UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide de la mise en place du processus de gestion des menaces, des vulnérabilités et des incidents

---

08-2024

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIÈRES

Introduction 1
Terminologie et acronymes 1
Terminologie 1
Acronymes 2
Mise en place du processus GMVI 3
Détermination du niveau d'impact des préjudices 4
Ojectif 4
Étapes 5
Processus 5
Rôles et responsabilités 6
Détermination de la probabilité de concrétisation 7
objectif 7
étapes 8
Processus 8
Rôles et responsabilités 10
Détermination de l'urgence d'agir 11
Objectif 11
étapes 12
Processus 12
Rôles et responsabilités 13
Détermination du niveau de coordination 14
Objectif 14
Étapes 15
Processus 15
Rôles et responsabilités 16
Escalade d'une MVI 17

Objectif 17
Étapes 18
Processus 18
Rôles et responsabilités 19
remédiation aux vulnérabilités 20
Objectif 20
Étapes 21
Processus 21
Rôles et responsabilités 22
Suivi de la prise en charge d'un événement de sécurité 23
Objectif 23
Étapes 24
Processus 25
Rôles et responsabilités 26
Résolution et leçons apprises 27
Objectif 27
Étapes 28
Processus 29
Rôles et responsabilités 30
Boite à outils 30
Références 31
Révisions 31
Annexe 1 : Grille de détermination du niveau d'impact des préjudices 32
Annexe 2 : Tableau de détermination de la probabilité de concrétisation d'une menace 33
Annexe 3 : Tableau de Détermination de la probabilité de concrétisation d'une menace 34
Annexe 4 : Détermination du niveau de coordination 35
Annexe 5 : Détermination des délais de remédiation 36

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Figure 1: Processus GMVI 3
Figure 2: Détermination du niveau d'impact des préjudices 4
Figure 3: Détermination de la probabilité de concrétisation 7
Figure 4: Détermination de l'urgence d'agir 11
Figure 5: Détermination du niveau de coordination 14
Figure 6: Escalade d'une MVI 17
Figure 7: Remédiation aux vulnérabilités 20
Figure 8: Suivi de la prise en charge d'une MVI 23
Figure 9: Bilan et leçons apprises 27

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

INTRODUCTION

La gestion des menaces, des vulnérabilités et des incidents est encadrée par la Loi sur la gouvernance et la gestion des ressources informationnelles (LGGRI). Cette loi instaure un cadre de gouvernance applicable aux organismes publics et aux entreprises du gouvernement du Québec pour assurer la protection des ressources informationnelles.

Ce guide est conçu pour aider les établissements de l'Université du Québec à mettre en place le processus de gestion des menaces, des vulnérabilités et des incidents du Centre gouvernemental de cyberdéfense.

Il vise à :

- Assurer la protection adéquate des ressources informationnelles;
- Standardiser la gestion des menaces, vulnérabilités et incidents (MVI) à l'échelle gouvernementale;
- Faciliter la coordination entre les différents acteurs lors de la prise en charge d'une MVI.

TERMINOLOGIE ET ACRONYMES

TERMINOLOGIE

Menace : Potentiel de causer des dommages à un système d'information par des moyens tels que des cyberattaques, des failles de sécurité ou des incidents physiques.

Vulnérabilité : Faiblesse dans un système d'information, des processus ou des contrôles qui peuvent être exploités par une menace pour causer des dommages.

Incident de sécurité : Événement qui compromet la confidentialité, l'intégrité ou la disponibilité de l'information.

Gestion des menaces, des vulnérabilités et des incidents (GMVI) : Processus intégré visant à identifier, évaluer, traiter, et remédier aux menaces, vulnérabilités et incidents de sécurité.

Ressources informationnelles : Ensemble des données, systèmes d'information, infrastructures et personnes qui traitent l'information.

Impact des préjudices : Niveau de dommage causé par un incident de sécurité, évalué en fonction de divers critères (financiers, opérationnels, réputationnels, etc.).

Probabilité de concrétisation : Estimation de la probabilité qu'une menace ou vulnérabilité soit exploitée avec succès.

Urgence d'agir : Nécessité d'intervenir rapidement pour éviter des préjudices supplémentaires.

Coordination : Niveau de collaboration requis entre les différentes entités pour gérer efficacement une MVI.

ACRONYMES

CESI : Centre d'expertise en sécurité de l'information de l'Université du Québec

CGSI : Chef gouvernemental de la sécurité de l'information

CDSI : Chef délégué de la sécurité de l'information

COMSI : Coordonnateur organisationnel des mesures de sécurité de l'information

ROCD : Responsable opérationnel de cyberdéfense

CGCD : Centre gouvernemental de cyberdéfense

CERT/AQ : Équipe de réponses aux incidents de sécurité de l'information de l'administration québécoise

NIST : National Institute of Standards and Technology

CSF : Cyber Security Framework

EIMSIG : Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale

RAG : Réseau d'alertes gouvernemental

RI : Ressources informationnelles

MCN : Ministère de la Cybersécurité et du Numérique

MISE EN PLACE DU PROCESSUS GMVI

La mise en place du processus de gestion des menaces, vulnérabilités et incidents se déploie sur 8 étapes :

1. **Détermination du niveau d'impact des préjudices** : évaluation des dommages potentiels.
2. **Détermination de la probabilité de concrétisation** : estimation de la probabilité que les menaces se réalisent.
3. **Détermination de l'urgence d'agir** : évaluation de l'urgence et de la nécessité d'une action rapide.
4. **Détermination du niveau de coordination** : identification du niveau de coordination requis en fonction de l'impact et de l'urgence.
5. **Escalade d'une MVI** : processus d'escalade des incidents nécessitant une coordination à un niveau supérieur.
6. **Remédiation des vulnérabilités** : délais pour corriger les vulnérabilités en fonction de leur criticité.
7. **Suivi de la prise en charge d'un événement de sécurité** : suivi régulier des menaces, vulnérabilités et incidents jusqu'à leur résolution.
8. **Résolution et bilan d'un incident de sécurité** : compilation des leçons apprises après la résolution d'un incident.

