

COURS AVEC SOUTIEN EN FRANÇAIS (CSF) 2023-2024 CAMPUS OF ÁLAVA

Link to website: <https://www.ehu.eus/en/web/vitoria-gasteizko-ingeniaritza-eskola/incoming-students>

Contact: esc-ingenieria.internacional@ehu.es

In addition to the general offer of courses taught in French, some Centers offer for incoming students "Cours avec Soutien en Français" (CSF): subjects taught in Spanish or Basque, in which the syllabus summary; lecturer tutoring, examinations and/or papers are available in French.

Cours Avec Soutien en Français taught in SPANISH:

FACULTY OF ENGINEERING - VITORIA-GASTEIZ (163)

	COURSE	SEMESTER ¹	CREDITS	SCHEDULE ²	LINK TO SYLLABUS
Bachelor's Degree in Computer Management and Information Systems Engineering					
26021	Lenguajes, Computación y Sistemas Inteligentes	1st	6	A	
26025	Sistemas de Gestión de Seguridad de Sistemas de Información	1st	6	M	

¹ SEMESTER: 1st: September 2023 to January 2024

2nd : January 2024 to May 2024

Annual: September 2023 to May 2024

² SCHEDULE: Morning (M)/ Afternoon (A): begins at 13.30.

³ Not available yet. It will be posted soon.

GUÍA DOCENTE 2023/24

163 - Escuela de Ingeniería de Vitoria-Gasteiz

GIIGSI10 - Grado en Ingeniería Informática de Gestión y Sistemas de Informa
Indiferente

2º curso

DESCRIPCIÓN Y CONTEXTUALIZACIÓN DE LA ASIGNATURA

Le contenu de cette matière appartient à une branche classique de l'informatique théorique antérieure aux ordinateurs modernes. Le point de départ est la théorie des automates et des langages formels directement appliquée à la définition des langages de programmation et à la construction des compilateurs.

Les formalismes abordés permettent d'abstraire le concept ordinateur/calcul pour analyser la calculabilité, la complexité et la traçabilité des algorithmes utilisés dans des domaines actuels comme l'optimisation des algorithmes et la cryptographie.

Nous utilisons l'algèbre d'ensembles et la spécification/description formelle des langages, il est donc intéressant d'avoir suivi la matière de Méthodologie de programmation première année de ce Grade, notamment la spécification.

Introduction de moteurs de reconnaissance et de génération de langages. Nous étudions des algorithmes montrant la relation/transformation entre automates, Machines de Turing, expressions régulières et grammaires, ainsi que leurs propriétés. L'utilisation de simulateurs permet de visualiser et de vérifier leur exécution en équipe, en vérifiant les résultats sur papier.

Introduction de concepts d'intelligence artificielle comme modèles alternatifs d'informatique. Ces aspects sont plus approfondis dans la matière de Systèmes d'appui à la décision de la troisième année de ce grade.

COMPETENCIAS / RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA

Identifier et résoudre des problèmes abordables via des modèles informatiques restreints (automates) ou alternatifs (systèmes intelligents).

Utiliser des grammaires et des expressions régulières pour définir des langages formels.

Utiliser un software de reconnaissance et de traitement des modèles.

Comprendre l'existence de limites intrinsèques aux processus informatiques et leurs conséquences.

Connaître et utiliser différents paradigmes de programmation et modèles informatiques alternatifs.

Travailler et analyser les problèmes et leurs solutions informatiques en utilisant la langue verbale, mathématique et graphique.

CONTENIDOS TEÓRICO-PRÁCTICOS

Calcul sans mémoire Automates et traducteurs finis. Langues et expressions régulières. Applications : analyse lexicale.

Mémoire avec restrictions Automates avec pile. Grammaire et langages sans contexte. Automates linéaires délimités. Applications : analyse syntactique.

Le modèle général d'ordinateur et ses limites. Machines de Turing.

L'universalité de l'informatique et la thèse de Church-Turing. Incalculabilité.

Introduction à la complexité informatique. Applications : cryptographie à clé publique.

Alternatives au modèle informatique Modèles de machine et paradigmes de programmation. Circuits et machines réels. Programmes impératifs, fonctionnels et logiques. Applications : raisonnement automatique.

