Nom de l'UE : Authentification et sécurité des données	Semestre : S9

Objectifs de l'UE

A l'issue de ces cours, l'étudiant saura :

- Identifier les processus nécessaires à la gestion des habilitations d'utilisateurs pour l'accès à des ressources
- Mettre en œuvre les outils permettant la création, la modification, et les droits d'accès d'une identité numérique
- Protéger les identités à l'aide de technologies adaptées
- Comprendre le fonctionnement des composants de l'infrastructure de sécurité dans le cloud
- Comprendre le fonctionnement des composants de l'infrastructure de sécurité dans le cloud
- Identifier les modèles de prestation des services dans le cloud (SaaS, laaS) et évaluer les prestations des fournisseurs du cloud
- Effectuer un examen des risques de la sécurité du cloud
- Évaluer les risques par rapport à la mise en œuvre et aux prestations techniques inhérentes aux différents types de cloud (public, privé et hybride)

Description des ECUE

Gestion des identités et des accès

- Gestion d'identités (Annuaires)
- Mise à jour des données, réplication d'annuaires
- Fédération d'identités (SSO)
- Sécurité des accès aux applications (authentification multi-facteur)

Sécurité du cloud

- Architecture et infrastructure fondamentales pour le cloud (privé, public, hybride)
- Sécurité des environnements virtualisés
- Gestion des correctifs et des configurations
- Sécurité des applications et gestion des changements
- Evaluation des risques et gouvernance de la sécurité dans le cloud

Pré-requis

Sécurité et sûreté des données, bases théoriques de la sécurité

Bibliographie

Tim Mather, Subra Kumaraswamy et Shahed Latif, Cloud security and privacy - An enterprise perspective on risks and compliance, Eyrolles, 3ème édition, 2009.

Fabrice Mattatia, RGPD et droit des données personnelles, Eyrolles, 4ème édition, 2019.