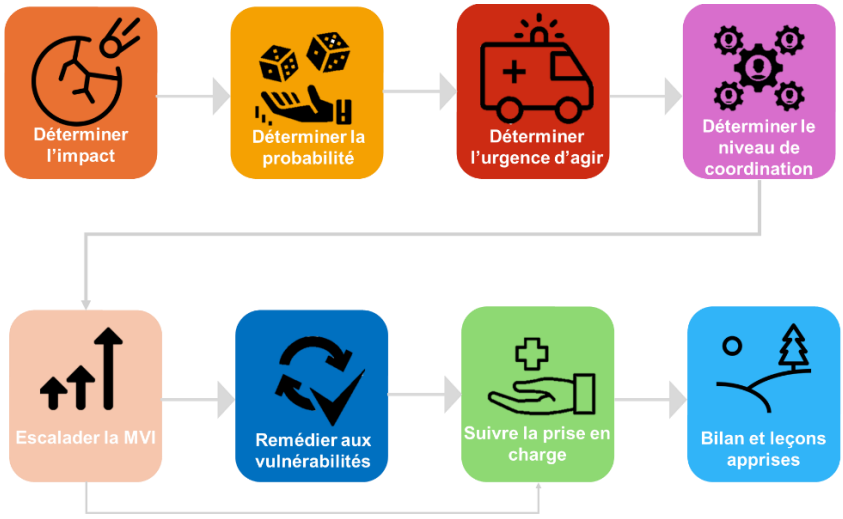

Figure 1 : Processus GMVI

DÉTERMINATION DU NIVEAU D'IMPACT DES PRÉJUDICES

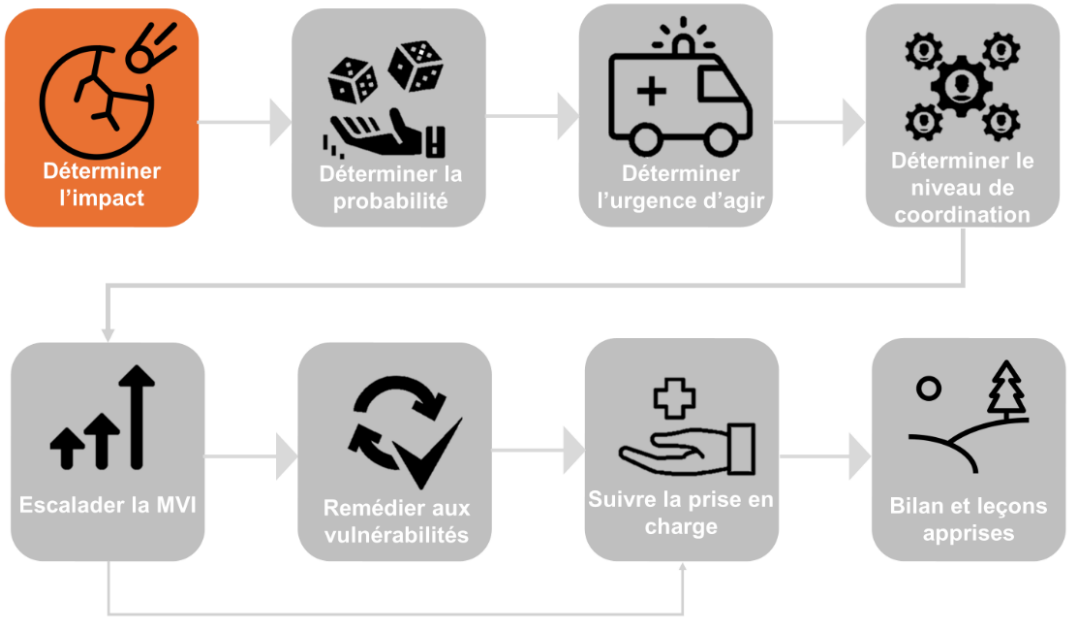

Figure 2 : Détermination du niveau d'impact des préjudices

Lorsqu'une MVI est détectée, la première étape consiste à déterminer le niveau d'impact des préjudices de cette MVI. Cette activité fournit les lignes directrices pour évaluer et classer l'impact potentiel sur les citoyens, les entreprises et le gouvernement.

Le CESI a produit un guide d'évaluation des menaces et des risques qui fournit des informations détaillées et une compréhension approfondie afin d'accomplir efficacement les activités de cette phase du processus.

OJECTIF

La détermination du niveau d'impact des préjudices vise à évaluer les conséquences potentielles des menaces et vulnérabilités sur les individus, les entreprises et les gouvernements. Cette évaluation est essentielle pour prioriser les actions de réponse, allouer les ressources de manière efficace et informer les décideurs sur l'ampleur des risques.

ÉTAPES

Les étapes de cette phase consistent à :

1. **Identifier le type de préjudice :** physique, psychologique, financier, opérationnel ou réputationnel.
2. **Évaluer le préjudice :** pour les citoyens, les entreprises et le gouvernement.
3. **Déterminer le niveau d'impact des préjudices :** conformément à la Grille de détermination du niveau d'impact des préjudices du processus GMVI fournie en annexe 1.

L'évaluation de l'impact des préjudices n'est pas un exercice ponctuel, mais continu. Au fur et à mesure que de nouvelles informations émergent ou que la situation évolue, il est crucial de :

- Réévaluer régulièrement : mener des évaluations régulières pour prendre en compte les nouveaux développements et ajuster les niveaux d'impact si nécessaire.
- Documenter les modifications : consigner toutes les réévaluations et les modifications apportées au niveau d'impact pour assurer la traçabilité.

PROCESSUS

1. **Identification des types de préjudices**
   - Recueillir les informations : recueillir des informations sur les types de préjudices potentiels en utilisant des sources internes et externes (rapports de sécurité, études d'impact, bases de données de vulnérabilités, etc.).
   - Classification : classer les préjudices identifiés en fonction de leurs caractéristiques spécifiques (physiques, psychologiques, financiers, opérationnels, réputationnels, à la sécurité de l'information).
2. **Évaluation des préjudices potentiels**
   - Préjudice pour les citoyens : évaluer les impacts potentiels des préjudices identifiés sur les citoyens, y compris la santé physique, la santé mentale et la sécurité financière.
   - Préjudice pour les entreprises : évaluer les impacts potentiels des préjudices identifiés sur les entreprises, y compris les pertes financières, les perturbations opérationnelles et la compétitivité.
   - Préjudice pour le gouvernement : évaluer les impacts potentiels des préjudices identifiés sur le gouvernement, y compris la prestation des services publics, l'économie, la réputation et les missions gouvernementales.

3. **Utilisation de la grille de détermination du niveau d'impact des préjudices**
   - Évaluation : utiliser la grille de détermination du niveau d'impact des préjudices pour attribuer un niveau d'impact (faible, modéré, élevé, très élevé) à chaque type de préjudice identifié.
   - Documentation : documenter les résultats de l'évaluation, en précisant les raisons pour lesquelles chaque niveau d'impact a été attribué.
4. **Réévaluation continue**
   - Surveillance : surveiller continuellement les menaces et vulnérabilités pour détecter tout changement dans leur potentiel de préjudice.
   - Réévaluation : réévaluer régulièrement les niveaux d'impact des préjudices en fonction des nouvelles informations et des évolutions dans le contexte de la menace.
5. **Documentation et communication**
   - Documentation : consigner toutes les évaluations et réévaluations dans des rapports détaillés pour assurer la traçabilité.
   - Communication : informer les parties prenantes concernées des résultats des évaluations et des réévaluations pour permettre une prise de décision éclairée.

RÔLES ET RESPONSABILITÉS

Le tableau suivant représente les rôles et les responsabilités relatifs à cette phase :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Identification des types de préjudices	C	I	R	C	A	C	C
Évaluation des préjudices potentiels	C	I	R	C	A	C	C
Classification des actifs	C	I	R	C	A	C	C
Mise à jour des évaluations	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

DÉTERMINATION DE LA PROBABILITÉ DE CONCRÉTISATION

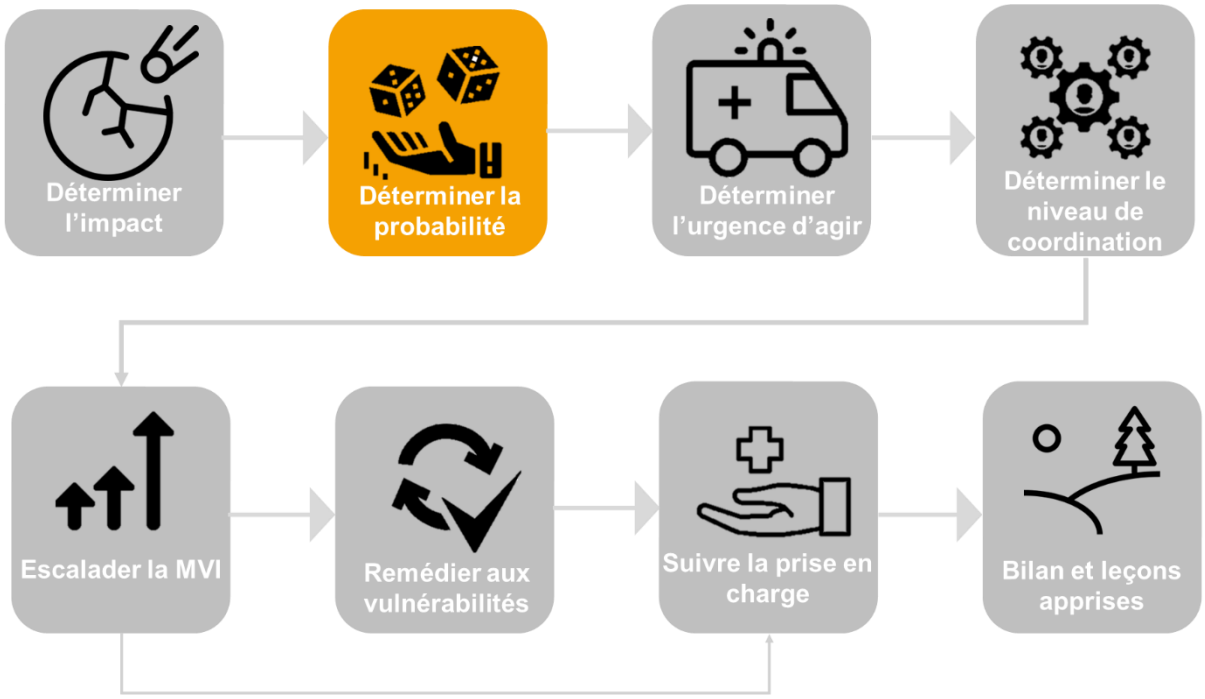

Figure 3 : Détermination de la probabilité de concrétisation

Cette phase vise à évaluer la probabilité que des menaces et des vulnérabilités spécifiques soient exploitées pour pouvoir prioriser les actions de remédiation et de mitigation.

