POLITIQUE DE SECURITE DES INFORMATIONS

A) SECURITE RESEAU

1- DROITS D'ACCES
2- MISE EN PLACE DES GPO
3- GESTION DE L'ANTIVIRUS
4- GESTION DE LA MESSAGERIE ET INTERNET
5- FORMATION DES UTILISATEURS

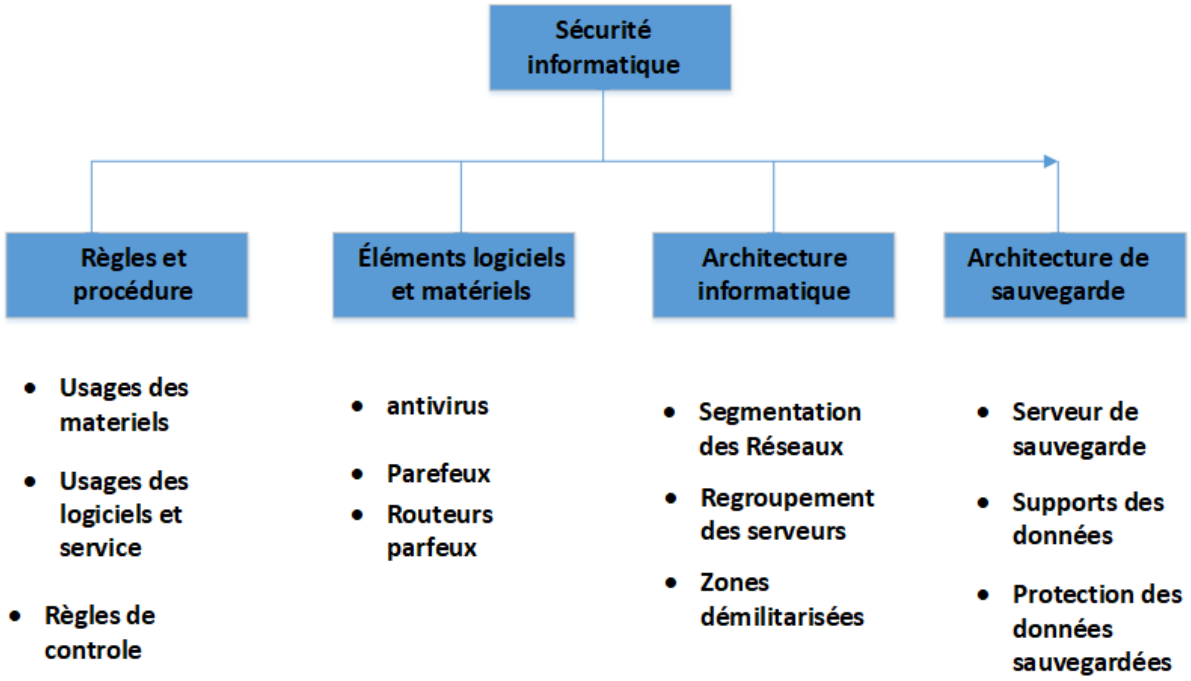
B) SECURITE DES APPLICATIONS

1- DROITS D'ACCES
2- CRYPTAGE

C) SAUVEGARDE DES DONNEES

1- SAUVEGARDE INTERNE
2- SAUVEGARDE A DISTANCE

I) POLITIQUE DE SECURITE DES INFORMATIONS



Les éléments de la sécurité informatique

A) SECURITE RESEAU

1- DROITS D'ACCES

Pour mettre en place notre politique de sécurité, un domaine a été créé. Ce dernier est géré par un contrôleur de domaine. L'accès à des données vous obligent à avoir des identifiants (Login/mot de passe) pour accéder à une session et pouvoir y retrouver toutes les informations auxquelles ce profil à droit. Ceci nous permet donc de retracer toutes les activités des utilisateurs grâce aux journaux de logs et de pouvoir contrôler le flux et l'accès aux données. Une série de lecteur partagé est créé, chacun mappé avec les utilisateurs devant y avoir accès ainsi que les autorisations (lecture/écriture/non autorisé).

La direction de l'informatique, délimite les aires à accès restreint et installe les systèmes de sécurité ainsi que le matériel nécessaire selon une évaluation des menaces et des risques (détection de feu, extincteurs)

La direction s'assure également de mettre en place les mesures nécessaires pour protéger les équipements et l'information qu'ils contiennent (accès au clé USB désactivé, accès restreint au bureau à chaque session, non autorisation aux commandes administrateurs).

2- MISE EN PLACE DES GPO

Les stratégies de groupes sont des ensembles de paramètres qui s'appliquent aux utilisateurs et ordinateurs. Elles permettent de gérer plus facilement la sécurité d'un poste ou de plusieurs postes dans un Domain. Elles permettent à titre d'exemples de rediriger le dossier Mes Documents, de déployer des Logiciels en fonction des services d'une entreprise ou des utilisateurs. Les GPO existent dès la création d'un Domain, c'est là que sont inscris les différents fonctionnements du domaine. Il en existe deux types à la création du domaine. Les GPO mis en place dans notre cas nous permettent de contrôler les différents profils et leurs droits. En effet grâce à ces GPO, nous arrivons à restreindre l'accès à certaines ressources des postes de travail en fonction des profils. Par exemple toutes les sessions des téléconseillers n'ont pas le droit d'installer des logiciels tiers sur les postes de travail. Plusieurs GPO ont été mis en place et sont classés en fonction des départements.

3- GESTION DE L'ANTIVIRUS

Un serveur d'antivirus a été mis en place dans le réseau. En effet sur ce serveur est installé ESET ANTIVIRUS qui effectue des mises à jours régulières en se connectant au serveur de ESET à partir d'internet. Il est également installé sur tous les postes de l'entreprise (Production, Administration). Vu la politique de sécurité mis en place, ces derniers effectuent directement leurs mises à jour depuis le serveur local et permet ainsi de nous protéger des risques d'infection virale ou de vers.

