En cours de validation

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail
Direction Recherche et Ingénierie De Formation
Centre de Développement des Compétences en Digital,
Intelligence Artificielle, Audiovisuel et Cinéma

Secteur Digital & Intelligence Artificielle

Filière : Infrastructure Digitale

Option Cybersécurité

PROGRAMME DE FORMATION

Version 3

10/08/2022

Filière : Infrastructure Digitale – Option Cybersécurité

Programme de formation, version 3 (10/08/2022)

Équipe de production

Coordination

Mohamed SLIMANI	Directeur CDC Digital, IA, Audiovisuel et Cinéma
Saïda BOUDIAF	Coordonnateur WebForce 3

Conception et rédaction

Fattoum MIHOUBI	Cheffe de projet pédagogique
Jonathan CROUZOULON	Chef de projet pédagogique
Mhamed MOURABIT	Expert technique
Dirane TAFEN	Expert technique

Suivi des versions

Version	Auteur	Date	Modifications
1.0	CDC Digital & IA	21/04/21	Draft sur canevas
1.0	WebForce 3	23/08/2021	Version 1 du programme de formation
1.1	WebForce 3	03/09/2021	Mise à jour du programme de formation suite aux dernières recommandations du CDC
1.2	CDC Digital & IA / Webforce 3	24/09/2021	Validation des compétences 1, 2 et 3 + élaboration de toutes les autres compétences du tronc commun (Compétences 4 à 8)
2	CDC Digital & IA / Webforce 3	29/09/2021	Validation des compétences du Tronc commun
3	Webforce 3	29/07/2022	Rédaction de l'option Cybersécurité

Remerciements

La production du présent document a été possible grâce à la collaboration et à la participation de nombreuses personnes, que ce soient des professionnels du métier ou des formateurs.

Il y a lieu de souligner la qualité des renseignements fournis par les personnes consultées à titre de professionnels du domaine de « Infrastructure Digitale » et de remercier particulièrement celles qui ont généreusement accepté de partager leur expérience du métier de technicien spécialisé en Filière : Infrastructure Digitale – Option Cybersécurité et celles qui ont participé à la validation de ce Projet de formation.

Par ailleurs, les travaux de l'équipe de production se sont déroulés en alternance dans les locaux du Centre des Compétences Digital et IA. L'équipe tient à remercier les directeurs ainsi que leur personnel pour leur accueil et leur soutien tout au long des travaux.

Table des matières

Acronymes

AST	Analyse en Situation de Travail
RM	Référentiel de Métier
APC	Approche Par Compétences
OFPPT	Office de la Formation Professionnelle et de la Promotion du Travail
SLA	Service Level Agreement
KPI	Key Performance Indicator
RGPD	Règlement général sur la protection des données
SI	Système d'information
NHT	Non Humain Trafic
OSSEC	Open Source HIDS SECurity (Système de détection d'intrusion gratuit et open source)
IA	Intelligence artificielle
NIST	National Institute of Standards and Technology
CSIRT	Computer Security incident Response Team
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
SHA	Secure Hash Algorithm
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
DGSSI	Direction Générale de la Sécurité de Systèmes d'Information
maCERT	Marocain Computer Emergency Response Team
UDP	User Datagram Protocol
SNMP	Simple Network Management Protocol

LAN	Local Area Network
WAN	Wide Area Network
IDE	Investissements directs à l'étranger
VLAN	Virtual Local Area Network
ACL	Access Control List
OSPF	Open Shortest Path First
EIGRP	Enhanced Interior Gateway Routing Protocol
RIP	Routing Information Router
OS	Operating System
MDT	Microsoft Deployment Toolkit
SSH	Secure Shell
HTTPS	HyperText Transfer Protocol Secure
SCCM	System Center Configuration Manager
WDS	Windows Deployment Service
ADDS	Active Directory Domain Service
SIEM	Security Information and Event Management
SEM	Security Event Management
SIM	Security Information Management
PRA	Plan de Reprise d'Activité
OSI	Open Systems Interconnection
TCP/IP	Transmission Control Protocol/Internet Protocol
DNS	Domain Name System
DCHCP	Dynamic Host Configuration Protocol

WSRM	Windows System Resource Manager
DMZ	Demilitarized Zone
Triangle CIA	Triangle : Confidentiality, Integrity, Availability
VPN	Virtual Private Network
SGBD	Système de Gestion de Base de Données
ISO	International Organization for Standardization
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
SOC	Security Operations Center
DevSecOps	Development - Security - Operations
PTES	Penetration testing execution standard
OSSTMM	Open Source Security Testing Methodology Manual
APT	Advanced Persistent Threat
CIS	Center for Internet Security
ANSSI	Agence nationale de la sécurité des systèmes d'information
UTM	Unified threat management
LLMNR	Link-local Multicast Name Resolution
WPAD	Web Proxy Auto-Discovery
TLS	Transport Layer Security
DLP	Data Loss Prevention
OWASP	Open Web Application Security Project
STRIDE	Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges

EBIOS	Expression des besoins et identification des objectifs de sécurité

Présentation du programme de formation

Le programme de formation Filière : Infrastructure Digitale – Option Cybersécurité s'inscrit dans les orientations retenues par le Département de la Formation Professionnelle, concernant la formation professionnelle. Il a été conçu suivant le Cadre méthodologique d'élaboration et de mise en œuvre des programmes de formation selon l'Approche Par Compétences qui exige, notamment, la participation conjointe des milieux du travail et de la formation.

Le programme de formation est défini par compétences, formulé par objectifs et structuré en modules. Il est conçu selon une approche globale qui tient compte à la fois de facteurs tels les besoins de formation, la situation de travail, les finalités, les buts ainsi que les stratégies et les moyens pour atteindre les objectifs.

Dans le programme de formation, on énonce et structure les compétences que le participant doit acquérir pour obtenir son Attestation de Poursuite de la Formation Filière : Infrastructure Digitale – Option Cybersécurité. Ce programme de formation doit servir de référence pour la planification de la formation et de l'apprentissage ainsi que pour la préparation du matériel didactique et du matériel d'évaluation.

La durée du programme de formation est de 1420 heures ; de ce nombre, 1240 heures sont consacrées à l'acquisition de compétences spécifiques et 180 heures à l'acquisition de compétences transversales. Le programme de formation est divisé en 15 modules dont la durée varie de 15 à 160 heures. Cette durée comprend le temps requis pour l'évaluation des apprentissages aux fins de l'obtention de L´attestation de Poursuite de la Formation.

Ce programme de formation a été élaboré en 2021.

NB : l'usage du masculin, dans le présent document, n'a pour but que d'alléger le texte pour en faciliter la lecture.

Conditions d'accès au programme de formation

Code : DIA_ID_TS

« Filière : Infrastructure Digitale – Option Cybersécurité »

Année d'approbation : 2021

Type de sanction : Formation Diplômante

Nombre d'unités : 94

Nombre de modules : 15

Durée totale : 1420 heures

Pour être admis au programme « Filière : Infrastructure Digitale – Option Cybersécurité »**, il suffit de satisfaire aux conditions suivantes :**

- Être bachelier scientifique ou technique ;
- Etude de dossier.

Le concours, pour ceux qui sont admissibles, est composé d'une entrevue permettant de vérifier :

- La motivation du candidat pour la formation ;
- La capacité du candidat à comprendre et à parler le français.

PREMIERE PARTIE

Tableau synthèse du programme de formation

Nombre de modules : 15

Code du programme : DIA_ID_TS

Durée en heures : 1420 heures

Niveau : BAC+2

Valeur en unités : 94

Code	Numéro	Compétence	Durée (heures)
DIA_ID_TS-01	1	Se situer au regard du métier et de la démarche de formation	**15**
DIA_ID_TS-02	2	Comprendre les enjeux d'un système d'information	**75**
DIA_ID_TS-03	3	Concevoir un réseau informatique	**120**
DIA_ID_TS-04	4	Maîtriser le fonctionnement d'un système d'exploitation client	**135**
DIA_ID_TS-05	5	Gérer une infrastructure virtualisée	**105**
DIA_ID_TS-06	6	Automatiser les tâches d'administration	**105**
DIA_ID_TS-07	7	Sécuriser un système d'information	**90**
DIA_ID_TS-08	8	Développer une veille technologique	**75**
DIA_IDOCS_TS-09	9	S'initier aux fondamentaux de la cybersécurité	**75**
DIA_IDOCS_TS-10	10	Appliquer les méthodologies des tests d'intrusions	**105**
DIA_IDOCS_TS-11	11	Analyser les attaques et les incidents de cybersécurité	**105**
DIA_IDOCS_TS-12	12	Assurer le durcissement de la sécurité des systèmes et réseaux informatiques	**90**
DIA_IDOCS_TS-13	13	Appréhender les méthodes d'investigation numérique	**90**

DIA_IDOCS_TS-14	14	Appliquer des stratégies de gestion des risques	**90**
DIA_IDOCS_TS-15	15	S'intégrer en milieu professionnel	**160**
Total en Heures			**715**

Buts du programme de formation

Le programme «Filière : Infrastructure Digitale – Option Cybersécurité» vise à former des personnes aptes à gérer une équipe de production, contrôler l'exécution et les réalisations des tâches, faire appliquer/exécuter les règles et les procédures en vue d'atteindre les objectifs de production, mettre en œuvre des actions d´améliorations et en assurer le suivi et tout en garantissant le respect des consignes de sécurité et des exigences de productivité et de qualité.

Le programme prépare également les participants à assumer le bon fonctionnement de l'unité de production dont ils auront la responsabilité. Il intervient au niveau des opérateurs pour faire respecter les procédures productivité et de sécurité.

Le profil en «Filière : Infrastructure Digitale – Option Cybersécurité» exerce son métier dans des entreprises du secteur de l'informatique Toutefois, sa formation doit pouvoir l'amener à travailler dans d'autres secteurs d'activités.

La polyvalence des participants est assurée par le développement de compétences transversales. Ce sont celles qui concernent l´hygiène, santé et sécurité en milieu de travail, l'utilisation d'un poste de travail informatique, la gestion de temps et des priorités, la résolution de problèmes, la gestion des approvisionnements, les soft skills ainsi que la communication.

La maîtrise des tâches professionnelles liées au métier est quant à elle assurée par l'acquisition des compétences managériales propres au métier. Ce sont celles qui concernent la gestion d'équipe, la mise en œuvre de système de maintenance, la gestion des projets ainsi que la mise en œuvre des actions d´améliorations continues.

Conformément aux buts généraux de la formation professionnelle, le programme «Filière : Infrastructure Digitale – Option Cybersécurité» vise à :

1. **Rendre la personne efficace dans l'exercice d'une profession ou d'un métier, soit :**

    - Lui permettre de jouer les rôles, d'exercer les fonctions et d'exécuter des tâches et des activités associées à une profession ou un métier ;
    - Lui permettre d'évoluer adéquatement dans un milieu de travail ;

- Lui permettre de développer des habiletés intellectuelles et techniques qui entraînent des choix judicieux ;
- Lui permettre de développer une préoccupation constante de la santé et de la sécurité au travail.

2. Assurer l'intégration de la personne à la vie professionnelle, soit :

- Lui permettre de connaitre le marché du travail en général ;
- Lui permettre de connaitre le contexte particulier de la profession choisie.

3. Favoriser l'évolution de la personne et l'approfondissement de savoirs professionnels, soit :

- Lui permettre de développer son autonomie et sa capacité d'apprendre ainsi que d'acquérir des méthodes de travail ;
- Lui permettre de comprendre les principes sous-jacents aux techniques et aux technologies utilisées ;
- Lui permettre de développer sa faculté d'expression, sa créativité, sons sens de l'initiative et son esprit d'entreprise ;
- Lui permettre d'adopter des attitudes essentielles à son succès professionnel, de développer son sens des responsabilités et de viser l'excellence.

4. Favoriser la mobilité professionnelle de la personne, soit :

- Lui permettre d'adopter une attitude positive à l'égard des changements ;
- Lui permettre de se donner des moyens pour gérer sa carrière.

Matrice des compétences

La matrice des compétences met en évidence les compétences générales (portent sur des activités communes à plusieurs tâches ou à plusieurs situations), les compétences spécifiques (portent sur des tâches et des activités directement liées au métier ou à la profession) ainsi que les grandes étapes du processus de travail.