Alternatives au modèle de problème. Spécifications non fonctionnelles. Arbres de décision. Classificateurs. Programmation probabiliste. Applications : systèmes qui apprennent.

METODOLOGÍA

Les cours magistraux (M) décrivent les différentes bases théoriques de la matière en introduisant des algorithmes comme exercices résolus en classe. De nouveaux exercices sont proposés pour être résolus en binômes dans les laboratoires (PL) avec un contrôle effectué par des simulateurs d'automates (JFLAP).

TIPOS DE DOCENCIA				
Tipo de Docencia	M	S	GA	GL
Horas de Docencia Presencial	45			15
Horas de Actividad No Presencial del Alumno	67,5			22,5

SISTEMAS DE EVALUACIÓN	
SISTEMA DE EVALUACIÓN CONTINUA	<input type="checkbox"/>
SISTEMA DE EVALUACIÓN FINAL	<input checked="" type="checkbox"/>

HERRAMIENTAS Y PORCENTAJES DE CALIFICACIÓN		
PRUEBA ESCRITA A DESARROLLAR	<input checked="" type="checkbox"/>	75
PRUEBA TIPO TEST	<input type="checkbox"/>	
DEFENSA ORAL	<input type="checkbox"/>	
REALIZACIÓN DE PRACTICAS (EJERCICIOS, CASOS O PROBLEMAS)	<input checked="" type="checkbox"/>	25
TRABAJOS INDIVIDUALES	<input type="checkbox"/>	
TRABAJOS EN EQUIPO (RESOLUCIÓN DE PROBLEMAS, DISEÑO DE PROYECTOS)	<input type="checkbox"/>	
EXPOSICIÓN DE TRABAJOS, LECTURAS...	<input type="checkbox"/>	
PORTFOLIO	<input type="checkbox"/>	

CONVOCATORIA ORDINARIA: ORIENTACIONES Y RENUNCIA

Note minimale de 5 sur 10 pour réussir la matière

Trois examens partiels comptant chacun pour 25 % de la note de la matière seront effectués. Une session de rattrapage facultative sur chacun des deux premiers blocs pour améliorer la note est possible en session ordinaire. Les travaux pratiques en laboratoire représentant 25% de la note seront évalués au moyen de tests individuels à la fin de ceux-ci.

Si l'étudiant renonce au contrôle continu, un examen final comptant pour 100 % de la note sera effectué. Le choix de cette modalité doit être communiquée au professeur avant la 9ème semaine de cours conformément à la réglementation en vigueur.

En cas d'absence de l'étudiant à l'examen final, celui-ci sera considéré comme non présenté.

CONVOCATORIA EXTRAORDINARIA: ORIENTACIONES Y RENUNCIA

Un examen final comptant 100% de la note sera effectué à l'examen de rattrapage. Aucune note d'évaluation précédente n'est alors prise en compte.

MATERIALES DE USO OBLIGATORIO

Présentations de la matière

Exemples résolus de la matière

Exercices de la matière

Simulateur JFLAP fourni

BIBLIOGRAFÍA

Ramón F. BRENA; "Autómatas y Lenguajes. Un enfoque de diseño", Tec de Monterrey, 2003.

Jean Gallier, "Introduction to the Theory of Computation", University of Pennsylvania, 2018.

Elaine RICH, "Automata, Computability and Complexity. Theory and Applications", Pearson/Prentice Hall, 2008

V. MATHIVET, "Inteligencia Artificial para desarrolladores. Conceptos e implementación en Java", ENI Ediciones, 2017

J.E. HOPCROFT, R. MOTWANI, J.D. ULLMAN: "Teoría de Autómatas, Lenguajes y Computación" 3ª ed. Pearson educación, 2007

S. RUSSELL, P. NORVIG: "Artificial Intelligence: A Modern Approach" 2ª ed. Prentice Hall, 2003

S.H. RODGER, T.W. FINLEY; "JFLAP: An Interactive Formal Languages and Automata Package". Jones and Bartlett, 2006

Bibliografía básica

S. ARORA, B. BARAK: "Computational Complexity: A Modern Approach" Cambridge University, 2009.

D. WOOD; "Theory of computation". John Wiley & Sons, 1987.

T. MITCHELL: "Machine Learning" McGraw Hill, 1997

G.F. LUGER, W.A. STUBBLEFIELD: "Artificial Intelligence. Structures and Strategies for Complex Problem Solving."