OBJECTIF

- Évaluer le risque : comprendre la probabilité que des menaces se matérialisent et que des vulnérabilités soient exploitées.
- Prioriser les ressources : allouer efficacement les ressources pour gérer les risques les plus probables, et qui ont le plus d'impact.
- Informer la haute direction : aider les décideurs à comprendre le niveau de risque et à prendre des mesures appropriées.

ÉTAPES

Les activités relatives à cette phase sont les suivantes :

1. **Identification des menaces et des vulnérabilités**
   - Menaces : sources potentielles de danger telles que les cybercriminels, les pirates, les erreurs humaines, les catastrophes naturelles, etc.
   - Vulnérabilités : faiblesses ou lacunes dans les systèmes, les processus ou les contrôles qui peuvent être exploitées par les menaces.
2. **Utilisation de critères de probabilité**
   - Degré de sophistication des acteurs : capacité des acteurs malveillants à exploiter les vulnérabilités.
   - Ciblage des victimes : niveau de ciblage spécifique des victimes par les acteurs malveillants.
   - Protection offerte par les mesures de sécurité : efficacité des mesures de sécurité en place pour protéger contre les menaces.
3. **Évaluation des menaces**
   - Utiliser le tableau de détermination de la probabilité de concrétisation d'une menace fournie en annexe 2 pour déterminer la probabilité de concrétisation d'une menace en fonction de trois critères principaux (degré de sophistication des acteurs, ciblage des victimes et protection offerte par les mesures de sécurité en place).
4. **Évaluation des vulnérabilités**
   - Utiliser le tableau fourni en annexe 3 pour déterminer la probabilité de concrétisation d'une vulnérabilité en fonction de la criticité et du contexte, en utilisant la norme CVSS (Common Vulnerability Scoring System).
5. **Réévaluation continue**
   - La probabilité de concrétisation doit être réévaluée régulièrement pour prendre en compte les nouvelles informations et les changements dans le contexte de la menace.

PROCESSUS

1. **Identification des menaces et des vulnérabilités**
   - Menaces : recueillir des informations sur les différentes menaces en utilisant des sources internes et externes (rapports de sécurité, bases de données de menaces, etc.).

- Vulnérabilités : identifier les vulnérabilités à l'aide des balayages, d'audits de sécurité, de tests d'intrusion, etc.

2. **Évaluation des menaces**
   - Degré de sophistication des acteurs : évaluer la capacité des acteurs malveillants à exploiter les vulnérabilités identifiées. Les acteurs peuvent varier à des amateurs (piratins) aux groupes de cybercriminels organisés.
   - Ciblage des victimes : déterminer si les acteurs malveillants ciblent des victimes spécifiques ou des secteurs d'activité particuliers. Les cibles peuvent varier des victimes générales aux cibles gouvernementales de haute importance.
   - Protection offerte par les mesures de sécurité : évaluer l'efficacité des mesures de sécurité en place pour protéger contre les menaces identifiées. Les mesures de sécurité peuvent varier, d'efficaces à inexistantes.
3. **Évaluation des vulnérabilités**
   - Utiliser le calcul CVSS pour évaluer la criticité des vulnérabilités. Le score CVSS, allant de 0 à 10, est utilisé pour déterminer le degré de probabilité de concrétisation.
   - Ajuster le niveau de probabilité basé sur des informations supplémentaires disponibles (renseignements sur les menaces actuelles, incidents précédents, etc.).
4. **Réévaluation continue**
   - Surveillance : surveiller continuellement les menaces et les vulnérabilités pour détecter tout changement dans leur probabilité de concrétisation.
   - Réévaluation : réévaluer régulièrement la probabilité de concrétisation des menaces et des vulnérabilités en fonction des nouvelles informations et des évolutions dans le contexte de la menace.
5. **Documentation et communication**
   - Documentation : consigner toutes les évaluations et réévaluations dans des rapports détaillés pour assurer la traçabilité.
   - Communication : informer les parties prenantes concernées des résultats des évaluations et des réévaluations pour permettre une prise de décision éclairée.

RÔLES ET RESPONSABILITÉS

Les rôles et les responsabilités de cette phase sont présentés dans le tableau suivant :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Identification des menaces et vulnérabilités	C	I	R	C	A	C	C
Évaluation des menaces	C	I	R	C	A	C	C
Évaluation des vulnérabilités	C	I	R	C	A	C	C
Réévaluation des probabilités	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

DÉTERMINATION DE L'URGENCE D'AGIR

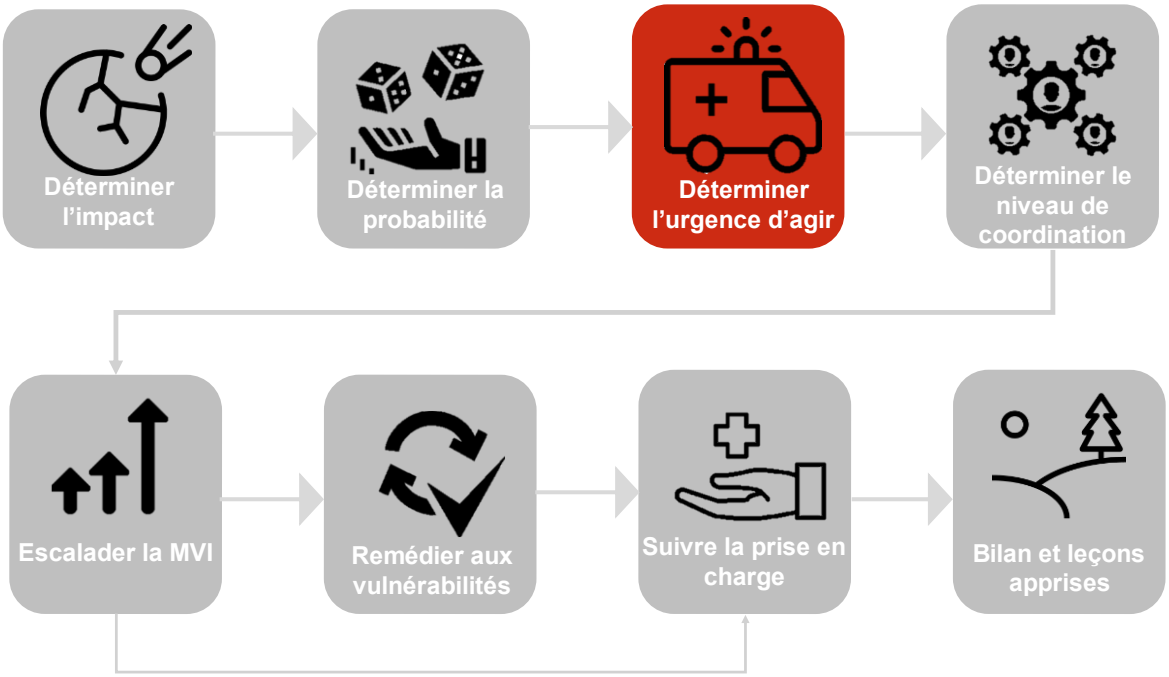

Figure 4 : Détermination de l'urgence d'agir

La détermination de l'urgence d'agir vise à évaluer la nécessité et la rapidité avec lesquelles une action doit être entreprise pour prévenir ou minimiser les préjudices causés par une menace, une vulnérabilité ou un incident de sécurité.

OBJECTIF

L'objectif de cette phase est de :

- Prioriser les interventions : identifier les situations qui nécessitent une réponse immédiate.
- Optimiser les ressources : allouer les ressources de manière efficace en fonction du degré d'urgence.
- Réduire les impacts : limiter les dommages potentiels en agissant rapidement sur les menaces et les vulnérabilités.