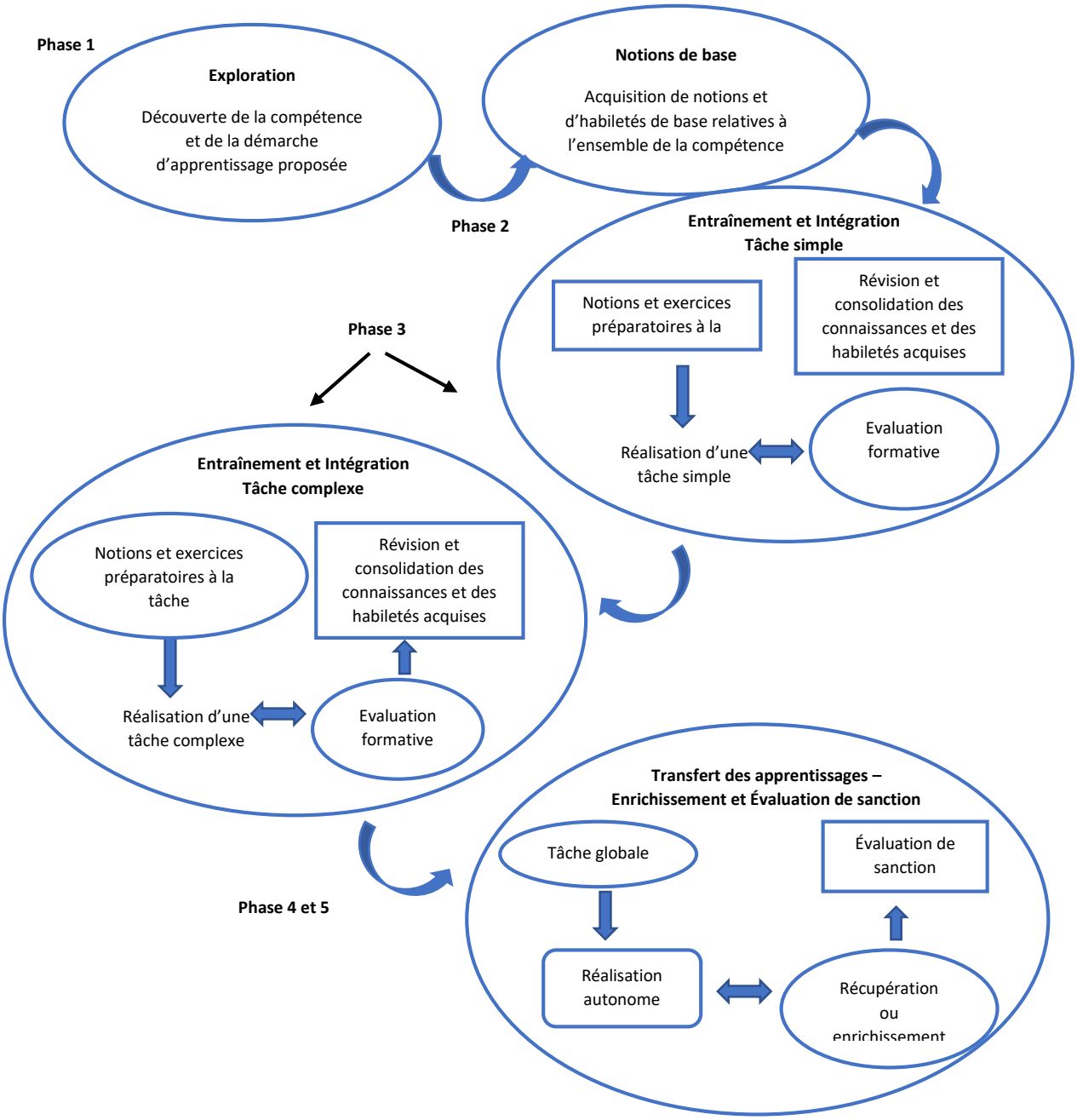
Le tableau est à trois entrées permettant de voir les liens qui unissent les éléments placés à l'horizontale (compétences transversales) et ceux placés à la verticale (compétences spécifiques). Le symbole △ montre qu'il existe une relation entre une compétence spécifique et une étape du processus de travail. Le symbole O marque quant à lui un rapport entre une compétence transversale et une compétence spécifique. Des symboles noircis ●▲indiquent en plus que l'on tient compte de ces liens dans la formulation d'objectifs visant l'acquisition des compétences spécifiques.

La logique qui a présidé à la conception de la matrice influe sur la séquence d'enseignement de ces modules. De façon générale, on prend en considération une certaine progression dans la complexité des apprentissages et le développement de l'autonomie du participant. De ce fait, les compétences spécifiques sont présentées dans l'ordre à privilégier pour l'enseignement et servent de point de départ pour l'agencement de l'ensemble des modules. Certains deviennent ainsi préalables à d'autres ou doivent être vus en parallèle.

Infrastructure Digitale - Option Cybersécurité		DUREE	PROCESSUS (Grandes étapes)						COMPÉTENCES TRANSVERSALES				TOTAUX
MATRICE DES OBJETS DE FORMATION			Situer le contexte du client	Valider le cahier des charges technique	Procéder aux opérations	Surveiller le système	Analyser les risques	Rédiger des rapports	Se situer au regard du métier et de la démarche de formation	Développer une veille technologique	Appréhender les méthodes d'investigation numérique	NOMBRE DE COMPÉTENCES	DUREE DE LA FORMATION
N°	NUMEROS								1	8	13	« Nb comp »	3
	Durée	h							15	75	90		180
2	Comprendre les enjeux d'un système d'information	75		△	△	△	▲		○		●		
3	Concevoir un réseau informatique	120		△	△	▲		▲	○	○	●		
4	Comprendre le fonctionnement d'un système d'exploitation	135		△	△	▲		▲	○		●		
5	Gérer une infrastructure virtualisée	90	△	△	△	▲		▲	○		●		
6	Utiliser la programmation pour les tâches d'administration	105	△	△	△	▲		▲	○	○	●		
7	Sécuriser un système d'information	90	▲	▲	▲	▲	▲	▲	○	●	●		
9	S'initier aux fondamentaux de la cybersécurité	75	▲	△	▲	▲	▲	▲	○	○	○		
10	Appliquer les méthodologies des tests d'intrusions	105	▲	△	▲	▲	▲	▲	○	○	○		
11	Analyser les attaques et les incidents de cybersécurité	105	▲	△	▲	▲	▲	▲	○	○	○		
12	Assurer le durcissement de la sécurité des systèmes et réseaux informatiques	90	▲	△	▲	▲	▲	▲	○	○	○		
14	Appliquer des stratégies de gestion des risques	90	▲	△	▲	▲	▲	▲	○	○	○		
15	S'insérer en milieu professionnel	160	△	△	△	△	△	△	●	●	●		
NOMBRE DE COMPETENCES		12										« Nb comp »	15
DUREE DE LA FORMATION		1240											1420

Phases d'acquisition d'une compétence

Pour favoriser l'atteinte des objectifs, il est suggéré de structurer les apprentissages de façon progressive, c'est-à-dire d'avoir recours à des activités d'apprentissage, d'évaluation formative, d'enseignement correctif ou d'enrichissement, selon le cas. Le processus d'acquisition de compétences est illustré par les schémas ci-dessous.



Rôle du formateur en Approche Par Compétences

Le formateur doit adapter son enseignement en tenant compte :

- D'une approche intégrée des objets de formation ;
- Du rythme individuel et de la façon d'apprendre des participants ;
- D'une responsabilité accrue des participants au regard de leurs apprentissages ;
- Du vécu professionnel des participants.

Pour exercer pleinement leur rôle, le formateur doit :

- Planifier et organiser leur enseignement ;
- Informer les participants ;
- Effectuer de l'animation pédagogique ;
- Evaluer les apprentissages.

Planification et organisation de l'enseignement

Cette fonction consiste tout d'abord à situer les modules dont il a la responsabilité et ensuite, à l'aide du logigramme de la séquence d'enseignement :

- Ajouter ou ajuster, au besoin, les phases préalables et les éléments du contenu ;
- Prévoir et produire des activités propres à ces modules ;
- Coordonner des activités d'apprentissage pour les participants ;
- Répartir les postes de travail et le matériel nécessaire ;
- Agencer et élaborer des activités d'apprentissage, d'évaluation, d'enseignement correctif et d'enrichissement.

Information au participant

Cette autre fonction consiste à :

- Situer les participants par rapport à l'ensemble du programme et, aussi, par rapport au module en cours ;
- Fournir aux participants les données utiles à une compréhension suffisante des tâches reliées au métier ;
- Faire ressortir l'importance et la pertinence des apprentissages à réaliser.

Note : Il revient à chaque formateur de situer les participants par rapport à l'ensemble de leur formation et de les stimuler dans leurs apprentissages et de leur fournir, au début de chaque cours et de chaque activité importante, les données nécessaires à ces fins.

Animation pédagogique

Le formateur doit :

- Guider les apprentissages par un rappel des objectifs, par la détermination des phases préalables et par la formulation d'indications sur les activités à réaliser ;
- Créer un climat de confiance reposant sur le respect des personnes et de leur autonomie, ainsi que sur la clarification des enjeux réels ;
- Maintenir l'intérêt des participants tout au long de leur cheminement par des propositions d'activités intéressantes et diversifiées, par un dosage judicieux du niveau de difficulté, par l'utilisation d'approches à caractère pratique et par une ouverture aux préoccupations personnelles des participants ;
- Encadrer les activités d'apprentissage par l'implantation d'un système souple et efficace de suivi des participants, par une assistance particulière aux participants en difficulté et par une direction adéquate des participants vers des activités d'apprentissage, d'évaluation, d'enseignement correctif et d'enrichissement ;
- Fournir des explications claires et justes au groupe et à chaque participant.

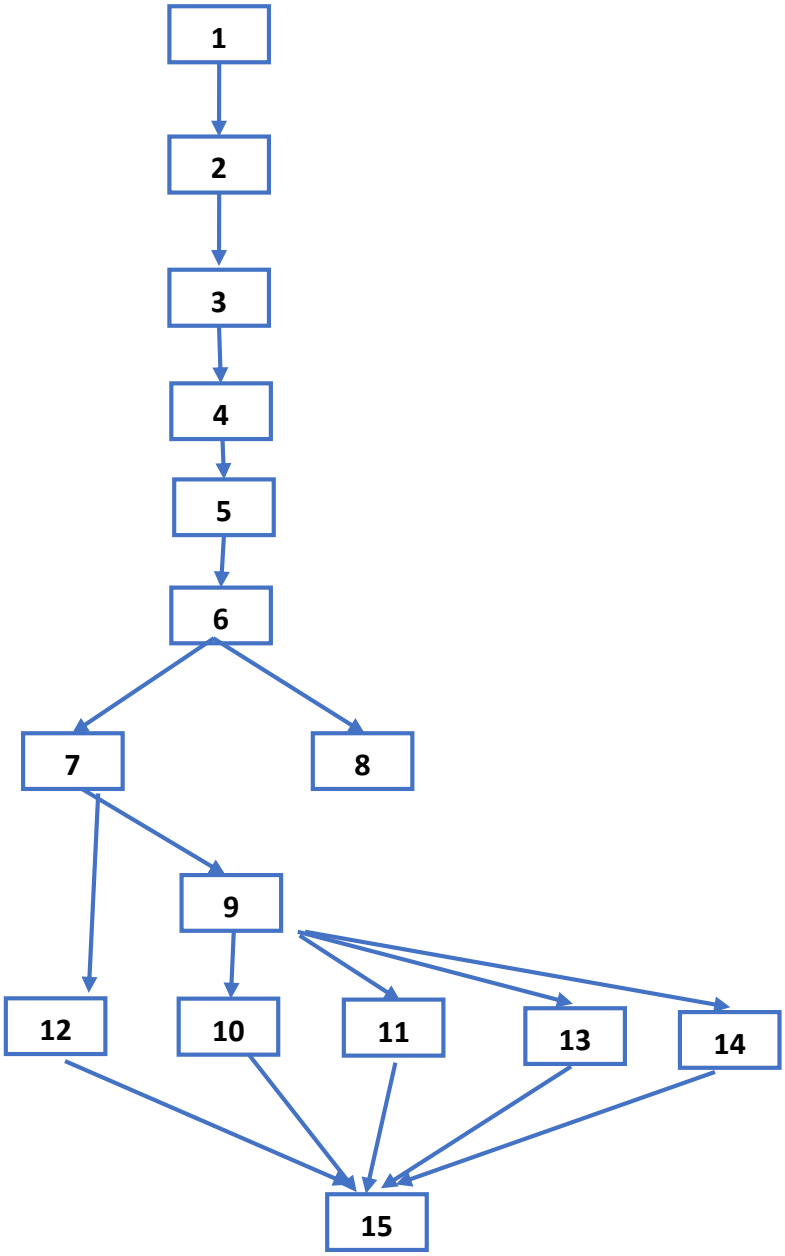
Évaluation des compétences

Le formateur assure le suivi mentionné précédemment :

- En produisant et en utilisant des instruments d'évaluation formative afin de guider le participant dans son cheminement et lui fournir des informations de façon continue sur l'état de son cheminement ;
- En administrant les épreuves aux fins de certification ;
- En fournissant les résultats de l'évaluation de certification à la personne responsable dans le centre de formation.

