratique pourrait être de prévoir des chasubles de différentes couleurs (rouge pour les membres de la cellule de crise, bleu pour les médias, vert pour les familles, etc.)

La prise en compte d'un fonctionnement dégradé de la cellule de crise est primordiale afin d'éviter tout stress inutile : panne d'électricité, documents non mis à jour, difficulté de connexions aux outils informatiques, etc.

1.6 Communication de crise

- Définir qui communique. Il ne doit y avoir qu'un seul canal de communication en interne et externe ;
- Définir qui prévenir et à quel moment ou fréquence ;

- Définir quels éléments peuvent être communiqués (Ex. Adaptation de la communication à l'événement en cours. Une cyberattaque n'engendrera pas la même communication) ;
- Rester très factuel ! ;
- Ne communiquer que l'essentiel ;
- Fixer un rythme adapté de production des messages en fonction de l'évolution de la situation et le maintenir (Point d'attention : il est suggéré de mettre en place une stratégie de communication qui permette de garder le contrôle sur la communication) ;
- Mettre en place un processus général d'anonymisation des données.

Préparer des trames pouvant être réutilisées (ex : Email type avertissant les équipes d'un incident grave, et rappelant les consignes à respecter ; informations à transmettre aux autorités ou vers l'extérieur tels que médias etc…).

Conformité au règlement RGPD :

- ⚠Attention à la diffusion protégée de données personnelles sur les passagers, clients et le personnel (transfert uniquement aux personnels dûment habilités à en connaître) éviter les mails adressés à l'ensemble du personnel ;

- Engagement de confidentialité renforcée pour les personnels de la cellule de crise (Exemple modèle CNIL et documents explicatifs disponibles en Annexe 1)

- Flash info sur la communication des personnels de la cellule gestion de crise qui doivent être informés de ce que l'on entend par données personnelles et sanctions en cas de violation (mentions obligatoires) Voir Annexe 1

- **Attention** : différents domaines en charge des opérations normales et habituelles dans la structure risquent en période de crise de passer à un décloisonnement : le passage de silos à réseaux doit alors être préparé afin d'éviter les blocages pour la cellule de crise. Il en est de même pour les différents moyens de communication qui doivent être centralisés et coordonnés. Ces derniers doivent également être régulièrement testés (autorité, préfecture, aéroports…)

1.7 Risque cyber

Des actions importantes sont à prévoir en amont :

- Construire ou utiliser des canaux sécurisés à chaque fois que cela est possible pour éviter la captation d'informations ;

- Préparer des boites mail dédiées sécurisées et éviter l'envoi de sms… (sauf dans le cas de communications cryptées, chiffrement des données, gestion des accès à l'information...) ;

- Une sensibilisation aux bonnes pratiques de sécurité informatique permet de réduire le risque de cyberattaque afin de protéger l'entreprise et les données personnelles traitées ou conservées (passagers, salariés, prestataires...) et favorise ainsi la sauvegarde des trois principes fondamentaux (confidentialité, intégrité, disponibilité) ;

- Les mesures préventives[1] énoncées ci-dessous (conformément aux recommandations de l'ANSSI) ont pour objectif de limiter tout risque d'incident de sécurité (destruction, perte, altération, divulgation non autorisée de données ou l'accès non autorisé) ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données;

Attention : L'ensemble des mesures ci-dessus ne dispense pas de la conformité à la Part-IS pour les opérateurs qui sont concernés.

1.8 Coordination ERP

Suivant les missions et activités de l'entreprise, la coordination de plusieurs ERP sera nécessaire :

- Organismes d'Etat (ex : services de recherche et d'urgence lors de missions de secours), autorité de surveillance aéronautique… ;
- Clients (ex : Hôpitaux lors de missions SAMU, clients détenant leur propre ERP etc.) ;
- Fournisseurs (ex. propriétaire ou copropriétaire des locaux etc..) ;
- Sous-traitants ;
- Aéroports/aérodromes lorsque l'incident / accident intervient sur leur site.

Lors de la définition de l'ERP, il faut donc définir :

- Quelles sont les organisations / entités avec lesquelles une coordination d'ERP peut être nécessaire : penser à associer les adresses et numéros de contacts associés ;
- Prévoir un protocole spécifique avec ces organisations / entités : qui est le donneur d'ordre, vérifier la compatibilité des ERP, tâches et responsabilités de chacun… ;
- Dans la mesure du possible, organiser des exercices communs.

1.9 Formation des personnels

Il convient de veiller aux points suivants :

La formation initiale des membres de la cellule de crise : exemple de la formation en amont des EPI (enquêteur de première information). Lors d'une Crise, la préservation des éléments clés recueillis dès le début de la connaissance de l'évènement est essentielle pour la bonne gestion à suivre. Attention toutefois à préserver totalement les lieux de survenue et ne déplacer des éléments qu'en cas de risque grave avéré. La formation initiale et récurrente des partenaires (ex : médecins régulateurs, agences intérim etc.).

