Absence de personnel Procédures de recrutement inadaptées Formalisation insuffisante à la sécurité Utilisation incorrecte du logiciel et du matériel Absence de sensibilisation à la sécurité Personnel Absence de mécanismes de surveillance Travail non surveillé d'une équipe extérieure ou de l'équipe d'entretien Absence de politiques relatives à la bonne utilisation de supports de télécommunications et de la Utilisation inadaptée ou négligente du contrôle d'accès physique aux bâtiments et aux salles Emplacement situé dans une zone sujette aux inondations Site Réseau électrique instable Absence de protection physique du bâtiment, des portes et des fenêtres Absence de procédure formelle relative à l'enregistrement et au retrait des utilisateurs absence de processus formel relatif à la revue des droits d'accès (supervision) Absence de disposition suffisantes (relatives à la sécurité) dans les contrats avec des clientset/ou des tiers Absence de procédure de surveillance des moyens de traitements de l'information Absence d'audits réguliers (supervision) Absence de procédures d'identification et d'appréciation des risques Absence de rapports d'erreur enregistrés dans les journaux administrateurs et les journaux opérations Réponse inadaptée du service de maintenance Vulnérabilité Accord de service absent ou insuffisant Absence de procédure de contrôle des modifications Absence de procédure de contrôle formelle du contrôle de la documentation SMSI Absence de procédure formelle de supervision du SMSI Absence de processus formel d'autorisation des informations à disposition du public Absnece de bonne attribution des responsabilités en sécuirité de l'information Absence de plans de continuité Organisation Absence de politique relative à l'utilisation des emails Absence de procédures d'introduction d'un logiciel dans des systèmes d'exploitation Absence d'enregistrements dans les journaux administrateurs et journaux opérations Absence de procédures relatives au traitement de l'information classée Absence de responsabilités en sécurité de l'information dans les descriptions de poste Dispositions absentes ou insuffisantes (relatives à la sécurtité de l'information) dans les contrats avec les Absnece de processus discilpinaire défini en cas d'incident en sécurité de l'information

Absence de politique formelle relative à l'utilisation des ordinateurs portables

Politique absente ou insuffisante relative au "bureau propre et à l'écran vide"

Absence de mécanismes de surveillance établis pour des violations de sécurité

Absence de procédures de la conformiyté des dispositions aux droits de propriété intellectuelle

Absence d'autorisation relative aux moyens de traitement de l'information

Absence de contrôle des actifs situés hors des locaux

messagerie

employés

Absence de contrôle efficace de modification de configuration Matériel Sensibilité aux variations de tension Sensibilité aux variations de température Stockage non protégé Manque de prudence lors de la mise au rebut reproduction non contrôlée Tests de logiciel absents ou insuffisants Failles bien connues dans le logiciel Pas de fermeture de session en quittant le poste de travail Mise au rebut et réutilisation de supports de stockage sans véritable effacement Absence de traces d'audit Attribution erronée des droits d'accès Logiciel distribué à grande échelle Application de programmes de gestion à de mauvaises données en termes de temps Interface utilisateur compliquée Absence de documentation Réglage incorrect de paramétres Logiciel Dates incorrectes Absence de mécanismes d'identification et d'authentification tel que l'authentification des utilisateurs Tableaux de mots de passe non protégés Mauvaise gestion des mots de passe Activation de services non nécessaires Logiciel neuf ou en phase de rodage Spécifications des développeurs confuses ou incomplètes Absence de contrôle efficacedes modofications Chargement et utilisation non contrôlés du logiciel Absence de copies de sauvegarde Absence de protection physique du bâtiment, des portes et des fénêtres Impossibilité de produire les comptes -rendus Absence de preuves d'envoi ou de réception d'un message Voies de communication non protégées Trafic sensible non protégé Mauvais câblage Point de défiallance unique Réseau Absence d'identification et d'authentification de l'expéditeur et du destinataire Architecture réseau non sécurisé Transfert de mot de passse en clair Gestion réesau inadaptée (résilience du routage) Connexions au réeseau public non protégées

Maintenance insuffisante/mauvaise installation des supports de stockage

Absence de programmes de remplacement périodique

Sensibilité à l'humidité, à la poussière, aux salissures

Sensibilités aux rayonnements électromagnétiques