Master spécialisé CyberSécurité en formation continue

1. Contexte et justification

La place des TIC dans nos sociétés est de plus en plus importante, aussi bien pour nos entreprises privées, nos administrations publiques que pour nos États eux-mêmes.

En effet, l'entreprise moderne est celle qui ouvre ses portes au public à travers l'Internet. L'internaute doit pouvoir consulter, interroger, modifier à distance une partie du système d'information de l'entreprise. Offrir la possibilité de mener des transactions financières à distance devient, dans tous les domaines, un enjeu stratégique. De ce fait, la sécurité de l'information constitue l'une des préoccupations majeures aussi bien pour les administrations publiques que pour les entreprises privées. Et comme c'est un secteur en plein essor et qu'il faut être en phase avec cette révolution numérique, nos écoles doivent produire des Hommes compétents, à mesure d'assurer la sécurité des systèmes d'information des institutions publiques comme privées.

Mieux encore, la capacité pour les États de protéger leurs ressources numériques et numérisables devient un enjeu de souveraineté nationale. Chaque État doit avoir à sa disposition des nationaux capables de protéger et défendre son cyberespace, de poursuivre des délinquants dans les nuages.

Les débouchés dans le secteur de la cybersécurité sont nombreux et concernent des domaines très variés comme la sécurisation des réseaux, le commerce électronique, la dématérialisation des procédures administratives, le conseil et l'audit de sécurité, la conception d'architecture réseau sécurisée, l'investigation numérique, etc.

Pour répondre à cette demande, l'École Supérieure d'Informatique de l'Université Nazi BONI (anciennement Université Polytechnique de Bobo-Dioulasso) propose une formation continue de niveau Master 2 en informatique, avec pour spécialité la cybersécurité.

Cette formation en **Cybersécurité** offerte en formation continue permet, d'une part, à des informaticiens de niveau Bac + 4 au moins de se spécialiser dans le domaine de la sécurité des systèmes informatiques et des réseaux. D'autre part, elle offre aux responsables en charge de la sécurité des systèmes d'information (RSSI) des entreprises et des institutions de renforcer leurs compétences dans le domaine de la cybersécurité. Elle vise à :

- sensibiliser les informaticiens à la problématique de la sécurité des systèmes numériques, en particulier en rapport avec les technologies émergentes (IoT, Cloud, e-services, etc.) ;
- donner une qualification de haut niveau permettant l'adaptation aux évolutions technologiques très rapides dans ce domaine ;
- répondre à la forte demande de spécialistes en sécurité des systèmes d'information.

2. Public cible et objectif de la formation

Le candidat à cette formation doit soit avoir un niveau Bac + 4 au moins en informatique ou dans un domaine connexe, soit disposer d'un diplôme d'ingénieur de conception (télécommunications, informatique) ou de tout autre diplôme équivalent. Pour les candidats de niveau Bac + 3, une validation des acquis professionnels est possible après justification d'une expérience d'au moins trois ans dans la gestion de la sécurité des systèmes d'information.

Dans tous les cas, l'admission est prononcée après un examen du dossier de candidature et d'un entretien éventuel. Le nombre de places est limité à vingt (20).

3. Dispositif de formation

La formation se fera en semi-présentiel. Elle comporte une phase en présentiel et une phase à distance.

3.1 Regroupement en présentiel

La partie FOAD (Formation ouverte et à distance) concernera les cours théoriques via une plate-forme dédiée. Des regroupements périodiques en présentiel sont prévus pour les travaux pratiques et les évaluations. A cet effet, il est prévu trois sessions de regroupement en présentiel :

- La première qui interviendra à la fin de l'animation théorique des trois premières UE et durera 6 jours. Cette session regroupera tous les apprenants. Elle portera sur des travaux pratiques des cours écoulés durant le premier trimestre de la formation. Elle aura lieu à Bobo-Dioulasso.
- La deuxième session des travaux pratiques durera 6 jours et portera sur les UE 4 à 7. Elle aura lieu à Bobo-Dioulasso..
- Le troisième regroupement concerne essentiellement les évaluations sommatives et aura lieu simultanément à Ouagadougou et à Bobo-Dioulasso.

La présence à ces regroupements est obligatoire. Les frais éventuels de transport et de séjour sont à la charge des apprenants.

3.2. Phase à distance

Dans cette phase, les échanges se feront à distance sur la plate-forme de la formation. Les tuteurs accompagneront les apprenants à l'appropriation des contenus et dans la réalisation des activités d'apprentissage.

Les rencontres synchrones en ligne (tchat ou visio-conférence) entre apprenants et tuteurs se feront sur rendez-vous communiqués aux apprenants par le coordonnateur du Master. Toutes les rencontres seront archivées afin de permettre aux apprenants de revenir après sur ces échanges.

Les modules sont structurés en unités d'apprentissage qui comportent chacune un contenu et des activités d'apprentissage et des ressources. Aussi bien des travaux individuels que collaboratifs seront soumis aux apprenants dans cette phase de la formation. Tous ces travaux devront être déposés sur la plate-forme.