ÉTAPES

Les activités relatives à cette phase sont les suivantes :

1. **Évaluation des critères de l'urgence d'agir**
   - Nombre d'organismes publics (OP) concernés : évaluer si l'incident affecte un seul OP ou plusieurs.
   - Probabilité d'évolution : Estimer la probabilité que l'incident s'aggrave ou affecte d'autres systèmes ou OP.
2. **Utilisation d'une échelle d'urgence**
   - L'échelle d'urgence présentée dans l'annexe 4 est utilisée pour classifier les incidents selon trois niveaux : faible, moyenne, élevée.
3. **Analyse combinée de l'impact et de l'urgence**
   - Combiner les résultats des sections impact des préjudices et probabilités de concrétisation avec les critères d'urgence pour déterminer le niveau de priorité de la réponse.
4. **Coordination de la réponse**
   - En fonction du niveau d'urgence, coordonner les actions avec les différents intervenants (CGSI, CDSI, COMSI, CESI, ROCD, etc.) pour une réponse efficace et rapide.

L'urgence d'agir doit être réévaluée régulièrement pour prendre en compte les nouvelles informations et les changements dans le contexte de la menace ou de la vulnérabilité.

PROCESSUS

1. **Évaluation initiale**
   - Identification initiale : dès la détection d'une menace, d'une vulnérabilité ou d'un incident, le COMSI procède à une évaluation initiale.
   - Documentation : documenter les détails initiaux de l'incident, y compris les parties affectées, l'heure et la date, et toute information pertinente.
2. **Utilisation de l'échelle d'urgence**
   - Critères d'urgence : utiliser les critères du tableau de l'urgence d'agir présenté en annexe 4. Cette évaluation repose sur le nombre d'organismes publics concernés et la probabilité d'évolution de la MVI.
   - Classification de l'urgence : classer l'incident selon les niveaux d'urgence (faible, moyenne, élevée) pour déterminer la rapidité et l'intensité de la réponse requise.

3. **Analyse**
   - Combinaison des résultats : intégrer les résultats de l'évaluation de l'impact des préjudices et de la probabilité de concrétisation avec l'évaluation de l'urgence pour obtenir une vue globale de la criticité de la MVI.
   - Priorisation : utiliser cette analyse combinée pour prioriser les actions de remédiation et allouer les ressources de manière efficace.
4. **Coordination de la réponse**
   - Définition du niveau de réponse : en fonction du niveau d'urgence, déterminer le niveau de coordination requis
   - Notification des parties prenantes : informer toutes les parties prenantes concernées de l'évaluation de l'urgence et des actions de réponse prévues.
   - Mise en œuvre des actions : coordonner et mettre en œuvre les actions nécessaires pour répondre à la MVI de manière appropriée et rapide.
5. **Réévaluation continue**
   - Réévaluation régulière : réévaluer régulièrement l'urgence d'agir pour tenir compte des nouvelles informations et des changements dans le contexte de la MVI.
   - Documentation des changements : consigner toutes les réévaluations et les ajustements apportés au niveau d'urgence pour assurer la traçabilité.

RÔLES ET RESPONSABILITÉS

Ci-dessous la matrice RACI pour cette phase :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Évaluation initiale de l'urgence	C	I	R	C	A	C	C
Utilisation de l'échelle d'urgence	C	I	R	C	A	C	C
Détermination du niveau de coordination	C	I	R	C	A	C	C
Communication des résultats	C	I	R	C	A	C	C
Mise en œuvre des actions	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

DÉTERMINATION DU NIVEAU DE COORDINATION

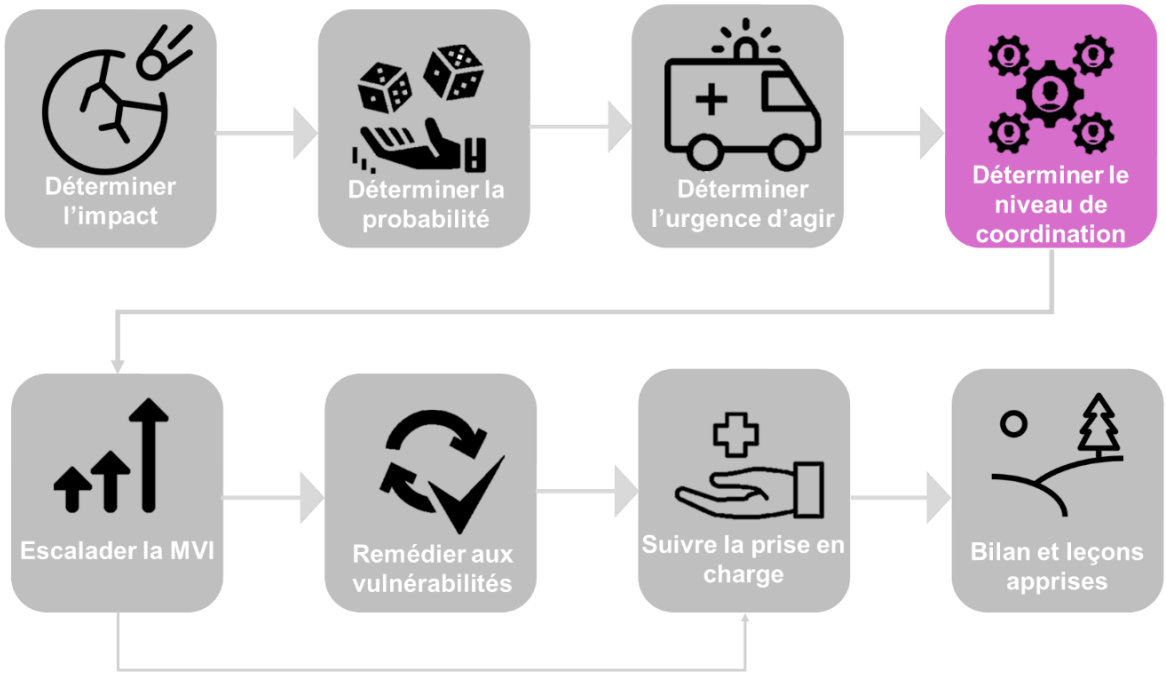

Figure 5 : Détermination du niveau de coordination

Cette phase a pour but d'établir le niveau approprié de coordination requis pour gérer efficacement une menace, une vulnérabilité ou un incident de sécurité en fonction de son impact, de sa probabilité de concrétisation et de l'urgence d'agir.

OBJECTIF

- Optimiser la réponse : assurer une réponse coordonnée et proportionnée à l'ampleur de la menace ou de l'incident.
- Faciliter la collaboration : définir clairement les rôles et responsabilités de chaque intervenant à chaque niveau de coordination.
- Améliorer l'efficacité : allouer les ressources de manière optimale pour traiter les incidents de sécurité de manière efficace.

ÉTAPES

Pour déterminer le niveau de coordination, il convient de suivre ces étapes :

1. **Combinaison des résultats des sections précédentes**
   - Impact des préjudices, probabilité de concrétisation et urgence d'agir. Ces résultats sont combinés pour évaluer globalement la gravité de la menace, de la vulnérabilité ou de l'incident.
2. **Utilisation de la grille de coordination**
   - La grille de coordination présentée à l'annexe 4 aide à déterminer le niveau de coordination requis en fonction de l'impact global et de l'urgence d'agir.
3. **Définition des niveaux de coordination**
   - Niveau 1 - coordination organisationnelle : la gestion de l'incident est assurée par l'établissement concerné, avec peu ou pas de soutien externe.
   - Niveau 2 – coordination opérationnelle : nécessite la coordination avec le Centre opérationnel de cyberdéfense (COCD).
   - Niveau 3 – coordination gouvernementale : implique plusieurs organismes publics et nécessite une coordination avec le Centre gouvernemental de cyberdéfense (CGCD).
   - Niveau 4 – coordination de la crise gouvernementale : crise majeure nécessitant l'intervention du Comité de crise gouvernemental en sécurité de l'information (CCGSI).

