UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Guide de la mise en place d'un plan de réponses aux incidents de cybersécurité

Avril 2024

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIÈRES

TABLE DES FIGURES ET DES TABLEAUX

TLP : VERT (DIFFUSION PERMISE)

INTRODUCTION

La capacité à répondre efficacement aux incidents de cybersécurité est essentielle pour assurer la résilience des établissements universitaires. Ce guide vise à offrir une approche et des outils au réseau de l'Université du Québec afin de gérer efficacement les incidents de cybersécurité et ainsi atténuer l'impact des cyberattaques, en couvrant les étapes clés depuis la préparation jusqu'à la résolution.

CONTEXTE

Le guide présenté ici s'inspire de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi25), la *Loi sur la Gouvernance et gestion des ressources informationnelles* (LGGRI), ainsi que le processus de *Gestion des menaces et des vulnérabilités informatiques* (GMVI). En alignant les pratiques recommandées avec les exigences légales et les processus opérationnels établis, ce guide vise à doter les établissements des outils nécessaires pour faire face aux menaces cybernétiques de manière proactive et conforme aux normes en vigueur.

OBJECTIF

Le présent guide vise à aider les établissements du réseau de l'Université du Québec à se conformer aux exigences légales et à mettre en place les bonnes pratiques sur le plan de gestion des incidents de cybersécurité.

TERMINOLOGIE

Menace : toute circonstance d'origine naturelle ou humaine qui pourrait entrainer des conséquences négatives sur un actif organisationnel.[1]

Vulnérabilité : absence ou faiblesse d'une protection d'actif qui rendent une menace plus susceptible de se produire.[1]

Impact : changement négatif pénalisant le niveau des objectifs d'affaires atteints.[2]

[1] Processus de gestion des menaces, des vulnérabilités et des incidents du Centre gouvernemental de cyberdéfense
[2] ISO/CEI 27005, clause 3.1

Risque de sécurité : possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise donc à l'organisme.[3]

Événement de sécurité : toute forme d'atteinte, présente ou appréhendée, telles une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'un organisme public.[4]

Incident de sécurité : Violation ou menace imminente de violation des politiques de sécurité de l'information, des politiques d'utilisation acceptable ou des pratiques de sécurité standard.[1]

Incident de confidentialité : l'accès non autorisé par la loi à un renseignement personnel ou l'utilisation non autorisée par la loi d'un renseignement personnel ou la communication non autorisée par la loi d'un renseignement personnel ou la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.[5]

Crise : Une crise est la résultante d'un événement causant des préjudices pouvant perturber l'image, la réputation et les services de l'organisation qui la subit ou lui nuit.[1]

PROCESSUS DE GESTION DES INCIDENTS DE CYBERSÉCURITÉ

Le processus de réponses aux incidents se déploie à travers plusieurs phases. Initialement, il implique la mise en place et la formation d'une équipe de réponses aux incidents, en mettant en place les ressources humaines, la technologie et les processus essentiels.

Au cours de la phase de préparation, l'établissement s'efforce de réduire la probabilité de l'occurrence d'un incident en sélectionnant et en mettant en œuvre des contrôles basés sur l'évaluation des risques.

Néanmoins, malgré la mise en œuvre de ces contrôles, un risque résiduel subsiste inévitablement. C'est pourquoi la phase de « *détection et analyse* » joue un rôle essentiel en mettant en œuvre des cas d'usage de détection afin d'alerter les équipes de réponses dès qu'un incident survient. En fonction de la gravité de l'incident, l'établissement peut atténuer son impact en le contenant et en adoptant des mesures appropriées. Une fois que l'incident a été géré de manière appropriée, l'établissement produit un rapport exhaustif exposant les origines et les

[3] ISO/CEI 27000, clause 2.68
[4] Paragraphe 7 de l'article 2 de la directive gouvernementale sur la sécurité de l'information
[5] Article 63.9 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

conséquences de l'incident, tout en proposant des mesures préventives visant à éviter de futures occurrences de cet incident.

