Directive du Bureau du Chef de l'Information: TI 7.05	Publié: 04/2021
Chapitre: Surveillance et évaluation	Dernière révision: 01/2024
Objet: **Évaluations du risque pour la cybersécurité**	

1 DIRECTIVE

1.01 Une évaluation du risque pour la cybersécurité sera effectuée à l'égard de tous les nouveaux systèmes ou services d'information essentiels du GNB. Par la suite, une évaluation du risque pour la cybersécurité sera effectuée tous les trois ans, ou chaque fois que le système ou le service d'information essentiel subit des modifications importantes.

2 BUT

2.01 L'objectif de la présente directive est de s'assurer que les menaces existantes à la sécurité sont traitées de façon appropriée et que les menaces nouvelles et changeantes seront prises en compte et traitées de façon appropriée.

On garantit ainsi une bonne consignation des risques pour l'information et de la non-conformité quant aux actifs évalués et on voit à ce que les responsables fonctionnels soient au courant des risques cernés afin que les mesures nécessaires soient prises.

3 PORTÉE

3.01 La présente directive s'applique à tous les ministères, y compris leurs dispositifs et membres du personnel, qui utilisent les réseaux du GNB.

La présente directive remplace le document sur les normes et directives de la PSSTIG publié en novembre 2006.

4 RESPONSABILITÉ

4.01 Le Bureau du chef de l'information (BCI) doit procéder à l'évaluation du risque pour la cybersécurité sur les systèmes essentiels et soumettre les résultats et les plans d'action proposés à l'approbation du responsable fonctionnel.

4.02 Le BCI est chargé de :

a) Gérer chaque évaluation du risque pour la cybersécurité. Le travail que cela implique peut être accompli par l'agent ministériel de la sécurité de l'information (AMSI), ou son représentant, ou encore un tiers.

b) Procéder à une évaluation du risque pour la cybersécurité si une nouvelle menace à la sécurité est repérée bien avant le prochain examen régulier de la sécurité.

5 DÉFINITIONS

5.01 Le « responsable fonctionnel » est un cadre supérieur de l'organisation qui est responsable de la gestion générale d'un ensemble défini de données relatif à un secteur d'activité. Il a le pouvoir de déterminer qui peut accéder aux données et les utiliser, et il bénéficie habituellement du soutien des gestionnaires de données. Le responsable fonctionnel approuve les processus et les politiques

visant à maintenir la qualité des données et à normaliser les processus de gestion des données.

5.02 L'évaluation du risque pour la cybersécurité » est un aperçu des risques pour la cybersécurité et des contrôles en matière de cybersécurité concernant un système ou une application technologique.

5.03 Un « service ou un système d'information essentiel » est un service ou un système d'information indispensable à la prestation de services essentiels du GNB.

5.04 Un « service essentiel du GNB » est un service essentiel, au GNB ou au public, afin d'éviter des pertes liées à la santé et à la sécurité, aux finances, à la confiance dans le gouvernement, à l'environnement ou à la détresse sociale.

6 DIRECTIVES CONNEXES

BCI TI, chapitre 8 – Sécurité physique et sécurité des systèmes

BCI TI, chapitre 9 – Sécurité des données

BCI TI, chapitre 11 – Sauvegarde et planification en cas de sinistre