Le maintien de compétences en E-learning avant prise de fonction en cellule de crise ou exercices réguliers (fréquence à adapter en fonction de la taille de la société, des activités, du turnover etc.).

La formation et l'utilisation de « personnels référents de support » qui sortent de l'équipe de gestion de crise les personnels qui ne sont plus « prêtes à agir » ou « en forme suffisante pour travailler ».

Le coordinateur de la gestion de crise à l'extérieur de la société doit être en phase avec l'ensemble des structures mises en place et doit se rendre visible et disponible auprès des équipes de gestion de l'ERP.

L'intégration « d'inputs » sur la non mise à jour de la documentation de secours papier et électronique utilisée peut permettre de s'assurer des points de départ cruciaux de lancement de la cellule de crise :

- Appel de tous les membres prévus et sortie des personnes non désirables ;
- Horaire utilisé pour gérer les actions (UTC ou locale)
    - Date de la mise à jour de la documentation utilisée afin de confirmer l'utilisation collective de la dernière version publiée
- E-formations disponibles et adaptées pour mettre à jour ses connaissances.

1.10 Planification et réalisation des exercices

Elle est nécessaire pour se familiariser avec et s'approprier le plan ERP pour l'activer quand nécessaire mais aussi pour vérifier la robustesse du processus.

Le partage des exercices (exemple ORSEC avec les préfectures) avec des structures autres afin d'avoir des avis neutres sur l'efficience des exercices isolés ou coordonnés avec des entités partenaires (ex : clients, services étatiques, secours, aérodromes, sous-traitants, etc.) est gage d'amélioration permanente du processus.

L'utilisation d'observateurs externes à l'entreprise lors d'exercices peut ainsi favoriser l'échange de bonnes pratiques et permettre un retour complet.

Un exercice sert à lister des remarques et points de dysfonctionnement : ne pas les occulter et le débriefer obligatoirement est nécessaire afin d'apprendre et d'ajuster !

Les exercices doivent être de tailles, de durées et de fréquences différentes afin de couvrir au maximum les scénarios et les divers participants : des petits exercices réguliers de 30/60 min fréquemment, des exercices de 3/4h et des exercices sur 2 jours (travail sur les relèves).

Le débriefing à chaud avec **tous** les participants est essentiel et ne doit pas être écourté en raison de la fatigue ou de l'heure tardive. Puis un compte rendu par écrit doit être rédigé et transmis à tous les participants.

Une mention sur l'importance de la communication entre les différents domaines et entités est nécessaire.

Chaque exercice doit être soigneusement préparé. Pour ce faire, il est recommandé de définir à l'avance les sujets suivants :

- Equipe d'organisation, organisation et planification du projet ;
- Objectifs de l'exercice ;
- Liste des participants ;
- Techniques d'animation, organisation de l'animation ;
- Liste des observateurs ;
- Organisation de l'observation (matrice d'observations, etc.) ;
- Processus de lancement de l'exercice (phase d'alerte) ;
- Besoins logistiques/matériels ;
- Information préalable des participants ;
- Chronogramme détaillé du scénario et injections de scénarios ad hoc ;
- Réactions/résultats attendus ;
- Débriefing de l'exercice/processus de retour d'expérience.

Un test régulier des moyens de communication, de l'infrastructure / réseau informatique de la salle de crise ainsi que des vidéoprojecteurs ou des écrans d'affichage doit être effectué.

Une vérification régulière des contacts téléphoniques listés dans les ERP (ou documents associés) est fortement recommandée en appelant les numéros indiqués.

1.11 Intégration du retour d'expérience

Vital pour s'adapter et éventuellement modifier le plan ERP (après mise en œuvre ERP ou exercice), le retour d'expérience se doit d'être intégré dans une démarche globale pour informer l'ensemble des acteurs, sensibiliser les personnels directement concernés et prévoir les structures adaptées en interne pour la gestion globale.

1.12 Conformité réglementaire

Il s'agit de respecter les cahiers des charges réglementaires si elles existent et d'éviter les écarts lors d'audits avec les autorités compétentes.

Exemple : IOSA demande l'intégration d'un système d'information gratuit auprès du grand public en cas d'accidentaéronautique.
Exemples :

- Convention de montréal de 1999 (Principe de responsabilité et droit à l'indemnisation) ;
- IOSA (Compagnie aérienne) demande l'intégration d'un système d'information gratuit auprès du grand public en cas d'accident aéronautique ;
- IOSA (Compagnie aérienne) impose la mise en place de test régulier de l'organisation ERP.
- Règlement (UE) N°1321/2014 (Organisme de maintenance et organisme de gestion du maintien de la navigabilité) : La notion d'ERP a fait son apparition dans le système de management ;
- Règlement (UE) N°996/2010 sur les enquêtes.

1.13 Veille

L'analyse des risques et un benchmark au travers d'une veille (fournie par les organismes étatiques officiels) peuvent permettre d'anticiper un mode de réponse (Ex. COVID ou guerre en Ukraine, Cyberattaque….)

