Université de Sherbrooke

DIRECTIVE 2600-097

TITRE :	**Directive relative à la gestion des situations d'exception**		
ADOPTION :	Comité de direction	Résolution :	CD-2024-03-25-07
ENTRÉE EN VIGUEUR :	25 mars 2024		

TABLE DES MATIÈRES

PRÉAMBULE

Qu'elles soient d'origine volontaire, accidentelle ou naturelle, les situations d'exception qui affectent les organisations sont nombreuses et variées. Elles prennent la forme d'incidents, d'urgences ou de crises et peuvent toucher des domaines aussi divers que la sécurité publique, l'environnement, la santé, la sécurité de l'information, les finances ou la réputation.

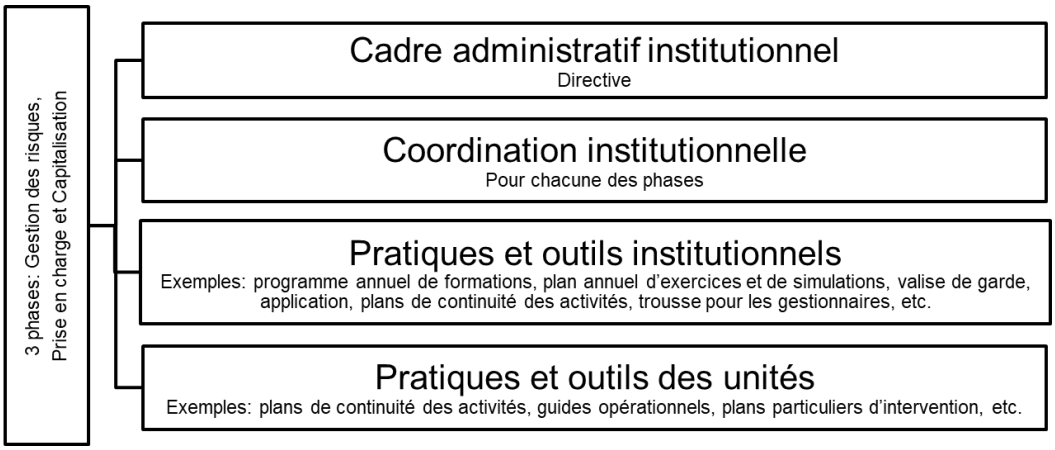
La gestion des situations d'exception nécessite une structure de gestion et des façons de faire spécifiques que l'on déploie en marge des activités courantes afin d'assurer une réponse rapide et efficace aux éléments perturbateurs et permettre, à terme, un retour à la normale.

Pour faire face à ces situations d'exception, l'Université de Sherbrooke met en place un Dispositif institutionnel de gestion des situations d'exception (DIGSE) reposant principalement sur:

- un cadre institutionnel proposant une approche concertée;
- une coordination institutionnelle des trois phases de la gestion des situations d'exception, incluant leur prise en charge;
- des pratiques et des outils institutionnels structurants;
- des pratiques et des outils conçus dans les unités et arrimés au volet institutionnel.

La présente directive précise le cadre organisationnel de ce Dispositif, notamment les niveaux hiérarchiques, les rôles et responsabilités des principaux acteurs de la gestion des situations d'exception, les processus de prise de décision et les mécanismes de communication.

Schéma 1. Les différentes composantes du DIGSE



1. OBJECTIFS

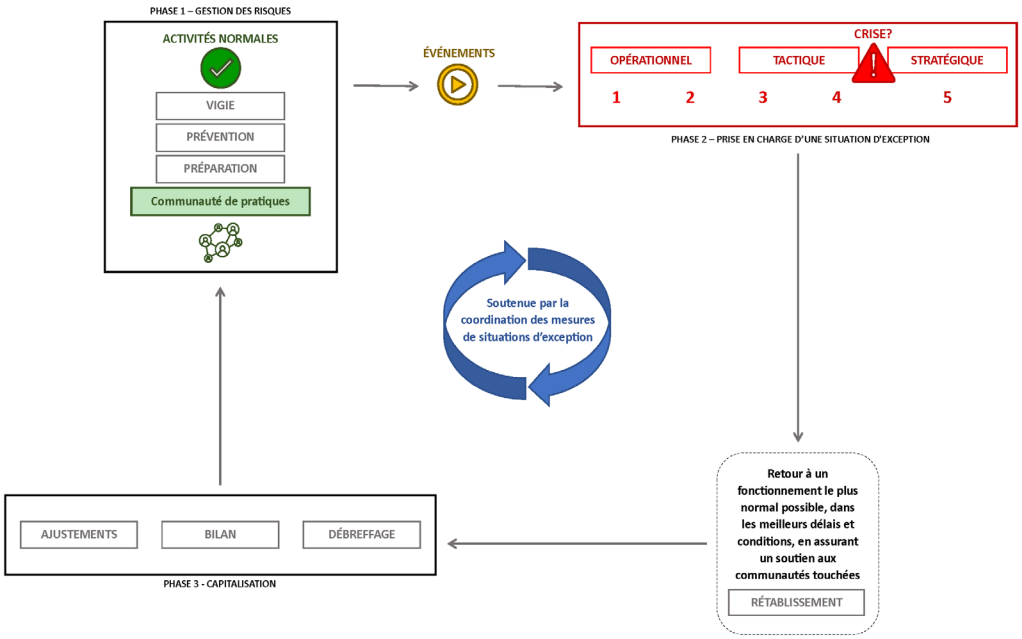
Le DIGSE forme un ensemble d'alignements et de moyens mis à la disposition de l'Université de Sherbrooke et de ses unités pour assurer une réponse rapide, efficace et coordonnée aux différentes situations d'exception. Il vise une optimisation des performances en matière de gestion des situations d'exception et une maximisation de l'efficacité opérationnelle.

Cette solution institutionnelle couvre les trois phases de la gestion des situations d'exception, à savoir la Gestion des risques (GDR), la Prise en charge (PEC) et la Capitalisation (CAP). Elle permet de répondre à tous les types de situations d'exception susceptibles de toucher l'ensemble de la communauté universitaire.

Plus spécifiquement, le DIGSE poursuit les objectifs suivants :

- assurer un milieu d'études et de travail sécuritaire qui favorise la santé des personnes et leur réussite;
- établir un cadre de référence institutionnel en matière de gestion de situations d'exception;
- déterminer les rôles et les responsabilités de chaque acteur de la gestion de situations d'exception, de même que les processus décisionnels à déployer;
- munir l'Université de pratiques et d'outils institutionnels flexibles;
- harmoniser et fédérer les pratiques et les outils en vigueur dans les unités;
- assurer le développement des compétences en gestion des situations d'exception;
- développer une culture de la gestion de situations d'exception.

Schéma 2. Le cycle de gestion d'une situation d'exception



2. DÉFINITIONS

Cellule tactique : cellule responsable de coordonner les actions et d'opérationnaliser les décisions établies par le Dirigeant ou par la cellule stratégique. Elle est en lien direct et constant avec l'équipe opérationnelle afin d'être au fait des actions prises et de l'état de situation sur le terrain.

Cellule stratégique : représente le plus haut niveau décisionnel dans la gestion des situations d'exception. Sa composition peut varier selon le type de situations d'exception. Elle comprend notamment le Dirigeant ou la personne qu'il a désignée.

Centre de coordination des situations d'exception (CCSE) : lieu principal où les acteurs identifiés (CMSE, chargé de mission, responsable du rétablissement, etc.) se réunissent afin d'assurer la gestion stratégique de la situation d'exception. Ce Centre possède les outils et les infrastructures nécessaires à son bon fonctionnement. Avec les outils numériques maintenant disponibles, il est possible que le CCSE soit virtuel, en tout ou en partie.

Centre des opérations d'urgence sur le site (COUS) : lieu physique où converge toute l'information que les intervenants sur le terrain possèdent et celle qui leur est destinée afin qu'ils puissent coordonner entre eux leurs opérations, avec le soutien du coordonnateur de site.

Chargé de mission : personne qui assume la direction d'une spécialité requise et qui est mobilisée dans la résolution d'une SE. Les missions sont notamment les communications, les immeubles, la sécurité de l'information, les technologies de l'information, les ressources humaines, la vie étudiante, les finances, le contentieux, ainsi que l'enseignement et la recherche.

