|  |  |
| --- | --- |
| **Bloc de compétences 3 Semestre 1** | |
| **Finalité métier :** Le métier de la cybersécurité consiste à répondre aux besoins de sécurité des services informatiques d’une organisation notamment au regard du développement des menaces et attaques en provenance d’internet et des risques liés aux usages numériques.  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.  Le métier implique de respecter la réglementation, les méthodes, les normes et standards qui prévalent dans la législation nationale et internationale ainsi que dans les recommandations des organismes gouvernementaux et professionnels. | **Contexte professionnel** : Vous travaillez pour le compte d’une société de conseil en technologies spécialisée dans la cybersécurité. Rattaché (e) au responsable de la sécurité des systèmes d’information (RSSI) de l’équipe sécurité, vous intervenez auprès des différents clients.  Vous serez chargée ou chargé de :   * Protéger les données à caractère personnel de vos clients * Préserver leur identité numérique * Sécuriser les équipements et les usages des utilisateurs * Veiller à la disponibilité, l’intégrité et la confidentialité des services informatiques |

|  |  |
| --- | --- |
| **3.1. Protéger les données à caractère personnel Semestre 1** | |
| **Votre mission :** Vous participez, avec votre collègue délégué à la protection des données (*Data Protection Officer* ou DPO) à différentes prestations de mise en conformité du règlement général pour la protection des données (RGPD) pour vos entreprises clientes. | **Contexte professionnel** : Vous travaillez pour le compte d’une entreprise de services du numérique (ESN) qui apporte son expertise auprès de ses clients en matière de conformité au règlement européen relatif à la protection des données personnelles afin de sécuriser leur système d’information et de respecter le cadre réglementaire en vigueur. Vous êtes jeune embauché(e) au sein du service informatique. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Séquence 3.1 A1** | **Préparer des séances de sensibilisation et de communication sur les données à caractère personnel (DCP) et leur traitement** | | | |
| Durée totale en heures du scénario pour la séquence  5 h | Votre travail consiste à participer à la conception de supports de sensibilisation exploités lors des réunions de communication RGPD afin de former le personnel impliqué dans les activités de collecte et de traitement des données à caractère personnel. | | | |
| **Compétences travaillées** | **Savoirs associés** | **Indicateurs de performance** | **Prérequis / Transversalités** |
| * 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. | Savoirs économiques, juridiques et managériaux   * Les données à caractère personnel : définition, réglementation, rôle de la CNIL. | * 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. * Des moyens de protection sont mis en place pour garantir la confidentialité et l’intégrité des données personnelles en tenant compte des risques identifiés. | Prérequis :  MOOC RGPD de la CNIL (résultats des évaluations du MOOC).  Transversalité :  Bloc 3 - 3.2. Préserver l’identité numérique de l’organisation. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Séance 1** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 2 h | Le DPO vous fournit le sommaire du contenu du support numérique qui servira à la présentation des concepts de base du RGPD. Il vous demande également de valider le questionnaire et de l’enrichir avec d’autres questions.   1. Élaborer le support de sensibilisation relatif au sommaire. 2. Vérifier et compléter le questionnaire interactif élaboré par le DPO prévu pour évaluer les acquis des utilisateurs. | * Fiches de savoirs relatives au RGPD (ressources CNIL, itgovernance.eu, fiches ANSSI, manuels). * Sommaire du support de communication (*les auteurs préciseront les notions de la réglementation (RGPD) qui devront être abordées* *en fonction de la progression pédagogique de CEJM - thème 4, question 2)*. * Lien du questionnaire interactif (*ce dernier présentera quelques réponses erronées que l’étudiant devra repérer et corriger).* | * Le support de sensibilisation est élaboré (possibilité d’y insérer des vidéos ou des diapositives de vulgarisation du RGPD). * Le questionnaire interactif est testé, corrigé et enrichi avec d’autres questions. |
| **Séance 2** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 2 h | Le DPO vous fournit un kit de ressources de gouvernance RGPD (*exemples de chartes informatiques, formulaires de contact, conditions de recueil de consentements, fiches d’inventaires de données, maquettes d’applications, sites avec utilisation de traceurs, cookies*…) pour initier les utilisateurs à la mise en place du RGPD. Ces ressources seront exploitées pendant la formation pour analyser et vérifier la mise en conformité des règles de collecte et de traitement des données à caractère personnel (DCP). Des éléments d’analyse et de correction devront être fournis aux utilisateurs en fin de séance. Pour chaque cas :   1. Analyser la pertinence des données collectées. 2. Vérifier les conditions de recueil du consentement. 3. Évaluer les éléments RGPD manquants. 4. Apporter les améliorations nécessaires au regard du RGPD. | * Fiches des principes de protection des données (*fiches CNIL, ANSSI, manuels, capsules vidéo*). * Kit de ressources de gouvernance RGPD (*les cas devront mobiliser l’ensemble des règles en matière de collecte et de traitement des DCP et les droits des personnes*). * Rapport d’audit vierge précisant les critères à analyser. * Tableau de synthèse vierge. | * Les écarts entre la pratique dans le cas étudié et les recommandations du RGPD sont diagnostiqués. * Le tableau de synthèse est mis à jour avec les éléments de correction des cas présentés. |
