SYLLABUS DE : (*SECURITE DES SYSTEMES D'INFORMATION*)

Formation en ***Sécurité Informatique***

Session de 2023 / 23024

Durée : 300 heures

Nom du formateur : NNOMZOA Raphael

Numéro de téléphone : 6 71 15 86 05/6 56 22 02 48

I- Description du métier de la spécialité

Effectue la conception, l'installation, la gestion et la sécurisation des réseaux, des serveurs et des ordinateurs.

II- Débouchés de la spécialité

Perspectives d'emploi

Les diplômés peuvent occupés des postes d'emplois suivants :

- ***Exemples d'emplois :***
  - ***Administrateur de systèmes***
  - ***Administrateur de réseaux***
  - ***Consultant en sécurité***

III- Prérequis de la formation

Dans le cadre de ta formation, pour l'apprenant/apprenant, l'action de formation vise à ;

- *maîtriser les technologies au cœur des réseaux informatiques et d'Internet;*
- *comprendre les principaux enjeux en cybersécurité;*
- *mettre en œuvre et gérer divers types d'infrastructures :*
  - *réseaux sans fil et connectés;*
  - *environnements Microsoft (Active Directory, Exchange);*
  - *système Linux.*
- *travailler sur des projets qui ciblent des problématiques concrètes vécues en entreprise.*
- *le montage d'un serveur courriel;*
- *la maintenance d'une infrastructure;*
- *du soutien technique aux usagers;*

- *le diagnostic et le dépannage d'un réseau dans des situations complexes.*

IV- Cibles

- *Etudiants*
- *Les élèves du secondaire (post-baccalauréat et pré-baccalauréat)*
- *Les travailleurs des entreprises exerçants dans le secteur informatique ou disposant des infrastructures informatiques*
- *Les religieux*

V- Matériel nécessaire

- ***Ordinateurs (desktops ou portables)***
- ***Logiciels (système d'exploitation, sécurité,…)***
- ***Server***

VI- Objectif Pédagogique Général

*Le programme de formation en **Sécurité Informatique** vise à former des techniciennes ou techniciens en informatique qui exerceront leur profession dans les domaines de l'administration, la sécurisation des réseaux informatiques et de la cybersécurité .*

VII- Objectifs Pédagogiques Spécifiques

N°	Objectifs P.	Description
OP1.	*Fondamentaux de la Sécurité Informatique*	*l'objectif visé est de maitriser les notions suivantes : la sécurité informatique, les attaques et les menaces, la cryptographie, la sécurité physique et logique*
OP2.	*Réseaux et Sécurité*	*L'apprenant doit être capable de : maitriser l'architecture des réseaux et protocoles, de sécuriser des réseaux et paramétrer le pare-feu, connaitre la détection d'intrusion (IDS) et prévention (IPS), sécuriser un réseau sans fil*
OP3.	*Systèmes d'Exploitation Sécurisés*	*L'apprenant doit être capable d'installer et configurer les paramètres de sécurité d'un system d'exploitation linux ou Windows, de mise à jour et enfin renforcer la sécurité d'un système d'exploitation*

OP4.	*Hacking Éthique et Tests de Pénétration*	*L'objectifs visé est de : maitriser la notion de hacking éthique, savoir implémenter les tests de pénétration, maitriser les outils de hacking éthique, savoir faire une analyse des vulnérabilités et élaborer les rapports de sécurité.*
OP5.	*Sécurité Applicative*	*Pour démontrer sa compétence l'apprenant doit être capable de : programmer des applications sécurisées dans un contexte Web et mobile; construire et manipuler des bases de données sécuritaires; configurer certains services sur des serveurs et du matériel informatique incluant des objets connectés*
OP6.	*Gestion des Risques et Conformité*	*Pour démontrer sa compétence l'apprenant doit être capable de : d'évaluer et gérer les risques et les incidents, connaitre les standards de sécurité, faire la planification d'un système sécurisé, mettre en œuvre des formations.*
OP7.	*Sécurité Cloud et Virtualisation*	*L'apprenant doit être capable de : sécuriser un environnement cloud, virtualiser et gerer des identités et des accès dans le cloud*
OP8.	*Projet Final et Simulation d'Attaque*	*Pour démontrer sa compétence l'apprenant doit être capable de: élaborer des projets intégrateurs et réalistes dans une stratégie sécuritaire; en répondant aux besoins d'un client réel dans une situation réelle, dans le cadre du cours Projet, en faisant un stage d'intégration en milieu de travail, à temps plein, pour toute la durée du stage.*