Logigramme des compétences

Filière : «Filière : Infrastructure Digitale – Option Cybersécurité »



Glossaire

Programme de formation professionnelle

Un programme est un ensemble cohérent de compétences à acquérir, formulé en termes d'objectifs et découpé en modules. Il décrit les apprentissages attendus du stagiaire en fonction d'une performance déterminée. Ses objectifs et son contenu sont obligatoires.

Buts de la formation

Les buts de la formation sont les énoncés des intentions éducatives retenues pour le programme. Il s'agit d'une adaptation des buts généraux de la formation professionnelle pour un programme de formation donné.

Compétence

Une compétence est un pouvoir d'agir, de réussir et de progresser qui permet de réaliser adéquatement des tâches ou des activités et qui se fonde sur un ensemble intégré de connaissances, d'habiletés, d'attitudes et de comportements. Les compétences sont de deux types :

- Les compétences spécifiques qui portent sur des tâches types du métier ou de la fonction de travail et qui rendent la personne apte à assurer avec efficacité la production d'un bien ou d'un service.
- Les compétences transversales qui portent sur une activité de travail ou de vie professionnelle qui déborde du champ spécifique des tâches du métier lui-même ; ces compétences peuvent être transférables à plusieurs activités de travail.

Objectifs généraux

Les objectifs généraux servent à catégoriser les compétences à faire acquérir par le stagiaire. Ils servent à orienter et à regrouper les objectifs opérationnels.

Objectifs opérationnels

L'objectif opérationnel est défini en fonction d'un comportement relativement fermé et décrit les actions et les résultats attendus du stagiaire. Il comprend cinq composantes :

- Le comportement attendu qui présente la compétence.
- Les conditions d'évaluation qui renseignent sur les conditions qui prévalent au moment de l'évaluation de sanction : contexte, matériel, etc.
- Les précisions sur le comportement attendu qui décrivent des éléments essentiels à la compréhension de la compétence.
- Les critères particuliers de performance qui définissent des exigences à respecter et accompagnent chacune des précisions sur le comportement. Ils permettent également de porter un jugement rigoureux sur l'atteinte de la compétence.
- Les critères généraux de performance qui définissent des exigences liées à l'accomplissement d'une tâche ou d'une activité et donnent des indications sur le niveau de performance recherché ou sur la qualité globale d'un produit ou d'un service. Ils sont également rattachés à l'ensemble ou à plusieurs précisions sur le comportement attendu.

Module de formation

Subdivision autonome d'un programme de formation professionnelle formant en soi un tout cohérent et signifiant.

Unité

Étalon servant à exprimer la valeur de chacun des modules d'un programme de formation en attribuant à ces composantes un certain nombre de points pouvant s'accumuler pour l'obtention d'un diplôme ; l'unité correspond à 15 heures de formation.

DEUXIEME PARTIE

Fiches prescrites et suggestions pédagogiques

Fiche prescrite

Compétence 1 : Se situer au regard du métier et de la démarche de formation	
Code de la compétence : DIA_ID_TS-01-01	**Durée : 15 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et/ou en groupe • À partir : - De mises en situations écrites et orales - De consignes - De spécifications fonctionnelles - De base documentaire • À l'aide : - D'internet - Du réseau professionnel	• Identification précise des différents métiers • Utilisation judicieuse des outils de recherche d'emploi • Suivi d'une démarche adéquate pour la connaissance du marché du travail • Connaissance approfondie du cadre de formation proposé
Éléments de la compétence	**Critères particuliers de performance**
A. Découvrir les métiers de l'Infrastructure digitale	• Compréhension générale des métiers liés à l'infrastructure • Identification globale des différents métiers de l'infrastructure • Recueil ciblé des compétences mobilisées
B. Identifier les modalités de formation	• Cartographie des compétences de l'année 1 • Cartographie des compétences de l'année de spécialisation • Usage des ressources de formation

Suggestions Pédagogiques

Compétence 1 :	**Se situer au regard du métier et de la démarche de formation**	**Code : DIA_ID_TS-01**
DURÉE : 15 h	**Compétences Préalables :** Aucune compétence préalable nécessaire	
Type de compétences : Transversale	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Découvrir les spécificités des métiers de l'Infrastructure digitale	A.1 – S'informer sur le marché du travail	• Identification des secteurs d'activité liés à l'Infrastructure digitale • Représentation du contexte de travail selon les secteurs des entreprises	• Seul ou en groupe • Selon les instructions verbales ou écrites du formateur • À l'aide des ressources fournis par le formateur (polycop, documents, cours) • Quizz sur le secteur d'activité du digital au Maroc • Vidéos témoignages et interviews de professionnels qui décrivent leur entreprise et leur métier	70%
	A.2 – Se renseigner sur les compétences métier	• Listing des comportements et postures professionnelles à adopter • Reconnaissances des missions et tâches à effectuer dans les métiers de l'infrastructure		

B. Identifier les modalités de formation	B.2 – Comprendre les objectifs de la formation	• Connaissance des objectifs à atteindre au terme de la formation • Utilisation des ressources pédagogiques • Recueil sur les différents modes d'évaluation durant le parcours de formation	• Seul ou en groupe • Selon les instructions verbales ou écrites du formateur • À l'aide des supports pédagogiques mis à disposition durant la formation sur la plateforme d'apprentissage • Investigations sur les secteurs d'activités auprès de professionnels et entreprises • Création d'un compte sur un réseau professionnel	30 %
	B.2 – Situer les compétences de la formation	• Visualisation sous forme de cartographie des compétences de l'année 1 • Visualisation sous forme de cartographie des compétences de l'année de spécialisation		
	B.3 – Projeter sa formation dans le milieu de travail	• Utilisation des réseaux professionnels • Compréhension des marchés de l'emploi (ouvert, cache) • Observation du milieu de travail		

Fiche prescrite

Compétence 2 : Comprendre les enjeux d'un système d'information	
Code de la compétence : DIA_ID_TS-01-02	**Durée : 75 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et/ou en groupe • À partir : - De mises en situations écrites et orales - De consignes - De spécifications fonctionnelles - De cahier des charges • À l'aide : - SGBD (/SQL Server) - D'un éditeur de texte (Word) -	• Identification précise des différentes fonctionnalités du système à informatiser • Modélisation correcte des différentes composantes du système d'information cible • Suivi d'une démarche adéquate pour la réalisation d'un projet d'informatisation d'un SI • Evolution cohérente du SI avec la stratégie de l'entreprise
Éléments de la compétence	**Critères particuliers de performance**
A. Acquérir les connaissances de base sur les systèmes d'information (SI)	• Compréhension précise des fonctions d'un système d'information • Distinction précise entre système d'information, système informatique et système d'information informatisé • Identification des composantes d'un système d'information
B. Identifier les différentes infrastructures informatiques	• Compréhension précise de la notion d'infrastructure informatique • Identification précise des éléments constitutifs d'une infrastructure informatique • Maitrise de la classification des différents types

	d'infrastructures informatique
C. Découvrir les principales étapes de construction d'un SI	• Identification claire des étapes de conception d'un SI • Mise en œuvre correcte d'un système d'information • Compréhension précise des différentes démarches de modélisation d'un système d'information
D. Comprendre le fonctionnement d'une base de données	• Distinction précise des différents types de bases de données • Modélisation correcte d'une base de données relationnelles • Implémentation correcte d'une base de données relationnelles

Suggestions Pédagogiques

Compétence 2 :	Comprendre les enjeux d'un système d'information	Code : DIA_ID_TS-02
DURÉE : 75 h	Compétences Préalables : **Compétence 1**	
Type de compétences : Spécifique	Compétences en parallèles : **Compétence à effectuer seule**	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Acquérir les connaissances de base sur les systèmes d'information (SI)	**A.1 - Comprendre la notion de SI**	• **Notion de SI, Système informatique et SI Informatisé** • **Fonctions et types du SI** • **Composantes d'un SI informatisé (Stations de travail, Serveurs ; Réseaux, systèmes d'exploitation)**	• **Seul ou en groupe** • **Selon les instructions verbales ou écrites du formateur** • **À l'aide des supports fournis par le formateur (polycop, documents, cours)** • **Activité type Quizz sur les concepts de base des SI et les domaines d'application des SI**	**20 %**
	A.2 –Identifier les principaux domaines d'application des SI	• **Informatique de gestion et informatique décisionnelle**		

		• **Informatique industrielle, embarquée et domotique** • **Bureautique** • **Jeux (Gaming)**		
B. Identifier les différentes infrastructures informatiques	**B.1 - Comprendre la notion d'infrastructure informatique**	• **Notion d'infrastructure informatique** • **Rôle de l'infrastructure informatique** • **Eléments constitutifs d'une infrastructure informatique (Cloud, en virtualisation)** • **Gestion de l'infrastructure informatique**	• **Seul ou en groupe** • **Selon les instructions verbales ou écrites du formateur** • **À l'aide des supports fournis par le formateur (polycop, documents, cours)** • **QCM sur les infrastructures SI existantes** • **Travaux pratiques sur les caractéristiques des différentes infrastructures**	**20 %**
	B.2 - Spécifier les architectures informatiques	• **Notion d'architecture de SI et son importance** • **Architecture centralisée** • **Architectures client/serveur** • **Architectures orientées services**		
C. Découvrir les principales étapes de	**C.1 - Comprendre les étapes conception du SI**	• **Compréhension de l'existant** • **Compréhension des besoins**	• **Seul ou en groupe**	

construction d'un SI		• **Identification des étapes de conception du SI**	• **Selon les instructions verbales ou écrites du formateur** • **À l'aide des supports fournis par le formateur (polycop, documents, cours)** • **QCM les étapes de mise en œuvre** • **Exercices d'application sur les processus de construction d'un SI**	**20 %**
	C.2 – Maîtriser les étapes de mise en œuvre du SI	• **Mise en œuvre et déploiement d'un SI** • **Mise en place des tests** • **Principe d'exploitation du SI** • **Identification du processus de maintenance du SI**		
D. Comprendre le fonctionnement d'une base de données	**D.1 - Identifier la notion de bases de données**	• **Introduction aux BD** • **Fonctionnalités d'un Système de Gestion de Base de Données (SGBD)**	• **Seul ou en groupe** • **Selon les instructions verbales ou écrites du formateur** • **À l'aide des supports fournis par le formateur (polycop, documents, cours)**	

	D.2 - Manipuler une BD relationnelle	• **Principes de bases de données relationnelles** • **Implémentation d'une BD relationnelle (DDL)** • **Exploitation d'une BD relationnelle (algèbre relationnel SQL)**	• **QCM sur les bases de données** • **Travaux pratiques sur l'utilisation de la base de données**	**40 %**

Fiche prescrite

Compétence 3 : Concevoir un réseau informatique	
Code de la compétence : DIA_ID_TS-03	**Durée : 120 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement • À partir : - Des manuels et sources de référence - D'un cahier des charges • À l'aide : - D'ordinateurs - De switch - De routeur - De panneau de brassage - D'accessoires de câblage - De documents pertinents (manuels de référence appropriés, guide d'utilisation) - Des outils et des utilitaires dédiés à l'analyse des couches d'un réseau - De logiciels de simulation et de configuration de routeurs	• Utilisation correcte des commandes appropriées • Utilisation appropriée des outils de référence • Emploi correcte des outils et utilitaires • Respect constant des consignes et du temps alloué • Respect des règles d'utilisation de l'équipement et du matériel informatique • Précautions continues concernant l'utilisation du matériel et des logiciels • Rapidité d'exécution
Éléments de la compétence	**Critères particuliers de performance**
A. Maîtriser les notions de base du réseau informatique	• Identification des différents types de réseaux • Identification correcte des fonctions de la connectivité réseau • Maitriser les système numériques