Sureté : Analyse de la menace géopolitique, réseau prévention des actes malveillants (Acteurs de l'état, ambassades, etc…)

Sécurité : Prévention aux risques (accidents et actes non intentionnels) mode benchmark avec les autorités, compagnies... Veille des info-sécurité DSAC et SIB EASA

II. Phase 2 : l'entrée dans la crise

Il faut pouvoir déterminer qu'un événement requiert un passage en mode crise. Pour cela, les 2 méthodes de questionnement suivantes peuvent être appliquées pour déterminer le passage en mode crise.

Approche par les moyens :

« Est-ce que mon organisation, mes processus et mes moyens actuels me permettent de répondre à la situation sans dégrader mes performances ou jusqu'à quel niveau acceptable de performance ? ».

Approche par les critères :

« Est-ce que l'évènement a un impact sur la vie d'un acteur, un moyen de production, ou la réputation d'une personne ? »

Un autre moyen pour aider à la décision du déclenchement d'une cellule de crise pourrait être l'établissement d'une classification de typologies d'événements structurée afin de déterminer les niveaux à activer.

Une classification à 3 niveaux peut être un bon exemple :
Crise / Evénement Majeur / Evénement mineur
(Ex : **Crise** = Accident, Incendie, Décès... / **Evènement Majeur** = Intégrité des installations, infrastructures, incident grave impactant l'exploitation, Evénement sureté ...../ **Evènement Mineur** = local..). Les événements autres qu'une crise déclenchant alors une organisation de gestion différente.

La cellule de crise n'existe pas uniquement pour décider mais elle doit également mettre à disposition des décideurs (étatiques par exemple) toutes les informations à sa connaissance pour permettre de décider au mieux :

- La cellule de crise collecte, vérifie et fait remonter l'information aux décideurs
- Cette remontée d'informations doit suivre un canal unique, défini en amont (idéalement) ou à défaut, au moment de l'établissement de la cellule
- S'astreindre à une remontée d'informations régulière est une bonne pratique, la fréquence de ces remontées étant à préciser au cas par cas. Il peut dans certains cas, être tout-à-fait pertinent de conserver le point de situation précédemment planifié, même s'il consiste à annoncer « RAS ».

2.1 Analyse par critères et pesée de l'évènement

Définir les conditions / les caractéristiques des événements qui nécessitent une activation de la cellule de crise

Par exemple : certaines organisations ne déclenchent une crise que s'il y a des morts, d'autres s'il y a une atteinte potentielle à la vie ou certaines définissent des niveaux différents d'activation de la cellule de crise (cf. Incerfa – Alerfa – Detresfa)

Voir Annexe 2

Bonne pratique : La mise en œuvre d'une check-list / logigramme (Outil d'aide à la décision) simplifiée peut permettre de ne pas se retrouver dans une situation de Procrastination / Stupéfaction.

Un passage en mode crise ne doit pas être jugé négativement lorsqu'il y a un doute.

2.2 Décision par le chef de cellule de crise ou son suppléant de déclencher la cellule de crise

Dans ce cas, c'est le directeur de crise qui déclenche la mise en route opérationnelle de la cellule de crise mais dans certaines organisations une autre entité interne peut s'en charger. Questions à se poser dans toute organisation :

- Qui est décisionnaire du déclenchement d'une cellule de crise : le Directeur ou d'autres personnes ?
- Penser à un plan B permet-il de gérer même si le chef de crise est non joignable ou non opérationnel ?
- Qui informe les membres de la cellule de crise et comment cette information est transmise ?

2.3 Ouverture de la salle de crise et validation des membres requis

En relation avec les 2 premiers points, toute organisation doit avoir anticipé le choix des personnes présentes dans la cellule de crise. La non-sélection de certains personnels doit s'anticiper afin qu'ils comprennent bien qu'ils ne sont pas laissés de côté en raison de tel ou tel évènement ou d'un délit de faciès mais plutôt sur l'intérêt de les laisser en backup à leur poste habituel afin de parfaitement gérer les développements liés aux évènements.
Chaque acteur de la gestion de crise doit être familiarisé avec l'ouverture de(s) cellule(s) de crise, il se peut qu'il soit le premier arrivé (check-list du 1er arrivé). Cette ouverture doit également prendre en compte d'éventuels désagréments non prévus : impossibilité d'ouvrir la boite à clés électronique en cas de coupure de courant par exemple.

2.4 Transmission de l'alerte

Jalon important de notification vers les bonnes personnes car trop communiquer peut amener à s'exposer au risque de trop diffuser (Ex. Fuites externes).

Bonne pratique : avoir une liste de contacts pour ne pas rechercher le jour J les destinataires (Ex : Responsable Assurance de la Cie, contact escales, réseau de compagnies etc…). Un déclenchement de transmission de l'alerte peut avoir lieu par effet domino (une personne du plan est en charge de prévenir une autre personne). La confirmation de la bonne exécution des actions doit être comprise comme obligatoire afin d'avoir un système efficace et organisé de manière parfaite. Chaque accusé réception vers les responsables de process ou check-list est l'assurance que les actions s'effectuent correctement, dans l'ordre et sans besoin de rattrapage.