Comité de direction de l'Université (CDU) : groupe composé du recteur ou de la rectrice, du recteur adjoint ou de la rectrice adjointe, du secrétaire général ou de la secrétaire générale et des vice-recteurs et vice-rectrices.

Communauté universitaire : ensemble des étudiantes et étudiants, des stagiaires rémunérés ou non, des membres du personnel, membres du corps professoral associé ou invité, des membres d'une instance décrite dans les Statuts de l'Université de Sherbrooke, ainsi que toute personne accueillie en vertu d'une convention d'études ou de stage et les stagiaires postdoctoraux.

Coordonnateur de site : généralement un cadre du SMSP ou la personne dont la mission est principalement affectée. Cette personne sera clairement désignée dès que possible par le CMSE.

Coordonnateur ou coordonnatrice des mesures de situations d'exception (CMSE) : personne responsable de la coordination institutionnelle de l'ensemble des actions touchant les trois phases de la gestion des situations d'exception, dont la prise en charge. Elle agit comme le pivot du DIGSE. Cette fonction est occupée par la directrice générale ou le directeur général du Service de la mobilité, de la sécurité et de la prévention (SMSP).

Dirigeant : le recteur ou la rectrice de l'Université, ou en son absence, la personne qu'il a désignée pour le remplacer.

Dispositif institutionnel de gestion de situations d'exception (DIGSE) : ensemble d'alignements et de moyens mis à la disposition de l'Université et de ses unités pour assurer une réponse rapide, efficace et coordonnée aux différentes situations d'exception.

Équipe opérationnelle : groupe de personnes qui, dans le cadre de la gestion d'une situation d'exception, réalisent des tâches en fonction de l'atteinte des objectifs fixés par le niveau tactique.

Événement : un événement survient dans le cours normal des choses. Il peut avoir une certaine ampleur, mais sa principale caractéristique réside dans le fait que l'unité où celui-ci survient peut le gérer elle-même, ou encore en faisant appel à d'autres services universitaires qui pourront l'épauler dans le cadre de leur mandat normal.

Incident de sécurité de l'information : événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

Missions : regroupement de tâches qui mobilisent des ressources d'une ou de plusieurs unités pour répondre à une catégorie de besoins générés par une situation d'exception.

Niveau de gravité : catégorisation d'une SE selon un chiffre de 1 à 5, qui est établie à l'aide des critères indicatifs et des exemples qui sont décrits dans l'annexe *Grille d'aide à l'évaluation des niveaux de gravité en lien avec la prise en charge des situations d'exception.* Le niveau de gravité induit d'une part l'ampleur de la SE à un moment précis et d'autre part les types de gestion à déployer et les intervenants internes et externes à être mobilisés (opérationnel, tactique et stratégique).

Plan de continuité des activités (PCA) : regroupement de procédures documentées, compilées et maintenues en disponibilité pour utilisation lors d'événements ou de situations d'exception, permettant à l'unité ou à l'Université d'assurer la continuité de ses activités essentielles à un niveau acceptable prédéfini. Pour les fins du présent DIGSE, les évaluations de risques font partie intégrante des plans de continuité des activités, afin de réaliser une planification intégrée des moyens d'atténuation et des stratégies de réponses aux incidents ou SE appréhendés.

Plan particulier d'intervention (PPI) : protocole de réponse visant à protéger la sécurité des personnes et la protection des infrastructures face à la matérialisation d'un risque précis (ex. : Plan de sécurité incendie, Procédurier de gestion des incidents de sécurité de l'information, Plan en cas de bris d'aqueduc, Plan de communication pour urgence météo, etc.). Un même PPI peut comprendre différentes sections qui définissent les adaptations pertinentes selon le lieu, le moment ou le contexte où survient la situation.

Poste de commandement (PC) : lieu à partir duquel se gèrent les tâches et les actions des équipes œuvrant sur le site d'une SE. Parfois, le PC peut occuper le même endroit que le COUS.

Responsable du rétablissement : personne en charge de la préparation et de la mise en œuvre graduelle du rétablissement. Son champ d'action concerne les actions à moyen et long terme, visant le retour à une normalité, notamment quant aux aspects réputationnels et psychosociaux.

Risque : danger éventuel, plus ou moins prévisible, inhérent à une SE ou encore éventualité d'un préjudice. L'importance d'un risque est estimée en fonction de l'impact de sa matérialisation (la gravité) et de la probabilité d'occurrence perçue de cette matérialisation (la vraisemblance).

Situation d'exception (SE) : événement qui sort de la norme ou de l'ordinaire. La situation d'exception se démarque par son caractère inhabituel ou son impact significatif. Une situation d'exception se produit généralement lorsque les circonstances sont extraordinaires, imprévues ou inhabituelles, ce qui peut nécessiter des mesures ou des actions exceptionnelles comme réponse. Il y a trois types de SE : l'incident, l'urgence et la crise. Chaque situation d'exception est unique et demande une analyse spécifique, qui peut évoluer dans le temps.

> **Incident** : SE qui cause une ou des perturbations locales, qui n'a pas une incidence directe et immédiate sur la santé et la sécurité des personnes et dont la gestion est généralement effectuée à même l'unité, avec le soutien du CMSE et la collaboration des autres services requis par la nature de la situation. L'incident est habituellement géré par une équipe opérationnelle et selon sa nature, peut-être sous la gouverne d'une petite cellule tactique ad hoc.
>
> **Urgence** : SE qui affecte des personnes, des opérations ou des installations, qui a le potentiel ou qui met effectivement en péril leur sécurité, leur intégrité physique et/ou psychique et qui nécessite une intervention immédiate. L'urgence peut être le résultat d'un incident s'étant aggravé. Elle implique souvent l'intervention de partenaires externes, comme les services d'incendie ou de

police. L'urgence est gérée par une équipe opérationnelle et, selon son ampleur, sous la gouverne d'une cellule tactique *ad hoc*.

Crise : SE qui engendre un niveau d'incertitude élevé, qui perturbe significativement les activités d'une ou de plusieurs unités et qui nécessite une réaction urgente et majeure. Une crise émerge souvent d'un incident ou d'une urgence qui a dégénéré, et elle implique l'intervention de partenaires ou d'instances externes. Pour gérer une crise, une cellule tactique gouverne les actions des équipes opérationnelles et une cellule stratégique est mobilisée, dont la composition variera selon l'ampleur ou la nature de la SE. Cette cellule stratégique formule les orientations à suivre et, pour la prise de décision, recourt au besoin aux instances supérieures de l'UdeS ou aux paliers de gouvernement appropriés.

Unité : rectorat, faculté, école centre universitaire de formation, institut universitaire de recherche ou service créé par le Conseil d'administration en vertu des Statuts de l'Université.

3. LISTE D'ACRONYMES

CAP : Capitalisation
CCSE : Centre de coordination des situations d'exception
CDU : Comité de direction de l'Université
CMSE : Coordonnateur ou coordonnatrice des mesures de situations d'exception
CSIO : Chef de la sécurité organisationnelle
COUS : Centre des opérations d'urgence sur le site
DIGSE : Dispositif institutionnel de gestion de situations d'exception
GDR : Gestion des risques
PC : Poste de commandement
PCA : Plan de continuité des activités
PEC : Prise en charge
PPI : Plan particulier d'intervention
SE : Situation d'exception
SMSP : Service de la mobilité, de la sécurité et de la prévention

4. CADRE LÉGAL ET NORMATIF

La présente directive et le Dispositif qu'elle met en place s'inscrivent dans un contexte réglementaire et législatif régi notamment par les lois, politiques, codes et règlements suivants :

- Loi sur la santé et la sécurité du travail (RLRQ, c. S-2.1) et ses règlements;
- Loi sur la sécurité civile (RLRQ, c. S-2.3) et ses règlements applicables;
- Loi sur la sécurité incendie (RLRQ, c. S-3.4) et ses règlements applicables;
- Loi sur le bâtiment (RLRQ, c. B-1.1) et ses règlements applicables;
- Politique québécoise de sécurité civile 2014-2024;
- Code national de prévention des incendies (CNPI);
- Règlements municipaux relatifs à la prévention des incendies qui sont en vigueur dans les municipalités où se trouvent les campus de l'Université;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, C. A-2.1

- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03);
- Norme CSA Z1600 : F17 (C2022) – Programme de gestion des urgences et de la continuité.

