CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

IR-04

Traitement des incidents

Juill. 2026

Votre gouvernement

Québec

IR

Gestion des incidents de cybersécurité

Incident Response

IR-04 — Traitement des incidents (PaFF)

Énoncés :

a. Mettre en oeuvre des capacités de traitement pour les incidents alignées sur le plan d'intervention en cas d'incident et y inclure les activités de préparation, de détection, d'analyse, de confinement, d'éradication et de reprise
b. Coordonner les activités de traitement des incidents avec les activités de planification d'urgence
c. Intégrer les leçons apprises découlant des activités de traitement aux procédures d'intervention en cas d'incident, à la formation et aux tests, et mettre en oeuvre les changements qui en résultent comme il se doit
d. S'assurer que la rigueur, l'intensité, la portée et les résultats des activités de traitement des incidents sont comparables et prévisibles dans l'ensemble de l'organisation

Responsable : Aucun

Discussion :

Les organisations reconnaissent que la capacité d'intervention en cas d'incident dépend des capacités des systèmes organisationnels et des processus liés à la mission et aux activités prises en charge par ces systèmes. Les organisations devraient tenir compte de l'intervention en cas d'incident lors de la définition, de la conception et du développement de processus opérationnels et de mission et des systèmes. L'information liée aux incidents peut provenir de différentes sources, y compris la surveillance des vérifications, des accès physiques et des réseaux, les rapports d'utilisatrice ou utilisateur et d'administratrice ou administrateur, et les plaintes du public ou d'organismes de surveillance, et signalés de la chaîne d'approvisionnement. L'efficacité des capacités de traitement des incidents comprend la coordination entre différentes entités organisationnelles (par exemple, les propriétaires des activités et de la mission, les propriétaires des systèmes, les autorités responsables, les ressources humaines, les bureaux de la sécurité physique et les bureaux de la sécurité du personnel, les services juridiques, le responsable de la gestion des risques, le personnel des opérations et les responsables de l'approvisionnement). Les incidents de sécurité soupçonnés comprennent la réception de courriels suspects susceptibles de contenir un programme malveillant. Les incidents d'approvisionnement incluent l'insertion de matériel malveillant ou de programme malveillant dans les systèmes organisationnels ou les composants des systèmes.