2.5 Cloisonnement et gestion de la communication

La communication médiatique doit se faire en parallèle de la gestion de crise mais surtout elle est indissociable : en effet elle évite que s'installent des rumeurs.

« Parle-t-on d'une communication opérationnelle ou d'une communication médiatique ? »

2.6 Les réponses immédiates

- **Médiatique** : Occuper le terrain (Messages d'attentes…) ne pas laisser les autres communiquer à la place de l'organisation.

Bonne pratique : Faire mention sur le site internet de la compagnie de manière succincte de l'évènement peut être adapté dans certaines situations.

-**Autorités** : En cas de crash, transmission de la liste des passagers vers autorités dans un délai court, idem pour la liste des marchandises dangereuses etc.

Bonne pratique : Créer une checklist reprenant les éléments à transmettre avec le phrasé et les détails adaptés ;

-**Ad hoc** : Savoir prendre des décisions impactantes (Ex : Arrêt des Opérations aériennes…). Ces décisions doivent se prendre dans le cadre du processus de culture juste interne à l'entreprise.

Mettre la personne la plus compétente et adaptée à la communication avec les médias (elle doit également être formée spécifiquement). Certaines personnes peuvent être de très bons directeurs, gestionnaires de crise sans pour autant être de bon communicants. Il ne faudra donc pas hésiter à les faire remplacer. Une mauvaise communication de crise peut très gravement aggraver la crise, retarder ou empêcher la sortie de crise pour l'entreprise.

Cela peut également avoir un impact majeur sur tout le domaine aéronautique (Cf. voir ce qu'il s'est passé avec le nuage de Tchernobyl : tout le monde se souvient du nuage et de la frontière alors que cela n'a jamais été dit - on peut rapprocher cela de l'effet Mandela).

2.7 Information au personnel et aux familles

La communication interne, quelle que soit la crise, est un point majeur à prendre en compte. En effet, des interprétations erronées, rumeurs et autres peuvent s'installer et être dangereuses.

Concernant la communication aux familles liées à la crise, une obligation réglementaire et réputationnelle existe et se doit d'être effectuée de la manière la plus adaptée en fonction des circonstances.

Le choix de personnes compétentes pour parler à chaque domaine (médias, familles, personnel…) est crucial.

Le niveau de connaissance de la crise peut différer d'un communicant à l'autre en fonction du groupe qu'il gère en prenant en compte le contexte, les éléments partageables et la population cible.

Ce message est utilisé entre les pilotes et personnels cabine lors d'un évènement grave à bord afin de transmettre d'une manière structurée par la personne émettrice les informations utiles, nécessaires, de manière claire et avec un accusé réception permettant de vérifier si la compréhension est bien totale au niveau de la personne réceptrice.

Exemple de transmission d'un **NITS** (Nature Intention Temporalité Spécificités) de A vers B: **Nature**: déclenchement de la cellule de crise suite à un évènement aérien. **Intention**: vous êtes attendu à la cellule de crise qui sera ouverte dans 15 minutes. **Timing**: transmettez-moi dès que possible votre

délai ». **Spécificités** : un retour de votre part au chef de la cellule de crise est nécessaire dès que l'action est effectuée.

III. Phase 3 : Gestion de la crise

3.1 Archivage des actions

Consigner tous les éléments propres à la mise en place de l'ERP (éléments recueillis, personnes présentes, actions menées, points de situation etc…) dans un journal de crise qui suivra l'insertion obligatoire de la référence jour et horaire de la mention.

Si des supports effaçables sont utilisés, il faut prévoir des photographies pour garder une trace de tous les échanges.

- **L'intérêt d'établir et de tenir à jour, tout au long de la crise, un « journal de bord » ou « de crise » (journal papier ou, préférentiellement numérique avec sauvegardes)**
  - La tenue d'un tel journal de bord a un grand intérêt dans le cas d'une crise longue, pour faciliter les relèves d'équipes par exemple.
  - En cas de remontées d'informations multiples, un tel journal permet également d'identifier aisément, a posteriori, « Qui a fourni quelle information à qui et à quelle heure » et facilite le « cross-check » entre plusieurs sources d'informations.
  - Ex :
    - *A 16h08 : Coup de téléphone reçu de …, annonçant X blessés*
    - *A 16h10 : Réception d'un mail du permanent de … Annonçant…*
    - *A 16h11 : Appel passé à …, qui confirme …*
    - *A 16h12 : Communication faite auprès du …*
  - Les 3 points clés du journal sont : bien noter l'heure de l'information, la source de l'information et le détail de l'information. Également ajouter si une action est ou doit être lancée.
  - Bonne pratique : définir un journal de bord numérique, sur un espace partagé par tous les membres de la cellule de crise (ex : via l'utilisation d'une équipe « TEAMS ») mais en s'assurant d'archiver en permanence les changements (pour revenir facilement à la version précédente en cas de bug) ;
  - Penser à bien définir qui renseigne ce journal de bord (le « coordinateur » par exemple).