Cette section offre une présentation des principales phases du processus de réponses aux incidents, englobant la préparation, la détection et l'analyse, l'assainissement, ainsi que les activités post-incident.

Le diagramme présenté ci-dessous offre une vue d'ensemble de ce processus. Chaque section qui suit ce schéma explore en détail les activités spécifiques de chaque phase.

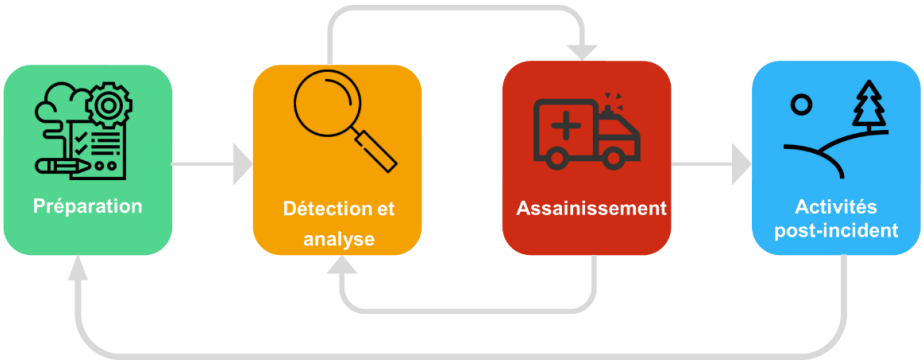

Figure 1 : Processus de réponse aux incidents de cybersécurité[6]

PRÉPARATION

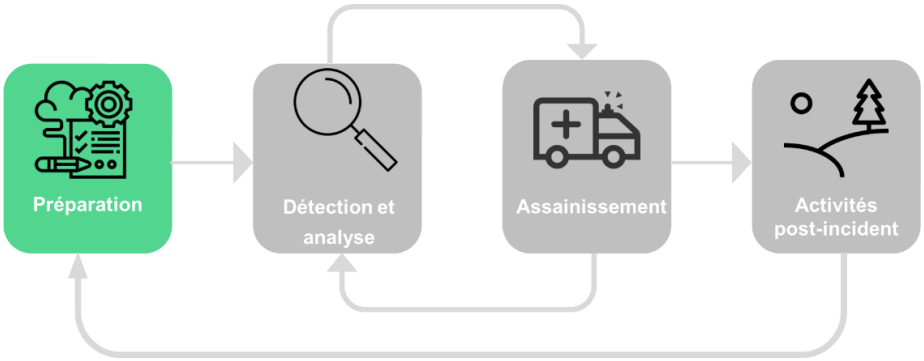

Figure 2 : Phase de préparation

La phase de préparation émerge comme une composante fondamentale, mettant les bases nécessaires à la résilience face aux menaces numériques. L'équipe de réponses aux incidents

[6] Processus de réponse aux incidents du NIST SP.800-61r2

s'engage dans une démarche méthodique visant à anticiper les éventualités, à identifier les risques, et à mettre en place les mesures nécessaires avant qu'un incident se matérialise.

La phase de préparation dans un plan de réponses aux incidents de cybersécurité comprend plusieurs activités essentielles. Ces activités visent à renforcer la capacité de l'établissement à anticiper, détecter et réagir efficacement aux incidents.

Le tableau ci-dessous illustre la matrice RACI de la phase de préparation, fournissant une vue d'ensemble des rôles et des responsabilités de manière générique. Il est conçu pour permettre à chaque établissement de l'adapter à son contexte spécifique en définissant clairement les acteurs impliqués et leurs responsabilités dans la préparation aux incidents de cybersécurité.

