

DIPLÔME D'UNIVERSITÉ

ACCESSIBLE EN
FORMATION CONTINUE



Lieu de la formation
Angers

Chiffres clés
98% de taux de réussite

Contact
Sylvie LAILLER
sylvie.lailler@univ-angers.fr
Tél. : 02 44 68 86 98

**Responsable
de la formation**
Yves NORMAND
yves.normand@univ-angers.fr

Adresse web
www.univ-angers.fr/formationcontinue



Partenaires



SÉCURITÉ DES SYSTÈMES D'INFORMATION EN SANTÉ (SSIS)

Objectifs

Le système de santé est en pleine évolution (nouveaux besoins des patients et des professionnels de santé, modification du contexte économique, réglementaire et politique, GHT). L'hôpital numérique et communicant constitue un levier très fort pour répondre à ces enjeux. La confidentialité des données de santé des patients doit être absolument garantie. Les professionnels de santé ont de fortes exigences en matière d'accessibilité à la bonne information et au bon moment : garantir l'intégrité et la disponibilité des données de santé. Le système d'information et la sécurité de l'information sont des éléments nécessaires et incontournables :

- Amélioration de la prise en charge des patients,
- Conformité réglementaire et normative (décrets, HAS, Hôpital Numérique,...).
- Développement des coopérations de santé.

La sécurité de l'information et du SI doit être une source de valeur pour l'organisation et les parties prenantes.

C'est dans ce contexte que s'inscrit la formation de Sécurité des systèmes d'information en santé (SSIS), validée par un Diplôme d'Université (DU) et vise les objectifs suivants :

- Définir une stratégie et une politique de gestion des risques, et de sécurité de l'information et des systèmes d'information en santé ;
- Mener à bien un audit du système de management de sécurité de l'information suivant les référentiels normatifs et les exigences réglementaires ;
- Élaborer et superviser l'élaboration d'un cahier des charges pour la mise en place d'un système d'information sécurisé de santé.
- Être capable de travailler en collaboration avec les différents métiers de son organisme : savoir-faire et savoir-être. Cette formation s'inscrit pleinement dans la mise en œuvre des systèmes d'information convergents des GHT.

Insertion professionnelle

- Responsable de la sécurité des systèmes d'information (RSSI) en santé
- Chef de projet Sécurité des SI
- Correspondant informatique et libertés
- Gestionnaire des risques
- Consultant, auditeur, en sécurité de l'information

Public visé

Professionnels en charge de la maîtrise d'ouvrage des systèmes d'information :

- Cadre de santé
- Qualiticien
- Personnel de la direction des systèmes d'information
- Personnel du service informatique
- Personnel du département d'information médicale
- Responsable ou référent de la sécurité du système d'information

Au sein d'un établissement de santé (public ou privé), d'un établissement sanitaire et médico-social, d'une ARS, d'un GCS santé ou télésanté, d'un cabinet de conseil, d'une compagnie d'assurance,...

Conditions d'admission :

- Être titulaire d'un diplôme Bac+2 et d'une expérience professionnelle dans le domaine
- OU par Validation des Acquis Professionnels et Personnels (VAPP) : être titulaire d'un diplôme de niveau Bac minimum et justifier d'une expérience professionnelle significative dans le domaine des systèmes d'information.



**ÉCOLE
D'INGÉNIEURS**
UNIVERSITÉ D'ANGERS



Mise à jour | Février 2018 | Impression service reprographie UA

62 Avenue de Notre Dame du Lac | 49000 Angers
Tél. : 02 44 68 75 00

— Programme

Module 1 :

Cadre juridique, gestion de projets et gestion des risques (6 jours)

- Cadre juridique de l'information en santé : cadre juridique des données de santé, éthique et déontologie, etc. - 3 jours
- Gestion de projets, outils et méthodes : les étapes clés d'un projet - conception - suivi d'avancement et reporting - 2 jours
- Gestion des risques en santé : introduction à la gestion des risques en santé - 1 jour

Module 2 :

Management et sécurité des systèmes d'information (18 jours)

- Conduite du changement - 2 jours
- Techniques de sécurité : sécurité informatique - gestion des accès et des identités numériques (IAM, Politique d'habilitation) - chiffrement et certificats électroniques - plan de secours informatique (PCA/PRA) - 7 jours
- Management de la SSI - Normes ISO 27000 : système de management de la sécurité des SI (SMSI) et savoir-être - audit et certification des SI - audit de sécurité en SI - analyse des risques - politique de sécurité (PSSI) - 8 jours
- Audit technique intrusif SSI - 1 jour

Module 3 :

Projet appliqué (120 heures)

- Mise en œuvre des connaissances sur un projet terrain réalisé dans le cadre de l'activité professionnelle habituelle

— À noter

Organisation de la formation :

- Durée : 180 heures (24 jours) + 120 heures de projet dans le cadre de l'activité professionnelle habituelle
- Calendrier : de janvier à juin, à raison d'un regroupement de deux journées toutes les deux semaines (7,5 heures par jour)
- Intervenants : enseignants universitaires et professionnels de l'ISSBA
- Examens : 1 journée d'épreuves écrites et ½ journée de soutenance

Modalités pratiques :

- Inscription : jusqu'au 3 décembre 2018
- Sélection des dossiers : du 10 au 14 décembre 2018 (sur dossier et entretien)
- Début de la formation : de janvier 2019 (examens fin juin 2019)
- Coût de la formation* : 2700 euros (+ droits universitaires). Prix forfaitaire exonéré de TVA.

Pour les personnes souhaitant demander un financement auprès d'un organisme (ANFH, UNIFAF, FONGECIF, OPCALIA, etc), la demande doit être adressée au minimum 3 mois avant le début de la formation.

Visitez notre site