3.2 Définition des actions à court et moyen terme

Mise en œuvre des actions définies dans la phase 1.

Affiner les actions en fonction du type et de la gravité de l'événement.

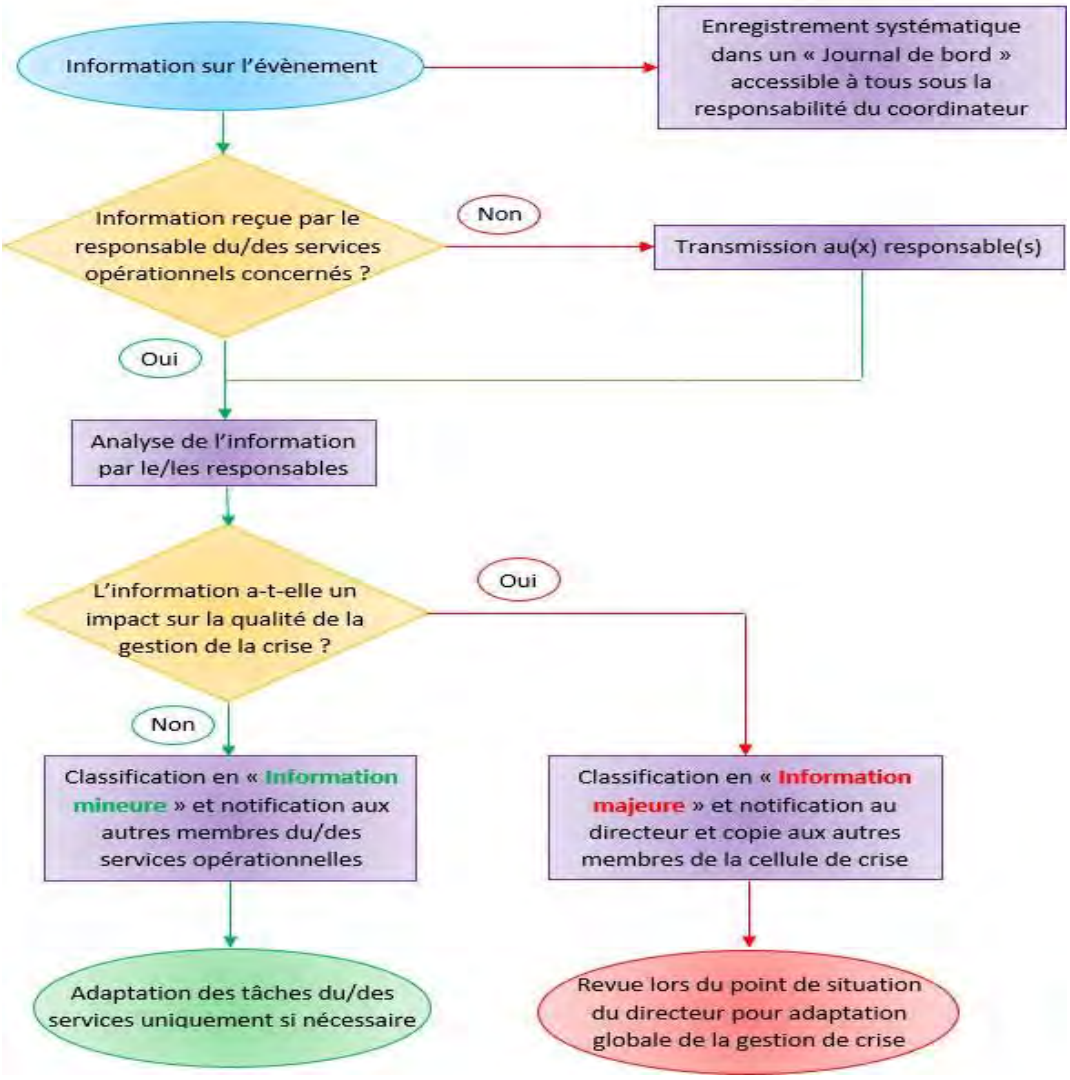
Prise en compte des éléments reçues d'autres cellules de crise le cas échéant - coordination des actions.

Qui / Quand / Comment / Pourquoi ?


DU TRAITEMENT DES ÉVÉNEMENTS À LA GESTION DES RISQUES
VÉRIFIEZ L'ADÉQUATION DE VOS ACTIONS DE SÉCURITÉ.
www.developpement-durable.gouv.fr
Deyms

3.3 Informations reçues ou transmises avec d'autres cellules de crise

Logigramme « Traitement de l'information dans la cellule de crise »



Enregistrer toutes les informations reçues/transmises en fichier numérique et/ou papier, en stipulant quand et à qui elles ont été reçues/transmises.

Définir la personne coordinatrice des éléments reçus/transmis, afin de gérer au mieux les entrées/sorties d'informations.

3.4 Assurer la continuité de fonctionnement de l'entité malgré la crise

Définir quelles activités peuvent continuer et celles qui doivent être suspendues (état psychologique du personnel, disponibilité des outils/ressources, etc.) et associer des moyens de liaisons de secours si nécessaire afin de garder le contact avec les personnels et poursuivre l'activité.