VIII- Les Évaluations Académiques

N°	Code Objectifs P.	Évaluations	Type	Résultat Attendu
1.	*OP1*	**L'évaluation est individuelle, en salle surveillée**	*théorique*	*L'apprenant/apprenante peut s'exprimer sur des notions liées à la sécurité informatique, à la cybersécurité, a piratage informatique.*
2.	*OP2*	**L'évaluation est individuelle, en salle surveillée**	*Théorique 25%* *Pratique 75%*	*L'apprenant/apprenante est capable de maitriser les différents types d'architecture et protocole.* *Configurer les différents pare-feu, intrusion et sécuriser n réseau sans fil de manière pratique.*

3.	*OP3*	**L'évaluation est individuelle, en salle surveillée**	*Théorique 25%* *Pratique 75%*	*L'apprenante/l'apprenant doit être capable cerner les différents outils de sécurité d'un système d'exploitation.* *Paramétrer les outils de sécurité (Windows/linux)*
4.	*OP4*	**L'évaluation est individuelle, en salle surveillée**	*Théorique 20%* *Pratique 80%*	*Restituer tos les actes de piratage, et cybersécurité* *Avoir acquis un savoir-faire en matière de cyberattaque*
5.	*OP5*	**L'évaluation est individuelle, en salle surveillée**	*Théorique 20%* *Pratique 80%*	*L'apprenante/apprenant doit présenter des aptitudes à pouvoir réagir dans la sauvegarde des données, la sécurisation d'une base de donnée, le développement des application de sécurité*
6.	*OP5*	**Projet de réalisation**	*Pratique 90%* *Théorique 10%*	projets intégrateurs et réalistes dans une stratégie sécuritaire

IX- LE CONTENU DE LA FORMATION

N°	Module	Coef.	Durée	CHAPITRES	Objectifs Pédagogiques
	Fondamentaux de la Sécurité Informatique ***(théorique 100%)***	3	24h	• ***Introduction à la sécurité informatique*** • ***Notions de base sur les attaques et les menaces*** • ***Principes de base de la cryptographie*** • ***Sécurité physique et logique Veillez décrire ci-dessous***	OP1
	Systèmes d'Exploitation ***théorique 25% pratique 75%***	5	48h	• ***Sécurité des systèmes d'exploitation (Windows, Linux)*** • ***Gestion des correctifs et mises à jour*** • ***Durcissement des systèmes***	OP1

	Réseaux et Sécurité ***Théorique 20%*** ***Pratique 80%***	5	48h	• ***Architecture des réseaux et protocoles*** • ***Sécurité des réseaux et pare-feu*** • ***Détection d'intrusion (IDS) et prévention (IPS)*** • ***Sécurité sans fil Veillez décrire ci-dessous***	OP2
	Hacking Éthique et Tests de Pénétration ***Théorique 25%*** ***Pratique 75%***	4	36h	• ***Introduction au hacking éthique*** • ***Méthodologie de tests de pénétration*** • ***Outils de hacking éthique*** • ***Analyse des vulnérabilités et rapports de sécurité***	
	Sécurité Applicative ***Théorique 10%*** ***Pratique 90%***	6	60h	• ***Sécurité des applications web*** • ***Développement sécurisé*** • ***Sécurité des bases de données*** • ***Sécurité des applications mobiles***	
	Gestion des Risques et Conformité ***Théorique 80%*** ***Pratique 20%***	3	36h	• ***Évaluation des risques et gestion des incidents*** • ***Conformité réglementaire et normes de sécurité*** • ***Planification de la continuité des activités et reprise après incident*** • ***Sensibilisation à la sécurité***	
	Sécurité Cloud et Virtualisation	4	36h	• **Sécurité dans les environnements cloud** • **Virtualisation et sécurité** • **Gestion des identités et des accès dans le cloud**	