B. Comprendre les modèles et les protocoles de communication IP	• Utilisation judicieuse des protocoles et des services de la couche réseau • Réalisation appropriée d'un plan d'adressage IP • Emploi exact des protocoles des couches transport et application de TCP/IP • Construction juste d'un réseau LAN
C. Appliquer les bases de la commutation	• Conception exacte de commutation, VLAN et routage inter VLAN
D. Mettre en œuvre un réseau d'entreprise	• Conception judicieuse de protocoles de routage • Configuration exacte de protocoles de routage
D. Mettre en œuvre un réseau d'entreprise	• Conception judicieuse de protocoles de routage • Configuration exacte de protocoles de routage

Suggestions Pédagogiques

Compétence 3 :	**Concevoir un réseau informatique**	**Code : DIA_ID_TS-03**
DURÉE : 120 h	**Compétences Préalables :** Compétences 1 / 2	
Type de compétences : Spécifique	**Compétences en parallèles :** Aucune	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Maîtriser les notions de base du réseau informatique	A.1. Identifier les différents types de réseaux	• Description des composants d'un réseau informatique • Différents types de réseaux • Tendances des réseaux (BYOD, Collaboration en ligne, Cloud Computing, Haut débit sans fil)	• À l'aide d'outil de simulation de réseau • Seul ou en équipe selon les instructions du formateur • Examiner les équipements réseaux et distinguer les différents ports à utiliser • À partir de mises en situation représentatives de l'environnement de travail et de directives du formateur • Travaux Dirigés	20 %
	A.2. Connaître les réseaux locaux (LAN)	• Les réseaux Ethernet • Topologies du réseau LAN • Introduction aux réseaux sans fil (802.11x)		

	A.3. Analyser les supports de transmission Ethernet	• Câblage en cuivre • Câblage UTP • Câblage à fibre optique • Supports sans fil	○ Comparaison entre les différents supports de transmission ○ Convertir des nombres entre les systèmes décimaux et binaires. ○ Convertir des nombres entre les systèmes décimaux et Hexadécimaux • Travaux pratiques ○ Raccordement et brassage des câbles Ethernet	
	A.4. Maitriser les systèmes numériques	• Système binaire • Système hexadécimal		
B. Comprendre les modèles et les protocoles de communication IP	B.1. Comprendre les modèles OSI et TCP/IP	• Modèle OSI et ses couches • Modèles TCP/IP et ses couches • Comparaison entre OSI et TCP/IP	• Seul ou en équipe selon les instructions du formateur • Travaux Dirigés ○ Réaliser des exercices de découpage en sous réseaux (VLSM) • Travaux Pratiques ○ Mettre en place un serveur DHCP et vérifier les différentes étapes d'attribution d'adresses	30%
	B.2. Comprendre la commutation Ethernet	• Différentes versions d'Ethernet • Trame Ethernet • Adresse MAC Ethernet • Méthodes de transmission et vitesse de commutation		

	B.3. Mettre en œuvre l'adressage IP	• Adressage IPv4 / Adressage IPv6 • Segmentation d'un réseau IPv4 / IPv6 en sous-réseau • VLSM • Paquet IPv4 et IPv6		
	B.4. Découvrir les services et les protocoles réseaux	• Protocole ICMP • Protocole TCP et UDP • Services réseaux (DNS, DHCP, FTP, messagerie (SMTP, POP, IMAP))		
C. Appliquer les bases de la commutation	C.1 Définir la commutation	• Différents types de switch • Transfert de trame • Domaines de commutation • Protocole ARP	• Seul ou en équipe selon les instructions du formateur • Travaux Pratiques ○ Tester le comportement d'un réseau, de	25 %

	C.2. Mettre en place un réseau LAN	• Conception d'un réseau LAN • Optimisation d'un réseau LAN • Dépannage d'un réseau LAN	concevoir des modèles de réseau et de mettre en pratique des hypothèses ○ Exemples de "découpage" en VLAN dans les entreprises ○ Configurer SSH et telnet ○ Démonstration de capture des trames avec l'outil Wireshark	
	C.3. Mettre en œuvre des VLAN	• Principe de fonctionnement des VLANs • Configuration des VLANs		
D. Mettre en œuvre un réseau d'entreprise	D.1 Comprendre le fonctionnement de protocoles de routage	• Détermination du chemin • Transmission de paquets • Fonctions et configuration de base d'un routeur • Principes de routage • Routage IP statique et dynamique	• Seul ou en équipe selon les instructions du formateur • Présenter et analyser de la table de routage de la station de travail et du routeur • Travaux Dirigés ○ Effectuer un routage statique pour une moyenne topologie ○ Tester le fonctionnement du protocole RIP	25 %
	D.2 Utiliser le routage dynamique	• Principes de routage à vecteur de distance • Protocole RIP		

Fiche prescrite

Compétence 4 : Maîtriser le fonctionnement d'un système d'exploitation client	
Code de la compétence : DIA_ID_TS-04	**Durée : 135 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir : - De consignes - Des spécifications fonctionnelles - Des spécifications techniques • À l'aide : - Plusieurs logiciels d'installation - Un ou plusieurs postes de travail connectés en réseaux - Plusieurs logiciels de configuration et de gestion de la sécurité	• Maîtrise aisée des composants et des concepts fondamentaux des systèmes d'exploitation • Connaissance adaptée des fonctionnalités de Windows • Maîtrise du système d'exploitation Windows • Maîtrise du système d'exploitation Linux • Maîtrise des commandes Shell • Manipulation aisée de PowerShell • Prise en main parfaite de l'installation d'un SE (Windows et Linux) • Compréhension approfondie des contrôles des droits d'utilisateurs (Windows et Linux) • Installation correcte des applications (Windows et Linux)
Éléments de la compétence	**Critères particuliers de performance**
A. Découvrir les systèmes d'exploitation (SE)	• Description correcte des éléments de base des systèmes d'exploitation • Compréhension facile des éléments (hard et soft) d'un poste de travail client et d'un serveur

B. Gérer un système d'exploitation Windows	• Réalisation judicieuse de l'installation d'un système d'exploitation Windows • Manipulation correcte de Post-déploiement (Création des utilisateurs, mise à jour • Réalisation précise de l'authentification des utilisateurs et de la gestion de leurs privilèges sous Windows • Maîtrise des solutions de sécurisation du réseau des menaces externes sous Windows
C. Gérer un système d'exploitation Linux	• Réalisation judicieuse de l'installation d'un système d'exploitation Linux • Maîtrise des commandes Shell sous Linux • Création facile des utilisateurs, mise à jour sous Linux • Maîtrise de l'installation des packages et applications sous Linux • Connaissance adaptée en programmation Shell

Compétence 4 :	**Maîtriser le fonctionnement d'un système d'exploitation client**	**Code : DIA_ID_TS-04**
DURÉE : 135 h	**Compétences Préalables :** Compétence 1/2/3	
Type de compétences : Spécifique	**Compétences en parallèles :** aucune	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Découvrir les systèmes d'exploitation (SE)	A.1– Analyser le fonctionnement d'un SE	• Description d'un système d'exploitation • Présentation des concepts fondamentaux d'un OS (les utilisateurs, les fichiers, la gestion de mémoire, les processus et les E/S) • Principe de fonctionnement d'un OS	• Seul ou en groupe • Selon les instructions verbales ou écrites du formateur • Cours et énoncés des travaux pratiques fournis par le formateur • Travaux pratiques de démonstration sur l'exploration des concepts fondamentaux. Manipulation des limitations des droits d'utilisateurs par	20%
	A.2 – Préparer les disques durs	• Description des disques durs • Systèmes de gestion de fichiers • Partitionnement et formatage des disques durs		

	A.3 – Découvrir les SE Client et serveur	• Identification des différents types de systèmes d'exploitation client • Identification des différents types de systèmes d'exploitation serveur • Configuration de la connectivité réseau	l'ajout, la modification et la suppression des utilisateurs, fichiers, et processus : Software • Travaux pratiques sur l'étude des caractéristiques d'un poste de travail : Hardware • Travaux pratiques de démonstration sur l'exploitation d'un poste de travail client et un serveur à travers VirtualBox • Travaux pratiques sur la configuration de la connectivité réseau	
B. Gérer un système d'exploitation Windows	B.1 – Explorer Windows	• Différentes versions de Windows • Fonctionnalités de Windows (Utilisation interface graphique) • Gestion du système d'exploitation Windows (gestion de la mémoire, des processus, des E/S, des fichiers, des répertoires, des programmes, panneaux de configuration, NTFS, gestion des tâches…) Utilisation de Powershell	- Seul ou en groupe - Selon les instructions verbales ou écrites du formateur ○ Travaux pratiques : - Installation de Windows OS (NTFS, configuration du nom d'utilisateur, droit des utilisateurs, mise à jour, paramètres réseaux)	40%

	B.2 Déployer un système d'exploitation Windows	• Installation de Windows (Prérequis, installation, Principe de déploiement) • Post-déploiement (Création des utilisateurs, mise à jour) • Personnalisation du mode d'installation : configuration du nom de l'ordinateur, les paramètres réseaux, … • Mise à niveau et migration	- Création d'image - Exploration de Windows par invite de commande (création des utilisateurs et mise à jour) - Exploration de Windows par PowerShell (création des utilisateurs et mise à jour) - Création des points sauvegarde et restauration - Protection contre les virus et autres malwares (Pare-feu, Windows Defender, etc.).	
	B.3 – Assurer la sécurité du client Windows	• Authentification dans Windows (Contrôle de comptes utilisateurs) • Permissions et partage de ressources (Contrôle d'accès) • Protection, sauvegarde et restauration des données locales • Outils de sécurité sous Windows (Pare-feu, Windows Defender)		
C. Gérer un système d'exploitation Linux	C.1 – Explorer Linux	• Principe de fonctionnement du système Linux • Identification des différentes distributions • Arborescence du système de fichiers	• Seul ou en groupe • Selon les instructions verbales ou écrites du formateur	40%

		• Installation basique du SE Linux	• À l'aide des supports fournis par le formateur (polycop, documents, cours) • Travaux pratiques : Installation de Linux • Travaux pratiques : - Installation du SE Linux (partitions, configuration des utilisateurs, configuration réseaux, périphérique et service) - Manipulation des commandes de base - Installation de package et applications - Programmation shell	
	C.2 – Manipuler le Shell Linux	• Gestion de base du système de fichiers • Droits d'accès et utilisateurs • Gestion des processus et redirection du flux Programmation Shell (Edition, structures de contrôle, filtrage)		
	C.3 – Paramétrer le déploiement de Linux	• Compression et archivage • Outils d'installation de package et applications (RPM, Deb, apt, yum, snap) • Paramétrage de l'installation de Linux (partitions, services et packages, configuration réseau…) • Configuration post-installation (périphérique, service, utilisateurs…)		

Compétence 5 : Gérer une infrastructure virtualisée	
Code de la compétence : DIA_ID_TS-05	**Durée : 120 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir : - De consignes - Des spécifications fonctionnelles - Des spécifications techniques - De cahier des charges • À l'aide : - De VirtualBox - De Docker - De VMWare - D'Hyper-V - De Proxmox - Images ISO des systèmes d'exploitation - D'ordinateur - De Serveur	• Connaissance exacte des concepts de base de la virtualisation ainsi que ses principaux avantages • Bonne maitrise des outils pour la création et la gestion d'une infrastructure virtualisée • Mise en place et gestion aisée d'une infrastructure virtualisée • Bonne maîtrise de la conversion P2V
Éléments de la compétence	**Critères particuliers de performance**
A. Découvrir la virtualisation	• Bonne maitrise des concepts de base de la virtualisation • Connaissance exacte des intérêts de la virtualisation
B. Aborder les différentes solutions de virtualisation	• Identification aisée des différentes solutions de virtualisation