4. Compétences attendues

La formation continue de Master en cybersécurité est de type professionnel. Il vise à rendre l'apprenant opérationnel en matière de gestion de la sécurité. A l'issue du Master, l'étudiant sera capable de :

- maîtriser les méthodes organisationnelles de conception de politique de sécurité (méthode EBIOS, normes ISO 17799 et ISO 27001…) ;
- investiguer les problèmes de sécurité d'un systèmes informatique ;
- maîtriser les techniques opérationnelles de gestion des authentifications des accès, de la confidentialité des échanges, de l'intégrité des données échangées et de la disponibilité des ressources d'un système d'information ;
- appréhender, dans toutes ses dimensions, les problématiques liées aux technologies émergentes (IoT, Cloud, etc.) ;
- mettre en perspective l'environnement technique, économique et juridique dans lequel doit être créée la politique de sécurité du système d'information.

5. Processus de la formation

La formation en Master cybersécurité a une durée d'une année académique. Dès l'inscription et le règlement des droits, l'étudiant reçoit un code d'accès qui lui permet d'accéder aux contenus et aux activités du Master. Les enseignements commenceront le 1er février 2021.

Le tutorat fonctionne par module. Un module est animé par un tuteur durant une ou deux semaines. Durant ce temps, les apprenants mèneront des échanges synchrones (tchat ou visio/audio-conférence) et asynchrones (forums) avec le tuteur. Ils auront également à traiter et à déposer des travaux de maison. Dans la note du module les travaux de maison comptent pour 40 %, tandis que l'examen écrit compte pour 60 %. Les regroupements en présentiel d'une durée d'une (1) semaine chacun auront lieu en fin avril, mi-août et mi-décembre. A l'issue des différentes compositions, seront déclarés admis les étudiants ayant validé 100 % des unités d'enseignement (UE) programmés. Toutefois, les étudiants n'ayant pas validé toutes les UE pourront se présenter à une session de rattrapage qui sera organisée à cet effet en fin février 2022.

En plus de la validations des UE, les apprenants doivent obligatoirement valider deux (2) certificats professionnels parmi une dizaine qui seront proposés durant les 16 mois que durera la formation. Ils sont également appelés à participer à au moins deux (2) évènements scientifiques en relation avec la sécurité des réseaux informatiques (worshop, conférence, journée de recherche en informatique, mastériales, etc).

La période des stages est de janvier à juin 2022. Les soutenances ont lieu dans la première semaine de juillet 2022. ***Si au bout des quatre sessions d'examens consécutives, l'étudiant n'a pas validé toutes les UE, il ne sera plus admis à se ré-inscrire.***

6. Modalité d'évaluation

Les évaluations régulières en ligne aident les étudiants à mieux assimiler les cours ; on y retrouve :

- les évaluations écrites suite à la transmission des rapports en ligne par les apprenants ;
- les évaluations de la participation aux activités/échanges synchrones (tchat, visio/audio conférence) et asynchrones (forum de discussion, glossaire, wiki, messagerie ...) ;
- les évaluations synchrones sur la base d'épreuves (QCM, QB, etc.) ;
- les évaluation des travaux collaboratifs réalisés en équipes d'apprenants ;
- les examens en salle à l'UNB et dans les campus des universités partenaires (UJKZ de Ouagadougou pour le moment).

7. Conditions d'inscription

La composition et la date de dépôt des dossiers de candidature seront communiquées dans le mois de décembre 2020. La liste des candidats sélectionnés sera communiquée en fin janvier 2021.

Les candidats retenus seront officiellement informés, par courrier électronique de leur sélection. **Aucune communication individuelle ne sera effectuée auprès des candidats non retenus.**

Après la publication des résultats du recrutement, les candidats retenus auront une semaine (07 jours) pour confirmer leur inscription et s'acquitter des frais de formation ainsi que des frais d'inscription.

Les candidatures retenues en liste d'attente seront examinées en fonction des désistements.

8. Conditions financières

Le communiqué du recrutement indiquera le coût de la formation ainsi que les modalités de règlement.

9. Programme de formation

Tableau 1 - Détails des UE du semestre 3.

UE	**ECU**
1-Bases de la Sécurité	Introduction à la sécurité informatique
	Fondements de la cryptographie
2-Sécurité des réseaux et systèmes	Sécurité des réseaux (protocoles de sécurité, architecture de sécurité, outils de sécurité)
	Sécurité des systèmes
3-Sécurité des services réseau	Virologie / Protection contre les virus
	Mise en œuvre et configuration des boîtiers de Sécurité ASA
	Sécurité des services réseau (DNSSEC, messagerie, HTTPS, VoIP, etc.)
4-Cryptographie et applications	Aspects algorithmiques de l'implémentation d'un cryptosystème
	Authentification forte et protocoles cryptographiques
	Confiance numérique
	PKI et signature électronique (y compris aspects juridiques et normatifs)
5-Investigation numérique (digital forensic)	Test de pénétration
	Investigation Numérique Légale
6-Identification / authentification	Identity Access Management
	Traitement d'images et reconnaissance de formes en biométrie
	Authentification biométrique : systèmes et usages
	Sécurité des e-services (y compris Infrastructures de Services Pour le paiement et Le contrôle d'identité)
7-Technologies émergentes et sécurité	Internet des objets (IoT) et sécurité
	SDN et sécurité
	Sécurisation des Services IaaS du Cloud
	Sécurité des systèmes à carte à puces

Tableau 2 - Détails des UE du semestre 4.

UE	**ECU**
8-Gestion de la sécurité	Plan stratégique de sécurisation des réseaux
	Administration de la sécurité
	Plan de continuité d'activité (ISO / IEC 27035,
	Management de la sécurité (Normes de la famille ISO 27000)
9-Audit des systèmes et réseaux	Audit des systèmes
	Audit des réseaux
	Audits / analyses techniques
10-Stage	Mémoire de fin de cycle