En cas d'infection, une analyse complète de tous les disques est immédiatement effectuée pour supprimer au plus tôt la menace.

4- GESTION DE LAMESSAGERIE ET INTERNET

La direction s'assure de mettre en place des mesures pour prévenir les SPAM informer et encadrer le personnel sur l'usage du courrier électronique et internet.

L'accès à internet n'est autorisé que chez le personnel administratif et l'ouverture des attachements de courriers électroniques est faits avec soin pour limiter l'exécution de code malveillant.

Un Planning d'accès à internet est aussi défini pour mieux faire la gestion de la QOS.

5- FORMATION DES UTILISATEURS

La formation des utilisateurs a pour objectif de les rendre autonome à l'usage des outils et applications qui sont utiles à l'exécution de leurs taches dans l'entreprise. A chaque nouvelle application développée par le département une formation des opérationnels est programmée et un manuel d'utilisation leur est fourni. L'autre volet de cette formation consiste en la sensibilisation sur les menaces liées à la sécurité du réseau interne (utilisation des clés USB, l'utilisation des sessions…) formation ou conduite à tenir en cas d'incident lié à la sécurité des personnes.

B) SECURITE DES APPLICATIONS

1- DROITS D'ACCES

Les identifiants d'ouverture de sessions assurent l'accès aux ressources de base (lecteurs uniquement), et ils ne garantissent pas l'accès aux applications nécessaire à l'exercice des activités. Les droits d'accès permettent de définir, situer et limité les actions utilisateurs sur des fonctionnalités bien définie dans une application. Selon le type des applications, ces droits peuvent varier mais ils comporteront sauf cas exceptionnel un droit d'**administration** de l'application et un droit d'accès aux fonctionnalités principales aux utilisateurs pour qui l'application est destinée. Pour les bases de données, la définition des droits revient au DSI qui les attribue aux administrateurs ou développeur selon leur profil.

2- CRYPTAGE

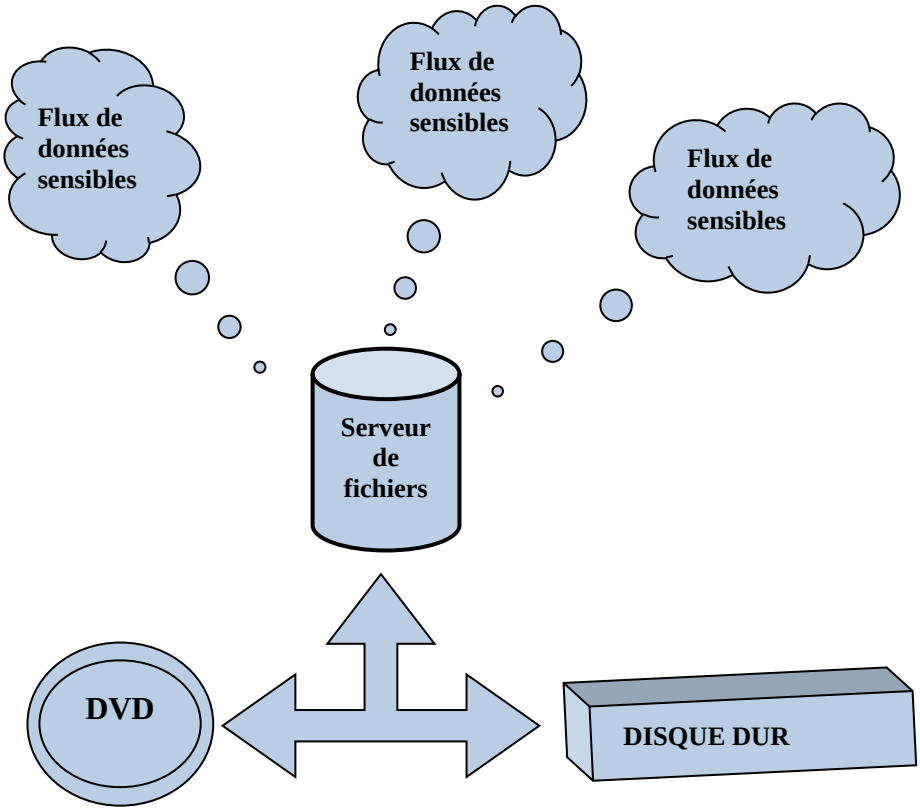
Le cryptage est un procédé visant à protéger la confidentialité de certaines données applicatives. Dans le cahier des charges de l'application doit être exprimé le besoin de rendre confidentiel certaines informations sensibles afin qu'en cas d'usurpation, ces données soient non utilisables.

La méthode de cryptage est laissée aux soins du développeur qui choisira celle qui convient selon les cas et les besoins de performances d'accès.

C) SAUVEGARDE DES DONNEES

1- SAUVEGARDE INTERNE

La sauvegarde des données demande beaucoup d'espace de stockage vue la taille des données à sauvegarder. Ainsi une procédure de sauvegarde des données très sensibles de l'entreprise a été mise en place pour les sauvegarder. Nous avons donc prévu de les stocker sur des supports amovibles (Disque dur externe, DVD).



2- SAUVEGARDE A DISTANCE

Quant à la sauvegarde externe des données, elle consiste à déposer certaines données sur un espace distant. Dans notre cas, il s'agit d'un espace chez OVH (**O**n **V**ous **H**éberge) accessible via un lien FTP ou un client FTP. Cet espace est sécurisé et nous permet parfois de

conserver certaines données telles que les mises à jour de certaines applications métiers, des sauvegardes de certaines applications et site web.