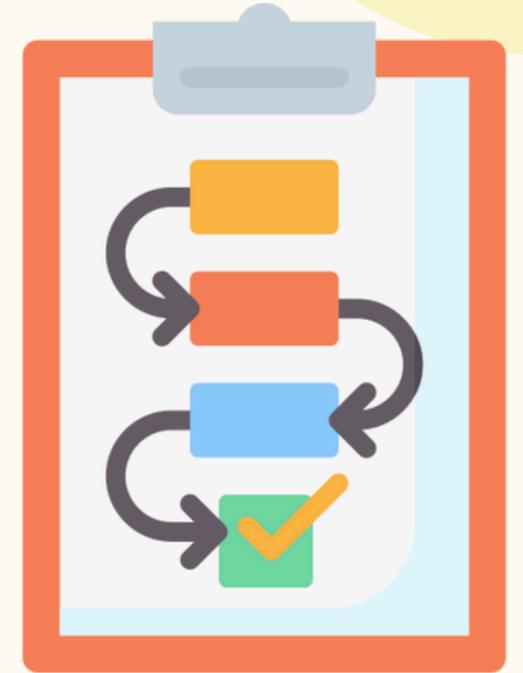




# POLITIQUE DE SÉCURITÉ DE L'EXPLOITATION

## Procédures d'exploitation documentées

**Objectif 20:** S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.



**01.** Des procédures bien documentées doivent être établies pour l'installation et la configuration des systèmes.

**02.** Une procédure bien documentée de redémarrage et de récupération de chaque système, en cas de défaillance, doit être définie et appliquée.

**03.** Une procédure bien documentée de sauvegarde et de maintenance, pour chaque système, doit être définie et appliquée.

**04.** Les contacts du support technique doivent être disponibles et tenus à jour, pour faire face notamment aux difficultés d'exploitation.

**05.** Les normes de sécurité de l'équipement doivent être documentées et suivies.

**06.** L'installation de logiciels n'ayant aucun rapport avec les activités de l'entité doit être prohibée.

**07.** L'utilisation de logiciels non autorisés, et sans une licence authentique, doit être strictement interdite.

**08.** Les procédures d'exploitation doivent être régulièrement auditées, contrôlées et mises à jour.

# POLITIQUE DE SÉCURITÉ DE L'EXPLOITATION

## Gestion des changements

**Objectif 21:** Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information, qui influent sur la sécurité de l'information, doivent être autorisés et contrôlés à travers un processus de gestion de changement avec des mécanismes régulateurs appropriés. Lorsque des changements sont effectués, un journal d'audit, contenant toutes les informations pertinentes, doit être créé et maintenu.

**01.** Il faut identifier et consigner les changements significatifs.

**02.** Il faut planifier les changements et la phase de test.

**03.** Il faut apprécier les incidences potentielles de ces changements sur la sécurité de l'information.

**04.** Une procédure d'autorisation formelle des changements proposés doit être mise en œuvre.

**05.** Il faut vérifier que les exigences de sécurité de l'information sont respectées.

**06.** Il faut transmettre les informations détaillées sur les changements apportés à toutes les personnes concernées.

**07.** Il faut mettre en œuvre les procédures de repli, incluant les procédures et les responsabilités en cas d'abandon et de récupération, suite à l'échec des changements ou à des événements imprévus.

**08.** Il faut mettre en place un processus de modification d'urgence permettant une mise en œuvre rapide et contrôlée des modifications requises par la résolution d'un incident



# POLITIQUE DE SÉCURITÉ DE L'EXPLOITATION

## Séparation des environnements de développement, de test et d'exploitation

**Objectif 22:** Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.

01. Les règles concernant le passage des logiciels du stade de développement au stade d'exploitation doivent être définies et documentées.
02. Il faut exécuter les logiciels de développement et les logiciels d'exploitation sur des systèmes informatiques différents et dans des domaines ou des répertoires différents
03. Il faut tester les modifications à apporter aux systèmes et aux applications dans un environnement de test avant de les appliquer aux systèmes en exploitation.
04. Les activités de développement doivent être séparées des activités de test.
05. Les compilateurs, les éditeurs et les autres outils de développement ou les utilitaires systèmes ne doivent pas être accessibles depuis les systèmes en exploitation, lorsqu'ils ne sont pas nécessaires.

06. Les utilisateurs doivent utiliser des profils différents pour les systèmes en exploitation et les systèmes de test, et les menus doivent afficher les messages d'identification adéquats pour réduire le risque d'erreur.
06. Il ne faut pas copier de données sensibles dans l'environnement du système de test, à moins qu'il ne soit doté de mesures de sécurité équivalentes.