Benjamin/Cummings Publishing Company, Inc, 1998.

Bibliografía de profundización

Revistas

Java Computability Tool kit (JCT): <http://humboldt.sunyit.edu/jct/>

Visual and interactive tools (JFLAP): <http://www.jflap.org/>

Machine Learning theory and examples:

<http://www.cs.cmu.edu/~avrim/ML07/index.html>

Implementación de algoritmos de IA en Java: <https://github.com/aima-java/aima-java>

Direcciones de internet de interés

OBSERVACIONES

DESCRIPCIÓN Y CONTEXTUALIZACIÓN DE LA ASIGNATURA

Cette matière concentre deux aspects principaux du grade : les systèmes de gestion et les systèmes d'information. Il se situe dans l'organisation des entreprises et identifie l'importance des trois axes de la cybersécurité pour la continuité des activités : Confidentialité, Intégrité et Disponibilité.

Les enseignants travaillent avec le vocabulaire précis du contexte de la sécurité pour permettre la réalisation d'un diagnostic adapté aux besoins de chaque organisation afin de tracer la voie vers une amélioration continue par le biais des systèmes de Gestion via la réduction progressive des vulnérabilités et la mise en place de sauvegardes sans laisser de côté la formation et la sensibilisation du personnel.

COMPETENCIAS / RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA

Connaître les principaux concepts nécessaires à l'analyse et à la gestion des risques des SI.

Connaître les caractéristiques des normes de gestion de la sécurité SI.

Concevoir, planifier et mettre en œuvre des politiques et des mesures de sécurité informatique appropriées en termes d'efficacité et de coûts.

Intégrer le savoir-faire en matière de sécurité informatique aux niveaux éthique, juridique et organisationnel.

Être en mesure d'effectuer des tâches techniques à intégrer dans un SGSI comme le contrôle de l'adéquation des mots de passe, la sauvegarde, le cryptage, l'utilisation d'anti-malware, les audits et la sécurité physique.

Concevoir des plans de formation pour les personnes liées aux systèmes d'information.

Travailler efficacement en groupe pour coordonner les tâches techniques et organisationnelles.

Connaître le cadre juridique régissant la performance professionnelle (LOPD, LSSI et loi sur les signatures électroniques).

CONTENIDOS TEÓRICO-PRÁCTICOS

Analyse et gestion des risques de sécurité des systèmes d'information.

Sauvegarde des informations.

Contrôle d'accès aux ressources d'information : identification et authentification. La signature numérique.

Logiciels malveillants : risques et mesures de sécurité.

Le facteur humain.

Cryptage de l'information : contextes d'utilisation et techniques de base.

Protection des logiciels.

Planification, organisation et gestion de la sécurité informatique, audits : techniques et normes.

Aspects juridiques, éthiques et organisationnels : la LOPD, la LSSI et la loi sur la signature électronique.

METODOLOGÍA

Les cours magistraux (M) introduisent les concepts par des présentations publiées sur la plateforme eGela, permettant de discuter des principaux axes de la gestion de la sécurité dans le contexte des organisations et de leur importance dans les systèmes d'information.

Les travaux pratiques (GL) permettent de résoudre des problèmes de sécurité typiques par la réflexion individuelle et collective en utilisant des méthodologies actives, y compris la classe inversée.

Les modalités sont variées et comprennent l'étude d'articles scientifiques, d'articles de presse, des exercices à résoudre en groupe, des processus de sélection de

logiciels de protection en groupe et la participation active aux journées de sécurité et de protection des données, entre autres. La présentation des travaux se fait par le biais de rapports et d'exposés publics et est évaluée par l'enseignant et ses collègues.