X-Le Dispositif de la formation

Éléments	Configuration
Matériel de Formation	- *Salle de formation climatisée* - *Tableau Blanc + Marqueurs* - *Connexion Internet*
Format Pédagogique	- *Cours théoriques de 3 à 4h en présentiel* - *Coaching personnalisé des apprenants*

Méthodes Pédagogiques	- *Cours Magistraux* - *Séances démonstratives* - *Exposés des apprenants* - *Etude de cas* - *Séances de Travaux Pratiques Assistés* - *TD*
Types de supports	- *Documents pour les cours magistraux* - *Document de l'apprenant* - *Documents Word et PDF pour les tests de préparation.*
Timing de la formation	- ***Durée :*** *?????????* - ***Planning hebdomadaire :***

XI- Le Séquençage

Module 1 : Fondamentaux de la Sécurité Informatique

Séances (03 -4h/séance)	Titre, Résumé, Approche Pédagogique	Objectifs Pédagogiques	Supports
Séance 01	**Généralités sur la sécurité – définitions – les différentes formes de sécurité -** *L'apprenante/apprenant se familiarise avec les concepts de sécurité informatique*	**OP1**	**Numérique (Word)**
Séance 02	**les attaques et les menaces informatiques – les différents types d'attaques et menaces – modes opératoires - cryptographie** *l'apprenante/apprenant prend connaissance des formes de cyberattaques et également des méthodes de sécurité et d'authentification à travers la cryptographie*		**Numérique(Word)**
Séance 03	**La cryptographie – la sécurité physique et logique** L'apprenant/apprenante apprend à le chiffrement symétrique à travers quelques codes et l'importance de la sécurité physique		**Numérique(Word)**
Evaluation	**Théorique**		**Physique**

Module 2 : Systèmes d'Exploitation Sécurisés

Séances (03 -4h/séance)	Titre, Résumé, Approche Pédagogique	Objectifs Pédagogiques	Supports
Séance 01	**Introduction aux systèmes d'exploitations – différents systèmes d'exploitation et leur niveau de sécurité** *L'apprenant/apprenante se familiarise avec l'environnement sécuritaire à partir d'un système d'exploitation*	**OP1**	Numérique(Word)
Séance 02	**Système Windows et paramètres de sécurité** *L'apprenant/apprenante acquiert la compétence de paramètre un système Windows en particulier les versions récentes*		Numérique, Logiciels
Séance 03	***Installation et paramétrage de système linux*** *L'apprenant/apprenant acquiert la compétence sr les outils de sécurité linux*		Numérique, Logiciels
Évaluation	**Théorique & pratique**		Physique

Module 3 : Réseaux et Sécurité

Séances (03 -4h/séance)	Titre, Résumé, Approche Pédagogique	Objectifs Pédagogiques	Supports
Séance 01	**Architecture des réseaux – les protocoles réseaux** Pour démontrer sa compétence, l'apprenant doit être capable de : déterminer une architecture réseau connaitre les modèles OSI et les protocoles TCP/IP et les antres protocoles internet	**OP2**	Numériques (Word)
Séance 02	**les protocoles réseaux et internet - Sécurité des réseaux - pare-feu** Pour démontrer sa compétence l'apprenant doit être capable de : Implémenter les normes de sécurité, en fonction des différents protocoles		Kit de sécurité Numérique (Word)
Séance 03	**Détection d'intrusion (IDS) et prévention (IPS)** **Sécurité sans fil** Pour démontrer sa compétence l'apprenant doit être capable de : d'implémenter un dispositif de sécurité pour les réseaux sans fil configurer et implémenter les systèmes IDS et IPS		Kit de sécurité Numérique (Word)
Évaluation	**Théorique & pratique**		physique/numérique