	• Bonne maitrise du choix de la solution de virtualisation adéquate pour des contextes et des besoins donnés • Utilisation judicieuse d'un hyperviseur type 2 pour la création d'une machine virtuelle
C. Mettre en place une solution de Virtualisation de Type 1	• Connaissance facile de certains exemples de solutions de virtualisation de type 1 • Utilisation judicieuse d'un hyperviseur type 1 pour la création d'un environnement de virtualisation • Création aisée des machines virtuelles et du réseau pour les faire communiquer et les connecter au réseau extérieur
D. Gérer le pool des ressources dans un hyperviseur type 1	• Connaissance exacte des différentes banques de stockage • Création aisée de 'Template' • Bonne maîtrise des différents types de provisionnement de machines en ressources
E. Manipuler les outils de migration du marché X2X (P2V, V2V, V2P)	• Connaissance aisée des différents outils de migration X2X • Bonne maîtrise de la conversion P2V

Compétence 5 :	**Gérer une infrastructure virtualisée**	**Code : DIA_ID_TS-05**
DURÉE : 120 h	**Compétences Préalables :** Compétences 1/2/3/4	
Type de compétences : **Spécifique**	**Compétences en parallèles :** aucune	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Découvrir la virtualisation	A.1 – Définir les concepts de base de la virtualisation	• Introduction à la virtualisation • Historique et évolution de la virtualisation • Présentation des machines virtuelles et ses principales caractéristiques • Les différents types de la virtualisation	• Seul ou en groupe • Cours et énoncés des quiz fournis par le formateur • Quiz sur les concepts de base de la virtualisation • Quiz sur les intérêts de la virtualisation	10 %
	A.2 – Comprendre l'intérêt de la virtualisation	• Intérêts de la virtualisation pour l'organisation • Intérêts de la virtualisation pour le service informatique		
B. Aborder les différentes solutions de virtualisation	B.1 – Manipuler un hyperviseur de type 2	• Définition et fonctionnement d'un hyperviseur type 2 • Présentation et comparaison des différents hyperviseurs de type 2 (VMWare Workstation	• Seul ou en groupe • Cours et énoncés des travaux pratiques fournis par le formateur	30 %

		Pro, VMWare Workstation Player, et VirtualBox) • Contexte et exemples de cas de métiers de l'hyperviseur type 2 • Création des machines virtuelles avec un hyperviseur type 2	• Travaux pratiques sur l'installation et l'utilisation de VirtualBox (hyperviseur type 2) pour la création de machines virtuelles et l'installation d'un système d'exploitation invité (exemple : Ubuntu) • Travaux pratiques sur l'installation et l'utilisation de Docker (comme un exemple de conteneur)	
	B.2 – Identifier un hyperviseur de type 1	• Définition et fonctionnement d'un hyperviseur type 1 • Présentation et comparaison des différents hyperviseurs de type 1 • Contexte et exemples de cas de métiers de l'hyperviseur type 1		
	B.3 – S'initier à la conteneurisation	• Définition et fonctionnement de la conteneurisation • Différents types de conteneurs • Conteneurisation versus virtualisation		
C. Mettre en place une solution de Virtualisation de	C.1 – Découvrir des solutions de virtualisation de type 1	• VMware vSphere • ProxmoxVE • Microsoft Hyper-V	• Seul ou en groupe • Cours et énoncés des travaux pratiques fournis par le formateur	30 %

Type 1	C.2 – Créer un environnement de virtualisation	• Introduction aux outils fournis par un hyperviseur de type 1 • Création des machines virtuelles (VMs)	• Travaux pratiques sur l'installation d'un hyperviseur type 1 • Travaux pratiques sur la création des machines virtuelles (VMs) et de réseaux de machines virtuelles	
	C.3 – Créer des réseaux dans l'environnement de virtualisation	• Configuration de réseaux logiques • Création de réseaux de machines virtuelles • Configuration de pools d'adresses IP et ajout de passerelle • Création de commutateurs logiques (virtual switches)		
D. Gérer le pool des ressources dans un hyperviseur type 1	D.1 – Intégrer les banques de stockage (données)	• Présentation des banques de données VMFS (Virtual Machine File System) • Présentation des banques de données NFS (Network File System) • Création de banques de données	• Seul ou en groupe • Cours et énoncés des travaux pratiques fournis par le formateur • Travaux pratiques sur la création de banques de données avec VMware • Travaux pratiques sur la création et le clonage des 'Template' avec VMware	20 %
	D.2 – Créer des 'Template'	• Notions de 'Template' (Modèle) de l'image du système d'exploitation (SE) invité • Création des 'Template' de l'image du SE invité • Clonage des 'Template'		

	D.3 – Optimiser les ressources des machines virtuelles	• Provisionnement statique • Provisionnement dynamique		
E. Manipuler les outils de migration du marché X2X (P2V, V2V, V2P)	E.1 – Identifier les types de migration (P2V, V2V, V2P)	• Conversion d'une machine physique en machine virtuelle (P2V) • Conversion d'un ordinateur virtuel en ordinateur virtuel (V2V), migration • Conversion d'une machine virtuelle en machine physique (V2P) • Présentation des outils de conversion	• Seul ou en groupe • Cours et énoncés des quiz ainsi que des travaux pratiques fournis par le formateur • Quiz sur les outils de migration X2X • Travaux pratiques sur la migration P2V avec VMware vCenter Converter Standalone	10 %
	E.2 – Convertir la machine physique en virtuelle (P2V)	• Exigences de la migration P2V • Les techniques P2V • Les étapes de la migration P2V		
	E.3 – S'initier au dépannage d'un environnement virtuel	• Vue d'ensemble sur les fichiers journaux et emplacements • Outils de résolution des pannes • Résolution des pannes simples		

Fiche prescrite

Compétence 6 : Automatiser les tâches d'administration	
Code de la compétence : DIA_ID_TS-06	**Durée : 120 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir : - De consignes - De descriptions de la syntaxe (algorithmes, langage de programmation, commandes, …) - Des exemples de tâches à automatiser - De cahiers des charges • À l'aide : - Des outils de programmation - D'outil flowchart de test des algorithmes (Exemple RAPTOR : https://raptor.martincarlisle.com/) - D'ordinateur	• Identification correcte des concepts fondamentaux de l'algorithmique • Connaissance claire des concepts fondamentaux de la programmation orientée objet • Maîtrise d'un langage de programmation et des commandes. • Utilisation juste des outils de programmation • Production aisée de scripts de gestion et d'automatisation de tâches d'administration • Maitrise du respect des cahiers de charges
Éléments de la compétence	**Critères particuliers de performance**
A. Découvrir les concepts de base de la programmation	• Identification précise de la démarche de résolution de problème • Connaissance conforme de l'algorithmique et de la programmation orientée objet

B. Développer des programmes	• Utilisation aisée des outils de programmation • Bonne maîtrise d'un langage de programmation • Production facile de scripts, leur correction et leur exécution
C. Appliquer l'administration système	• Manipulation précise de Commandes d'administration de base • Maîtrise des pipelines • Administration organisée des ordinateurs à distance
D. Créer des programmes pour les tâches d'administration	• Identification correcte des commandes (PowerShell, Bash) • Production aisée de scripts python de gestion • Réalisation adaptée de la programmation et de la planification de tâches
E. Créer des fichiers logs	• Maîtrise de la manipulation de fichiers par des scripts • Production aisée de fichiers log

Compétence 6 :	Automatiser les tâches d'administration	Code : DIA_ID_TS-06
DURÉE : 120 h	Compétences Préalables : **Compétence 1/2/3/4/5**	
Type de compétences : Spécifique	Compétences en parallèles : **aucune**	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Découvrir les concepts de base de la programmation	**A.1 – Découvrir la programmation structurée**	• **Description de la méthode de résolution d'un problème : raisonnement par algorithme** • **Description d'un algorithme** • **Les structures de base du langage python**	• **Seul ou en groupe** • **Cours et énoncés des travaux dirigés fournis par le formateur** • **Travaux dirigés sur l'écriture d'algorithmes** • **Travaux dirigés sur les classes** • **Travaux dirigés sur les opérateurs, le traitement itératif et le traitement conditionnels**	**40 %**
	A.2 – Découvrir la programmation orientée objet	• **Programmation orientée objet** • **Notions de classe et d'objets** • **Notion d'attributs et de méthodes** • **Syntaxe du langage python**		

	A.3 – Utiliser les conditions et les boucles	• **Opérateurs mathématiques et logiques** • **Traitement conditionnel** • **Traitement itératif**	• **Utilisation d'un outil de test des algorithmes (Exemple : https://raptor.martincarlisle.com/)**	
B. Développer des programmes	**B.1 – Concevoir des programmes**	• **Installation et découverte des outils de programmation** • **Ecriture des programmes dans l'environnement de développement** • **Exécution des programmes dans l'environnement de développement**	• **Seul ou en groupe** • **Travaux pratiques d'installation (éventuellement) de l'environnement de développement** • **Travaux pratiques sur la traduction des algorithmes en scripts (python à titre d'exemple)** • **Travaux pratiques sur les commandes PowerShell, Bash** • **Travaux pratiques sur les modules spécifiques pour les opérations de gestion** • **Ecriture et exécution des scripts** • **Correction des éventuelles erreurs (logiques et syntaxiques)**	**20 %**
	B2 – Créer un script pour faciliter les opérations de gestion	• **Description des opérations de gestion** • **Structures relatives aux tâches de gestion (les modules spécifiques, listes, dictionnaires, …)** • **Exécution de scripts de gestion** • **Ecriture et exécution en ligne de commandes**		
C. Appliquer l'administration	**C.1 – Connaitre les commandes de**	• **Tests de commande d'administration**	• **Seul ou en groupe**	**20 %**

système	base d'administration	Windows • Exécution de commande d'administration Linux • Ecriture de commande d'administration réseaux	• Travaux pratiques : commande Windows • Travaux pratiques : commande d'administration Linux • Travaux pratiques : Manipulation de commandes d'administration réseaux • Travaux pratiques : administration à distance Windows • Travaux pratiques : : administration à distance Linux	
	C.2 – Administrer les ordinateurs à distance	• Connaissance aisée de connexion SSH et bureau à distance • Tests de fonctionnement de commandes d'administration à distance		
D. Créer des programmes pour les tâches d'administration	D.1 – Automatiser les tâches redondantes	• Spécification des tâches redondantes • Création de scripts pour les tâches redondantes • Tests de fonctionnement de scripts en conditions réelles • Planification des tâches avec les outils système	• Seul ou en groupe • Travaux pratiques : automatisation de tâches redondantes • Travaux pratiques : planification tâches récurrentes • Travaux pratiques : correction de scripts • Travaux pratiques : test temps d'exécution des scripts	10 %
	D.2 – Optimiser l'exécution des	• Identification des erreurs des manipulations par la méthode manuelle		

	tâches d'administration	• Avantages de l'automatisation des tâches • Réduction de temps de réalisation de tâche par l'automatisation		
E. Créer des fichiers logs	E.1 – Comprendre la persistance des données	• Flux vers les fichiers • Méthode de création, lecture, écriture, modification et suppression dans un fichier	• Seul ou en groupe • À l'aide des supports fournis par le formateur (polycop, documents, cours) • Travaux pratiques sur la manipulation de fichiers • Travaux pratiques sur la création de fichiers log • Travaux pratiques sur l'évaluation de fonctionnement des scripts • Réalisation d'un projet en programmation (notions d'un cahier des charges)	10%
	E.2 - Manipuler les fichiers logs	• Ecriture de scripts pour la création de logs (scripts avancés) • Test/exécution des scripts		
	E.3 - Tester le fonctionnement des scripts	• Collecte des résultats retournés par le script • Évaluation des cas de test • Déploiement des scripts		

Fiche prescrite

Compétence 7 : Sécuriser un système d'information	
Code de la compétence : DIA_ID_TS-07	**Durée : 75 heures**
Contexte de réalisation	**Critères généraux de performance**
Individuellement et / ou en groupe À partir : - De consignes - De spécifications fonctionnelles - De spécifications techniques - De cahier des charges À l'aide : - D'ordinateur - D'hyperviseur type 2 (VirtualBox, VMware Workstation) - De machines virtuelles (Kali Linux, Ubuntu, Metasploitable) - De firewall - D'openSSl	• Maîtrise des notions de base de la sécurité • Utilisation aisée des outils permettant la sécurisation du système d'information et la remédiation aux failles • Bonne maitrise de la cryptographie • Identification précise des failles de sécurité dans un contexte prédéfinie • Connaissance aisée des outils et processus requis pour l'amélioration continue de la sécurité SI
Éléments de la compétence	**Critères particuliers de performance**
A. Découvrir les notions de base de la sécurité des systèmes d'information (SI)	• Maitrise des notions de base de la sécurité • Connaissance aisée des principales attaques de sécurité