| **Séance 3** | **Tâches à réaliser** | **Ressources fournies** | **Résultats attendus** |
| 1 h | Vous souhaitez sensibiliser les utilisateurs sur la collecte de leurs données numériques et leurs droits sur ces données.  Vous allez vous appuyer sur votre expérience personnelle pour synthétiser les démarches d’exercice de ces droits RGPD dans un diagramme de flux.   1. Tester au préalable votre droit d’accès à vos données auprès d’un organisme (site internet). 2. Exercer au préalable d’autres droits (rectification, effacement, déréférencement…) sur vos données auprès de l’organisme concerné. 3. Télécharger un dossier d’archives de vos publications sur un des réseaux sociaux auxquels vous êtes abonnés. 4. Synthétiser l’exercice de ses droits dans deux diagrammes distincts. | * Fiches de savoirs RGPD (droits des personnes). | * Les rapports des informations demandées sont envoyés par l’organisme sollicité (et *ne seront pas diffusées*). * Un exemple de format des rapports reçus décrit les informations présentes (*éventuellement avec des extraits non significatifs*). * Les diagrammes de flux décrivent le processus d’exercice des droits d’un usager sur ses données à caractère personnel. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.1 B1** | **Accompagner le responsable de traitement des données dans la mise en œuvre du projet RGPD** | | | | | |
| 4 h | Votre travail consiste à accompagner une association sportive qui a fait appel à votre entreprise pour la mise en conformité au RGPD de ses activités et de son site Internet. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * Recenser les traitements sur les données à caractère personnel au sein de l’organisation. * Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel. | Savoirs technologiques   * Typologie des risques et leurs impacts. * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.   Savoirs économiques, juridiques et managériaux   * Les données à caractère personnel : définition, réglementation, rôle de la CNIL. | | * La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur. * Le recensement des traitements des données à caractère personnel est exhaustif. | | Prérequis :  Séquence 3.1 A1  Transversalités :  Bloc 1 - 1.1. Gérer le patrimoine informatique.  Bloc 1 - 1.2. Répondre aux incidents et aux demandes d’assistance et d’évolution.  Bloc 3 - 3.2. Préserver l’identité numérique de l’organisation.  B3.3. Sécuriser les équipements et les usages des utilisateurs. |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2 h | Vous accompagnez la personne habilitée à traiter les DCP dans le processus de recensement des activités et des données, y compris celles collectées hors du site internet.   1. Recenser les données personnelles collectées hors du site internet. 2. Identifier les données collectées sur le site (formulaire de contact, d’inscription…). 3. Identifier les acteurs internes ou externes qui traitent et/ou hébergent ces données. 4. Remplir le registre de traitements selon le modèle numérique fourni par votre collègue DPO. | | * Fiches de savoirs relatives au traitement des données personnelles (CEJM/A). * Modèle de fiche de registre des DCP (*modèle de registre simplifié fourni par la CNIL adapté au contexte*). * Site Internet de l’entreprise cliente. * Synthèse des entretiens, fiches d’inscription papier. | | * Le registre de traitements est mis à jour (fiche de registre par activité). | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2 h | Votre collègue DPO a analysé le registre de traitement des données réalisé par vos soins et complété par le responsable de traitement. Il a élaboré une liste de vérifications à effectuer sur le site Internet du client pour évaluer sa conformité aux exigences RGPD en matière de collecte et de traitement des DCP.   1. Effectuer les vérifications demandées. 2. Proposer un plan d’action de mise en conformité RGPD. | | * Fiches de savoirs RGPD (DCP et les conditions de leur traitement). * Liste des points de vigilance (*charte informatique, informations claires aux personnes, respect du droit de la personne, politique de confidentialité, mentions légales*…). | | * Les résultats des vérifications demandées sont transcrits dans un rapport d’analyse. * Le plan d’action liste les mesures d’amélioration au regard des objectifs du RGPD. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Séquence 3.1 C1** | **Évaluer le niveau de sécurité des données personnelles de l’entreprise cliente et apporter des mesures correctives à l’AIPD** | | | | | |
