# UTC505 - Lille - HTT à distance : Introduction à la cyberstructure de l'internet : réseaux et sécurité

|  |  |
| --- | --- |
| Politique de sécurité de l’information | Conditions générales d’utilisation.  Politique de sécurité des réseaux partenaires. Politique de zoning (l’information ne passe pas par backoffice). Lors de ma co à internet : double co à firewall |
| Organisation de la sécu de l’information | Réseaux fermés ?  Séparation des rôles d’admin et d’habilitateur. |
| Gestion des biens | Inventaire des biens informatiques, des éléments du réseau. Cela donne des niveaux de sensibilité, par une classification. Notion de coûts : plus le niveau est élevé plus le coût est fort. |
| Sécu liée aux ressources humaines | Veille ? information et sensibilisation du personnel ?  Définir des profils, recrutement, plan de formation. Notion de responsabilité des administrateurs. |
| Sécu physique et environnementale | Data center. Restrictions des entrées.  Protection des locaux. |
| Gestion d’exploitation et des télécomm | Cryptage des données. Gestion des routeurs, firewall. Gestion de tous les composants réseau. |
| Contrôle d’accès | Authentifications et mots de passe. Accès restreints à certains environnements. Niveau de complexité de mot de passe : les admin auront des mots de passe plus longs car sensibilité accrue. |
| Acquisition dvp et maintenance des | Routeurs et firewall. Comment on dvp les mises à jour ? Comment détecter les failles et comment je mets à jour ? |
| Gestion des incidents | Personnes en cyber pour gérer les incidents. En interne ou extérieur. Réponses automatisées. Remontée d’alerte. SOC : security operation sector. SIEM : … |
| Gestion du PCA | Assurer la continuité de service du réseaux. |
| Conformité | RGPD : Règlement Général de protection des données. |