B. Protéger le SI	• Bonne maitrise des règles de sécurité pour la sécurisation de l'information • Identification aisée des composants pour la sécurisation de l'accès physique • Application correcte des bonnes pratiques de sécurisation des postes de travail et des serveurs • Utilisation judicieuse des pare-feu logiciel pour le filtrage du trafic réseau
C. Découvrir la cryptographie et les solutions de gestion et de partage de clés	• Bonne maîtrise de la cryptographie • Connaissance aisée de l'architecture PKI et ses fonctions
D. S'initier à l'audit de sécurité des SI	• Bonne maitrise des concepts basiques et exigences relatifs aux audits de Sécurité SI • Utilisation judicieuse des outils de test d'intrusion

Suggestions Pédagogiques

Compétence 7 :	**Sécuriser un système d'information**	**Code : DIA_ID_TS-07**
DURÉE : 75 h	**Compétences Préalables :** Compétences 1/2/3/4/5/6	
Type de compétences :	**Compétences en parallèles :** Compétence 8	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉREE
A. Découvrir les notions de base de la sécurité des systèmes d'information (SI)	A.1 – Connaître les concepts de base de la sécurité informatique	• Importance de la sécurité dans les SI • Terminologie et définitions : classification de la sécurité, vulnérabilités, menaces, risques, attaques, victimes, actifs, contre-mesures • Objectifs et propriétés de la sécurité	• Seul ou en groupe • Cours et énoncés des quiz fournis par le formateur • Quiz sur les notions de base de la sécurité informatique • Travaux pratiques sur l'exploitation des menaces de sécurité pour mener des attaques (internes et externes) de sécurité	20 %
	A.2 – Identifier les attaques de sécurité visant un SI	• Classification des attaques et des hackers • Attaques internes • Attaques externes • Besoin d'identification des vulnérabilités		

B. Protéger le SI	B.1 – Présenter la politique de sécurité du SI	• Démarche sur la mise en place d'une politique de sécurité du SI et gestion des risques • Normes et méthodes de gestion des risques • Approche PDCA • Veille technologique	• Seul ou en groupe • Cours et énoncés des quiz fournis par le formateur • Quiz sur les notions de la sécurisation de l'information et de la protection physique • Travaux pratiques sur l'application des bonnes pratiques et la configuration des outils nécessaires pour sécuriser un système d'exploitation (pour postes de travail et/ou serveurs) • Travaux pratiques sur la mise en place, configuration, et test d'un pare-feu • Quiz sur les notions de base relatives à l'assurance d'une amélioration continue de la sécurité SI	40 %
	B.2 – Appliquer les droits nécessaires pour sécuriser l'information	• Contrôle d'accès • Méthodes d'authentification (mot de passe, biométrique, renforcée, etc.) • Règles d'autorisation et traçabilité		
	B.3 – Sécuriser l'accès physique	• Contrôle d'accès physique : description des composants et des phases de contrôle d'accès • Vidéoprotection : définition et composants • Autres outils pour sécuriser l'accès physique		

	B.4 – Sécuriser les équipements informatiques	• Sécurisation des postes de travail et des serveurs • Sécurisation des commutateurs et des routeurs • Anti-Virus : Fonctionnement et techniques de recherche des virus • Filtrage du trafic avec des Pare-feu logiciel		
C. Découvrir la cryptographie et les solutions de gestion et de partage de clés	C.1 – Utiliser la cryptographie et les certificats numériques	• Objectifs de la cryptographie • Cryptographie symétrique et Cryptographie asymétrique • Fonction de hachage • Certificats X.509	• Seul ou en groupe • Cours et énoncés des quiz fournis par le formateur • Quiz portant sur la cryptographie, la gestion des clés et l'architecture PKI • Travaux dirigés sur la cryptographie • Travaux pratiques sur le chiffrement, le déchiffrement, et la génération des certificats numériques à l'aide d'openSSL	20 %
	C.2. –Découvrir l'architecture PKI (Public Key Infrastructure)	• Architecture PKI • Fonctions de gestion d'une PKI • Protocoles PKI : CMP et CMS		

D. S'initier à l'audit de sécurité des SI	D.1 – Connaître les concepts généraux relatifs aux audits de Sécurité SI	• Objectifs des audits de sécurité SI • Classification des audits • Les référentiels d'audit (COBIT, ISO 27002)	• Seul ou en groupe • Cours et énoncés fournis par le formateur • Quiz sur les référentiels, la démarche et les exigences relatives à l'audit de sécurité • Travaux pratiques sur l'utilisation des outils de test d'intrusion pour l'identification des failles de sécurité et l'exploitation de certaines failles pour mener des scénarios d'attaques.	20 %
	D.2 – Décrire les phases d'audits	• Pré-audit • Analyse de l'infrastructure existante • Test d'intrusion • Rapport d'audit		
	D.3 –Identifier les exigences relatives à la prestation d'audits	• Exigences relatives au prestataire d'audit o (Responsabilités, déontologie) • Exigences relatives aux auditeurs (qualités personnelles, compétences)		

Fiche prescrite

Compétence 8 : Développer un processus de veille technologique	
Code de la compétence : DIA_ID_TS-01-08	**Durée : 45 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir : - De consignes - De notes de cours - De travaux pratiques - De spécifications fonctionnelles - De spécifications techniques - De cahier des charges • À l'aide : - De logiciel de modélisation - De logiciel web - De site web - D'ordinateur	- Identification précise du concept de la veille technologique (VT) - Détermination claire des objectifs et enjeux de la VT - Compréhension aisée et maitrise de mise en place d'un processus de la VT - Maitrise des outils de la VT - Maitrise des notions de sécurité ainsi que le règlement général de protection des données personnelles
Éléments de la compétence	**Critères particuliers de performance**
A. Définir la veille technologique (VT)	- Connaissance claire de la terminologie VT - Identification correcte des bénéfices de la VT
B. Découvrir le concept de la veille technologique	- Reconnaissance juste des objectifs de la VT - Détermination exacte des enjeux de la VT

C. Mettre en place un processus de veille technologique	• Maitrise de la mise en place de processus de la VT • Elaboration exacte d'un organigramme pour dégager les étapes de la VT • Schématisation précise d'un plan de mise en route
D. Découvrir la notion de Sécurité et RGPD	• Connaissance du concept RGPD • Maitrise des principes de RGPD • Suivi des évolutions sécuritaires du monde informatique

Suggestions Pédagogiques

Compétence 8 :	**Développer un processus de veille technologique**	**Code : DIA_ID_TS-01-08**
DURÉE : 45 h	**Compétences Préalables :** Compétences 1/2/3/4/5/6	
Type de compétences : **Spécifique**	**Compétences en parallèles :** Compétence 7	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Définir la veille technologique (VT)	A.1 – Connaitre les différentes terminologies de la VT	• Définition de la veille technologique • Exemples de focus de la veille	• Seul ou en groupe • Cours et énoncés des travaux pratiques fournis par le formateur • Cahier des charges d'une étude de cas • Travaux pratiques sur la gestion d'une VT dans une entreprise	10%
	A.2 – Définir les bénéfices de la VT	• Différents types de veille • Avantages de la veille technologique		

B. Découvrir le concept de la veille technologique	B.1 – Définir les objectifs de la VT	• Acquisition des informations • Collecte, transmission et stockage des données	• Seul ou en groupe • Cours et énoncés des travaux pratiques fournis par le formateur y compris un cahier des charges d'une étude de cas dans un domaine d'activité. • Travaux pratiques pour dégager les différents objectifs du VT à travers l'étude cas déjà donnée • Travaux pratiques pour manipuler et maitriser le travail avec les différents outils de la VT sur des cas de figures bien particuliers	50 %
	B.2 – Découvrir les enjeux de la VT	• Innovations dans un domaine d'activité • Méthodologie d'étude de l'existant • Définition des orientations stratégiques		
	B.3 – Enumérer les différents types d'outils de la VT	• Outils à base d'agrégateurs de contenu • Outils à base de lecteurs de flux RSS		
	B.4 – Manipuler les principaux outils de la VT	• Usage des réseaux sociaux : Twitter, Facebook, Instagram et TweetDeck de Twitter • Prise en main des applications web (outil dev.to, netvibes et freeCodeCamp.org) •		

C. Mettre en place un processus de veille technologique	C.1 – Identifier les différentes étapes de la VT	• Formalisation des activités de la veille • Enumération des sources d'informations pertinentes	• Seul ou en groupe • Cours et énoncés des travaux pratiques fournis par le formateur y compris cahier des charges d'une étude de cas dans un domaine d'activité • Travaux pratiques : concevoir et mettre en place un processus de VT dans une entreprise	20 %
	C.2- Elaborer le processus de la VT	• Analyse des informations • Utilisation des outils de VT efficaces • Partage des résultats dans l'entreprise		
D.. Découvrir la notion de Sécurité et RGPD	D.1 –Définir le concept RGPD	• Définition de la RGPD • Failles de sécurité	• Seul ou en groupe • Selon les instructions verbales ou écrites du formateur • Travaux pratiques pour mettre en place et assimiler le concept RGPD sur une étude de cas	20 %
	D.2 –Comprendre le but de RGPD	• Enjeux de la RGPD • Public cible de la RGPD • Notion des données personnelles • Sécurité des données à caractère personnel		

Fiche prescrite

Compétence 9 : S'initier aux fondamentaux de la cybersécurité	
Code de la compétence : DIA_IDOCS_TS-09	**Durée : 75 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir de : - Consignes - Notes de cours - Documentation en ligne • À l'aide : - Ordinateur - Accès Internet	• Compréhension claire des piliers de la Cybersécurité • Connaissance aisée des postures de la Cybersécurité • Connaissance générale des métiers de la Cybersécurité
Éléments de la compétence	**Critères particuliers de performance**
A. Identifier la terminologie liée à la Cybersécurité	• Définition claire de la Cybersécurité • Compréhension correcte des objectifs de la Cybersécurité
B. Découvrir les différents normes et standards de la Cybersécurité	• Connaissance basique des normes ISO • Connaissance aisée des standards de gestion de vulnérabilités

C. Définition des critères de la Cybersécurité	• Différenciation exacte des trois critères de la Cybersécurité • Identification claire des niveaux de chaque critère de Cybersécurité
D. Découvrir les métiers de la Cybersécurité	• Connaissance générale des métiers de la Cybersécurité et leurs parcours • Connaissance générale des tendances de la Cybersécurité

Suggestions Pédagogiques

Compétence : 9	**S'initier aux fondamentaux de la cybersécurité**	**Code : DIA_IDOCS_TS-09**
DURÉE : 75 h	**Compétences Préalables :** Compétences 1/2/3/4/5/6/7/8	
Type de compétences : Spécifique	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Identifier la terminologie liée à la Cybersécurité	A.1 – Définir la Cybersécurité	• Définition de la Cybersécurité selon la norme ISO • Terminologie de la Cybersécurité • Exemples des tactiques, techniques et procédures utilisées par les attaquants	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Quizz sur les notions indispensables de la Cybersécurité • Travaux pratiques : Réalisation d'une recherche Internet sur les dernières techniques d'attaques.	20%
	A.2 – Connaitre les objectifs de la Cybersécurité	• Posture défensive • Posture offensive • Enjeux d'une politique de sécurité des SI		

B. Découvrir les différentes normes et standards de la Cybersécurité	B.1 – Connaitre les normes de la sécurité organisationnelle	• Norme 27001 • Norme 27005	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Quizz sur les différents standards • Travaux pratiques : Etudes de cas sur les enjeux de la Cybersécurité sur le Cloud	25%
	B.2 – Identifier les normes de la sécurité technique	• Standards de gestion de vulnérabilités (CVE, CVSS, CWE, NIST VDE, EXPLOIT-DB • OWASP		
	B.3 – Connaitre les référentiels réglementaires de la cybersécurité	• GDPR • Loi 09-08		
C. Définir des critères de la Cybersécurité	C.1 – Identifier les trois critères de base de la Cybersécurité à partir de la norme ISO 27005	• Disponibilité de l'information • Confidentialité de l'information • Intégrité de l'information	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Déclinaison des niveaux de chaque critère via un cas pratique	25%