Rester proche des équipes, faciliter les échanges afin de détecter les éventuels besoins de soutien.

3.5 Interface de la cellule de crise avec d'autres groupes de travail, communication et lignes directrices

C'est le rôle du coordinateur et ceci doit être formalisé pour éviter des décisions prises dans l'urgence. En cas de crise ayant nécessité l'activation de plusieurs cellules de crise dans des organisations impliquées dans la gestion de l'évènement, l'un des aspects importants à prendre en compte est la concomitance et donc la nécessaire coordination entre ces équipes activées. La fixation très tôt de la liste des points de contact et leurs coordonnées permettra de ne pas perdre de temps dès les premiers besoins d'échanges.

3.6 Planification des points de situation

Réaliser des points de situation à intervalles réguliers ou avant chaque grande étape.
Points de situation interne (cellule de crise interne) et externe (autres cellules de crise) le cas échéant.
Qui les organise ?
Les points de situation ne doivent pas être interrompus, prévenir les autres entités qu'un point sera fait à X heure et pour une durée de Y min. Il faut envisager de débrancher/décrocher les téléphones ou de les confier à une personne extérieure au point de situation qui fera patienter.
L'utilisation d'un maitre du temps peut s'avérer très utile afin de ne pas rater les rappels ou actions programmées…

3.7 Organisation de la relève des membres de la cellule de crise (gestion de la fatigue et du stress)

Définir qui devra être remplacé.
A quel moment déclencher les "remplaçants" ? Par qui ?

IV. Phase 4 : la sortie de crise

4.1 La décision de fermeture de la cellule de crise

Le directeur de crise prend la décision de fermer la cellule de crise lorsque tous les éléments en sa possession lui permettent de conclure que toutes les actions menées pour gérer la crise sont terminées ou maîtrisées.

4.2 Débriefing de l'équipe de gestion de crise

Réaliser un debriefing à chaud et un debriefing quelques semaines après la fermeture de la cellule de crise.
Comment organiser ce debriefing (réunion ou questionnaire ? Par étapes ?) S'adapter à la durée de la crise. A l'initiative de qui ?

4.2.1 Fermeture de la salle de gestion de crise

Fermer la salle de gestion de crise est loin d'être anodin. En effet, les retours dans les différentes boites à clés des trousseaux, le rangement du matériel et la restitution de tous les objets rendus disponibles assurera par sa qualité la prochaine ouverture. Le recensement d'éléments à remplacer doit être minutieux et doit se faire rapidement afin d'être prêt au plus vite pour le prochain exercice ou crise naissante. Un retour d'expérience des acteurs de la cellule sur le matériel utilisé permettra sans délai de changer certains produits qui sont inadaptés. La reconstitution des stocks est également incluse dans cette fermeture. Cette phase est appelée chez les militaires « le reconditionnement » et représente une phase majeure de la préparation collective.

4.2.2 Collecte et mise en sécurité des documents liés à la gestion de crise

Un classement de tous les documents produits ou utilisés amènera les acteurs en charge de la gestion de crise à archiver, protéger, détruire le cas échéant l'ensemble des productions. Une partie pourra être désidentifiée et ré-utilisée pour préparer de nouveaux exercices. Toutes les références doivent être notées avec sérieux en cas de questionnement ou retour en arrière sur des éléments utilisés.

4.2.3 Information sur la fin de crise vers les employés

L'information de fin de crise doit se faire d'une manière officielle et à moment précis afin d'éviter une désorganisation dans le temps avec certains commençant à ranger leur matériel alors que d'autres sont toujours à leur poste. Tous les employés et personnes en lien avec la crise ou l'entreprise doivent avoir un point clair et qui ne prête à aucune confusion.

4.2.4 Après crise et gestion de la reprise

Lorsque la crise ne nécessite plus l'activation de la cellule mais n'est pas complètement terminée, un responsable sera désigné pour coordonner l'après-crise. Ce responsable a pour mission de coordonner l'ensemble des actions nécessaires et d'en conserver la trace dans la main courante ou le journal de bord.
Si besoin, il peut mobiliser des ressources complémentaires au sein de la compagnie pour l'assister dans sa mission. Cette personne est le Directeur d'après-crise à qui le Directeur de crise transfère l'ensemble du dossier lors de la fermeture de la cellule de crise. Une cellule d'écoute et d'accompagnement de fin de crise peut permettre de prendre en compte les ressentis des acteurs encore sous le choc ou épuisés par ces heures ou jours d'action.

V. Intégration du retour d'expérience

5.1 Mise à jour des processus et procédures

A froid, donc bien après les premières heures de fin de crise, un processus de mise à jour des procédures se doit d'être lancé afin d'alléger, de renforcer, d'adapter les actions menées et surtout prévues dans la documentation d'évènements graves. Cette mise à jour se doit d'être complète jusqu'à l'information des modifications en passant par l'arbitrage de nouvelles mises en œuvre dans les processus.