Plus spécifiquement à l'Université, la présente directive fait référence ou s'appuie sur les Politiques et Directives suivantes :

- 2500-004 – Politique de santé et sécurité en milieu de travail et d'études;
- 2500-014 – Politique sur les affaires juridiques;
- 2500-015 – Politique visant à prévenir et à faire cesser le harcèlement et la discrimination;
- 2500-036 – Politique de sécurité de l'information;
- 2500-042 – Politique visant à prévenir et à combattre les violences à caractère sexuel;
- 2500-051 – Règles de gouvernance à l'égard des renseignements personnels;
- 2600-042 – Directive relative à la santé et à la sécurité en milieu de travail et d'études;
- 2600-049 – Directive en matière de biosécurité et de biosûreté;
- 2600-056 – Directive relative aux situations issues de comportements perturbateurs mettant ou pouvant mettre en danger la sécurité et la santé de personnes ou l'intégrité des biens;
- 2600-061 – Directive sur les activités sociales avec consommation d'alcool organisées par les associations étudiantes;
- 2600-063 – Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels;
- 2600-070 – Guide de radioprotection;
- 2600-074 – Procédure de dévoilement, de signalement ou de plainte de violence à caractère sexuel;
- 2600-083 – Procédure de signalement et de plainte en lien avec la Politique visant à prévenir et à faire cesser le harcèlement et la discrimination;
- 2600-089 – Procédure relative à la gestion des allégations en matière de conduite responsable de la recherche;
- 2600-093 – Directive de gestion des incidents de sécurité de l'information;
- 2600-094 – Directive relative à la protection des renseignements personnels.

5. CHAMPS D'APPLICATION

La présente directive incombe prioritairement au comité de direction de l'Université. Elle doit toutefois, et sans limitation, être appliquée par l'ensemble des gestionnaires du rectorat, des facultés, écoles, instituts et services, en plus des responsables de projets.

Elle s'applique aux lieux suivants :

- Campus principal, incluant le Parc Innovation-ACELP;
- Campus de la santé;
- Campus de Longueuil, incluant le Pavillon Jean-Marc Lepage;
- Sites de formation délocalisés de Saguenay et de Moncton;
- Tout autre lieu où un membre de la communauté universitaire vit une situation d'exception nécessitant une prise en charge par l'Université.

6. PRINCIPES DIRECTEURS

6.1. Protéger et préserver

Au premier chef, il importe de protéger la santé et la sécurité des personnes, mais aussi dans, certaines circonstances, la continuité des activités, l'intégrité des biens, des infrastructures et de l'environnement, de même que la réputation de l'Université.

6.2. Collaborer

Quand une situation d'exception se déclare, l'ensemble des unités concernées (missions) doivent collaborer à sa gestion, selon les besoins et les priorités identifiés par la structure de gestion mise en place, sans égard aux conditions courantes ou aux activités régulières. Le coordonnateur des mesures de situations d'exception (CMSE) est responsable de la gestion de la situation d'exception, dont la mise en place de la structure de gestion appropriée.

7. CARACTÉRISTIQUES D'UNE SITUATION D'EXCEPTION

Il y a trois types de situations d'exception : l'incident, l'urgence et la crise (Tableau 1). Leur niveau de gravité se mesure à l'aide d'une analyse reposant sur sept critères (Tableau 2). L'évaluation globale de cette gravité repose sur le nombre de critères touchés et l'impact spécifique sur chacun d'entre eux, et prend la forme d'un chiffre de 1 à 5 (Tableau 3). À des fins d'aide à la décision, des exemples de situations typiques illustrant ces paramètres sont décrits dans une Grille d'aide à l'évaluation des niveaux de gravité (Annexe A).

Tableau 1. Exemples de situations d'exceptions

Types	Nature	Exemples
Incident	Sécurité	Menace, actes de malveillance, harcèlement, agression, vol, méfait, délit de fuite, vandalisme, rapatriement, etc.
	Opérationnelle	Bris d'équipement, panne d'électricité, défaillance structurelle d'un bâtiment, panne informatique, manifestation, grève, publication négative dans un média, perte temporaire de service, etc.
Urgence	Médicale et santé publique	Traumatismes, accident vasculaire cérébral, crise cardiaque, problèmes respiratoires, pandémie, épidémie, menaces biologiques, etc.
	Incendie	De véhicule, d'immeuble, de forêt, etc.
	Matières dangereuses	Explosion, fuite chimique, déversements, exposition à des vapeurs toxiques, fuite de gaz, contamination radioactive, etc.
	Sécurité publique	Braquage, alerte à la bombe, accident de transport, etc.
	Naturelle et climatique	Tornade, inondation, orage violent, tremblement de terre, ouragan, tempête de neige sévère, tempête de grêle, séisme, canicule, sécheresse, vague de froid, glissement de terrain, etc.
	Infrastructures et technologiques	Effondrement de bâtiment, panne de courant majeure, panne d'approvisionnement en eau, cyberattaque, défaillance des systèmes névralgiques, etc.
Crise	Toute catégorie possible	Tout incident ou toute urgence qui dégénère et atteint le seuil 5 indiqué au Tableau 3.

Tableau 2. Critères pour mesurer l'impact des situations d'exception

Critères d'impact
1. Santé et sécurité des personnes
2. Phénomènes psychosociaux
3. Interruption des activités
4. Menaces à l'environnement (matières dangereuses ou contaminants)
5. Pertes financières
6. Conformité aux lois et règlementations
7. Impact négatif sur la réputation

Tableau 3. Niveaux de gravité des situations d'exception

Niveau 1 : Incident ou urgence qui a un impact relativement circonscrit sur une unité ou un petit nombre d'unités. Une équipe opérationnelle est déployée. Le CMSE mobilise et coordonne les efforts de l'équipe opérationnelle et des autres services universitaires ou externes requis. Une cellule tactique minimaliste peut être mobilisée au besoin. Elle est coordonnée par le CMSE.
Niveau 2 : Plusieurs unités sont touchées ou une intervention significative est appréhendée (escalade). Une équipe opérationnelle est déployée. Le CMSE mobilise et coordonne les efforts de l'équipe opérationnelle et des autres services universitaires ou externes requis. Une cellule tactique *ad hoc* est déployée. Elle est coordonnée par le CMSE. Certaines autres missions pertinentes peuvent être mises en veille ou mobilisées pour des interventions précises.
Niveau 3 : Incident ou urgence qui a un impact important sur une ou plusieurs unités ou encore qui durera dans le temps. En plus de l'équipe opérationnelle, une cellule tactique est mobilisée. Avec un tel niveau, une crise est considérée comme potentielle, donc certains membres d'une éventuelle cellule stratégique sont informés et mis en veille par le CMSE.
Niveau 4 : Une ou plusieurs unités sont touchées significativement. Le niveau élevé d'incertitude laisse présager l'éclatement d'une crise à court ou moyen terme. Une cellule stratégique est mise en veille pour réaction probable à court terme et informée en détail de la situation. Certains des membres de la cellule stratégique sont consultés, selon les missions impliquées.
Niveau 5 : Incident ou urgence qui est devenu une crise avérée. Elle nécessite généralement l'apport de ressources externes et des interventions de niveau gouvernemental. Les instances supérieures sont impliquées. Une cellule stratégique est mobilisée et impliquée pour donner des orientations à la cellule tactique. Selon les décisions de la cellule stratégique, la cellule de crise du Conseil d'administration peut être informée, mise en veille ou mobilisée.

8. GESTION D'UNE SITUATION D'EXCEPTION

La gestion d'une situation d'exception s'articule en trois phases :

1. Phase 1 : Gestion des risques (GDR), comportant la vigie, la prévention et la préparation.
2. Phase 2 : Prise en charge (PEC), comportant la détection, la mobilisation et la réaction, incluant le rétablissement.
3. Phase 3 : Capitalisation (CAP), comportant le débreffage, les bilans et les ajustements.

8.1 Gestion de risques (GDR)

La gestion des risques permet d'identifier et d'évaluer les risques. Elle vise à diminuer la probabilité d'occurrence des situations d'exception et à en minimiser les impacts négatifs.