PROCESSUS

1. **Évaluation initiale :** le COMSI évalue l'impact global et l'urgence d'agir pour déterminer le niveau initial de coordination requis en utilisant la grille de coordination.
2. **Consultation et validation :** si un niveau de coordination supérieur est envisagé (niveau 2, 3 ou 4), le COMSI consulte avec le ROCD et le CGCD pour validation et ajustement.
3. **Notification et mise en œuvre :** informer les parties prenantes concernées (CGSI, CDSI, ROCD, CESI, etc.) et mettre en œuvre les actions nécessaires en fonction du niveau de coordination déterminé.
4. **Suivi et réévaluation :** surveiller l'évolution de la MVI et réévaluer le niveau de coordination si nécessaire, en ajustant les actions en conséquence.

Le CESI met son expertise et ses ressources à la disposition des établissements de l'Université du Québec, quel que soit le niveau de coordination requis.

RÔLES ET RESPONSABILITÉS

Les rôles et les responsabilités de cette phase sont présentés dans le tableau suivant :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Évaluation initiale du niveau de coordination	C	I	R	C	A	C	C
Consultation et validation	C	I	R	C	A	C	C
Notification des parties prenantes	C	I	R	C	A	C	C
Mise en œuvre des actions	C	I	R	C	A	C	C
Suivi et réévaluation	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

ESCALADE D'UNE MVI

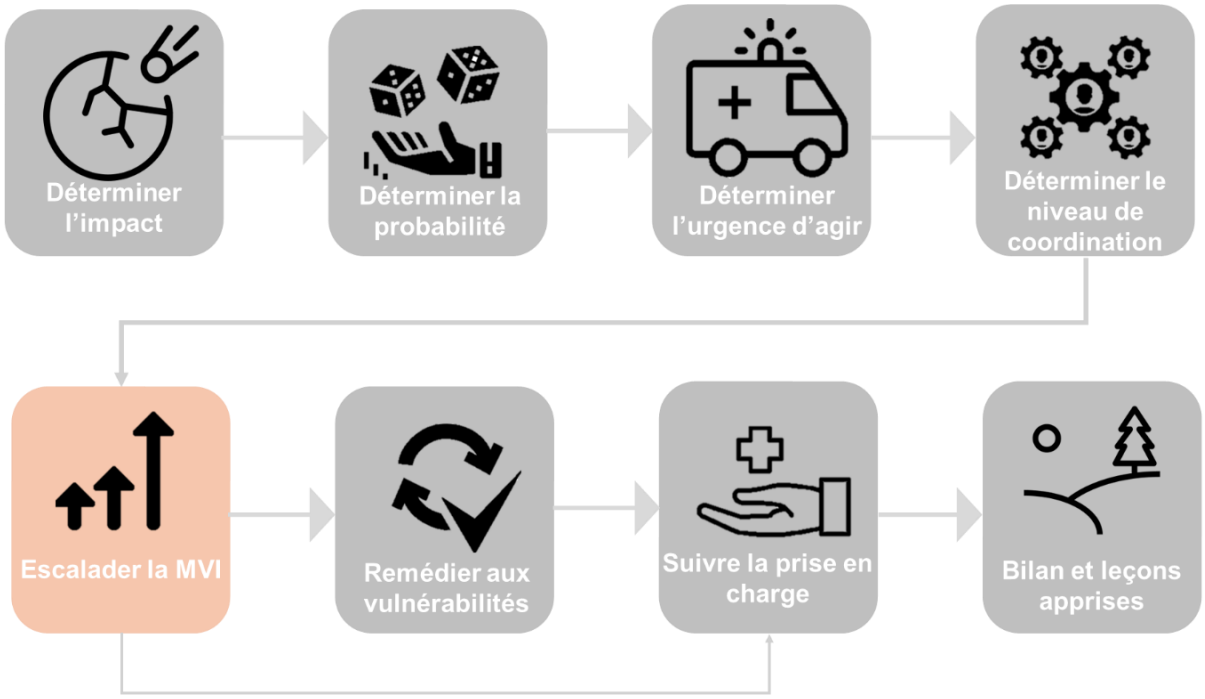

Figure 6 : Escalade d'une MVI

L'escalade permet de garantir qu'une menace, une vulnérabilité ou un incident soit géré de manière appropriée et coordonnée lorsque les ressources ou l'autorité d'un établissement ne suffisent plus pour y faire face.

OBJECTIF

- Assurer une gestion efficace : veiller à ce que les MVI soient traités par le niveau approprié d'autorité et de ressources.
- Faciliter la coordination : impliquer rapidement les parties prenantes appropriées pour une réponse coordonnée.
- Prévenir l'aggravation : agir rapidement pour empêcher que la situation ne s'aggrave.

ÉTAPES

Le processus d'escalade est composé des activités suivantes :

1. **Détection initiale et évaluation**
   - Détection : lorsqu'une MVI est détectée, le COMSI évalue immédiatement la situation pour déterminer si elle peut être gérée localement.
   - Évaluation initiale : utiliser les résultats des sections précédentes pour évaluer l'impact, la probabilité et l'urgence de la MVI.
2. **Critères de déclenchement de l'escalade**
   - Impact élevé : si l'impact de la MVI est évalué comme élevé ou très élevé.
   - Complexité : si la complexité de la MVI dépasse les capacités de l'établissement à la gérer.
   - Ressources insuffisantes : si les ressources disponibles au sein de l'établissement sont insuffisantes pour répondre efficacement à la MVI.
   - Coordination requise : si la MVI nécessite une coordination avec d'autres organismes ou autorités externes.
3. **Niveaux d'escalade**
   - Niveau 1 à niveau 2 : escalade au Centre opérationnel de cyberdéfense (COCD) lorsque l'incident ne peut être géré efficacement au sein de l'établissement.
   - Niveau 2 à niveau 3 : escalade au Centre gouvernemental de cyberdéfense (CGCD) lorsque l'incident affecte plusieurs organismes ou nécessite une réponse gouvernementale.
   - Niveau 3 à niveau 4 : escalade au Comité de crise gouvernemental en sécurité de l'information (CCGSI) en cas de crise majeure nécessitant une intervention à l'échelle gouvernementale.

PROCESSUS

1. **Notification :** le COMSI informe le ROCD ou le COCD en cas de besoin d'escalade.
2. **Documentation :** consigner toutes les informations pertinentes concernant la MVI, y compris les évaluations initiales et les raisons de l'escalade.
3. **Validation :** le ROCD ou le COCD valide la nécessité de l'escalade et confirme le niveau approprié de réponse.
4. **Confirmation :** notification aux parties prenantes concernées du niveau d'escalade et des actions à entreprendre.

5. **Coordination :** le niveau approprié de coordination est activé, impliquant toutes les parties prenantes nécessaires (CGSI, CDSI, ROCD, CGCD, CESI, etc.).
6. **Réponse :** mise en œuvre des actions de réponse coordonnées, y compris les mesures de remédiation, de communication et de suivi.
7. **Suivi régulier :** le suivi continu de la MVI est assuré pour vérifier l'efficacité des actions entreprises et ajuster la réponse si nécessaire.
8. **Réévaluation :** réévaluer régulièrement la situation pour déterminer si d'autres escalades ou ajustements sont nécessaires.