	C.2 – Définir les niveaux de chaque critère	• Niveau 1 • Niveau 2 • Niveau 3 • Niveau 4		
D. Découvrir les métiers de la Cybersécurité	D.3 – Identifier les domaines de la Cybersécurité	• Sécurité du développement • Gouvernance • Gestion des risques • Sécurité physique	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Quizz sur les différents métiers envisageables pour un technicien spécialisé en Cybersécurité dans le cadre de son évolution professionnelle Travaux pratiques : Mise en situation : Mise en évidence de quelques métiers de Cybersécurité à travers un cas de gestion d'un incident Cybersécurité et blockchain	30%
	D.1 – Découvrir le référentiel métier de l'ANSSI	• Analyste SOC • Pentester		
	D.2 – Connaitre les tendances des métiers de la Cybersécurité	• Métier de consultant DevSecOps • Administrateur sécurité Blockchain		

Fiche prescrite

Compétence 10 : Appliquer les méthodologies des tests d'intrusions	
Code de la compétence : DIA_IDOCS_TS-10	**Durée : 105 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir de : - Consignes - Notes de cours - Documentation en ligne - Travaux pratiques - Cahier des charges • À l'aide de : - Ordinateur - Accès Internet - Environnement de test	• Connaissance générale sur les méthodologies des tests d'intrusion • Utilisation maitrisée des outils de scan • Rédaction claire du rapport final
Éléments de la compétence	**Critères particuliers de performance**
A. Connaitre les méthodologies de test d'intrusion	• Connaissance claire des standards en la matière • Connaissance générale sur les méthodes d'audit sécurité
B. Identifier les vulnérabilités au sein d'un système d'information	• Utilisation maitrisée des outils de test d'intrusions • Compréhension minutieuse des rapports de scan

C. Exploiter les vulnérabilités au sein d'un système d'information	• Connaissance aisée des méthodes d'exploitation • Exploitation maitrisée des vulnérabilités identifiées
D. Mettre en place un rapport de test d'intrusion	• Rédaction structurée du rapport final • Explication claire des recommandations

Suggestions Pédagogiques

Compétence : 10	**Appliquer les méthodologies des tests d'intrusions**	**Code : DIA_IDOCS_TS-10**
DURÉE : 105 h	**Compétences Préalables :** Compétences 1/2/3/4/5/6/7/8/9	
Type de compétences : Spécifique	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Découvrir les méthodologies de test d'intrusion	A.1 – Distinguer la méthodologie OSSTMM	• Utilisation de la méthodologie • Etapes de la méthodologie	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Quizz sur les méthodes et les typologies des tests d'intrusion • Travaux pratiques : Préparer des templates de rapport pour chaque méthodologie et un comparative entre les 3 standards de tests d'intrusion	20%
	A.2 – Identifier la méthodologie PTES	• Utilisation de la méthodologie • Etapes de la méthodologie		
	A.3 – Distinguer la méthodologie OWASP	• Utilisation de la méthodologie • Etapes de la méthodologie		

B. Identifier les vulnérabilités au sein d'un système d'information	B.1 – Collecter les informations de manière passive	• Moteurs de recherche • Réseaux sociaux pour la reconnaissance • Outils d'automatisation OSINT • Frameworks de collecte d'informations	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Installation et manipulation des outils de scan et réalisation des scripts d'exploitation sur une système ou une application	30 %
	B.2 – Identifier les vulnérabilités des services utilisés	• Outils de scan (nmap, Nessus, Nexpose, etc.) • Analyse et évaluation des vulnérabilités • Élimination des faux positifs		
C. Exploiter les vulnérabilités au sein d'un système d'information	C.1- Exploiter les vulnérabilités identifiées	• Frameworks et base de données d'exploitation de vulnérabilités (Metasploit, exploit-db, Cobalt Strike, Empire) • Gestion des exploits (buffer overflow exploits) • Tests d'intrusion (Linux, Windows, web OWASP top 10, active directory) • Réalisation des mouvements latéraux et élévation de privilèges dans un système compromis	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Test d'intrusion guidé sur des serveurs (smb, ftp, http, AD, etc ...) en suivant les étapes d'une méthodologie étudiée	30%
	C.2- Maintenir l'accès après l'exploitation du système	• Réalisation des mouvements latéraux et élévation de privilèges dans un système compromis • Utilisation de porte dérobée (backdoor) • Récupération des informations pour exploiter d'autres systèmes.		

D. Mettre en place un rapport de test d'intrusion	D.1 – Synthétiser les vulnérabilités à corriger	• Tableau de bord • Classification des résultats en fonction de la criticité des failles	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Rédaction d'un rapport à partir d'un modèle standard	20 %
	D.2 – Détailler les solutions envisageables de correction	• Mode opératoire de correction • Double vérification sur le système		

Fiche prescrite

Compétence 11 : Analyser les attaques et les incidents liés à la Cybersécurité	
Code de la compétence : DIA_IDOCS_TS-11	**Durée : 105 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir : - Consignes - Notes de cours - Documentation en ligne - Travaux pratiques • À l'aide : - Ordinateur - Plateforme technique - Accès Internet	• Compréhension maitrisée du processus de gestion des incidents • Identification claire des indicateurs de compromission • Réponse efficace aux incidents de sécurité • Connaissance suffisante des normes et standards de gestion et analyses de logs
Éléments de la compétence	**Critères particuliers de performance**
A. S'approprier la notion d'un incident de sécurité	• Compréhension maitrisée des éléments d'un incident de sécurité • Connaissance aisée des étapes du Kill Chain
B. Appliquer les procédures de gestion des incidents	• Modélisation claire du processus de gestion des incidents

	• Utilisation maitrisée des normes de gestion des incidents sécurité comme le NIST 800-61r2
C. Effectuer le Threat Hunting	• Compréhension maitrisée de la notion • Maitrise claire des étapes du processus de Threat Hunting
D. Répondre à des incidents de Cybersécurité	• Connaissance aisée des stratégies de réponse aux incidents • Utilisation pratique des Framework de réponse aux incidents (GRR, Velociraptor)

Suggestions Pédagogiques

Compétence 11	**Analyser les attaques et les incidents de Cybersécurité**	**Code : DIA_IDOCS_TS-11**
DURÉE : 105 h	**Compétences Préalables :** Compétences 1/2/3/4/5/6/7/8/9/10	
Type de compétences : Spécifique	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. S'approprier la notion d'un incident de sécurité	A.1 – Définir un incident de sécurité	• Impacts possibles d'un incident de sécurité • Qualification d'un incident de sécurité	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Classification d'un incident de sécurité à partir d'un cas pratique Etude de l'exemple MITRE ATT&CK	20%
	A.2 – Analyser le Kill Chain	• Notion du Kill Chain • Etapes du Kill Chain		
B. Appliquer les procédures de gestion des incidents	B.1 – Présenter le processus de gestion des incidents de sécurité	• Modèle de la norme ISO 27035:2011 • Détails de chaque étape constituant le processus	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques :	30%

	B.2 – Appliquer les procédures 800-61 R2 du NIST	• Présentation des quatre phases du processus • Focus sur la partie communication	Déclinaison du processus à travers une étude de cas	
C. Effectuer le Threat hunting	C.1 – Définir le Threat Hunting	• Notion de menaces persistantes avancées (APT) • Méthodologies de Threat Hunting	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Manipulation d'un outil open source de Threat Hunting	30%
	C.2- Identifier les étapes du processus	• Identification des étapes • Place du Threat Hunting dans la stratégie de sécurité		
D. Répondre à des incidents de cybersécurité	D.1 – Définir les étapes d'un plan de base de réponse aux incidents	• Définition d'un plan de réponse aux incidents • Présentation d'un exemple de plan de réponse	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Utilisation d'un framework de réponse à incident (GRR, Velociraptor)	20 %
	D.2 – Automatiser la réponse aux incidents	• Processus à mette en place • Technologies d'automatisation		

Fiche prescrite

Compétence 12 : Assurer le durcissement de la sécurité des systèmes et réseaux informatiques	
Code de la compétence : DIA_IDOCS_TS-12	**Durée : 90 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir de : - Consignes - Notes de cours - Documentation en ligne - Référentiels et standards en la matière - Travaux pratiques • À l'aide de : - Ordinateur - Plateforme technique - Accès Internet	• Connaissance suffisante des protocoles réseaux • Connaissance suffisante des systèmes d'exploitation • Maitrise technique des outils d'audit • Application maitrisée des correctifs
Éléments de la compétence	**Critères particuliers de performance**
A. Présenter les normes et les standards de durcissement	• Connaissance claire des différents standards et leurs champs d'application • Compréhension maitrisée du processus d'audit de configuration
B. Maitriser le durcissement du réseau	• Maitrise des configurations réseaux • Application maitrisée des recommandations

C. Maitriser le durcissement d'un système	• Maitrise des configurations systèmes • Application maitrisée des recommandations
D. Déployer des solutions DLP et de traçabilité	• Connaissance claire des solutions de traçabilité • Maitrise des configurations

Suggestions Pédagogiques

Compétence 12 :	**Assurer le durcissement de la sécurité des systèmes et réseaux informatiques**	**Code : DIA_IDOCS_TS-12**
DURÉE : 90h	**Compétences Préalables : 1/2/3/4/5/6/7/8/9**	
Type de compétences : Spécifique	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Présenter les normes et les standards de durcissement	A.1 – Identifier les normes et référentiels de durcissement	• Normes ANSSI • Référentiel CIS	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle • Travaux pratiques : Conception d'une architecture sécurisée et rédaction des guides de durcissement de ses composants	20%
	A.2 – Connaitre les bonnes pratiques de l'administration sécurisée	• SI d'administration (bastion) • Outils d'administrations (local/centralisé) • Automatisation des règles de durcissement (Lynis, PingCastle, CIS-CAT)		
B. Maitriser le durcissement du réseau	B.1 – Identifier les composants basiques d'un réseau informatique	• Pare feux (UTM inclus) • VPN (OpenVPN, Wireguard et IPSEC)	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle	25%

	B.2 – Appliquer les configurations de sécurité sur les composants d'un réseau informatique	• Durcissement des protocoles réseaux (NBTS, LLMNR, WPAD, TLS) • Durcissement d'un Firewall	• Travaux pratiques : Appliquer les règles de durcissement des composants réseaux présents au laboratoire et mesure de score de conformité	
C. Maitriser le durcissement d'un système	C.1 – Identifier des systèmes d'exploitation	• Système Windows (serveurs et poste de travail) • Systèmes Linux	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle • Travaux pratiques : Appliquer les règles de durcissement des OS présents au laboratoire et mesure de score de conformité	25%
	C.2- Appliquer les configurations de sécurité sur les OS	• Durcissement Windows • Durcissement Linux		
D. Déployer des solutions DLP et de traçabilité	D.1 – Configurer une solution DLP	• Définition de la notion DLP • Configuration des politiques de détection	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle • Travaux pratiques : Déploiement de solutions DLP et traçabilité open source	30 %
	D.2 – Configurer une solution de gestion de la traçabilité	• Définition la traçabilité • Configuration des politiques de traçabilité		

Fiche prescrite

Compétence 13 : Appréhender les méthodes d'investigation numérique	
Code de la compétence : DIA_IDOCS_TS-13	**Durée : 90 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir de : - Consignes - Notes de cours - Documentation en ligne - Référentiels et standards en la matière - Travaux pratiques • À l'aide de : - Ordinateur - Plateforme technique - Accès Internet	• Utilisation appropriée des outils d'investigation • Analyse approfondie des traces • Maitrise de la rédaction de rapports d'investigation
Éléments de la compétence	**Critères particuliers de performance**
A. Maîtriser la technologie SIEM (SEM / SIM)	• Utilisation maitrisée des outils SIEM • Analyse intelligente des logs
B. Appréhender les méthodologies d'investigation réseaux et systèmes	• Bonne connaissance des méthodes • Application maitrisée des méthodes d'investigation

C. Maitriser les outils d'investigation	• Prise en main maitrisé des outils • Utilisation adéquate des outils d'investigation
D. Rédiger des rapports d'investigation	• Compréhension claire des modèles de rapports • Rédaction structurée des rapports