8.1.1 Vigie

Chaque unité est responsable de procéder à la vigie relative à ses champs de compétences. Pour ce faire, elle identifie les risques pouvant affecter sa mission au sein de l'Université, en fonction des critères présentés au Tableau 2. Elle sera ainsi en mesure de les surveiller, de les prévenir et de se préparer à y répondre adéquatement. Cette vigie implique notamment la surveillance de l'apparition ou de l'évolution des risques identifiés, la détection de la matérialisation de ces risques et l'analyse des informations pertinentes à leur caractérisation. Chaque unité s'assure également de demeurer à l'affût des tendances et de maintenir une collaboration avec ses partenaires internes et externes engagés dans la gestion de situations d'exception. Elle partage aussi les informations pertinentes diligemment, en particulier avec le SMSP.

8.1.2 Prévention

De concert avec le SMSP et le Service des communications, chaque unité doit, lorsque c'est pertinent, mener des campagnes d'éducation et de sensibilisation auprès de la communauté. Pour certains risques, des moyens physiques de mitigation doivent être envisagés, implantés ou améliorés en continu (ex. : gicleurs, pare-feu informatiques, logiciels antivirus, etc.). Certains de ces moyens de mitigation sont requis par des lois, règlements, normes et codes. Les Services concernés, comme le Service des immeubles, le Service des technologies de l'information et le SMSP, doivent être impliqués pour mettre à jour les moyens de prévention requis.

8.1.3 Préparation

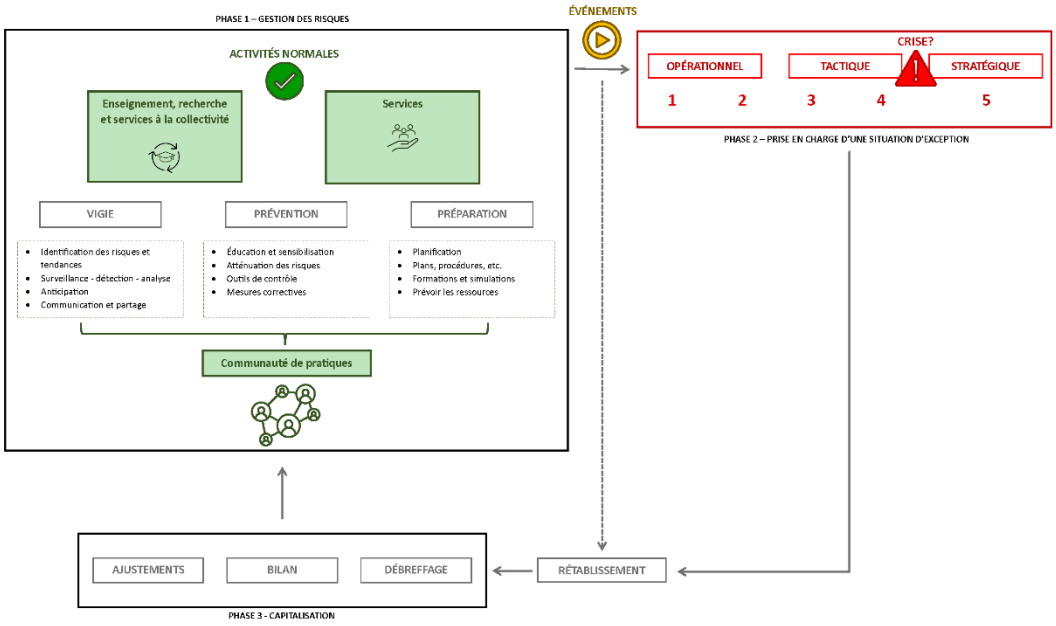
Chaque unité doit être prête à répondre rapidement et efficacement aux événements aux situations d'exception afin de prévenir leur escalade et de circonscrire leurs effets négatifs. Il est en ce sens de la responsabilité des gestionnaires de consacrer à cette tâche le temps et les effectifs nécessaires.

Les unités doivent notamment préparer des plans de continuité des activités (PCA) arrimés aux plans de continuité institutionnels et, lorsque pertinent, conclure des ententes avec des partenaires stratégiques, balisant les champs d'intervention respectifs et couvrant les modalités de collaboration, d'échange ou de fournitures de services, de même que les systèmes d'échanges de renseignements. Les PCA doivent comprendre notamment la caractérisation des processus essentiels, l'identification des interdépendances, une analyse des risques, de même que l'établissement des stratégies de continuité et des mesures d'intervention (actions).

Les unités doivent également se doter de plans particuliers d'intervention (PPI) spécifiques à leur contexte ou à leurs champs d'expertise. Ces PPI doivent être arrimés aux plans institutionnels.

Dans une optique d'amélioration continue, les gestionnaires des unités doivent finalement participer aux activités de formation, de même qu'aux pratiques et aux simulations, quand c'est pertinent.

Schéma 3. Illustration des détails de la phase 1 – Gestion des risques (GDR)



8.2 Prise en charge (PEC)

La prise en charge d'une SE repose sur la mise en place rapide d'une structure de gestion adaptée aux circonstances. À chaque type de SE correspond son mode de gestion. L'incident et l'urgence sont généralement gérés par une équipe opérationnelle, tandis que la crise appelle le déploiement d'une cellule tactique ou même stratégique, selon son ampleur. Lorsqu'une cellule stratégique est mise en place, elle est automatiquement appuyée par une cellule tactique et une équipe opérationnelle. C'est le même principe quand une cellule tactique est mise en place, elle s'accompagne d'une équipe opérationnelle. Il est important de noter que la prise en charge peut se faire en amont d'une éventuelle situation d'exception, donc dans une perspective préventive. En pareil cas, un plan d'intervention spécifique est préparé par une ou des équipes opérationnelles et validé par la cellule tactique. Le cas échéant, ce plan aura été préparé en fonction des grandes orientations édictées par la cellule stratégique.

8.2.1 Réaction

8.2.1.1 Détection

La détection d'un événement qui sort de la norme ou de l'ordinaire se produit souvent au sein des unités, par des membres de l'unité ou des systèmes de détection (ex. : systèmes de sécurité informatique, système d'alarme incendie, etc.). Il est également possible que des partenaires externes (ex. : police, Centre gouvernemental de cyberdéfense, etc.) soient les premiers à détecter une situation d'exception ou un événement à potentiel de le devenir. Dans tous les cas, une détection rapide permettra de faciliter sa gestion et de réduire ses impacts. Cette détection va de pair avec la validation diligente de l'information. Il est important d'identifier les sources d'informations et de mesurer leur crédibilité et fiabilité, dès le départ.

8.2.1.2 Évaluation

Dès qu'une SE est anticipée ou en cours, la personne responsable de l'unité qui en fait la détection doit rapidement prendre contact avec le CMSE. Ensemble, ils procèdent à l'évaluation du niveau

de gravité, à l'aide de la Grille d'aide à l'évaluation des niveaux de gravité en lien avec la prise en charge des situations d'exception (Annexe A). Ce dernier est estimé en fonction de l'impact de sa matérialisation, qu'elle soit avérée ou appréhendée. Il est à noter que l'évaluation d'une situation d'exception varie dans le temps. Elle peut augmenter en importance, comme elle peut diminuer. Le système de gestion s'y adapte.

8.2.1.3 Mobilisation

Équipe opérationnelle

L'incident et l'urgence sont gérés sur le terrain par une ou plusieurs équipes opérationnelles qui réalisent leurs tâches en fonction de l'atteinte des objectifs fixés par le niveau tactique. Pour les urgences, la gestion des équipes est habituellement effectuée à partir d'un Poste de commandement (PC) ou d'un Centre des opérations d'urgence sur le site (COUS). Pour les autres types de SE, l'équivalent d'un COUS pourrait être situé dans les locaux de l'unité principalement affectée ou encore prendre une forme virtuelle.

Cellule tactique

La cellule tactique est automatiquement mobilisée par le CMSE lorsque plusieurs équipes opérationnelles ou plusieurs missions sont requises. Pour des SE de niveaux 1 et 2, la cellule tactique est habituellement *ad hoc* et son nombre de participants s'avère relativement limité. Toutefois, pour les situations d'exception de niveaux 3 à 5, elle sera constituée d'un nombre important de chargés de missions, selon une composition induite par le type de SE, tel que décrit dans le Tableau 4.

