

SECURITE DES ACCES (PRINCIPES DU BESOIN D'EN CONNAITRE ET D'UTILISER)

Objectif

IL FAUT METTRE EN ŒUVRE UNE POLITIQUE DE LA SÉCURITÉ DES ACCÈS BASÉE SUR LES EXIGENCES MÉTIER ET DE SÉCURITÉ DE L'INFORMATION : UN ACCÈS AU SYSTÈME D'INFORMATION ET AUX DONNÉES, BASÉ RESPECTIVEMENT SUR LES PRINCIPES DU BESOIN D'EN CONNAÎTRE ET DU BESOIN D'UTILISER ET, PARTANT, DU MOINDRE PRIVILÈGE. CHAQUE UTILISATEUR N'A ACCÈS QU'AU SYSTÈME D'INFORMATION ET AUX DONNÉES DONT IL A BESOIN POUR ACCOMPLIR LES TÂCHES QUI LUI SONT ASSIGNÉS.

1

Spécifier les mesures de sécurité pour les applications métier.

2

Appliquer le principe du besoin d'en connaître : « Nul ne peut, du seul fait de son grade ou son titre, avoir accès aux informations sensibles s'il n'est pas habilité et s'il n'a pas besoin d'en connaître pour réaliser ses tâches (différentes tâches ou fonctions impliquent des besoins d'en connaître différents, d'où des profils d'accès différents) ».

3

Appliquer le principe du besoin d'utiliser : « Nul ne peut, du seul fait de son grade ou son titre, avoir accès aux moyens de traitement des informations sensibles, s'il n'est pas habilité et s'il n'a pas besoin de les utiliser pour accomplir son travail (matériels informatiques, applications, procédures, salles) ».

4

Effectuer un cloisonnement des rôles pour le contrôle des accès.

5

Mettre à jour régulièrement les droits d'accès attribués aux utilisateurs.

6

Revoir régulièrement les privilèges et les droits d'accès en cas de changement de poste de travail.

Règle

La sécurité logique complète la sécurité physique. Son objectif est de protéger les systèmes d'information contre l'intrusion et d'assurer la confidentialité des données.

La sécurité logique est composée de la sécurité des accès, de la sécurité des applicatifs et de la sécurité des échanges.