Suggestions Pédagogiques

Compétence 13 :	**Appréhender les méthodes d'investigation numérique**	**Code : DIA_IDOCS_TS-13**
DURÉE : 90 h	**Compétences Préalables : 1/2/3/4/5/6/7/8/9/11**	
Type de compétences : Spécifique	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Maîtriser la technologie SIEM (SEM / SIM)	A.1 – Connaitre le fonctionnement d'un SIEM	• Définition d'un SIEM • Solutions du marché	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle des fournisseurs • Travaux pratiques : Installation et configuration d'un SIEM Open Source (ELK)	30%
	A.2 – Concevoir les règles de corrélation	• Utilisation de SIEM pour la détection d'intrusion (Elastic et Splunk) • Conception des tableaux de bords		
B. Appréhender les méthodologies d'investigation réseaux et systèmes	B.1 – Identifier le processus d'investigation	• Identification • Préservation • Analyse • Documentation • Présentation	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne	20%

	B.2 – Répertorier les indicateurs de compromission	• Matrice ATT&CK • Analyse numérique des données	• Travaux pratiques : Analyse des données volatiles avec le framework Volatility	
C. Maitriser les outils d'investigation	C.1 – Identifier les outils d'investigation du marché	• FTKIMAGER • Autopsy, • Cellebrite • Encase	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Utilisation des outils d'investigation à travers une étude de cas (image de disque d'une machine compromise)	40%
	C.2- Appliquer les outils sur un cas pratique	• Investigation numérique sous Windows et Linux • Investigation numérique sous iOS		
D. Rédiger des rapports d'investigation	D.1 – Identifier les éléments d'un modèle de rapport	• Structure générale • Contenu détaillé	• Seul ou en groupe • Cours fournis par le formateur • Documentation en ligne • Travaux pratiques : Rédaction d'un rapport à partir de l'étude de cas de la compétence précédente	10 %
	D.2 –Structurer le rapport d'investigation	• Analyse de preuves • Indicateurs de compromission • Recommandations		

Fiche prescrite

Compétence 14 : Appliquer des stratégies de gestion des risques	
Code de la compétence : DIA_IDOCS_TS-14	**Durée : 90 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et / ou en groupe • À partir de : - Consignes - Notes de cours - Documentation en ligne - Travaux pratiques • À l'aide de : - Ordinateur - Accès Internet - Outils	• Application maitrisée des méthodes de gestion des risques • Modélisation claire des menaces • Bonne connaissance des outils de sensibilisation
Éléments de la compétence	**Critères particuliers de performance**
A. Effectuer la modélisation de menaces	• Compréhension claire du processus de modélisation • Utilisation maitrisée des outils de modélisation
B. Gérer les risques	• Connaissance maitrisée des éléments constituant un risque • Utilisation maitrisée des outils de gestion des risques

C. Sensibiliser les utilisateurs aux risques de sécurité	• Connaissance claire du processus de sensibilisation • Maitrise des outils de sensibilisation
D. Effectuer des campagnes de phishing	• Compréhension claire des attaques de phishing • Gestion efficace d'une campagne de sensibilisation

Suggestions Pédagogiques

Compétence 14 :	**Appliquer des stratégies de gestion des risques**	**Code : DIA_IDOCS_TS-14**
DURÉE : 90 h	**Compétences Préalables : 1/2/3/4/5/6/7/8/9**	
Type de compétences : Spécifique	**Compétences en parallèles :** Compétence à effectuer seule	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Effectuer la modélisation de menaces	A.1 – Identifier les phases de la modélisation des menaces	• Conception • Détection • Correction • Vérification	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle du fournisseur • Travaux pratiques : Modélisation des menaces de déni de service et du spoofing en utilisant le Framework STRIDE	20 %
	A.2 – Découvrir le framework de modélisation	• STRIDE de Microsoft • OWASP		
B. Gérer les risques	B.1 – Définir les scénarios de risques	• Relation menace et vulnérabilité • Probabilité et impact	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle des normes	30%

	B.2 – Se familiariser avec les méthodes EBIOS Risk Manager et ISO 27005	• EBIOS Risk Manager • Norme ISO 27005	• Travaux pratiques : Etude de cas : Analyse de risque du travail à distance	
C. Sensibiliser les utilisateurs aux risques de sécurité	C.1 – Définir un programme de sensibilisation	• Analyse • Planification • Déploiement • Mesure • Optimisation	• Seul ou en groupe • Cours fournis par le formateur • Documentation officielle des normes • Travaux pratiques : Elaboration d'un programme de sensibilisation et utilisation du kit pour effectuer une campagne de sensibilisation sur la protection des mots de passe	25%
	C.2- Prendre en main les outils de sensibilisation	• Le kit de sensibilisation aux risques numériques • CYBERMOI/S		
D. Effectuer des campagnes de phishing	D.1 – Définir une attaque par phishing	• Caractéristiques de l'attaque phishing • Types de phishing	• Seul ou en groupe • Cours fournis par le formateur	25 %

	D.2 – Effectuer un test de phishing	• Outil gophish • Eléments de protection	• Documentation officielle des normes • Travaux pratiques : Lancement d'un test de phishing sur un groupe d'utilisateurs de la classe et mesure des indicateurs	

Fiche prescrite

Compétence 15 : S'intégrer en milieu professionnel	
Code de la compétence : DIA_IDOSR_TS-15	**Durée : 160 heures**
Contexte de réalisation	**Critères généraux de performance**
• Individuellement et sous la supervision du formateur encadrant et du tuteur en entreprise • À partir : - Besoin spécifique en entreprise - De mises en situations écrites et orales - De consignes - De spécifications fonctionnelles - De base documentaire • À l'aide : - Divers outils disponibles selon le lieu du stage	• Plan d'action de recherche active de stage • Adoption d'une attitude professionnelle • Respect des échéances • Résolution de la problématique posée • Qualité des productions • Cohérence entre le rapport fourni et les tâches effectuées • Soutenance des activités réalisées durant la période de stage
Éléments de la compétence	**Critères particuliers de performance**
A. Préparer son stage en milieu de travail	• Cohérence du plan de recherche d'emploi/stage • Respect des règles de communication écrite/orale • Pertinence de la lettre de motivation Description pertinente des techniques de recherche de stage
B. Réaliser des activités en milieu de travail	• Attitudes professionnelles positives • Manipulation judicieuse des données numériques

	• Résolution correcte des problèmes • Respect d'une démarche méthodique • Respect des règles de santé/sécurité • Respect de la hiérarchie • Bonne exécution des tâches à effectuer • Capacités de planification des activités de travail • Pertinence du journal de bord
C. Rédiger un rapport faisant état des activités exercées	• Sens de l'autonomie • Rédaction du rapport selon les normes • Pertinence des informations du rapport • Cohérence entre le rapport et le vécu en entreprise • Bonne présentation des activités du stage • Transition entre la perception du métier (cursus) et la réalité du milieu de travail

Suggestions Pédagogiques

Compétence 15 :	**S'intégrer en milieu professionnel**	**Code : DIA_IDOSR_TS-15**
DURÉE : 160 h	**Compétences Préalables :** Compétences 9/10/11/12/13/14/15	
Type de compétences : Spécifique	**Compétences en parallèles :** N/A	

ÉLÉMENTS DE LA COMPÉTENCE	APPRENTISSAGES DE BASE	ÉLÉMENTS DE CONTENU	ACTIVITÉS D'APPRENTISSAGE	DURÉE SUGGÉRÉE
A. Préparer son stage en milieu de travail	A.1- Décrire les attitudes nécessaires à la recherche dynamique d'un lieu de stage	• Esprit d'initiative • Sens des responsabilités • Attitude positive • Esprit méthodique	• Activités et jeux de rôles permettant aux stagiaires d'acquérir : ✓ Prise de connaissance des informations et modalités relatives aux stages ✓ Critères de sélection des entreprises ✓ Choix des entreprises susceptibles de recevoir des stagiaires ✓ Démarches pour décrocher un stage ✓ Attitudes et comportements en entreprise	25%
	A.2- Exploiter les moyens de recherche de stage	• Buts du stage : ✓ Observation de diverses facettes du métier ✓ Réalisation d'activités professionnelles ✓ Renforcement des habiletés cognitives et perceptuelles ✓ Changement de perception qu'entraîne un séjour en entreprise ✓ Familiarisation avec le milieu • Documents officiels : ✓ Lois ✓ Règlements		

		✓ Conventions diverses (de stage…) ✓ Assurances ✓ Politiques de l'entreprise • Types d'entreprises : ✓ Grande ✓ Moyenne ✓ PME, Start up • Catégories d'entreprises : ✓ Services ✓ Production • Répertoire des entreprises • Consultation d'une banque de données • Lettre de demande de stage • Curriculum vitae • Contacts téléphoniques • Messagerie électronique • Plateformes de réseautage (Linkedin…) • Demandes d'entrevues		
	A.3- Décrire le comportement à adopter en milieu de travail	• Attitude d'écoute • Sens de l'observation • Respect des règles de santé / sécurité • Tact et discrétion • Attitude positive • Communication de qualité • Intérêt marqué pour toute nouvelle expérience de		

		travail • Souci de l'excellence		
B. Réaliser des activités en milieu de travail	B.1- Connaître l'environnement du milieu de travail	• Milieu socio-économique : ✓ Produits ✓ Marché • Associations professionnelles • Structures • Équipement • Évolution technologique • Relations interpersonnelles • Santé et sécurité • Éléments à consigner : ✓ Possibilité du marché du travail (nouveaux emplois, emplois à la hausse, création d'emplois) ✓ Conditions de travail (horaire, salaire, santé et sécurité au travail) ✓ Contraintes du marché du travail (chômage, compétition, mobilité, formation, spécialité, développement technologique, instabilité économique)	• Activités sur: ✓ Aspects du métier qui différent de la formation reçue ✓ Ecosystème, environnement socio-économique ✓ Compréhension des termes du cahier des charges sous la supervision de l'encadrant en entreprise ✓ Observation du contexte de travail et diverses facettes du métier ✓ Réalisation des tâches professionnelles telles qu'elles sont spécifiées dans le CC ✓ Participation à divers échanges interprofessionnels	50%
	B.2- Réaliser des activités professionnelles	• Tâches professionnelles en rapport : ✓ Au service à la clientèle ✓ À la planification du travail ✓ À la demande de l'utilisateur final		

		✓ Au diagnostic ✓ À l'installation d'ordinateurs et de périphériques ✓ À l'installation d'applications ✓ Au développement d'applications ✓ Aux divers paramétrages et configurations ✓ À l'entretien d'un parc informatique ✓ Etc…		
	B.3- Adopter une méthodologie d'organisation du travail	• Journal de bord comprenant : ✓ Evénements de la journée ✓ Activités réalisées ✓ Fiches de travail ✓ Objectifs d'apprentissages ✓ Objectifs personnels… • Importance du journal de bord : ✓ Suivi des activités ✓ Evaluation ✓ Validation (tuteur en entreprise/formateur)		
C. Rédiger un rapport faisant état des activités exercées	C.1- Rédiger un compte rendu d'activités selon les normes en vigueur	• Observations : ✓ Sur le contexte de travail ✓ Sur les tâches observées • Tâches effectuées • Éléments d'un rapport : ✓ Présentation ✓ Introduction ✓ Développement ✓ Conclusion • Validation	• Activités sur : ✓ Rapport faisant état des observations et tâches effectuées par le stagiaire au cours du stage ✓ Comparaison de la perception du métier avec les réalités du milieu de travail ✓ Présentation orale des activités réalisées en stage devant un groupe de stagiaires et formateurs ✓ Synthèse/bilan personnel vis-à-vis	25%

		• Soutenance (présentation orale des activités réalisées en stage devant un groupe de stagiaires et formateurs)	du vécu en milieu de travail	
	C.2- Enumérer ses aptitudes associées au métier	• Aptitudes : ✓ Au plan professionnel ✓ Au plan social • Goûts • Champs d'intérêt : ✓ Personnels ✓ Professionnels		
	C.3- Comparer les perceptions du métier avec les réalités du milieu de travail	• Métier et formation : ✓ Eléments du processus ✓ Outillage ✓ Équipement ✓ Technologie ✓ Rythme de production ✓ Tâches et opérations ✓ Importance et indices de difficultés relatives aux tâches et aux étapes du processus ✓ Autorité ✓ Ponctualité ✓ Assiduité		