

| Exigences de sécurité  | Cotation | Points | Remarques  |
|--|----------|--------|--|
| Sécurité des ressources humaines   |          |        |  |
| – Recrutement  | 5        |        | Vérification de l'identité et de situation légale  |
| – Gestion des arrivées départ  | 5        |        | "Circuit" arrivé/départ (Perception et réintégration doc. et matériel, gestion des comptes)  |
| – Sensibilisation et formation à la Sécurité Numérique                   | 3        |        | Sensibilisation a la sécurité des systèmes d'information   |
| Gestion des actifs   |          |        |  |
| – Cartographie des actifs  | 3        |        | Quels sont les moyens informatiques et comment ils sont reliés entre eux   |
| – Classification des actifs  | 2        |        | Le cas échéant, pour ce qui est classifié au regard de l'IGI1300   |
| – Protection des informations  | 1        |        | Quelles mesures sont prises (Physiques et organisationnelles)  |
| Gestion des accès logiques   |          |        |  |
| – Droits d’accès aux ressources  | 3        |        | Qui gère les droits d'accès et comment ils sont appliqués  |
| – Contrôle d’accès logique aux SI  | 5        |        | Quel dispositif protège l'accès logique (Mot de passe, certificat, carte ...)  |
| – Gestion des habilitations  | 3        |        | Habilitations au sens de l'IGI1300 (Protection des données classifiées)  |
| – Gestion des sessions inactives   | 1        |        | Comment sont contrôlées et gérées les sessions inactives   |
| – Traçabilité des accès  | 1        |        | Comment sont tracé les accès (journaux logiciels, SMSI ...)  |
| Gestion des authentifiants   |          |        |  |
| – Gestion des mots de passe  | 5        |        | Rythme de changement, politique de complexité...   |
| – Gestion des certificats électroniques                                  | 1        |        | Le cas échéant   |
| Sécurité physique  |          |        |  |
| – Contrôle d’accès physique aux locaux                                   | 5        |        | Quel dispositif protège l'accès physique aux locaux (bareaudage, clé, verrou...)   |
| – Traçabilité des accès physiques aux locaux                             | 3        |        | Journaux de lecteur de badge, registre...  |
| – Protection des zones de sécurité physique                              | 2        |        | Système d'alarme volumétrique, périmétrique ...  |
| Sécurité de l’exploitation des SI  |          |        |  |
| – Durcissement des ressources informatiques                              | 2        |        | Mesures mises en place (démarche qui consiste principalement à réduire à l'indispensable les objets installés sur le système, ainsi qu'à éliminer les utilisateurs et les droits non indispensables, tout en conservant les fonctionnalités requises.) |
| – Sauvegardes et restauration  | 1        |        | Dispositif, fréquence, tests...  |
| – Gestion des correctifs de sécurité                                     | 3        |        | Mise à jour de sécurité, automatique, liste de diffusion   |
| – Lutte contre les codes malveillants                                    | 5        |        | Anti-virus, parefeu logiciel, anti spam ....   |
| – Administration des SI  | 1        |        | Qui est responsable de l’administration des systèmes d'information?  |
| Sécurité des communications  |          |        |  |
| – Politique de sécurité des communications                               | 1        |        | Existence, date de mise à jour, références...  |
| – Sécurisation des transmissions de données                              | 3        |        | Dispositif de chiffrement, méthode, canaux ...   |
| – Accès à distance aux SI  | 1        |        | Par quels moyens, avec quelles protections ?   |
| – Accès au réseau interne depuis des équipements non maîtrisés           | 1        |        | Le cas échéant (oui /non)  |
| Maintenance des SI   |          |        |  |
| – Maintien du niveau de sécurité des SI                                  | 1        |        | Comment, Qui, procédure ?  |
| – Sécurité de la maintenance des SI                                      | 2        |        | Qui maintient, Comment, quelle procédure et/ou dispositif de sécurité ?  |
| – Mise au rebut  | 3        |        | Procédure, destruction des supports  |
| Relation avec les tiers  |          |        |  |
| – Gestion de la sécurité avec les sous-traitants                         | 3        |        | Vérification d'un niveau de sécurité au moins équivalent   |
| Gestion des incidents et des alertes                                     |          |        |  |
| – Veille et gestion des vulnérabilités techniques                        | 1        |        | Matériel et logiciel, inscription aux listes, diffusion des CVE...   |
| – Détection et dispositif de gestion des incidents                       | 1        |        | Comment, qui, où ?   |
| – Journalisation des incidents et des alertes                            | 1        |        | Comment, qui, procédure ?  |
| – Gestion de crise   | 1        |        | Procédure, dispositif  |
| Gestion de la continuité d’activité                                      |          |        |  |
| – Définition, mise en œuvre et maintien du plan de continuité d’activité | 1        |        | Existence, qui, fréquence ?  |
| – Protection des données de sauvegarde                                   | 2        |        | Lieu d'entrepôt, sauvegardes déconnectées...   |
| Mise à jour des systèmes et logiciels                                    |          |        |  |
| – Sécurité des postes de travail   | 5        |        | Mise à jour de sécurité, automatique, liste de diffusion   |
| – Utilisation de terminaux personnels (BYOD)                             | -3       |        | oui/non, mesures de protection   |
| – Privilèges des utilisateurs sur les postes de travail                  | 3        |        | Compte administrateur, droits étendus...   |
| – Stockage des informations  | 1        |        | Comment, où ?  |
| – Protection des données critiques                                       | 1        |        | Comment, où ?  |
| – Configuration du navigateur internet                                   | 1        |        | limitations, sécurisations   |
| Gestion de la documentation  |          |        |  |
| – Référentiel documentaire   | 1        |        | Existence d'une documentation de référence ? Quels accès   |
| – Gestion de la documentation  | 1        |        | qui, comment ?,avec un focus sur les documents en sensible identifié diffusion restreinte et secret  |
| Contrôle et évaluation   |          |        |  |
| – Contrôles récurrents de conformité à la PSSI                           | 2        |        | Qui, fréquence ?   |
| – Audits ponctuels de conformité à la PSSI                               | 2        |        | Qui, fréquence ?   |
| Organisation de la sécurité  | 1        |        | Description sommaire des rôles et fonctions  |
|  |          |        |  |
| Responsabilités liées au PAS   | 1        |        | Comment sont elles prises en compte et gérées  |
|  |          |        |  |
| Procédures d’évolution du PAS  | 1        |        | Comment sont elles prises en compte et gérées  |
|  |          |        |  |
| Mesures de sécurité  | 1        |        | Comment sont elles prises en compte et gérées  |