Activité	RÔLE					
	CSIO	COMSI	Équipe de réponses aux incidents	Propriétaire de l'actif	Services TI	Utilisateur
Établir une politique de réponse aux incidents	A	R	C	I	I	I
Élaborer un plan de réponses aux incidents	A	C	R	C	I	I
Documenter les procédures de réponses et les carnets de jeu	C	A	R	I	I	I
Établir des relations avec les parties externes	A	R	C	I	I	
Catégoriser les actifs informationnels	A	C	C	R	I	I
Mettre en place les capacités de détection et de prévention	A	R	C	I	I	I
Identifier les menaces et les vulnérabilités	C	A	R	C	I	
Mettre en place les mesures de mitigation	C	A	C	C	R	
Mettre en place des cas d'usage de détection	I	A	R	I	I	

Activité	RÔLE					
	CSIO	COMSI	Équipe de réponses aux incidents	Propriétaire de l'actif	Services TI	Utilisateur
Effectuer la veille sur les vulnérabilités et les menaces	I	A	R	I	I	
Former et sensibiliser les acteurs impliqués	A	R	I	I	I	I
R : Réalise A : Approuve C : Contribue I : Informe						

Tableau 1 : Rôles et responsabilités dans la phase de préparation

DÉTECTION ET ANALYSE

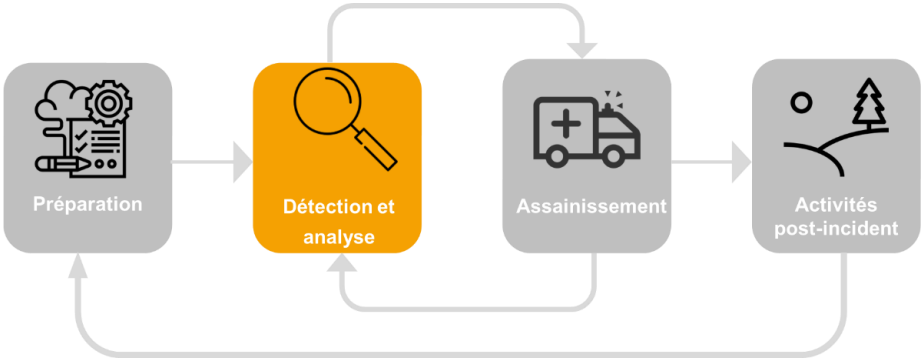

Figure 3 : Phase de « Détection et Analyse »

Un événement est une occurrence observable au sein d'un système ou d'un réseau. Les événements de sécurité sont ceux qui présentent une conséquence négative potentielle, tels que les défaillances physiques ou logiques d'un système, l'accès non autorisé à des données sensibles, ou l'exécution de code malveillant. Au cours de cette phase, l'équipe de réponses aux incidents identifie les événements de sécurité qui peuvent éventuellement mener à des incidents de cybersécurité.

Alors que l'équipe de réponses aux incidents est principalement chargée de détecter la majorité des événements de sécurité grâce à une surveillance continue, il est également possible que des utilisateurs, des partenaires ou d'autres sources soient à même de détecter des événements de sécurité. Dans cette perspective, il est essentiel d'impliquer toutes les parties prenantes dans la réponse aux incidents, favorisant une collaboration active et une communication appropriée.

En encourageant la participation des parties prenantes, l'équipe de réponses aux incidents peut bénéficier d'une diversité d'observations et d'informations cruciales pour une évaluation exhaustive des événements de sécurité. Cette approche inclusive contribue à renforcer la posture de sécurité globale de l'établissement en tirant parti de la vigilance collective.

Lorsqu'un incident est détecté, il devient essentiel de le catégoriser en fonction de sa gravité, permettant ainsi un traitement adapté à son niveau de criticité. Le CESI recommande d'établir une catégorisation des incidents selon la « Grille de détermination du niveau d'impact des préjudices » du « Processus de gestion des menaces, des vulnérabilités et des incidents » publié par le Centre gouvernemental de cyberdéfense.