La cellule tactique est responsable de coordonner les actions et d'opérationnaliser les décisions établies par le Dirigeant ou par la cellule stratégique. Elle est en lien direct et constant avec l'équipe opérationnelle afin d'être au fait des actions prises et de l'état de situation sur le terrain. Le CMSE préside la cellule tactique et assure la liaison auprès de la cellule stratégique ou du Dirigeant. Il peut s'adjoindre tout soutien qu'il juge nécessaire pour le fonctionnement de la cellule tactique.

Rôles de la cellule tactique

- assurer la conduite tactique de la gestion de la SE;
- procéder à une analyse détaillée de situation, produire un état des lieux et le mettre à jour tout au long de la prise en charge;
- élaborer et coordonner la mise en œuvre des stratégies de gestion de crise, incluant la coordination avec les parties prenantes et la supervision des communications;
- assurer une liaison permanente avec les organisations et les services externes;
- diffuser les communications internes et externes;
- prévoir et s'assurer du déploiement des ressources humaines et matérielles requises;
- s'assurer de la capacité de réponse des équipes opérationnelles et veiller à ce qu'elles possèdent les ressources nécessaires à la réalisation des objectifs.

Tableau 4. Missions pouvant être mobilisées pour la cellule tactique

Sous la coordination du CMSE, qui est responsable de la mobilisation des missions		
Mission	**Acronyme**	**Personne chargée de mission***
Communications[1]	*Comms*	DG du S Comm
Sécurité de l'information[2]	*SI*	CSIO
Technologies de l'information[2]	*TI*	DG STI
Protection des renseignements personnels	*PRP*	SG adjoint
Immeubles et infrastructures	SdI	DG SdI
Ressources humaines	RH	DG SRH
Vie étudiante et Psychologie-orientation[3]	VE-SPO	DG SVE
Bureau Respect	B. Resp.	Conseillère
Ombudsman	Omb.	Ombudsman
Relations internationales	USI	DG USherbrooke International
Contentieux	Légal	Conseillère juridique affectée par la SG
Ressources financières et services commerciaux[4]	RF – Svc Commerc.	DG SRF
SMSP (Sécurité, mobilité ou SSMTE)[5]	*SMSP*	Officière, officier ou Directeur SSMTE.
Recherche et Enseignement[6]	*Nom de la faculté*	Doyenne, Doyen ou DA de la faculté concernée
Responsable du rétablissement	*Resp. Rét.*	Personne nommée par le CMSE

***** : Chaque chargé de mission doit nommer et préparer une personne qui pourra le remplacer au besoin, dès la mobilisation par le CMSE.

[1] : La mission Communications est la mission qui est d'emblée mise en veille ou mobilisée pour toutes les SE.

[2] : Les missions Sécurité de l'information et Technologies de l'information sont soumises à des exigences légales particulières. Selon le type de SE, il est possible que ces deux missions n'en constituent qu'une seule, sous la gouverne de la mission SI. Plus de détails sont donnés à la section 8.2.1.8.

[3] : Selon le type de SE, la mission VE pourrait être accompagnée d'une mission.

[4] : Selon le type de SE, la mission RF pourrait être accompagnée ou remplacée par une mission Services commerciaux, notamment lorsque des assureurs doivent être intervenir.

[5] : Selon le type de SE, la mission du SMSP pourrait être subdivisée en missions Sécurité, Mobilité ou Santé et sécurité en milieu de travail et d'études.

[6] : La mission Recherche et enseignement constitue la raison d'être de l'UdeS. Les cinq principes directeurs du DIGSE visent à préserver cette mission et à permettre son rétablissement.

Cellule stratégique

La cellule stratégique représente le plus haut niveau décisionnel. Elle est informée ou mise en veille dès les niveaux 3 ou 4 et automatiquement activée pour le niveau 5. C'est le CMSE qui la mobilise. Sa composition peut varier selon le type de SE. Habituellement, ce sont les vice-rectrices et vice-recteurs et la ou le secrétaire général desquels relèvent les unités touchées et celles mobilisées

pour répondre à la SE qui sont appelés à y participer. Le Dirigeant conserve toujours la prérogative d'y participer lui-même ou d'y affecter toute autre personne de son choix. À moins que le Dirigeant ne soit lui-même présent, c'est généralement la rectrice adjointe ou le recteur adjoint qui préside la cellule. Chaque personne membre de la cellule stratégique doit désigner une autre personne pour la remplacer et la préparer en conséquence, dès la mobilisation par le CMSE.

Le CMSE est la courroie de transmission de l'information et des décisions entre les cellules tactique et stratégique. Il peut s'adjoindre tout soutien qu'il juge nécessaire.

Rôles de la cellule stratégique

- assurer la conduite stratégique de la gestion de la SE;
- donner l'orientation générale de la réponse à la SE;
- établir ou confirmer les décisions à déployer;
- approuver les grands axes de communication;
- confirmer les cadres d'entente des partenariats avec les organismes et instances externes imputables ou parties prenantes à la gestion de la situation;
- valider ou émettre les décisions et les alignements stratégiques, comme l'arrêt partiel ou complet des activités.

8.2.1.4 Coordonnatrice ou coordonnateur des mesures de situations d'exception (CMSE)

Le CMSE est le pivot du DIGSE. Il est responsable de la coordination institutionnelle de l'ensemble des actions touchant les trois phases de la gestion des situations d'exception.

Rôles de la personne CMSE

Avant une situation d'exception :

- tenir à jour les composantes institutionnelles du DIGSE;
- s'assurer de l'harmonisation des outils et des pratiques en vigueur dans les unités;
- veiller à ce que le DIGSE soit arrimé aux réalités des autorités externes, dont les Villes et les organismes de sécurité civile;
- conclure des ententes avec des partenaires externes stratégiques, balisant les champs d'intervention respectifs et couvrant les modalités de collaboration, d'échange ou de fournitures de services, de même que les systèmes d'échanges de renseignements;
- planifier l'organisation et l'aménagement des Centres de coordination des situations d'exception (CCSE);
- élaborer le programme annuel de formations et le plan annuel d'exercices et de simulations;
- promouvoir le développement des compétences en gestion des situations d'exception;
- travailler au développement d'une culture de la gestion de situations d'exception;
- désigner son remplaçant.

Pendant une situation d'exception :

- évaluer la gravité de la situation et déterminer le mode de gestion approprié. Lorsqu'une situation avérée ou potentielle est signalée par une personne responsable d'une unité, l'évaluation se fait en collaboration avec celle-ci;
- déclencher les procédures d'alerte et de mobilisation associée au mode de gestion retenu. Selon le niveau de gravité de la SE, il s'agira de mettre en veille ou de mobiliser les cellules

tactique et stratégique appropriées. Si une équipe opérationnelle est déjà mobilisée, il coordonnera les efforts des missions impliquées;
- veiller au bon fonctionnement des cellules de crise, en coordonner les actions et s'assurer de la mise en œuvre des mesures adoptées;
- colliger l'information et s'assurer de la redistribuer aux parties prenantes;
- réévaluer régulièrement la SE et maintenir un portrait global de son évolution, notamment à l'aide des rapports de situation;
- faire le point régulièrement avec le Dirigeant ou, le cas échéant, avec la cellule stratégique, ainsi qu'avec les parties prenantes internes et externes;
- déterminer au besoin le lieu et le moment de l'ouverture du Centre de coordination des situations d'exception (CCSE);
- collaborer avec les partenaires externes;
- recommander au besoin le confinement ou l'évacuation d'un secteur donné;
- agir comme courroie de transmission entre les cellules tactique et stratégique;
- s'assurer que les journaux de bord des cellules tactique et stratégique sont tenus.
- de manière générale, favoriser un climat de collaboration entre les acteurs, en assurant notamment une communication claire.

Après une situation d'exception :

- s'assurer que les différentes missions impliquées tiennent des débreffages sur les actions de leurs équipes opérationnelles;
- organiser les séances de débreffage de la cellule tactique et de la cellule stratégique;
- mettre à jour et réviser le DIGSE en y apportant les modifications nécessaires.
- accompagner les unités pour qu'elles intègrent elles aussi les modifications nécessaires dans leurs outils.