5.2 Amélioration continue du process

A chaque fin de gestion de crise, il est obligatoire d'avoir des mises à jour du processus de gestion documentaire ou des actions mais ceci doit également être mis en œuvre lors des exercices réguliers ou des travaux au sein de l'équipe en charge des préparations et gestion d'évènements.

5.3 Mise en place des exercices réguliers

Périodiquement, l'organisme met à l'essai ses procédures de traitement des crises et des situations d'urgence. Pour cela, il définit une banque de données d'exercices types : scénarios, les personnels à avertir, la fréquence etc. Cette boucle retour permet de mettre à jour les exercices déjà effectués et d'améliorer le plan correspondant.
Une des questions clés à se poser au sein de l'organisation est : où s'arrête l'exercice ?
Le fait de faire varier les contextes est intéressant car les actions des acteurs impliqués peuvent être extrêmement différentes pendant et hors heures ouvrables.
Intégrer l'intervention d'une personne extérieure ayant le rôle d'observateur amène un œil neutre qui permet de poser les bonnes questions et permet d'avancer sur des points peut être peu apparents.

La capitalisation des bonnes pratiques doit aussi être intégrée lors de ces exercices. Les actions qui fonctionnent et sont reconnues positives sont très importantes à noter et à mettre en œuvre lors des futures phases d'entraînement ou réelles.

Quoi qu'il en soit, un retour d'expérience a lieu après chaque exercice afin d'améliorer ce qui n'a pas fonctionné. En effet, il n'est pas imaginable d'avoir tous les éléments qui auront fonctionné à 100%, des ajustements seront donc très probablement nécessaires.

Bonnes pratiques, documents et liens d'intérêt

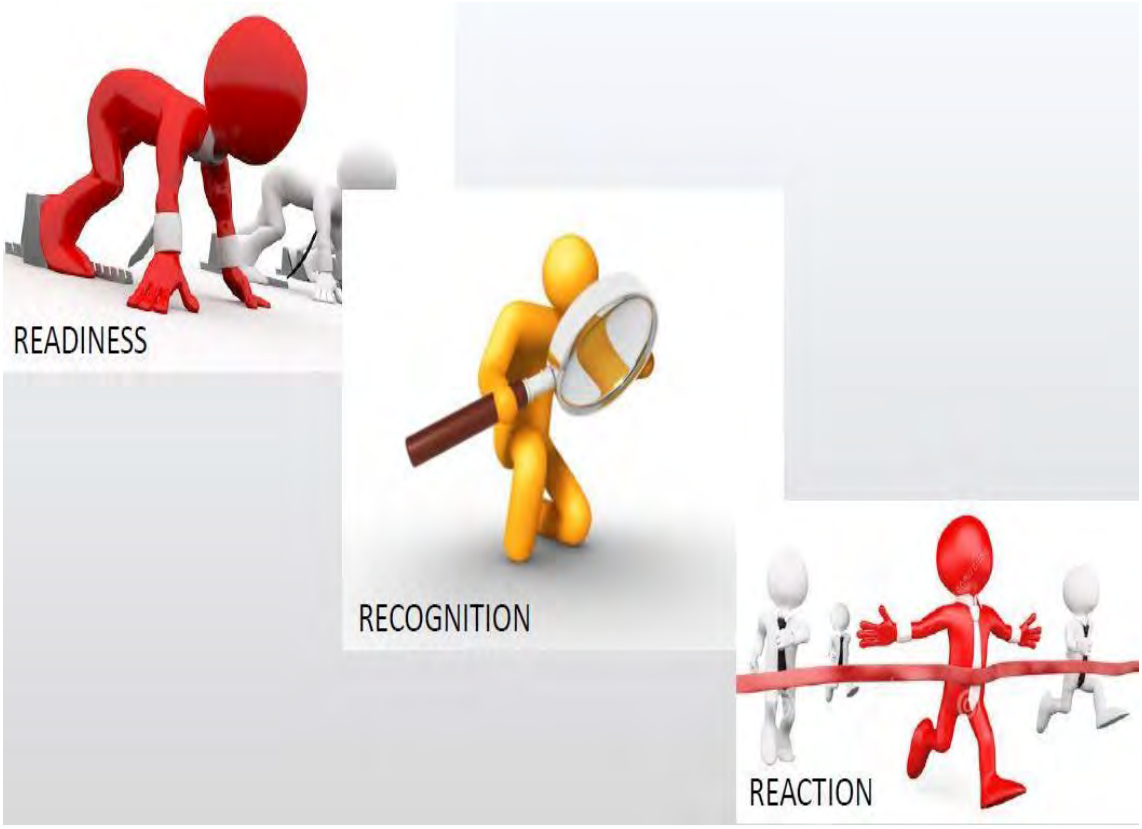
Méthode 3R :

Cette méthode développée en accord avec des groupes de travail EASA propose un œil complémentaire sur l'analyse des évènements en vérifiant si les acteurs, équipes ou organisations sont « prêts à agir », « reconnaissent la problématique ou le niveau d'action nécessaire » et adoptent la bonne « réaction ».

