# USSI91 - Informatique S4

## Présentation

## Programme

### Contenu

Mis à jour le 18-05-2026

**Code : USSI91**

Unité spécifique de type cours

5 crédits

**Responsabilité nationale :** EPN06 - Mathématique et statistique / Giorgio RUSSOLILLO

Positionnement : Semestre 4 **UE : Informatique** ECTS : 5

Nombre d'heures : 99h

Modalité : Présentiel (100%)

L'UE Informatique est constituée de 3 éléments constitutifs d'UE :

- Entreposage et fouilles de données
- Introduction à la cybersécurité
- Langage Python – S4

La note finale associée à cette UE est calculée en pondérant les notes des 3 ECUE avec les coefficients associés.

**ECUE 1 : Entreposage et fouilles de données (Coef : 3) - 50h (Cours, TD, TP) - 15h (Estimation temps de travail personnel)**

**Objectifs :** Gérer l'entreposage des différentes données et retrouver des données à des fins marketing, comptable, financière ou pour la direction.

**Contenu :**

1. Structures spécifiques des bases de données de Data warehouse (star schema)
2. OLAP
3. Méthodologies générales
4. Pré-traitement des données
    a. Analyses de la qualité des données,
    b. Techniques d'appréhension des valeurs manquantes ou aberrantes
    c. Techniques de construction de bases de travail (agrégations, etc.)
    d. Données et techniques de fouille
5. Méthodes supervisées
    a. Rappels de théorie de l'apprentissage
    b. Arbres de décision
    c. Réseaux de neurones, deep learning
    d. Méta-algorithmes
    e. boosting, bagging

**Compétences visées :**

- Pouvoir lire et analyser un grand nombre de données collectées par les entreprises.
- Comprendre les liens entre la collecte des données et l'activité globale de l'entreprise.
- Pouvoir anticiper les tendances aussi bien marketing que comptables ou encore financières.

**Modalités d'évaluation :** Contrôle continu (rendus de TP)

**ECUE 2 : Introduction à la cybersécurité (Coef : 2) - 28h (Cours, TP, Projet) - 5h (Estimation temps de travail personnel)**

**Objectifs :**

- Comprendre l'évolution historique de la cybercriminalité et les tendances actuelles
- Identifier et sécuriser les menaces spécifiques aux environnements Big Data (réseaux sans fil, objets connectés, etc.)
- Maîtriser les principales techniques d'attaque et les moyens de s'en prémunir
- Savoir diagnostiquer et corriger les vulnérabilités d'un système d'information
- Mettre en place une stratégie de cybersécurité adaptée aux enjeux du Big Data

**Contenu :**

1. Cybercriminalité : Passé, Présent et Futur (7 heures)
    1. Historique des principales cyberattaques
    2. Analyse des menaces actuelles et émergentes
    3. Hiérarchisation des dangers en fonction des types d'attaques
    4. Études de cas sur des incidents notables
    5. TD de recherche sur certaines attaques remarquables (3,5 heures)
2. Sécurité des Environnements Big Data (7 heures)
    1. Sécurité des réseaux sans fil et de l'IoT
    2. Durcissement de la sécurité des équipements mobiles et connectés
    3. Gestion de la sécurité des objets connectés (IoT)
    4. Présentation des guides et bonnes pratiques ANSSI
    5. TD sur la problématique de l'IoT et les dangers futurs que leur développement entraîne (3,5 heures)
3. Techniques d'Attaque et de Défense (7 heures)
    1. Typologie des attaques informatiques
    2. Méthodes d'exploitation des failles (injections SQL, etc.)
    3. Analyse des tendances des ransomwares
    4. Rôle de l'intelligence artificielle en cybersécurité
    5. Top 10 des vulnérabilités OWASP
    6. TD sur la Méthodologie des attaques par Injection SQL (3,5 heures)
4. Diagnostic et Correction des Failles (7 heures)
    1. Analyse et cartographie d'un réseau d'entreprise
    2. Identification et priorisation des vulnérabilités
    3. Mise en place de correctifs et de mesures de sécurité
    4. Élaboration d'un plan de cybersécurité pour une infrastructure Big Data
    5. TD Analyse Réseau local (3,5 heures)

**Modalités d'évaluation :** Contrôle continu

**ECUE 3 : Langage Python – S4 (Coef : 1) - 21h (TP) - 10h (Estimation temps de travail personnel)**

**Objectifs :** La continuité du semestre précédent avec des nouveaux objectifs

**Contenu :**

1. Proposition de projet : un projet doit traiter au moins une des thématiques suivantes
    1. Machine Learning
    2. Deep Learning N
    3. LP (Natural Language Processing)
    4. Computer Vision
2. Identification des objectifs et problématiques correspondantes
3. Rédaction d'un plan de travail pendant 5 séances
    1. Préparation de dataset bruts
    2. Preprocessing de dataset
    3. Développement des méthodes d'IA
    4. Expérimentation
4. Recherche sur l'état de l'art des méthodes existantes :
    1. Quelles sont les méthodes utilisées ?
    2. Avantages et inconvénients de ces méthodes
    3. Proposition une nouvelle méthode
5. Rédaction un rapport de projet o Présentation du projet
    1. Description méthode utilisée, pourquoi cette méthode ?
    2. Résultats obtenus
    3. Perspectives

**Compétences visées :** Maitriser le langage Python et ses utilisations dans l'IA

**Modalités d'évaluation :** Contrôle continu + projet : en groupe, soutenance + démonstration (dernière séance). Notation du code et du rapport.

## Modalités de validation

- Contrôle continu
- Projet(s)