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

Tableau 2 : Grille de détermination du niveau d'impact des préjudices[7]

[7] Processus de gestion des menaces, des vulnérabilités et des incidents du Centre gouvernemental de cyberdéfense

Une fois qu'un incident a été rigoureusement catégorisé au sein du cadre de la réponse aux incidents, il est impératif de s'orienter vers le processus d'escalade. Cette phase intervient lorsque la complexité, l'ampleur ou la gravité de l'incident dépasse les capacités ou les mandats initiaux de l'équipe de réponses aux incidents. Le processus d'escalade représente une démarche structurée qui permet d'assurer une réponse adaptée et proportionnée aux défis posés par l'incident.

En mobilisant le processus d'escalade, l'établissement peut activement tirer parti de ressources supplémentaires, d'expertises spécialisées, ou de niveaux hiérarchiques supérieurs selon la nature et la criticité de l'incident. Ce mécanisme assure une gestion efficace des incidents en veillant à ce que des mesures appropriées soient prises dans les délais requis, minimisant ainsi les impacts potentiels sur les opérations et la sécurité de l'information.

Le CESI recommande son intégration au processus d'escalade des établissements et met à disposition ses compétences en tant qu'acteur stratégique et technique pour renforcer la réponse aux incidents.

Selon l'impact de l'incident, le Centre gouvernemental de cyberdéfense propose le niveau de coordination présenté dans le tableau ci-dessous.

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

Tableau 3 : Détermination du niveau de coordination[8]

Le tableau suivant représente une cartographie des activités et des rôles et responsabilités essentiels au sein de la phase de « Détection et Analyse ».

[8] Processus de gestion des menaces, des vulnérabilités et des incidents du Centre gouvernemental de cyberdéfense

	RÔLE					
Activité	**CSIO**	**COMSI**	**Équipe de réponses aux incidents**	**Propriétaire de l'actif**	**Services TI**	**Utilisateur**
Surveiller en continu les systèmes et les réseaux	I	A	R	I	I	I
Corréler les événements des systèmes et des réseaux	I	A	R	I	I	I
Détecter les événements de sécurité	R	R	R	R	R	R
Analyser les événements de sécurité	I	A	R	I	I	I
Catégoriser l'incident	I	A	R	I	I	I
Déclarer un incident de sécurité	A	R	C	I	I	I
Gérer la priorité dans la file des incidents	I	A	C	I	I	I
Déclencher le processus d'escalade	A	R	C	I	I	I
Documenter l'incident	I	A	R	I	I	I
Déterminer les étapes de correction	A	R	I	I	I	I
Coordonner la réponse à l'incident	A	R	C	I	I	I
R : Réalise A : Approuve C : Contribue I : Informe						

Tableau 4 : Rôles et responsabilités dans la phase de « détection et analyse »

ASSAINISSEMENT

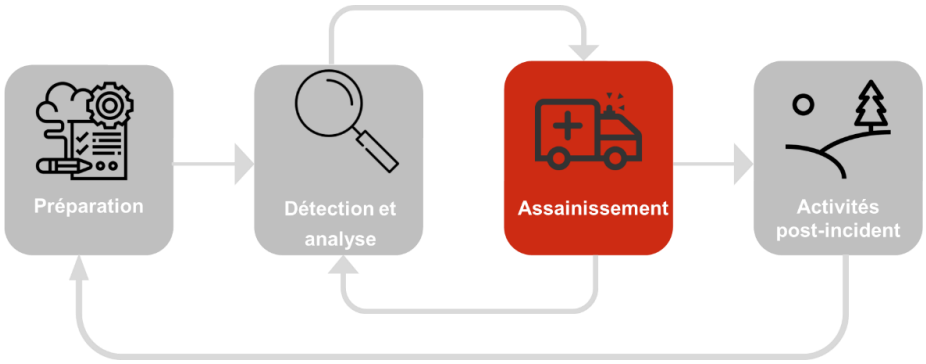

Figure 4 : Phase d'assainissement

La phase d'assainissement a pour objectif principal de contenir rapidement les effets d'un incident et d'empêcher sa propagation. Elle englobe le confinement de la menace, son éradication et la reprise des activités.