Readiness : Prêts, avec niveau de travail adapté, entrainés, engagés.

Recognition : détection, identification, compréhension, rappels à connaissances.

Reaction : immédiate, adaptée dans le temps, adaptée, effective.



Elle peut être utilisée dans l'analyse des différentes actions jouées en exercice ou qui se sont déroulées dans la crise. Un scoring est alors établi avec quelques exemples ci-dessous :

« L'équipe de levage a été contactée mais n'a pas pu être jointe car déjà partie sur une réparation. Non disponibles, ces acteurs obtiendront un code R puisqu'ils n'étaient pas prêts à agir, et donc incapables de reconnaître la problématique à gérer et avec une absence totale de réaction ».

« Cette même équipe en attente d'intervention est prête à agir mais n'a pas reconnu la demande exacte d'intervention : elle sera scorée R1 (seul le readiness est présent).

« Le score le plus élevé étant R123 avec l'équipe prête à agir, ayant reconnu parfaitement les actions de levage à effectuer et ayant réagi de manière adaptée en appliquant les procédures prévues »

Ces scores permettent d'orienter ensuite en fonction des acteurs ou équipes des ressources pouvant aider à gérer le R1, une meilleure connaissance et aide à la compréhension des tâches à effectuer pour le R2 ou des moyens adaptés pour améliorer le suivi des procédures afin de répondre au R3.

Annexe 1

Gestion des données personnelles et communication

Exemple d'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel :

Je soussigné/e Monsieur/Madame _____, exerçant les fonctions de _____ au sein de la société _____ (ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à _____, le jj/mm/aaaa, en X exemplaires

Nom :

Signature :

RGPD

PROTECTION DES DONNÉES PERSONNELLES

Qu'est-ce qu'une donnée personnelle ?

Toute information relative à un particulier identifié ou identifiable, directement ou indirectement, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité

Par exemple :

Règlement général sur la protection des données (RGPD) du 27 avril 2016

Code pénal

- Partie législative (Articles 111-1 à 727-3)
  - Livre II : Des crimes et délits contre les personnes (Articles 211-1 à 227-33)
    - Titre II : Des atteintes à la personne humaine (Articles 221-1 à 227-33)
      - Chapitre VI : Des atteintes à la personnalité (Articles 226-1 à 226-32)
        - Section 5 : Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques. (Articles 226-16 à 226-24)

Naviguer dans le sommaire du code

› Article 226-16

Version en vigueur depuis le 01 juin 2019

Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

NOTA :

Conformément à l'article 29 de l'ordonnance n° 2018-1125 du 12 décembre 2018, ces dispositions entrent en vigueur en même temps que le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés au 1er juin 2019.

Annexe 2

Une structure à 3 niveaux reprenant les alertes en circulation aérienne (INCERFA, ALERFA, DETRESFA) existe et peut être utilisée pour définir à quel moment la structure est considérée face à une crise et donc avec déclenchement des différentes phases :

La mise en alerte et gestion d'une crise en vol suit un processus réglementé en trois phases afin de passer d'une incertitude suite à des informations initiales, à une alerte pour mettre en place des niveaux de réaction chronologiques, pour finir par un stade de détresse qui lance les actions de gestion de la crise qui aura été confirmée (accident aérien, déclenchement de balise de détresse…). Le GT a identifié une possibilité d'intérêt pour certaines structures à utiliser ce type de phases de déclenchement d'actions amenant une mise en œuvre « crescendo » des services et ressources pour faire face à une crise.

Rendant le service d'alerte, les organismes de la circulation aérienne peuvent proposer le déclenchement des phases suivantes :

- INCERFA : phase d'incertitude : l'incertitude existe quant à la sécurité d'un appareil et de ses occupants, phase de recherches.

Dans le cadre du déclenchement éventuel d'une crise, la phase INCERFA peut permettre le recueil d'éléments et analyse des premiers indices faisant ressortir la possibilité de faire face à une crise suite à un évènement.

- ALERFA : phase d'alerte : les recherches n'ont rien donné ou on a de bonnes raisons de penser qu'un aéronef est en difficulté et que la sécurité de ses occupants peut être en jeu.

Au niveau des avancées de recueil d'éléments renforçant le doute de survenue d'une crise, la structure organisationnelle de réaction à la situation peut se mettre en place afin de prendre la forme de la phase ALERFA) : la structure prévue pour gérer la future crise est mise en marche en permettant de constituer les équipes en préparant les personnels et ressources en mode alerte.

- DETRESFA : phase de détresse, on a de bonnes raisons de croire que la sécurité d'un aéronef et de ses occupants est en jeu et qu'il nécessite une assistance immédiate.

L'alerte ayant été confirmée, la phase 3 de la gestion de crise est lancée avec l'activation des actions prévues dans le plan de crise correspondant à la phase DETRESFA)

LIEN VERS LE DOCUMENT DE DEFINITION DES 3 PHASES DE GESTION DE CRISE AERIENNE :