8.2.1.5 Chargée ou chargé de mission

Plusieurs champs d'expertise sont requis pour répondre aux divers besoins spécifiques qui sont susceptibles de se manifester dans le cadre de la gestion d'une SE. Ces champs d'expertise sont désignés sous le nom de "mission". Les rôles attribués aux personnes chargées de mission sont généralement les mêmes que ceux de leurs fonctions habituelles, c'est-à-dire d'assumer l'imputabilité de la prestation de service dans leur domaine et d'orienter les actions de leurs équipes opérationnelles vers l'atteinte des objectifs. Évidemment, la prestation de service attendue peut toutefois s'avérer plus intense et exigeante que celle des opérations de routine, notamment en nécessitant du travail en dehors des heures normales.

Rôle de la personne chargée de mission

Avant une situation d'exception :

- s'assurer de bien maîtriser le contenu du DIGSE, ainsi que son rôle en gestion de SE;
- s'assurer de l'état de préparation de sa mission pour réagir aux diverses SE possibles;
- identifier un substitut et le préparer;
- participer aux formations et aux exercices;
- produire et maintenir à jour ses outils, dont les plans de continuité des activités (PCA);
- participer aux formations, aux pratiques et aux exercices.

Pendant une situation d'exception :

- lorsque mobilisé, participer aux rencontres de la cellule tactique;
- mettre en veille, mobiliser ou trouver les ressources nécessaires à la réalisation de sa mission;
- assurer la direction et le contrôle des activités de sa mission en fonction des objectifs fixés;
- s'assurer de la tenue de journal de bord des activités de sa mission;
- assurer la collecte, la validation, la synthèse et la circulation des informations pertinentes;
- planifier les relèves pour le personnel de sa mission;
- en temps opportun, préparer le rétablissement de la situation, planifier et mettre en œuvre le désengagement de ses ressources.

Après une situation d'exception :

- préparer et tenir des séances de débreffage avec son équipe opérationnelle;
- colliger les informations qui émanent des séances de débreffage;
- participer aux débreffages des autres équipes où il est convié;
- à la suite de ces débreffages, intégrer les modifications nécessaires dans les outils spécifiques de sa mission.

8.2.1.6 Responsable du rétablissement

Le responsable du rétablissement est la personne en charge de la préparation et de la mise en œuvre graduelle du rétablissement. Il relève du CMSE et assiste aux délibérations de la cellule tactique. Sa vision et ses objectifs sont tournés vers des actions à moyen et long terme. Il propose à la cellule tactique des objectifs, des priorités et des mesures à mettre en place pour entamer un retour vers la normalité. Au besoin, il gère une petite équipe qui sera dédiée au rétablissement et qui l'aidera dans ses recherches et analyses. Le responsable du rétablissement pense notamment aux aspects réputationnels et psychosociaux d'une SE.

8.2.1.7 Coordonnateur de site

Le coordonnateur de site est généralement un cadre du SMSP. Cette personne sera clairement désignée rapidement par le CMSE. Dans certains cas, notamment pour des incidents de sécurité de l'information, une personne responsable de l'unité ou de la mission en cause peut être désignée. Le coordonnateur de site s'occupe du COUS et participe à la gestion des équipes opérationnelles et des partenaires externes, le cas échéant. Dans certains cas, il peut être colocalisé avec un PC. Le Coordonnateur de site relève du CMSE, à qui il transmet toute information qu'il juge pertinente pour les prises de décision de la cellule tactique, ainsi qu'au besoin des rapports d'évolution de la situation dans son secteur.

Rôle de la personne coordonnatrice de site

Avant une situation d'exception :

- s'assurer de bien maîtriser le contenu du DIGSE et les outils pertinents pour sa tâche, ainsi que son rôle en gestion de SE;
- participer aux formations, aux pratiques et aux exercices.

Pendant une situation d'exception :

- lorsque mobilisé, se déployer à l'endroit indiqué et y établir son COUS;

- une fois sur place, prendre contact avec les responsables des lieux, les équipes opérationnelles, ainsi que les partenaires externes, le cas échéant;
- assurer la collecte, la validation, la synthèse et la circulation des informations pertinentes entre les partenaires du COUS;
- faire rapport régulièrement au CMSE ou à toute personne que ce dernier lui a désignée, notamment dès que des faits nouveaux sont établis ou que des changements de situation surviennent;
- si pertinent, s'assurer qu'un périmètre de sécurité adéquat a été mis en place;
- si pertinent, s'assurer que la circulation reste sécuritaire et fluide sur le site;
- si pertinent, s'assurer que les victimes ont été secourues et en faire rapport dès que possible au CSME;
- tenir à jour un rapport chronologique de ses actions (journal de bord);
- planifier les relèves pour le personnel de sa mission;
- en temps opportun, planifier et mettre en œuvre le désengagement de ses ressources.

Après une situation d'exception :

- préparer et tenir des séances de débreffage avec son équipe opérationnelle;
- colliger les informations qui émanent des séances de débreffage;
- participer aux débreffages des autres équipes où il est convié;
- à la suite de ces débreffages, intégrer les modifications nécessaires dans les outils spécifiques de sa mission.

8.2.1.8 Missions particulières en cas d'incident de sécurité de l'information

En cas d'incident de sécurité de l'information, le Chef de la sécurité de l'information organisationnelle (CSIO) assume le rôle qui lui est dévolu selon le cadre légal découlant de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03)*. C'est un statut particulier qui s'arrime au DIGSE. Le CSIO prend en charge le volet opérationnel de la gestion d'un incident de sécurité de l'information, alors que le CMSE est responsable du volet tactique et stratégique, à partir du moment où le DIGSE est déployé. Le CSME s'assurera notamment dans ce contexte de la continuité des activités et de la reprise des services critiques. Le CMSE et le CSIO feront ensemble le lien entre la cellule tactique et la cellule stratégique.

Rôle de la personne CSIO

Avant une situation d'exception :

- s'assurer de la mise en place des mécanismes institutionnels robustes en matière de préparation, détection, analyse, information, confinement, éradication et rétablissement;
- participer aux formations, aux pratiques et aux exercices.

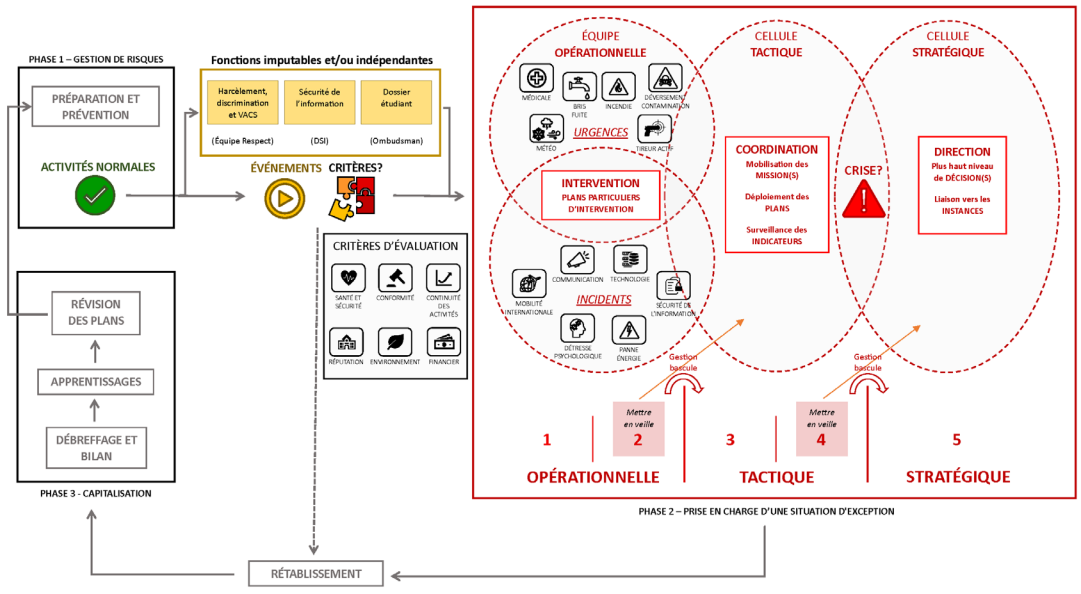
Pendant une situation d'exception :

- convoquer et coordonner la cellule opérationnelle;
- autoriser et valider les contremesures mises en place;
- documenter le plan d'action opérationnel la cellule de crise opérationnelle;
- orienter les ressources en soutien;
- s'assurer de la continuité des services;
- coordonner la priorisation du rétablissement des services;
- soutenir le rétablissement des services.