RÔLES ET RESPONSABILITÉS

Les rôles et les responsabilités de cette phase sont présentés dans le tableau suivant :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Détection initiale et évaluation	C	I	R	C	A	C	C
Notification initiale	C	I	R	C	A	C	C
Validation et confirmation	C	I	R	C	A	C	C
Coordination de la réponse	C	I	R	C	A	C	C
Suivi post-escalade	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

REMÉDIATION AUX VULNÉRABILITÉS

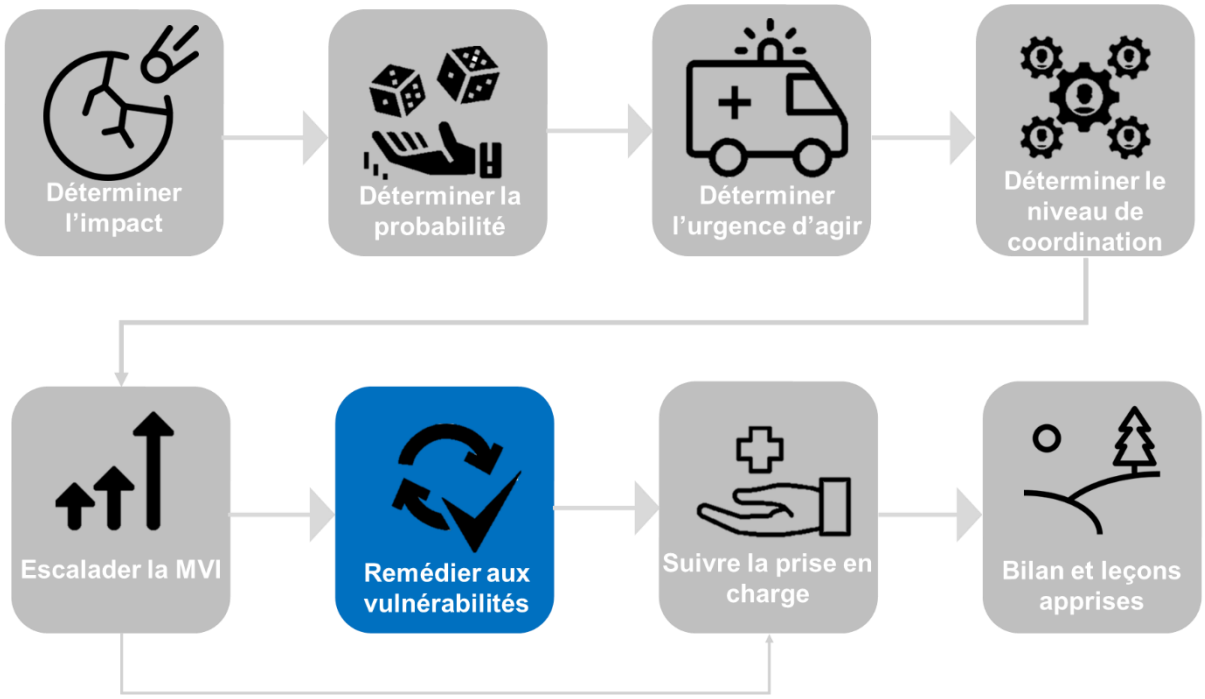

Figure 7 : Remédiation aux vulnérabilités

Le délai de remédiation est le temps alloué pour corriger une vulnérabilité identifiée afin de prévenir son exploitation. Cette section décrit le processus de détermination et de gestion des délais de remédiation des vulnérabilités.

OBJECTIF

L'objectif de cette phase est de :

- Prévenir l'exploitation : réduire le risque d'exploitation des vulnérabilités par des acteurs malveillants.
- Maintenir la sécurité : assurer la sécurité continue des systèmes d'information.
- Conformité : respecter les réglementations et les politiques de sécurité de l'information.

ÉTAPES

Afin de déterminer le délai nécessaire pour remédier aux vulnérabilités, il sera important de suivre ces étapes :

1. **Identification des vulnérabilités**
   - Source d'identification : vulnérabilités identifiées par des outils de balayage, des audits de sécurité, des rapports de menaces, etc.
   - Classification des vulnérabilités : utilisation de la norme CVSS (Common Vulnerability Scoring System) pour évaluer contextuellement la criticité des vulnérabilités.
2. **Évaluation de la criticité**
   - Criticité basée sur CVSS : Utilisation du score environnemental de CVSS pour déterminer la gravité de la vulnérabilité.
   - Impact potentiel : évaluation de l'impact potentiel de l'exploitation de la vulnérabilité sur les systèmes, les données et les opérations.
3. **Détermination des délais de remédiation**
   - Délai standard : établir des délais standardisés pour la remédiation des vulnérabilités en fonction du tableau présenté dans l'annexe 5.
   - Délai adapté : ajuster les délais standardisés en fonction des facteurs contextuels.

PROCESSUS

1. Élaboration d'un plan de remédiation : Développer un plan détaillé pour la correction de chaque vulnérabilité identifiée, incluant les actions nécessaires, les responsables et les délais.
2. Application des correctifs : déployer les correctifs ou les mesures de mitigation nécessaires pour remédier aux vulnérabilités.
3. Tests post-remédiation : effectuer des tests pour vérifier l'efficacité des correctifs appliqués.
4. Suivi de l'avancement : suivre l'avancement de la remédiation pour s'assurer que les délais sont respectés.
5. Validation de la remédiation : confirmer que les vulnérabilités ont été correctement corrigées et que les systèmes sont sécurisés.
6. Réévaluation des vulnérabilités : réévaluer périodiquement les vulnérabilités pour s'assurer qu'elles sont toujours pertinentes et ajuster les délais de remédiation si nécessaire.

RÔLES ET RESPONSABILITÉS

Ci-dessous la matrice RACI pour cette phase :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Identification des vulnérabilités	C	I	R	C	A	C	C
Évaluation de la criticité	C	I	R	C	A	C	C
Détermination des délais de remédiation	C	I	R	C	A	C	C
Planification de la remédiation	C	I	R	C	A	C	C
Mise en œuvre de la remédiation	C	I	R	C	A	C	C
Suivi et validation	C	I	R	C	A	C	C
Réévaluation et ajustement	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

SUIVI DE LA PRISE EN CHARGE D'UN ÉVÉNEMENT DE SÉCURITÉ

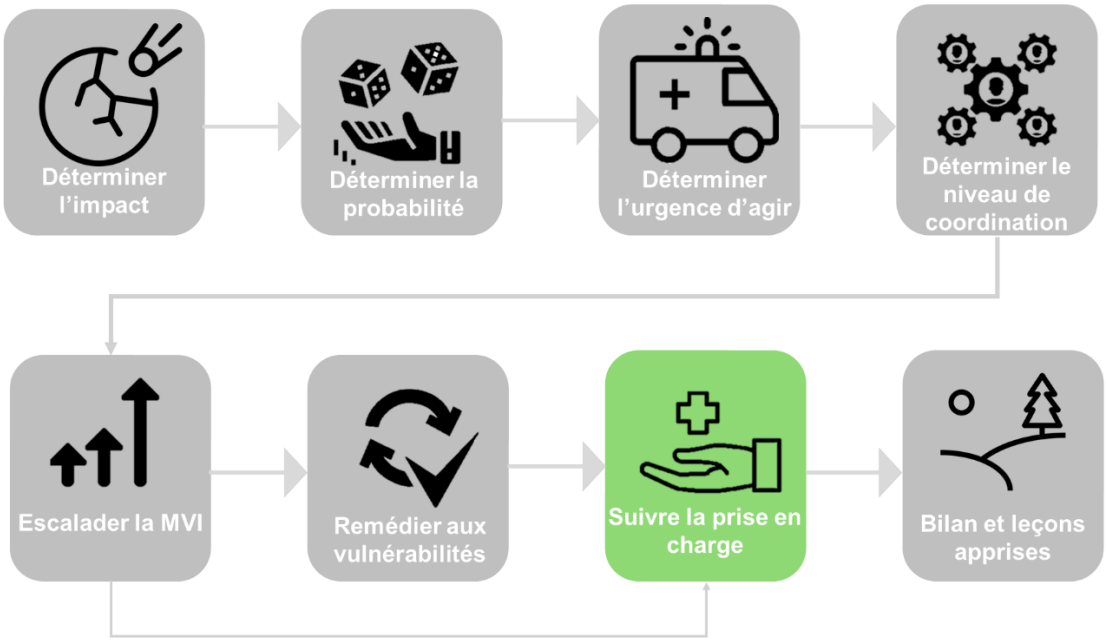

Figure 8 : Suivi de la prise en charge d'une MVI

Cette section décrit les étapes et les responsabilités associées au suivi continu des menaces, des vulnérabilités et des incidents jusqu'à leur résolution complète.

OBJECTIF

- Assurer la traçabilité : documenter toutes les étapes de la prise en charge des incidents.
- Évaluer l'efficacité des réponses : s'assurer que les actions de réponse sont efficaces et appropriées.
- Coordonner les efforts : faciliter la coordination entre les différentes parties prenantes impliquées dans la gestion de la MVI.
- Prévenir les récurrences : utiliser les leçons apprises pour prévenir la récurrence des incidents similaires.

