Domaine d'activité 3 : Cybersécurité des services informatiques

La sécurité des services informatiques constitue un enjeu économique important.

La personne titulaire du diplôme participe à la mise en œuvre d'une politique de cybersécurité définie par le prestataire informatique et à son intégration dans la politique de sécurité de l'organisation.

En lien avec les besoins métiers de l'organisation et de sa transformation numérique, il s'agit de répondre à l'exigence de sécurité du système d'information en prenant en compte toutes ses dimensions (technique, organisationnelle, humaine, juridique, réglementaire).

En fonction de la spécialité du diplôme, la personne titulaire participe à la sécurité des solutions d'infrastructure ou à la sécurité des solutions applicatives et de leur développement.

Activités de tronc commun

Activité 3.1. Protection des données à caractère personnel

- Recensement des traitements sur les données à caractère personnel au sein de l'organisation
- Identification des risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel
- Application de la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
- Sensibilisation des utilisateurs à la protection des données à caractère personnel

Activité 3.2. Préservation de l'identité numérique de l'organisation

- Protection de l'identité numérique d'une organisation
- Déploiement de moyens appropriés de preuve électronique

Activité 3.3. Sécurisation des équipements et des usages des utilisateurs

- Information des utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promotion des bons usages à adopter
- Identification des menaces et mise en œuvre des défenses appropriées
- Gestion des accès et des privilèges appropriés
- Vérification de l'efficacité de la protection

Activité 3.4. Garantie de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

- Caractérisation des risques liés à l'utilisation malveillante d'un service informatique
- Recensement des conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité
- Identification des obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation
- Organisation de la collecte et de la conservation de la preuve électronique
- Application des procédures garantissant le respect des obligations légales

Option A « Solutions d'infrastructure, systèmes et réseaux »

Activité A3.5. Cybersécurisation d'une infrastructure réseau, d'un système, d'un service

- Vérification des éléments contribuant à la sûreté d'une infrastructure informatique
- Prise en compte de la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure
- Mise en œuvre et vérification de la conformité d'une infrastructure à un référentiel, une norme ou un standard participant à la sécurité
- Prévention des attaques
- Détection des actions malveillantes
- Analyse d'incidents de sécurité, proposition et mise en œuvre de contre-mesures

Conditions d'exercice

La personne titulaire du diplôme participe à la mise en œuvre de la politique de sécurité de l'organisation en prenant en compte les enjeux éthiques et déontologiques.

Elle contribue à la protection des données de l'organisation, à la sensibilisation des utilisateurs aux usages et à la sécurisation de leurs accès aux services informatiques.

Elle applique les procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle.

En fonction de sa spécialité, elle est en mesure :

- de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements des serveurs, des services et des terminaux traitants ;
- d'appliquer les recommandations de sécurité dans le développement d'une application informatique.

Elle participe à la détection, à l'investigation et à la réponse aux incidents de sécurité dans son domaine d'expertise.

Ressources et moyens mis à disposition	**Relations**
Description de l'organisation : son métier, ses processus, ses acteurs et son système d'information. Description du prestataire informatique et des modalités de gestion du système d'information. Description du système informatique. Référentiels, normes et méthodes adoptés au sein de l'organisation. Réglementation, normes et standards du secteur informatique. Contrat de prestation de service. Environnement de production opérationnel. Cahier des charges fourni par l'organisation cliente (avec les spécifications fonctionnelles et éventuellement techniques du service à concevoir). Logiciel de gestion d'incidents.	<u>Relations internes</u> Direction de l'organisation Membres de l'équipe du prestataire informatique Utilisateurs Fraudeurs internes <u>Relations externes</u> Organisation cliente Entreprises de services du numérique Éditeurs de logiciels Fournisseurs de services d'informatique en nuage (*cloud)* Fournisseurs d'équipements informatiques Organisations en charge de la sécurité des systèmes d'information Police et justice Fraudeurs externes

Résultats attendus

Application des règles déontologiques participant à la sécurité et des chartes en vigueur.

Respect de la législation en vigueur concernant la protection des données à caractère personnel.

Utilisateurs sensibilisés à la politique de sécurité.

Politique de sécurité de l'organisation respectée en matière de protection :

- des données à caractère personnel et des données de l'organisation ;
- des identités numériques ;
- des ressources numériques ;
- des accès utilisateurs.

Gestion des incidents de sécurité dans les délais.

Selon la spécialité :

- les solutions d'infrastructure systèmes services et réseaux sont sécurisées ;
- les solutions applicatives et leur développement sont sécurisés.

En termes de comportement et de communication

- Savoir anticiper, gérer des priorités et faire preuve de sang-froid.
- Être capable de collaborer au sein d'une équipe d'informaticiens et d'échanger avec les utilisateurs, les clients et les partenaires.
- Avoir l'esprit d'initiative et être autonome dans ses actions.
- S'adapter à des situations complexes, sous contraintes.
- Avoir une communication écrite et orale adaptée avec les acteurs internes et externes :
  - rendre compte synthétiquement des actions entreprises et des réalisations ;
  - adapter sa communication aux différents types d'interlocuteurs ;
  - respecter les règles de confidentialité.
- S'impliquer dans l'actualisation de ses connaissances professionnelles et se former si nécessaire.
- Savoir transférer la gestion des risques à un tiers de confiance (assurance, sous-traitance).