Après une situation d'exception :

- démobiliser les équipes prêtées;
- convoquer et mener le débreffage opérationnel;
- colliger les informations qui émanent des séances de débreffage;
- participer aux débreffages des autres équipes où il est convié;
- à la suite de ces débreffages, intégrer les modifications nécessaires dans les outils de sa mission.

Schéma 4. Détail de la phase 2 – Prise en charge d'une situation d'exception (PEC)



8.2.2 Rétablissement

Le rétablissement à la suite d'une SE correspond aux actions et aux efforts déployés pour restaurer le cours normal des activités. L'objectif est de favoriser un rétablissement dans les meilleurs délais des services et des activités minimalement acceptables. Le niveau de qualité pourrait donc ne pas être optimal dans un premier temps, mais graduellement, le retour à une normalité semblable à celle qui existait avant la SE constitue l'objectif ultime de la phase de rétablissement. Ce rétablissement implique donc la réparation des dommages et le soutien psychosocial, mais il est convenu et attendu que la nouvelle « normalité » ne sera peut-être jamais comme celle d'avant, notamment à cause des apprentissages réalisés et des changements qui seront mis en place pour prévenir une nouvelle SE du même genre que la précédente. Des plans spécifiques de rétablissement doivent être faits pour chaque SE, et ce pour chaque mission mobilisée. Le cas échéant, la personne responsable du rétablissement agit comme pivot pour cette étape.

8.3 Capitalisation (CAP)

La capitalisation permet de tirer des apprentissages des expériences vécues, dans une perspective d'amélioration continue. Cette étape vise notamment la révision des stratégies, des pratiques et des outils, notamment les plans de continuité d'activités, les procédures opérationnelles et les plans particuliers d'intervention. Elle s'articule autour d'une rétroaction, de bilans et d'ajustements liés aux apprentissages.

8.3.1 Débreffages

Il existe deux types de rétroactions : le débreffage immédiat (à chaud), ainsi que le débreffage opérationnel et stratégique. Le premier survient tout de suite après l'événement, et vise à colliger les principaux éléments à retenir. Le second se tient généralement six semaines plus tard et vise le partage détaillé des faits et des expériences entre les équipes afin de procéder à l'amélioration des pratiques.

Tableau 5. Types de débreffage

Types	Moments	Objectifs	Sujets
Immédiat	Immédiatement après la conclusion de la situation d'exception.	Noter les principaux éléments. Procéder à des ajustements rapides.	Question sur les rôles, les tâches et les objectifs assignés, les problèmes rencontrés (de procédures, de santé et de sécurité).
Opérationnel et stratégique	Environ 6 semaines après la conclusion de la situation d'exception.	Partager les expériences et les faits entre les équipes. Améliorer les pratiques, réviser les procédures opérationnelles, les plans et les collaborations.	Les personnes concernées sont invitées à raconter leur expérience.

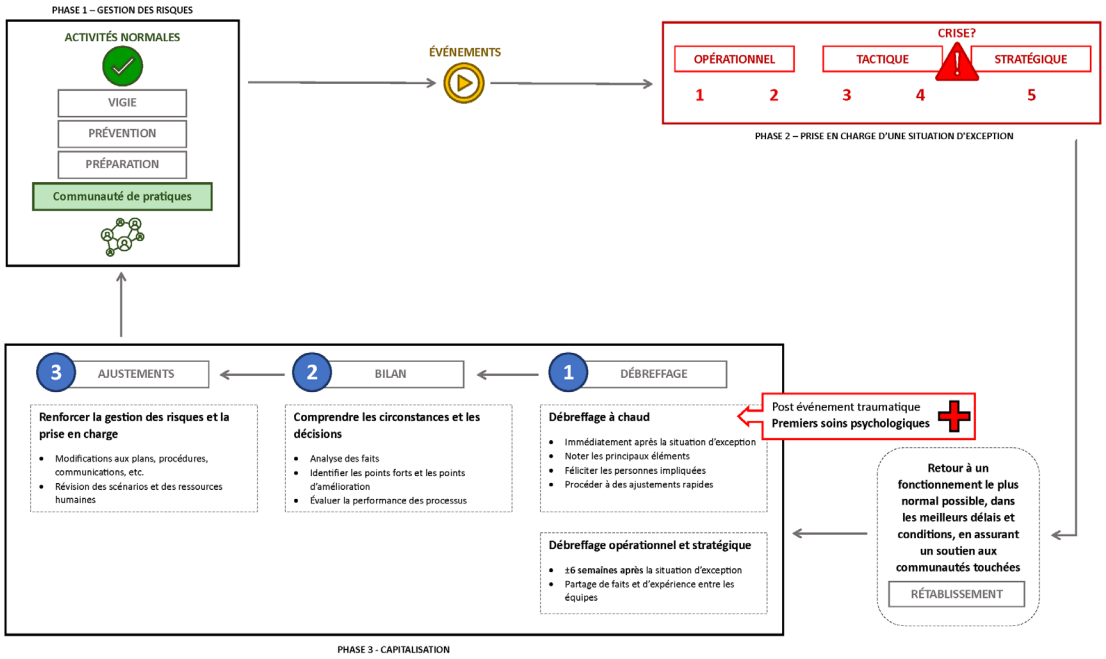
8.3.2 Bilans

Procéder aux bilans de la prise en charge d'une situation implique de faire une analyse des faits pour mieux comprendre les circonstances et les décisions qui ont été prises. Il faut identifier les points forts et les points d'amélioration, de même qu'évaluer la performance des processus. Le bilan se conclut par des recommandations d'amélioration, qui peuvent s'appliquer à tous les niveaux du DIGSE.

8.3.3 Ajustements

À partir des recommandations colligées lors du bilan, il importe de renforcer les phases de gestion des risques et de prise en charge des situations d'exception. Plus spécifiquement, des ajustements doivent être apportés aux PCA, aux PPI, aux plans de formations, aux communications, au stockage et à la logistique, etc. Si nécessaire, il faut revoir aussi les analyses de risque et l'élaboration des scénarios de SE plausibles, ainsi que les attributions de ressources humaines ou financières. Cette étape clôt la phase de capitalisation. Elle est essentielle pour renforcer la résilience organisationnelle.

Schéma 5. Détail de la phase 3 – Capitalisation (CAP)



9. RESPONSABILITÉ

Le membre du comité de direction de l'Université de qui relève le Service de la mobilité, de la sécurité et de la prévention (SMSP) veille à l'application et à la diffusion de la présente directive, ainsi qu'à sa mise à jour, au moins une fois tous les 5 ans.

10. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur au moment de son adoption par le comité de direction de l'Université.

ANNEXE A : GRILLE D'AIDE À L'ÉVALUATION DES NIVEAUX DE GRAVITÉ EN LIEN AVEC LA PRISE EN CHARGE DES SITUATIONS D'EXCEPTION

NOTES: Ce Tableau est un outil d'aide à la décision. Comme chaque situation d'exception est unique, il ne saurait être question d'appliquer cette grille de manière rigide.

