PRÉSIDENCE
DE LA RÉPUBLIQUE
DU SÉNÉGAL

DCSSI

POLITIQUE DE SÉCURITÉ D'EXPLOITATION

JOURNALISATION ET SURVEILLANCE

OBJECTIF: Enregistrer les événements et générer des preuves.

Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et revus régulièrement.
Dans ce cadre, des mesures appropriées doivent aussi être prises pour prévenir l'accès non autorisé aux données sensibles et aux données à caractère personnel contenues dans les journaux d'évènements. En outre, les administrateurs systèmes ne doivent pas avoir la possibilité d'effacer ou de désactiver les journaux concernant leurs propres activités.

01

Les journaux d'événements doivent contenir les informations suivantes:

- les identifiants des utilisateurs ; les activités du système ;
- la date, l'heure et les détails relatifs aux événements significatifs (exemple : ouvertures et fermetures de sessions) ;
- l'identité ou l'emplacement du terminal si possible et l'identifiant du système ;
- les enregistrements des tentatives d'accès au système réussies ainsi que celles avortées ;
- les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées;
- les modifications apportées à la configuration du système
- l'utilisation des privilèges;
- l'emploi des utilitaires et des applications ;
- les fichiers qui ont fait l'objet d'un accès et la nature de l'accès
- les adresses et les protocoles du réseau ;
- les alarmes déclenchées par le système de contrôle d'accès.

Instruction Présidentielle Relative à la politique de sécurité des Systèmes d'Information de l'Etat du Sénégal N°003/PR DU 03 Janvier 2017

PRÉSIDENCE
DE LA RÉPUBLIQUE
DU SÉNÉGAL

DCSSI

POLITIQUE DE SÉCURITÉ D'EXPLOITATION

JOURNALISATION ET SURVEILLANCE

OBJECTIF: **Enregistrer les événements et générer des preuves**.

02 Les moyens de journalisation et l'information journalisée doivent être protégés contre les risques de falsification et les risques d'accès non autorisés.

03 Les fichiers de journalisation doivent être analysés par des outils automatiques destinés à cet effet.

04 Il faut journaliser les activités de l'administrateur système et les activités de l'opérateur système, protéger et revoir régulièrement les journaux.

05 Un système de détection des intrusions hors du contrôle des administrateurs système et réseau doit être utilisé pour vérifier la conformité des activités d'administration système et réseau.

Instruction Présidentielle Relative à la politique de sécurité des Systèmes d'Information de l'Etat du Sénégal N°003/PR DU 03 Janvier 2017

PRÉSIDENCE
DE LA RÉPUBLIQUE
DU SÉNÉGAL

DCSSI

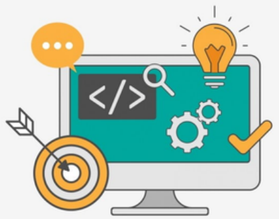
POLITIQUE DE SÉCURITÉ D'EXPLOITATION

JOURNALISATION ET SURVEILLANCE

OBJECTIF: **Enregistrer les événements et générer des preuves**.

06 Les journaux doivent être vérifiés de façon permanente.

07 Tous les événements majeurs doivent être enregistrés sur n'importe quel ordinateur ou système manipulant des données sensibles, y compris, mais sans s'y limiter, les échecs de connexion, les modifications de données, l'utilisation de comptes privilégiés, les changements de mode d'accès, les modifications apportées aux logiciels installés ou au système d'exploitation et les modifications apportées aux autorisations accordées aux utilisateurs.



Instruction Présidentielle Relative à la politique de sécurité des Systèmes d'Information de l'Etat du Sénégal N°003/PR DU 03 Janvier 2017