ÉTAPES

Les étapes de suivi de la prise en charge sont les suivantes :

1. **Enregistrement initial de l'incident**
   - Identification : documenter initialement la MVI, incluant les détails de détection, l'heure et la date, et les parties affectées.
   - Classification : attribuer un niveau de criticité à la MVI basé sur les évaluations initiales.
2. **Notification et communication**
   - Notification : informer toutes les parties prenantes concernées dès la détection de la MVI.
   - Communication continue : maintenir une communication régulière avec les parties prenantes pour les mettre à jour sur l'état de la MVI.
3. **Développement et mise en œuvre du plan d'action**
   - Élaboration du plan : développer un plan d'action détaillé pour la remédiation de la MVI, incluant les actions à entreprendre, les responsables et les délais.
   - Mise en œuvre : exécuter les actions de remédiation conformément au plan établi.
4. **Suivi et surveillance continue**
   - Surveillance active : utiliser des outils de surveillance pour suivre l'évolution de l'incident et détecter toute nouvelle activité suspecte.
   - Mises à jour régulières : fournir des mises à jour régulières sur l'état de la MVI, les avancements des actions de remédiation et les résultats obtenus.
5. **Validation de la remédiation**
   - Vérification : effectuer des tests pour vérifier que les actions de remédiation ont été efficaces et que ma MVI a été résolue.
   - Validation finale : obtenir une validation formelle de la résolution de la MVI par les parties prenantes concernées.
6. **Documentation et rapport final**
   - Documentation complète : Documenter toutes les actions entreprises, les résultats des tests de vérification et les leçons apprises.
   - Rapport final : produire un rapport final détaillé résumant l'incident, les actions de remédiation et les recommandations pour l'avenir.

PROCESSUS

1. **Initiation du suivi**
   - Identification : dès la détection de la MVI, le COMSI initialise le processus de suivi.
   - Enregistrement : documentation initiale de tous les détails pertinents de la MVI.
2. **Surveillance continue**
   - Utilisation d'outils : utiliser des outils de surveillance et d'analyse pour suivre en temps réel l'évolution de l'incident.
   - Détection de nouveaux indices de compromission : identifier rapidement toute nouvelle activité ou tout indice de compromission lié à la MVI.
3. **Mise à jour et communication**
   - Mises à jour régulières : informer régulièrement les parties prenantes des progrès réalisés et des éventuels nouveaux développements.
   - Communication avec les parties prenantes : maintenir une communication ouverte et continue avec toutes les parties prenantes.
4. **Validation et fermeture de la MVI**
   - Tests de vérification : effectuer des tests pour s'assurer que la MVI a été résolue de manière adéquate.
   - Validation : obtenir la validation de la résolution de la MVI par toutes les parties concernées.
   - Fermeture : fermer officiellement la MVI et mettre à jour la documentation.
5. **Analyse post incident et amélioration continue**
   - Analyse des causes : effectuer une analyse approfondie des causes de la MVI pour identifier les faiblesses et les opportunités d'amélioration.
   - Leçons apprises : documenter les leçons apprises et intégrer les recommandations dans les processus GMVI futurs.

RÔLES ET RESPONSABILITÉS

Les rôles et les responsabilités de cette phase sont présentés dans la matrice suivante :

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Enregistrement initial de l'incident	C	I	R	C	A	C	C
Notification et communication	C	I	R	C	A	C	C
Développement et mise en œuvre du plan d'action	C	I	R	C	A	C	C
Suivi et surveillance continue	C	I	R	C	A	C	C
Validation de la remédiation	C	I	R	C	A	C	C
Documentation et rapport final	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

RÉSOLUTION ET LEÇONS APPRISES

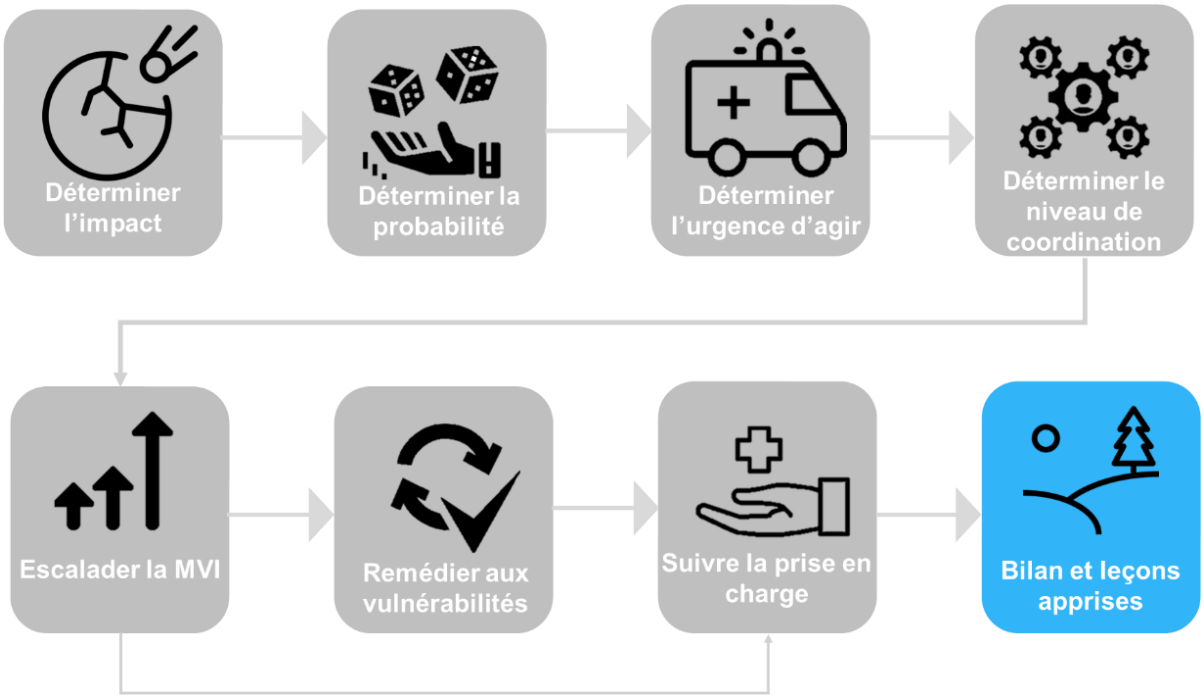

Figure 9 : Bilan et leçons apprises

Cette section vise à détailler les actions nécessaires pour clôturer un incident de sécurité, documenter les leçons apprises et renforcer les mesures de sécurité pour prévenir des incidents futurs.

OBJECTIF

- Assurer une clôture complète : vérifier que toutes les actions correctives ont été mises en œuvre et que la MVI est entièrement résolue.
- Documenter les leçons apprises : capturer les informations et les enseignements tirés de la MVI pour améliorer les processus futurs.
- Renforcer la sécurité : mettre en place des mesures pour prévenir la récurrence de l'incident.

ÉTAPES

Les étapes de cette phase sont les suivantes :

1. **Clôture technique de l'incident**
   - Vérification finale : s'assurer que toutes les actions correctives ont été effectuées et que les systèmes affectés sont sécurisés.
   - Validation de la résolution : Obtenir une validation formelle de la résolution de l'incident par les parties prenantes concernées.
2. **Documentation de l'incident**
   - Rapport de l'incident : rédiger un rapport détaillé incluant la description de l'incident, les actions entreprises, les résultats obtenus et les leçons tirées.
   - Journal de l'incident : maintenir un journal complet des événements, des décisions prises et des actions effectuées.
3. **Analyse post-incident**
   - Analyse des causes : examiner les causes profondes de l'incident pour comprendre ce qui a conduit à sa survenue.
   - Évaluation de l'efficacité des réponses : évaluer l'efficacité des actions de réponse et de remédiation pour identifier les points forts et les domaines d'amélioration.
4. **Recommandations et améliorations**
   - Recommandations : formuler des recommandations basées sur l'analyse post-incident pour améliorer les processus et les mesures de sécurité.
   - Plan d'action : développer un plan d'action pour mettre en œuvre les recommandations et renforcer la sécurité des systèmes.
5. **Communication des résultats**
   - Rapport aux parties prenantes : communiquer les résultats de l'analyse post-incident et les recommandations aux parties prenantes concernées.
   - Session de bilan : organiser une session de bilan avec toutes les parties prenantes pour discuter des résultats et des leçons tirées.
6. **Suivi et implémentation des améliorations**
   - Mise en œuvre des améliorations : mettre en œuvre les améliorations et les recommandations identifiées lors de l'analyse post-incident.
   - Suivi de l'avancement : suivre l'avancement des actions d'amélioration et ajuster les mesures si nécessaire.