La sélection d'une stratégie de confinement représente un maillon essentiel dans la réaction face aux incidents de cybersécurité. Lorsqu'un incident survient, la capacité à prendre des décisions rapides, telles que l'arrêt d'un système, sa déconnexion du réseau, ou la désactivation de certains services, peut être déterminante pour contenir les dégâts potentiels.

Les établissements doivent anticiper différents scénarios d'incident et élaborer des stratégies de confinement adaptées. Il est essentiel de définir des niveaux de risque acceptables en cas d'incident, établissant ainsi des seuils au-delà desquels une intervention plus radicale est justifiée. Ces critères préalablement définis servent de base à la prise de décision, permettant une réaction rapide et cohérente.

La documentation claire de ces stratégies, assortie de critères détaillés, simplifie la prise de décision, même dans des situations d'urgence. Des directives bien définies permettent à l'équipe de réponses aux incidents de comprendre rapidement les étapes à suivre, assurant ainsi une exécution cohérente et efficace, tout en minimisant les impacts potentiels sur les opérations.

Après avoir confiné une menace, l'étape d'éradication s'avère nécessaire pour éliminer tous les éléments malveillants liés à l'incident. Cela englobe la suppression de logiciels malveillants, la désactivation des comptes d'utilisateurs compromis, ainsi que l'identification et la mitigation de

toutes les vulnérabilités exploitées. Durant cette étape, il est crucial d'identifier tous les systèmes compromis au sein de l'établissement afin de les remettre en état.

Dans le cadre de l'étape de récupération, les membres de l'équipe de réponses aux incidents travaillent à rétablir le fonctionnement normal des systèmes précédemment compromis. Ils s'assurent du bon fonctionnement de ces systèmes et, le cas échéant, corrigent les vulnérabilités pour prévenir de futurs incidents. Les actions entreprises pendant l'étape de récupération peuvent inclure la restauration de systèmes à partir de sauvegardes saines, la reconstruction complète de systèmes, le remplacement des fichiers compromis par leurs versions originales, l'application de correctifs de sécurité, la modification des mots de passe, ainsi que le durcissement de la sécurité des systèmes.

Pour garantir l'intégrité des investigations de l'incident, il sera nécessaire d'assurer la préservation des preuves. Celle-ci consiste à figer l'état des systèmes et des données au moment de la détection, créant une image numérique. Cette capture inclut journaux d'événements, configurations, et autres artefacts pertinents. La sécurisation rigoureuse de ces données garantit leur authenticité et leur admissibilité en cas d'enquête légale. Au-delà des exigences légales, cette préservation sert l'établissement en fournissant une base solide pour l'analyse post-incident, permettant de reconstruire les scénarios et de renforcer les défenses.

Les rôles et responsabilités dans la phase d'assainissement sont définis dans le tableau suivant :

Activité	RÔLE					
	CSIO	COMSI	Équipe de réponses aux incidents	Propriétaire de l'actif	Services TI	Utilisateur
Sélectionner une stratégie de confinement	A	R	I	I	I	I
Prendre les décisions face à l'incident	A	R	C	A	C	I
Isoler le système ciblé	C	A	C	C	R	I
Assurer la communication interne et externe	A	R	I	I	I	I
Éliminer le contenu malicieux	I	A	R	I	I	I
Éradiquer la menace	I	A	C	I	R	I

Activité	RÔLE					
	CSIO	COMSI	Équipe de réponses aux incidents	Propriétaire de l'actif	Services TI	Utilisateur
Rétablir les systèmes	I	A	C	I	R	I
Préserver les preuves	I	A	R	I	I	I
Créer une image des systèmes compromis	I	A	C	I	R	I
Documenter l'incident	I	A	R	I	I	I
R : Réalise A : Approuve C : Contribue I : Informe						