| 8 h | Rattaché au RSSI junior de l’équipe sécurité, vous intervenez auprès de votre client PME (15 salariés) pour apprécier les risques liés à la sécurité des données à caractère personnel qui peuvent impacter la vie privée des utilisateurs (*Privacy Impact Assessment – PIA ou Analyse d’Impact relative à la Protection des Données - AIPD*).  Vous êtes également chargé d’accompagner la personne responsable de traitement pour corriger certaines vulnérabilités. | | | | | |
| **Compétences travaillées** | **Savoirs associés** | | **Indicateurs de performance** | | **Prérequis / Transversalités** |
| * 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. | Savoirs technologiques   * Typologie des risques et leurs impacts. * Sécurité et sûreté : périmètre respectif. * Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.   Savoirs économiques, juridiques et managériaux   * Les données à caractère personnel : définition, réglementation, rôle de la CNIL. | | * 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. * 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 personnelles en tenant compte des risques identifiés. | | Prérequis :  Séquence 3.1 A1.  Etude de cas traitant de l’AIPD en CEJM/A (Ex : Captoo de la CNIL).  Bloc 1 - 1.4. Travailler en mode projet.  Transversalités :  Bloc 1 - 1.1. Gérer le patrimoine informatique.  Bloc 1 - 1.2. Répondre aux incidents et aux demandes d’assistance et d’évolution.  Bloc 3 - 3.2. Préserver l’identité numérique de l’organisation.  Bloc 3 - 3.3. Sécuriser les équipements et les usages des utilisateurs. |
| **Séance 1** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2 h | Afin d’évaluer l’efficacité des mesures techniques mises en œuvre au sein de l’entreprise pour assurer la sécurité des DCP et leur traitement, le responsable RSSI s’appuie sur la fiche de contrôles recommandés par la CNIL et le PIA réalisé par le responsable de traitement pour élaborer un plan de tests.  Pour chacune des mesures prises par le responsable de traitement, le RSSI a détaillé les vérifications à effectuer pour valider sa conformité au règlement. Une planification de la répartition de ces contrôles est réalisée dans l’outil de gestion de projet collaboratif de votre entreprise.   1. Prendre en charge les activités de contrôle qui vous incombent. 2. Évaluer l’efficacité de la mesure en fonction du résultat attendu. | | * Fiches de savoirs relatives au RGPD (appréciation des risques potentiels, AIPD). * Planning de répartition des contrôles à effectuer. * Tableau des tests à réaliser par fiche de mesures. * Document numérique de l’évaluation du niveau de sécurité des données personnelles fournie par la CNIL adapté au contexte (*pour chaque mesure prise en charge, une liste de contrôles sera proposée, leur degré de complexité devra tenir compte de la progression du bloc 1 et des apports en CEJMA*). * Infrastructure de l’entreprise (schéma réseau, machines virtuelles postes clients et serveurs web/bases de données/sauvegarde) et identifiants d’accès aux différentes machines et services. | | * Le tableau de bord des tâches est mis à jour. * Le document numérique d’évaluation de l’efficacité des mesures de sécurité des données personnelles est mis à jour. | |
| **Séance 2** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 4 h | À partir de l’analyse précédente, un plan d’action a été élaboré et une liste de mesures correctives a été planifiée dans l’outil de gestion de projet.   1. Réaliser les corrections qui vous sont attribuées pour améliorer les mesures protectrices de la vie privée des personnes. 2. Tester les corrections apportées. | | * Infrastructure de l’entreprise. * Plan d’action. * Fiches d’aide à la correction de certaines mesures (*les mesures correctives peuvent porter sur la sécurité des postes de travail et de l’informatique mobile, la gestion des habilitations, la journalisation des accès, l’authentification renforcée des utilisateurs, les sauvegardes, la mise en place de la journalisation des accès, la suppression ou la désactivation de comptes obsolètes …)* | | * Les corrections demandées sont effectuées. * Le document numérique d’évaluation de l’efficacité des mesures de sécurité de la vie privée est mis à jour suite aux corrections réalisées. | |
| **Séance 3** | **Tâches à réaliser** | | **Ressources fournies** | | **Résultats attendus** | |
| 2 h | Le responsable de traitement vous demande de mettre à jour la copie de l’AIPD qu’il vous fournit suite aux mesures correctives que vous avez mises en place.   1. Installer l’outil AIPD. 2. Importer le fichier dans l’outil AIPD. 3. Mettre à jour le document. 4. Exporter le document dans le format souhaité par le responsable de traitement. | | * Fichier d’analyse d’impact relative à la protection des données (AIPD) de l’entreprise. * Outil AIPD. | | * L’outil AIPD est installé et configuré. * L’analyse d’impact relative à la protection des données est mise à jour et validée par le RSSI. * L’AIPD est exportée au format exigé par le responsable de traitement. | |