

# GUIDE DU NIVEAU DU PDG : ENCADREMENT DE LA CYBER-SÉCURITÉ

## GOUVERNANCE

*La cyber-sécurité de votre organisation commence et se termine au plus haut niveau de gestion. Le PDG, avec le conseil d'administration, doit maintenir la compréhension des risques et assumer l'obligation de rendre compte et la responsabilité ultimes des activités de cyber-sécurité et du personnel de l'organisation. Vous devez :*

- Embaucher un responsable de la sécurité des systèmes d'information (RSSI) s'il n'y en a pas ou, si les ressources sont trop limitées, nommer une personne au sein de votre organisation pour remplir la fonction de RSSI.
- Travailler avec le RSSI ou tout autre personnel technique pour établir et maintenir une stratégie et un cadre de cyber-sécurité adaptés aux cyber-risques spécifiques de l'organisation en utilisant les normes et directives internationales, nationales et industrielles.
- Expliquer clairement les rôles et responsabilités du personnel en mettant en œuvre et en gérant la cyber-sécurité de l'organisation.
  - Travailler avec le RSSI pour identifier les rôles de cyber-sécurité et les droits d'accès appropriés pour tous les niveaux de personnel.
  - Superviser la communication et la collaboration afin de garantir que la gestion de la cyber-sécurité est holistique, surtout si les responsabilités en matière de cyber-sécurité sont partagées par plusieurs membres du personnel ou divisions au sein de l'organisation (comme de distinguer les secteurs verticaux de l'information, du risque et des technologies).
- Vous assurer que le RSSI dispose d'une ligne de communication claire et directe pour vous signaler les menaces en temps opportun, ainsi qu'au conseil d'administration.
- Inviter le RSSI ou tout autre personnel technique à informer régulièrement la haute direction.
- S'assurer que les politiques de sécurité, les normes, les mécanismes d'application et les procédures de l'organisation sont uniformes dans toutes les équipes et les secteurs d'activité.

## ÉVALUATION ET GESTION DES RISQUES

*La garantie d'une sensibilisation et d'une préparation solides à la cyber-sécurité dépend de l'analyse continue basée sur les risques. Pour améliorer la cyber-sécurité de votre entreprise :*

- Établissez une évaluation et une gestion des risques de cyber-sécurité comme priorité dans les processus de gestion et de gouvernance des risques élargis de votre organisation. Travaillez avec votre RSSI ou tout autre personnel technique sur un plan pour effectuer une évaluation des risques impliquant les points suivants :
  - Décrire les actifs de votre organisation et leurs différents niveaux de dépendance technologique ;
  - Évaluer la maturité de votre organisation et les risques inhérents associés aux dépendances technologiques de ses actifs ;
  - Déterminer l'état de maturité souhaité de votre organisation ;
  - Comprendre où les menaces de cyber-sécurité s'inscrivent dans la liste des priorités de risque de votre organisation ;
  - Identifier les écarts entre votre état actuel de cyber-sécurité et l'état cible souhaité ;
  - Mettre en œuvre des plans pour atteindre et maintenir la maturité ;
  - Évaluez et affectez des fonds pour investir dans la sécurité et corriger les écarts existants,
  - Réévaluer continuellement la maturité, les risques et les objectifs de cyber-sécurité de votre organisation ; et
  - Envisager l'utilisation de tests d'intrusion de tiers ou une simulation ;
  - Envisager des mesures de protection telles que l'achat d'une cyber-assurance.
- Dirigez les efforts des employés pendant le processus d'évaluation des risques afin de faciliter les réponses opportunes de l'ensemble de l'établissement.
- Analysez et présentez les résultats de l'évaluation des risques pour la supervision exécutive, y compris les principales parties prenantes et le conseil.

- Supervisez les changements pour conserver ou améliorer la préparation à la cyber-sécurité souhaitée, y compris la budgétisation adéquate, de votre organisation, en veillant à ce que les mesures prises pour améliorer la cyber-sécurité soient proportionnelles aux risques et rentables pour votre organisation.
- Supervisez les performances de la surveillance continue afin de rester flexible et agile dans le traitement des cyber-risques en évolution.

## CULTURE ORGANISATIONNELLE

*La cyber-sécurité de votre organisation n'est pas un processus ponctuel ou le travail de quelques employés ; il s'agit d'un facteur à prendre en compte dans toutes les décisions et opérations de l'entreprise et d'une pratique qui doit être maintenue par tous les employés. Afin d'encourager une cyber-sécurité continue et holistique au sein de votre organisation :*

- Initiez des discussions sur la cyber-sécurité avec l'équipe de direction et communiquez régulièrement avec le personnel responsable de la gestion des cyber-risques.
- Formez tous les employés à la cyber-sécurité, en veillant à ce que tout le personnel soit à jour sur (et ait signé des documents indiquant qu'ils acceptent de respecter) les politiques de cyber-sécurité de votre organisation et à ce que votre service informatique ou tout autre personnel technique les informe sur les meilleures pratiques.
- Instaurez une formation récurrente à la cyber-sécurité pour tous les employés en ce qui concerne leurs responsabilités de sécurité à court et à long terme.
- Veillez à ce que la cyber-sécurité soit toujours prise en compte lorsque votre organisation évalue les fournisseurs potentiels et partage des données avec des tiers.
- Intégrez une évaluation de la cyber-sécurité d'une organisation en tenant compte des fusions et acquisitions.
- Passez annuellement en revue les politiques de cyber-sécurité de votre organisation.
- Encouragez le partage volontaire des informations sur les menaces et incidents de cyber-sécurité au sein de votre organisation et avec des homologues fiables.
- Encouragez l'innovation qui intègre les problèmes de sécurité et la planification dès le début.