Module 4 : Hacking Éthique et Tests de Pénétration

Séances (03 -4h/séance)	Titre, Résumé, Approche Pédagogique	Objectifs Pédagogiques	Supports
Séance 01	**Introduction au hacking éthique** *L'apprenant/apprenante doit prendre connaissance des différentes attaques et surtout les plus récentes sur internet*	**OP3**	Numériques (Word)
Séance 02	**Outils de hacking éthique Méthodologie de tests de pénétration** L'apprenant/apprenante doit acquérir la compétence sur les pratiques de cybersécurité		Kit de sécurité Numérique (Word)
Séance 03	**Méthodologie de tests de pénétration - Analyse des vulnérabilités et rapports de sécurité** *L'apprenant/apprenante doit acquérir la compétence sur les pratiques de cybersécurité et d'n esprit d'analyse*		Numériques (Word) Kit de sécurité
Évaluation	**théorique & pratique**		numérique et physique

Module 5 : Sécurité Cloud et Virtualisation

Séances (03 -4h/séance)	**Titre, Résumé, Approche Pédagogique**	**Objectifs Pédagogiques**	**Supports**
Séance 01	**Notions de cloud - Généralités sur le cloud** *Pour démontrer sa compétence l'apprenant/apprenante doit être capable de :* - *connaitre 'importance du cloud* - *sauvegarder dans un cloud* - *sécuriser dans le cloud*	**OP4**	Numériques (Word)
Séance 02	**Virtualisation – sécurité - Gestion des identités** *Pour démontrer sa compétence l'apprenant/apprenante doit être capable de :* - *installer et configurer un logiciel* - *d'implémenter une sécurité virtuelle*		Numériques (Word) logiciel ordinateur
Séance 03	**Gestion des identité et des Accès** *Pour démontrer sa compétence l'apprenant/l'apprenante doit être capable de :* - *implémenter les codes de sécurité à partir d'un chiffrement* - *implémenter un système d'authentifications* - *contrôler les accès aux données sur le cloud*		ordinateur logiciels
Évaluation	**théorique & pratique**		numérique

Module 6 : Sécurité Applicative

Séances (03 -4h/séance)	**Titre, Résumé, Approche Pédagogique**	**Objectifs Pédagogiques**	**Supports**
Séance 01	**Développement applications web -sécurité** Pour démontrer sa compétence l'apprenant/apprenante doit être capable de : - participer à la conception d'applications - effectuer le développement et la maintenance. Les applications développées	**OP4**	ordinateur logiciels Numériques (Word)
Séance 02	**bases de données - applications mobiles** *Pour démontrer sa compétence l'apprenant/apprenante doit être capable de* - programmer des applications sécurisées (internet et mobiles) - construire et manipuler des bases de données - configurer certains services sur des serveurs logiques		Numériques (Word) logiciel ordinateur
Séance 03	**sécurisation : bases de données – applications mobiles** Pour démontrer sa compétence l'apprenant/apprenante doit être capable de : - sécuriser les base de données - sécuriser les applications mobiles - faire la maintenance des applications développées		Numériques (Word) logiciel ordinateur
Évaluation	**théoriques & pratique**		numérique

Module 7 : Gestion des Risques et Conformité

Séances (03 -4h/séance)	**Titre, Résumé, Approche Pédagogique**	**Objectifs Pédagogiques**	**Supports**
Séance 01	**Évaluation - gestion des risques et des incidents** Pour démontrer sa compétence l'apprenant/apprenante doit être capable de : - savoir-faire preuve d'un esprit logique; - être méthodique et organisé; - développer esprit d'analyse et de synthèse;	**OP5**	ordinateur logiciels Numériques (Word)
Séance 02	**Conformité réglementaire et normes de sécurité - Planification de la continuité des activités** Pour démontrer sa compétence l'apprenant/apprenante doit être capable de : - maitriser les standards internationaux en matière de sécurité informatique et réseau - chiffrer les informations selon les différentes certifications (wifi) - implémenter ne planification des taches		ordinateur logiciels Numériques (Word)
Séance 03	**reprise après incident - Sensibilisation à la sécurité** Pour démontrer sa compétence l'apprenant/apprenante doit être capable de : - savoir former les usagers qui se servent d'un ordinateur o qi travaillent dans un environnement de système d'information - administrer un serveur dans le cadre de la supervision - savoir mettre en place ne stratégie de reprise après une panne		ordinateur logiciels Numériques (Word)
Évaluation	**théorique**		Numériques (Word)