Niveau de gravité	Santé et sécurité des personnes	Phénomènes psychosociaux (sur le campus dans certains cas, mais pour décès considérer aussi ailleurs que sur le campus)	Interruption des activités ¶	Menaces à l'environnement	Pertes financières	Impact légal, règlementaire et/ou contractuel[1]	Impact négatif sur la réputation §
1	Menace e violence; ou accident sans blessé; ou dommages matériels limités avec intervention limitée des services externes (pompiers, ambulanciers ou policiers).	Incident critique¤; ou autres enjeux psychosociaux dont l'impact est limité à un petit groupe et dont la durée dans le temps est limitée.	Fermeture pour moins de 24h d'un petit nombre de locaux non-critiques* (ex. bureaux, salles de classe, laboratoires d'enseignement ou laboratoires de recherche, MAIS pas d'animalerie. Services informatiques : 4 à 12h	Déversement ou relâchement mineur** de matières dangereuses qui peut avoir entraîné un déploiement mineur de ressources externes (pompiers, ambulanciers ou policiers1).	Perte non explicable de moins de 25k$, selon une première estimation.	Aucun impact sur le respect des obligations légales, règlementaires internes2 ou contractuelles. Seule l'imputabilité d'employés est en jeu. Celle des dirigeants n'est pas menacée.	Information négative isolée et/ou temporaire publiée dans les médias traditionnels ou sociaux, ou encore rumeurs, dont le potentiel d'escalade est faible et qui n'a pas d'impact appréhendé sur la réputation.
2	Menace de violence importante; ou accident avec blessés légers et/ou dommages matériels importants.	Incident critique¤; ou autres enjeux psychosociaux dont l'impact est étendu à une unité et dont la durée dans le temps ne devrait être grande.	Perte d'accès de 24-48h pour des activités académiques; ou perte d'accès 0-24h et pour des activités de recherche critiques*. Services informatiques : 4h à durée indéterminée, révisée à 12h et moins en moins de 4h après le début.	Déversement ou relâchement mineur** avec dommages matériels limités et contenu à l'intérieur d'un ou deux lieux entraînant l'évacuation d'un étage ou plus ; ou bien sur une superficie limitée sur des terrains extérieurs.	Perte non explicable entre 25k$ et 50k$, selon une première estimation.	Peu d'impact sur le respect des obligations légales, règlementaires internes ou contractuelles. Seule l'imputabilité d'employés est en jeu. Celle des dirigeants n'est vraisemblablement pas menacée.	Information négative persistante, ou rumeurs, diffusée sur les médias traditionnels ou sociaux et/ou qui concernent plusieurs personnes, unités ou activités de l'UdeS. Potentiel d'escalade et pas d'impact sur la réputation.

[1] Prendre note que le niveau de gravité peut également varier en fonction des éléments suivants :

1- **La gravité de la faute commise eu égard au domaine du droit**. Par exemple, un acte criminel commis par une personne employée dans l'exercice de ses fonctions sera d'une gravité supérieure à une erreur de bonne foi commise par une personne employée dans le cadre d'un contrat avec un partenaire.
2- L**e type de préjudice causé en raison du non-respect des obligations**. Il existe trois types de préjudices : corporel, matériel et moral.
3- La **vraisemblance de droit** ainsi que les **chances raisonnables de succès** d'un recours entrepris devant une cour de justice ou un tribunal administratif ou un organisme ayant un pouvoir d'enquête.

[2] Le terme « obligations règlementaires internes » réfère à tout document officiel et institutionnel de l'Université, par exemple, un règlement, une politique, une directive et une procédure. Ce terme réfère également à tout document officiel des unités, par exemple, un règlement complémentaire, une procédure, une règle et une directive.

Niveau de gravité	Santé et sécurité des personnes	Phénomènes psychosociaux (sur le campus dans certains cas, mais pour décès considérer aussi ailleurs que sur le campus)	Interruption des activités ¶	Menaces à l'environnement	Pertes financières	Impact légal, règlementaire et/ou contractuel[1]	Impact négatif sur la réputation §
3	Menace sérieuse de violence impliquant plusieurs personnes ; ou accident sérieux avec blessés (aucun grave ou dont la vie est menacée) et/ou dommages matériels importants.	Incident critique¤; ou autres enjeux psychosociaux dont l'impact est très grand, étendu à une unité et dont la durée s'annonce assez grande.	Perte d'accès de 2 à 7 jours pour des activités académiques ou de 24-48h et pour des activités de recherche critiques*. Services informatiques : 4h à durée indéterminée, révisée à 24h et moins en moins de 4h après le début.	Déversement ou relâchement majeur*** de matières dangereuses avec dommages matériels importants à l'intérieur d'un bâtiment.	Perte non explicable entre 50k$ et 100k$, selon une première estimation; ou cas de fraude présumée ou vraisemblable, de cette même ampleur.	Le non-respect des obligations légales, règlementaires internes ou contractuelles pourrait entraîner le dépôt d'une plainte ou d'un recours fondé devant une cour de justice, un tribunal administratif ou un organisme ayant un pouvoir d'enquête. L'imputabilité des dirigeants est peu menacée.	Publications négatives persistantes sur les médias traditionnels ou sociaux qui concernent un grand nombre de personnes, d'unités ou d'activités de l'UdeS. Escalade avérée et impact anticipé sur la réputation.
4	Cas de violence avérée; ou accident grave avec blessés (dont certains graves ou dont la vie est peut-être menacée) et/ou dommages matériels importants.	N/A	Perte d'accès de 7 jours ou plus pour des activités académiques ou de plus de 48h et pour des activités de recherche critiques*. Services informatiques : 4h à durée indéterminée, révisée à 24h et plus en moins de 4h après le début.	Déversement; ou relâchement majeur*** de matières dangereuses avec dommages matériels importants sur terrains extérieurs de l'UdeS et ressources gouvernementales (MELCCFP) impliquées.	Perte non explicable de plus de 100k$, selon une première estimation; et/ou cas de fraude présumée ou vraisemblable, de cette même ampleur.	Le non-respect des obligations légales, règlementaires internes ou contractuelles est porté à la connaissance de l'Université et/ou est allégué publiquement. L'imputabilité des dirigeants est menacée.	Publications négatives persistantes sur les médias traditionnels ou sociaux qui concernent un grand nombre de personnes, d'unités ou d'activités de l'UdeS. Escalade et impact avéré sur la réputation.
5	Attaque avérée; ou accident grave avec multiples blessés (dont certains graves ou dont la vie est menacée); ou des personnes décédées et/ou dommages matériels importants.	Incident critique¤; ou autres enjeux psychosociaux dont l'impact est démesuré, est étendu à toute l'institution, la région ou plus et dont la durée s'annonce très grande ou indéterminée.	Perte d'accès de 14 jours ou plus pour des activités académiques ou de plus de 72 heures et pour des activités de recherche critiques*. Services informatiques : 4h à durée indéterminée, révisée à plus de 48h en moins de 12h après le début.	Déversement ou relâchement majeur*** de matières dangereuses qui dépasse les limites des terrains extérieurs de l'UdeS et ressources gouvernementales (MELCCFP) impliquées.	Perte non expliquée de plus de 100k$, selon une première estimation; et/ou cas de fraude confirmée, de cette même ampleur.	Le non-respect des obligations légales, règlementaires internes ou contractuelles est allégué ou confirmé devant une cour de justice ou un tribunal administratif ou un organisme ayant un pouvoir d'enquête. L'imputabilité des dirigeants est compromise.	Publications négatives persistantes sur les médias traditionnels ou sociaux qui concernent un grand nombre de personnes, d'unités ou d'activités de l'UdeS. Grande ampleur et impact important sur la réputation.

Légende :

¤ : Les incidents critiques sont des événements anormaux, bouleversants ou traumatisants qui ont des répercussions sur les individus et sur le milieu d'études et de travail en augmentant la détresse psychologique et en créant une rupture avec le niveau de fonctionnement habituel chez les individus et dans le milieu touché.

¶ : Pour ce qui est des incidents de sécurité de l'information et de services informatiques, voir les tableaux et schémas spécifiques à cet effet dans le *Procédurier de gestion des incidents de sécurité de l'information*.

§ : Pour les impacts négatifs sur la réputation, s'il s'agit des conséquences découlant d'une SE qui n'est pas purement réputationnelle, toujours considérer au moins le même niveau de risque que la catégorie d'origine de la SE en question.

***** : Locaux ou activités de recherche critiques : Laboratoire dont la perte affecte plusieurs autres laboratoires ou un grand nombre de personnes; Pour les animaleries, la santé des animaux ou l'intégrité des données de recherche sont mises en péril; Bibliothèques ou centres documentaires.

****** : Déversement mineur = volume total de moins de 208 litres; Le ou les produits déversés sont identifiés et ne présentent pas de risque incontrôlé pour la santé des personnes, l'intégrité du bâtiment ou de l'environnement. L'incident a peu de chance de dégénérer et le personnel SSMTE peut intervenir de façon sécuritaire.

******* : Déversement majeur = volume total de plus de 208 litres ou plusieurs contenants de moins de 208 litres impliqués; Le ou les produits déversés ne sont pas identifiés ou ils présentent des incompatibilités dangereuses, amenant un risque hors de contrôle pour la santé des personnes, l'intégrité du bâtiment ou de l'environnement. L'incident a le potentiel de dégénérer et le personnel SSMTE ne peut pas intervenir de façon sécuritaire.