PROCESSUS

1. **Validation de la résolution :** Le COMSI amorce la phase de clôture une fois que l'incident est résolu.
2. **Vérification finale :** effectuer une vérification finale pour s'assurer que toutes les actions de remédiation ont été mises en œuvre avec succès.
3. **Rapport de l'incident :** documenter toutes les étapes de la gestion de l'incident, y compris les actions entreprises et les résultats.
4. **Analyse post-incident :** analyser les causes de l'incident et évaluer l'efficacité de la réponse.
5. **Formulation des recommandations :** développer des recommandations pour améliorer les processus de sécurité basés sur les leçons apprises.
6. **Développement du plan d'action :** créer un plan d'action pour mettre en œuvre les recommandations et renforcer la sécurité.
7. **Communication des résultats :** partager les résultats et les recommandations avec les parties prenantes.
8. **Session de bilan :** organiser une session de bilan pour discuter des leçons apprises et des prochaines étapes.
9. **Mise en œuvre des améliorations :** implémenter les améliorations identifiées.
10. **Suivi continu :** suivre l'avancement des actions d'amélioration et ajuster les mesures si nécessaire.

RÔLES ET RESPONSABILITÉS

Activité	CGSI	CDSI	COMSI	ROCD	CGCD	CERT/AQ	CESI
Validation de la résolution	C	I	R	C	A	C	C
Documentation de l'incident	C	I	R	C	A	C	C
Analyse post-incident	C	I	R	C	A	C	C
Formulation des recommandations	C	I	R	C	A	C	C
Développement du plan d'action	C	I	R	C	A	C	C
Communication des résultats	C	I	R	C	A	C	C
Mise en œuvre des améliorations	C	I	R	C	A	C	C
Suivi de l'avancement	C	I	R	C	A	C	C
Légende : R : Responsable A : Autorité C : Consulté I : Informé							

BOITE À OUTILS

Le CESI a produit un ensemble de documents afin d'aider les établissements de l'Université du Québec à gérer efficacement les menaces, les vulnérabilités et les incidents de cybersécurité :

- Catégorisation des actifs basée sur l'approche de l'analyse des préjudices
- Formulaire d'analyses de préjudices de sécurité et de validation des résultats
- Guide d'évaluation des menaces et des risques
- Guide sur la mise en place d'un plan de réponses aux incidents de cybersécurité
- Gabarit de plan de réponses aux incidents de cybersécurité
- Gabarit de rapport d'incident
- Gabarit d'analyse post-mortem
- Gabarit de processus d'escalade
- Gabarit de présentation du rapport de l'incident

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

RÉFÉRENCES

Processus de gestion des menaces, des vulnérabilités et des incidents du Centre gouvernemental de cyberdéfense.

RÉVISIONS

Date	Action	Auteur	Version
2024-08-13	Revue linguistique	Joanne Lussier	1.0
2024-07-30	Intégration des commentaires des membres du CESI	Mehdi Tanazefti CESI de l'UQ	0.9
2024-07-11	Version initiale	Mehdi Tanazefti CESI de l'UQ	0.8

ANNEXE 1 : GRILLE DE DÉTERMINATION DU NIVEAU D'IMPACT DES PRÉJUDICES

TYPE DE PRÉJUDICE	NIVEAU D'IMPACT			
	FAIBLE	MODÉRÉ	ÉLEVÉ	TRÈS ÉLEVÉ
Préjudice pour les **citoyens**				
Préjudice physique causé aux personnes	Inconfort physique	Douleur physique, blessure, traumatisme, difficultés, maladie	Incapacité physique	Pertes de vie
Préjudice psychologique causé aux personnes	Stress	Détresse, traumatisme psychologique	Maladie ou trouble mental	Traumatisme psychologique généralisé
Perte financière pour des personnes	Inconfort et stress causés	Qualité de la vie altérée	Sécurité financière compromise	
Préjudice pour les **entreprises**				
Perte financière pour des entreprises	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	
Préjudice **gouvernemental**				
Préjudice causé à la prestation de services	Incidence sur la performance du service	Incidence sur les résultats du service non essentiel	Incidence sur le résultat d'un service essentiel	Viabilité des services essentiels compromise
Préjudice causé à l'économie québécoise		Incidence sur le rendement	Perte de la compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Préjudice causé à la réputation		Légère perte de confiance envers un organisme	Importante perte de confiance de la population envers un ou plusieurs organismes	Relations diplomatiques Embarras (au Québec ou à l'étranger)
Préjudice causé à la mission du gouvernement		Entrave à l'établissement de politiques gouvernementales importantes	Entrave à l'application efficace des lois	Cessation des activités du gouvernement
Médiatisation			Risque élevé ou médiatisation confirmée	Médiatisation négative importante anticipée ou confirmée
Protection des renseignements personnels (PRP)			Risque élevé de répercussions sur la PRP	Répercussions confirmées sur la PRP

ANNEXE 2 : TABLEAU DE DÉTERMINATION DE LA PROBABILITÉ DE CONCRÉTISATION D'UNE MENACE

CRITÈRE	PROBABILITÉ DE CONCRÉTISATION D'UNE MENACE			
	FAIBLE	MODÉRÉE	ÉLEVÉE	TRÈS ÉLEVÉE
Degré de sophistication des acteurs	Piratins	Groupe de cybercriminels avec des moyens modestes, peu organisé	Groupe de cybercriminels avec beaucoup de moyens, bien organisé	Groupe de cybercriminels avec des ressources abondantes
Ciblage des victimes	Généralistes	Secteurs d'activité connexes	Gouvernemental, à l'échelle mondiale	Gouvernemental fédéral ou provincial
Protection offerte par les mesures de sécurité en place	Efficace	Partielle	Peu efficace	Aucune protection

ANNEXE 3 : TABLEAU DE DÉTERMINATION DE LA PROBABILITÉ DE CONCRÉTISATION D'UNE MENACE

	PROBABILITÉ DE CONCRÉTISATION D'UNE MENACE			
	FAIBLE	MODÉRÉE	ÉLEVÉE	TRÈS ÉLEVÉE
Calcul avec la norme CVSS 3,1				
Pointage CVSS	0,0-3,9	4,0-6,9	7,0-8,9	9,0-10,0

ANNEXE 4 : DÉTERMINATION DU NIVEAU DE COORDINATION

NIVEAU IMPACT AJUSTÉ	URGENCE D'AGIR (3.3)		
	FAIBLE	MOYENNE	ÉLEVÉE
TRÈS ÉLEVÉ	Niveau 3 - CGCD	Niveau 4 - CCGSI	Niveau 4 - CCGSI
ÉLEVÉ	Niveau 3 - CGCD	Niveau 3 - CGCD	Niveau 4 - CCGSI
MOYEN	Niveau 2 - COCD	Niveau 2 - COCD	Niveau 3 - CGCD
FAIBLE	Niveau 1 - OP	Niveau 2 - COCD	Niveau 3 - CGCD

ANNEXE 5 : DÉTERMINATION DES DÉLAIS DE REMÉDIATION

NIVEAU D'IMPACT (3.1)	PROBABILITÉ DE CONCRÉTISATION (3.2)			
	FAIBLE	MOYENNE	ÉLEVÉE	TRÈS ÉLEVÉE
TRÈS ÉLEVÉ	8 jours	8 jours	8 jours	2 jours
ÉLEVÉ	30 jours	30 jours	8 jours	8 jours
MODÉRÉ	60 jours	30 jours	30 jours	30 jours
FAIBLE	60 jours	60 jours	60 jours	60 jours
Actif **exposé** à Internet **avec** correctif disponible				