TIPOS DE DOCENCIA					
Tipo de Docencia	M	S	GA	GL	
Horas de Docencia Presencial	45			15	
Horas de Actividad No Presencial del Alumno	67,5			22,5	

SISTEMAS DE EVALUACIÓN	
SISTEMA DE EVALUACIÓN CONTINUA	<input type="checkbox"/>
SISTEMA DE EVALUACIÓN FINAL	<input checked="" type="checkbox"/>

HERRAMIENTAS Y PORCENTAJES DE CALIFICACIÓN		
PRUEBA ESCRITA A DESARROLLAR	<input checked="" type="checkbox"/>	60
PRUEBA TIPO TEST	<input type="checkbox"/>	
DEFENSA ORAL	<input type="checkbox"/>	
REALIZACIÓN DE PRACTICAS (EJERCICIOS, CASOS O PROBLEMAS)	<input checked="" type="checkbox"/>	40
TRABAJOS INDIVIDUALES	<input type="checkbox"/>	
TRABAJOS EN EQUIPO (RESOLUCIÓN DE PROBLEMAS, DISEÑO DE PROYECTOS)	<input type="checkbox"/>	
EXPOSICIÓN DE TRABAJOS, LECTURAS...	<input type="checkbox"/>	
PORTFOLIO	<input type="checkbox"/>	

CONVOCATORIA ORDINARIA: ORIENTACIONES Y RENUNCIA

Dans le cadre du contrôle continu, des travaux obligatoires de divers types seront effectués tout au long du cours, tant individuellement qu'en groupe. Les livrables comprendront des rapports et des présentations à exposer en classe à évaluer par le professeur et par les pairs selon des critères préétablis.

Pour l'évaluation continue, les travaux pratiques, les rapports et les exposés publics représentent 40 % de la note finale. Un examen final écrit sera effectué pour 60 % de la note finale. Un minimum de 3,5 sur 10 est nécessaire pour approuver la matière.

Si l'étudiant choisit de ne pas se soumettre au contrôle continu, il sera évalué par un examen final comptant pour 100 % de la note. Cette renonciation doit être communiquée au professeur avant la 9ème semaine de cours conformément à la réglementation en vigueur.

Si l'étudiant ne se présente pas à l'examen final, il est considéré comme non présenté.

CONVOCATORIA EXTRAORDINARIA: ORIENTACIONES Y RENUNCIA

L'évaluation en session de rattrapage se fait par un seul examen écrit dans lequel les sujets abordés dans les cours magistraux et travaux pratiques sont examinés, les cas étant mis à jour d'une année à l'autre. Le matériel pertinent exposé par les étudiants eux-mêmes sera mis à la disposition des autres sur la plate-forme eGela pour consultation.

MATERIALES DE USO OBLIGATORIO

Notes de classe, matériel de soutien à l'enseignement en classe et en laboratoire. LOPD, LSSI et Digital Signature Act.

BIBLIOGRAFÍA

Álvaro Gómez Vieites, "Enciclopedia de la Seguridad Informática", Ra-Ma 2011 (2ª edición actualizada)

Jesús Costas Santos, "Seguridad y Alta Disponibilidad", Ra-Ma 2011.

Revistas

IEEE Security & Privacy

.Seguridad <https://revista.seguridad.unam.mx/> (acceso 18/07/2021)

Direcciones de internet de interés

INCIBE: Instituto Nacional de Ciberseguridad (antes INTECO)

<https://www.incibe.es> (acceso: 18/07/2021)

Criptored: red telemática de criptografía y seguridad de la información

<http://www.criptored.upm.es/> (acceso: 18/07/2021)

Intypedia: Information Security Encyclopedia

<https://www.intypedia.com/> (acceso: 18/07/2021)

RedIRIS: Servicio de Seguridad

<https://www.rediris.es/cert/> (acceso: 18/07/2021)

SBD: Security By Default

<http://www.securitybydefault.com/> (acceso: 18/07/2021)

Hispacec

<https://hispacec.com/> (acceso: 18/07/2021)

Agencias Española y Vasca de Protección de Datos

<https://www.agpd.es> (acceso: 18/07/2021)

<https://www.avpd.euskadi.eus/> (acceso: 18/07/2021)

Un informático en el lado del mal (Chema Alonso)

<https://www.elladodelmal.com/> (acceso: 18/07/2021)

Softzone (seguridad)

<https://www.softzone.es/category/seguridad/> (acceso: 18/07/2021)

Cyberseguridad

<https://cyberseguridad.net/> (acceso: 18/07/2021)

Noticias seguridad

<https://noticiasseguridad.com/> (acceso: 18/07/2021)