Tableau 5 : Rôles et responsabilités dans la phase d'assainissement

POST-INCIDENT

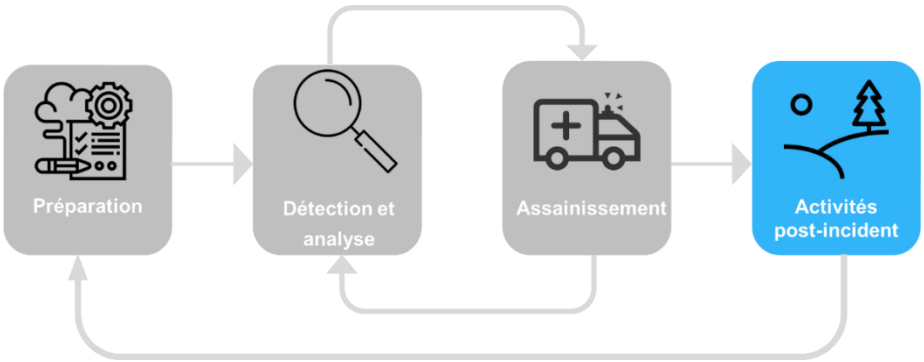

Figure 5 : Phase post-incident

La phase post-incident vise à revenir sur l'origine et les circonstances de chaque incident dans le but d'identifier les activités, les contrôles ou les politiques qui contribueront à prévenir de futurs incidents.

Cette phase permet l'analyse post-mortem de l'incident en examinant les journaux d'événements, les vecteurs d'attaque et en reconstruisant le scénario de l'attaque. Cette investigation détaillée permet de comprendre la séquence des événements, l'origine de l'incident, et les failles exploitées.

Une fois les causes identifiées, la phase post-incident se tourne vers la formulation de recommandations et d'améliorations. Cela peut englober des ajustements dans les politiques de sécurité, des mises à jour dans les procédures opérationnelles, ou des investissements dans

de nouvelles technologies de sécurité. L'objectif est de renforcer la posture de sécurité globale de l'établissement.

La phase post-incident ne marque pas simplement la fin du processus de gestion d'un incident, mais représente plutôt le point de départ d'un processus d'amélioration continue en mettant les leçons apprises comme intrants à la phase de préparation.

Dans cette phase, il sera approprié d'identifier les indicateurs clés de performance (KPI) afin d'évaluer et de perfectionner les capacités de réponse aux incidents. Ces indicateurs offrent des mesures quantifiables qui permettent de surveiller l'efficacité, l'efficience et la robustesse de la stratégie adoptée.

Activité	RÔLE					
	CSIO	COMSI	Équipe de réponses aux incidents	Propriétaire de l'actif	Services TI	Utilisateur
Effectuer l'analyse post-mortem	I	A	R	C	C	C
Produire le rapport de l'incident	I	A	R	C	C	C
Communiquer le rapport de l'incident	A	R	C	C	C	I
Mettre à jour les politiques, les procédures et les mécanismes de protection	A	R	C	C	C	
Déterminer les actions à entreprendre	A	R	C	C	C	
Mesurer les performances (KPI)	A	R	C	C	C	C
Mettre en place un plan d'action	A	R	C	C	C	C
Améliorer le processus de réponse aux incidents	A	R	C	C	C	C
R : Réalise A : Approuve C : Contribue I : Informe						

Tableau 6 : Rôles et responsabilités dans la phase post-incident

RÉFÉRENCES

NIST SP.800-61r2 Computer Security Incident Handling Guide

ISO/IEC 27035-1:2023 Technologies de l'information Gestion des incidents de sécurité de l'information Partie 1 : Principes et processus

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

Directive gouvernementale sur la sécurité de l'information

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

RÉVISIONS

Date	Action	Auteur	Ver.
2024-04-25	Revue linguistique	Joanne Lussier	1.0
2024-04-01	Intégration des commentaires des membre du CESI	Mehdi Tanazefti CESI de l'UQ	0.9
2024-02-26	Version initiale	Mehdi Tanazefti CESI de l'UQ	0.8