Bloc de compétences n°3 - Cybersécurité des services informatiques

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités pour répondre aux besoins de sécurité des services informatiques d'une organisation cliente notamment au regard du développement des menaces et attaques en provenance du cybermonde et des risques liés aux usages numériques. Elle travaille pour le compte de l'entité informatique interne à une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.

Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.

La personne titulaire du diplôme participe à la mise en œuvre de l'environnement technologique nécessaire à la sécurité des services informatiques.

Ressources

- Description de l'organisation cliente : son métier, le caractère sensible des activités conduites, ses processus, ses acteurs (internes et externes) et son système d'information.
- Description du prestataire informatique de l'organisation cliente : ses compétences, ses méthodes, ses outils, ses procédures et ses référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité et de sûreté.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisées dans le cadre de la mise à disposition d'un service sécurisé.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Cahier des charges fourni par l'organisation cliente : spécifications fonctionnelles et éventuellement techniques, définition du périmètre d'intervention, exigences en termes de protection des données, des applications et des équipements.

Degré d'autonomie, responsabilités

La personne titulaire du diplôme participe à la mise en œuvre de la politique de gestion de la sécurité informatique de l'organisation cliente, en veillant à documenter ses actions. Elle travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de cette organisation.

Elle participe notamment à l'information et à la sensibilisation des utilisateurs aux risques en recommandant les pratiques adaptées. Elle contribue à la sécurisation des accès aux services informatiques : protection des accès aux ressources numériques, aux données, aux équipements et aux applications. En fonction de sa spécialité, elle intervient plus particulièrement sur la sécurité des infrastructures ou des développements d'application.

Dans une petite structure, elle peut travailler en autonomie en tenant compte des risques spécifiques identifiés pour l'organisation cliente. Elle prend en charge l'information, la sensibilisation et la formation des utilisateurs aux questions de sécurité informatique.

Dans une structure plus importante, elle travaille au sein d'une équipe en rendant compte de ses activités.

Compétences	**Indicateurs de performance**	**Savoirs associés**
Protéger les données à caractère personnel ▪ Recenser les traitements sur les données à caractère personnel au sein de l'organisation ▪ Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel ▪ Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel ▪ Sensibiliser les utilisateurs à la protection des données à caractère personnel	La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur. La charte informatique contient des dispositions destinées à protéger les données à caractère personnel. Des supports de communication pertinents sont accessibles et adaptés aux utilisateurs. Le recensement des traitements des données à caractère personnel est exhaustif. Des moyens de protection sont mis en place pour garantir la confidentialité et l'intégrité des données à caractère personnel en tenant compte des risques identifiés.	<u>Savoirs technologiques</u> Typologie des risques et leurs impacts. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Sécurité et sûreté : périmètre respectif. Sécurité des terminaux utilisateurs et de leurs données : principes et outils. Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Gestion des droits d'accès aux données : principes et techniques. Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction

Préserver l'identité numérique de l'organisation ▪ Protéger l'identité numérique d'une organisation ▪ Déployer les moyens appropriés de preuve électronique	L'identité numérique de l'organisation est protégée en s'appuyant sur des moyens techniques et juridiques. La preuve électronique est déployée de manière sécurisée et dans le respect de la législation.	physique et logique. Protection et archivage des données : principes et techniques. Chiffrement, authentification et preuve : principes et techniques. Sécurité des applications *Web* : risques, menaces et protocoles. Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.
Sécuriser les équipements et les usages des utilisateurs ▪ Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter ▪ Identifier les menaces et mettre en œuvre les défenses appropriées ▪ Gérer les accès et les privilèges appropriés ▪ Vérifier l'efficacité de la protection	Des supports de communication interne sont accessibles aux utilisateurs et adaptés à leurs destinataires. Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées : - l'accès physique au terminal et à ses données est sécurisé ; - les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ; - les flux réseaux sont identifiés et sécurisés. Les accès et privilèges respectent les règles organisationnelles : - les utilisateurs sont authentifiés ; - les habilitations sont configurées ; - l'accès aux données est contrôlé ; - les privilèges sont restreints. L'efficacité de la protection mise en œuvre est évaluée.	<u>Savoirs économiques, juridiques et managériaux</u> Les données à caractère personnel : définition, réglementation, rôle de la CNIL. L'identité numérique de l'organisation : risques et protection juridique. Droit de la preuve électronique. La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique. Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise. Obligations légales de notification en cas de faille de sécurité. Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions. Les organisations de lutte contre la cybercriminalité.

Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ▪ Caractériser les risques liés à l'utilisation malveillante d'un service informatique ▪ Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité ▪ Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation ▪ Organiser la collecte et la conservation des preuves numériques ▪ Appliquer les procédures garantissant le respect des obligations légales	Les risques associés à l'utilisation malveillante d'un service informatique sont caractérisés. Les conséquences des actes malveillants sur un service informatique sont identifiées. Les obligations légales en matière d'archivage et de protection des données sont identifiées et respectées. Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation. Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées : - un schéma présentant la segmentation du réseau est disponible ; - les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ; - l'authentification et la confidentialité des échanges sont vérifiées ; - la sécurité de l'administration est prise en compte ; - les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ; - les accès aux données sont contrôlés à chaque étape d'une transaction ; - les systèmes et les applications sont actualisés en fonction des alertes de sécurité ; - les vulnérabilités connues sont contrôlées.	

Option SISR **Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service** ▪ Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique ▪ Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure ▪ Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité ▪ Prévenir les attaques ▪ Détecter les actions malveillantes ▪ Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures	Les dispositifs participant à la disponibilité sont validés (les éléments critiques sont résilients, la charge est répartie efficacement, la qualité des services sensibles est assurée). Les failles potentielles sont identifiées grâce à une activité de veille sur les vulnérabilités. Les bonnes pratiques de sécurité sont prises en compte. Les éléments de sécurité de l'architecture sont conformes et documentés. Les exigences de sécurité sont prises en compte dans le projet de mise en en œuvre d'une solution d'infrastructure. Les dispositifs de détection et de protection des attaques sont opérationnels. Les processus de résolution d'un incident ou d'un problème sont respectés. Le compte rendu d'intervention est clair et explicite. Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité Les contre-mesures sont documentées de manière à en assurer le suivi. La communication écrite et orale est adaptée à l'interlocuteur.	<u>Savoirs technologiques</u> Sûreté des infrastructures réseaux : bonnes pratiques, normes et standards. Cybersécurité : bonnes pratiques, normes et standards. Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. Outils de sécurité : prévention et détection des attaques, gestion d'incidents. <u>Savoir économique, juridique et managérial</u> Responsabilité civile et pénale de l'administrateur système et réseau.