SÍLABO POR COMPETENCIAS

CURSO:INFORMÁTICA FORENSE Y DELITOS INFORMÁTICOS

DOCENTE: ING. JORGE LUIS BARROZO GUILLEN

SÍLABO DE INFORMÁTICA FORENSE Y DELITOS INFORMÁTICOS

I. DATOS GENERALES

Línea de Carrera	Seguridad Informática
Semestre Académico	2026-I
Código del Curso	3305554
Créditos	4
Horas Semanales	Hrs. Totales: 5 Teóricas: 3 Practicas: 2
Ciclo	X
Sección	A
Apellidos y Nombres del Docente	Barrozo Guillen Jorge Luis
Correo Institucional	jbarrozo@unjfsc.edu.pe
N° de Celular	969325208

II. SUMILLA Y DESCRIPCIÓN DEL CURSO

La Informática o computo forense es una ciencia relativamente nueva dentro de la criminalística, esta última responsable de aportar el acervo probatorio (indicios, evidencias y peritajes) de la comisión del delito y circunstancias de su perpetración, la identificación de su autor y víctima- agraviado; sin embargo por tratarse de una disciplina forense de reciente incorporación, a la fecha no ha logrado estandarizar sus procedimientos periciales, aunque algunos proyectos están en desarrollo, como el C4PDF (Código de Prácticas para Digital Forensics), Manual de Código Abierto para Computación Forense, las Guías de Estándares, Habilidades y Herramientas de la IOCE (International Organization of ComputerEvidence) y el tratamiento de la Evidencia Digital detallado en el RFC 3227, que fue emitida por la Internet Society y la IETF. El desarrollo del curso será en dos perspectivas e integrales: Aspectos legales y técnicos, desde la inspección e investigación del lugar de los hechos o escena del delito hasta el examen y contra examen que es objeto el perito como órgano de prueba.

El contenido de la sumillas del curso está estructurado de la siguiente manera: (I) los delitos informáticos en el Perú. (II) Fundamentos Técnicos de la Informática Forense (III) La Evidencia Digital. (IV) Análisis de Evidencias y Técnicas Antiforense.

III. CAPACIDADES AL FINALIZAR EL CURSO

	CAPACIDAD DE LA UNIDAD DIDACTICA	NOMBRE DE LA UNIDAD DIDACTICA	SEMANAS
UNIDAD I	Conoce y diferencia las tipologías de los delitos informáticos y computacionales prescritas en el Código Penal Peruano y la ciberseguridad en el Gobierno Nacional del Perú.	**LOS DELITOS INFORMÁTICOS EN EL PERÚ.**	**1-4**
UNIDAD II	Reconoce los conceptos básicos de la informática forense y el los procedimientos que se tiene en cuenta para conseguir el análisis forense, además de las metodologías ISO para el tratamiento de las pruebas digitales.	**FUNDAMENTOS TÉCNICOS DE LA INFORMÁTICA FORENSE.**	**5-8**
UNIDAD III	Identifica y explica la fuente y naturaleza de la evidencia digital en el caso presentado.	**LA EVIDENCIA DIGITAL**	**9-12**
UNIDAD IV	Maneja técnicas y herramientas para el análisis forense.	**ANÁLISIS DE EVIDENCIAS Y TÉCNICAS ANTIFORENSE**	**13-16**

IV. INDICADORES DE CAPACIDADES AL FINALIZAR EL CURSO

NÚMERO	INDICADORES DE CAPACIDAD AL FINALIZAR EL CURSO
1	**Expone** la historia de los delitos informáticos, características, Tipología, El ciberdelincuente.
2	**Sustenta** los Marcos Jurídicos y derechos humanos, Ley de Delitos Informáticos en el Perú, Convenio de Budapest
3	Fundamenta en los Ciberdelitos organizados, Hacktivismo, terrorismo, espionaje, Guerra en el ciberespacio, Dark Web
4	**Participa** sobre la Ciberseguridad y prevención de la ciberdelincuencia, estrategias, políticas y programas, aplicaciones y medidas prácticas
5	**Se fundamenta** en la doctrina criminalista, Teoría de la prueba, metodología de investigación, Informática forense: definición, problemática, importancia.
6	**Expone** el Peritaje Informático: definición, principios, perito informático y su inserción legal, actividades periciales
7	**Explica** el Análisis Forense – Tipos, Modos, la metodología para realizar un análisis forense, marco tecnológico pericial.
8	**Argumenta** sobre la metodología de trabajo en forense digital según las ISO 27037 y 27042.
9	**Reúne** la evidencia digital: Características, Admisibilidad, relevancia
10	**Practica** las Guías RFC 3227, Guía de la IOCE, Electronic crime scene investigation a guide for first responders
11	**Aplica** las herramientas de la informática forense. Tipos de herramientas forenses
12	**Identifica** por las herramientas forenses open source en la informática forense.
13	**Demuestra** la recolección de la evidencia digital en una escena del crimen cibernético. ISO/IEC 27037.
14	**Emplea** las herramientas de Análisis de evidencias. Analizando fuente de evidencia.
15	**Prepara e**l informe pericial informático, objeto de la pericia, metodología.
16	**Identifica** las Técnicas Antiforense, ingeniería reversa, consideraciones antes de iniciar la investigación.

V.- DESARROLLO DE LAS UNIDADES DIDACTICAS:

Unidad didáctica I: LOS DELITOS INFORMÁTICOS EN EL PERÚ

CAPACIDAD DE LA UNIDAD DIDÁCTICA I: Conoce y diferencia las tipologías de los delitos informáticos y computacionales prescritas en el Código Penal Peruano y la ciberseguridad en el Gobierno Nacional del Perú.

Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
	Cognitivos	Procedimental	Actitudinal		
1	**Reconoce** la historia de los delitos informáticos, características, tendencias Tipología. El ciberdelincuente.	**Critica** la historia de los delitos informáticos, características, Tipología, El ciberdelincuente.	**Valora** la historia de los delitos informáticos, características, Tipología, El ciberdelincuente.	**Expositiva** (Docente/Alumno) • Uso de tecnología digital • Medios y materiales de uso presencial **Debates** Monitoreados • Individuales • Grupales **Lecturas** • Uso de repositorio digital **Lluvia de ideas** Expositivas	**Expone** la historia de los delitos informáticos, características, Tipología, El ciberdelincuente.
2	**Interpreta** Marcos Jurídicos y derechos humanos, Ley de Delitos Informáticos en el Perú, Convenio de Budapest.	**Discute** Marcos Jurídicos y derechos humanos, Ley de Delitos Informáticos en el Perú, Convenio de Budapest	**Integra** los Marcos Jurídicos y derechos humanos, Ley de Delitos Informáticos en el Perú, Convenio de Budapest		**Sustenta** los Marcos Jurídicos y derechos humanos, Ley de Delitos Informáticos en el Perú, Convenio de Budapest
3	**Diferencia** los Ciberdelitos organizados, Hacktivismo, terrorismo, espionaje, Guerra en el ciberespacio, Dark Web	**Expresa interés** en los Ciberdelitos organizados, Hacktivismo, terrorismo, espionaje, Guerra en el ciberespacio, Dark Web	**Asume** en los Ciberdelitos organizados, Hacktivismo, terrorismo, espionaje, Guerra en el ciberespacio, Dark Web		Fundamenta en los Ciberdelitos organizados, Hacktivismo, terrorismo, espionaje, Guerra en el ciberespacio, Dark Web
4	**Reconoce** la Ciberseguridad y prevención de la ciberdelincuencia, estrategias, políticas y programas, aplicaciones y medidas prácticas.	**Conversa** sobre la Ciberseguridad y prevención de la ciberdelincuencia, estrategias, políticas y programas, aplicaciones y medidas prácticas	**Participa** sobre la Ciberseguridad y prevención de la ciberdelincuencia, estrategias, políticas y programas, aplicaciones y medidas prácticas		**Participa** sobre la Ciberseguridad y prevención de la ciberdelincuencia, estrategias, políticas y programas, aplicaciones y medidas prácticas.
	EVALUACIÓN DE LA UNIDAD DIDÁCTICA				
	EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**	
	Estudios de Casos: Cuestionarios	Trabajos individuales y/o grupales, Soluciones a Ejercicios propuestos		Participación puntual en las clases, respondiendo las preguntas del docente.	

Unidad Didáctica II : **FUNDAMENTOS TÉCNICOS DE LA INFORMÁTICA FORENSE.**

CAPACIDAD DE LA UNIDAD DIDÁCTICA II: Reconoce los conceptos básicos de la informática forense y el los procedimientos que se tiene en cuenta para conseguir el análisis forense, además de las metodologías ISO para el tratamiento de las pruebas digitales.

Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
	Cognitivos	Procedimental	Actitudinal		
5	**Comprende** la doctrina criminalista, Teoría de la prueba, metodología de investigación, Informática forense: definición, problemática, importancia.	**Debate** la doctrina criminalista, Teoría de la prueba, metodología de investigación, Informática forense: definición, problemática, importancia.	**Aprecia** la doctrina criminalista, Teoría de la prueba, metodología de investigación, Informática forense: definición, problemática, importancia.	**Expositiva** (Docente/Alumno) • Uso de tecnología digital • Medios y materiales de uso presencial **Debates** Monitoreados • Individuales • Grupales **Lecturas** • Uso de repositorio digital **Lluvia de ideas** • Expositivas	**Se fundamenta** en la doctrina criminalista, Teoría de la prueba, metodología de investigación, Informática forense: definición, problemática, importancia.
6	**Analiza** el Peritaje Informático: definición, principios, perito informático y su inserción legal, actividades periciales.	**Investiga** sobre el Peritaje Informático: definición, principios, perito informático y su inserción legal, actividades periciales.	**Participa en** el Peritaje Informático: definición, principios, perito informático y su inserción legal, actividades periciales		**Expone** el Peritaje Informático: definición, principios, perito informático y su inserción legal, actividades periciales
7	**Evalúa** el Análisis Forense – Tipos, Modos, la metodología para realizar un análisis forense, marco tecnológico pericial.	**Utiliza** el Análisis Forense – Tipos, Modos, la metodología para realizar un análisis forense, marco tecnológico pericial.	**Acepta** el Análisis Forense – Tipos, Modos, la metodología para realizar un análisis forense, marco tecnológico pericial.		**Explica** el Análisis Forense – Tipos, Modos, la metodología para realizar un análisis forense, marco tecnológico pericial.
8	**Diferencia** la metodología de trabajo en forense digital según las ISO 27037 y 27042.	**Debate** sobre la metodología de trabajo en forense digital según las ISO 27037 y 27042.	**Debate** sobre la metodología de trabajo en forense digital según las ISO 27037 y 27042.		**Argumenta** sobre la metodología de trabajo en forense digital según las ISO 27037 y 27042.
	EVALUACIÓN DE LA UNIDAD DIDÁCTICA				
	EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**	**EVIDENCIA DE DESEMPEÑO**		

		Estudios de Casos: Cuestionarios	Trabajos individuales y/o grupales, Soluciones a Ejercicios propuestos	Participación puntual en las clases, respondiendo las preguntas del docente.

***Unidad Didáctica III* : LA EVIDENCIA DIGITAL**	***CAPACIDAD DE LA UNIDAD DIDÁCTICA III:*** *Identifica y explica la fuente y naturaleza de la evidencia digital en el caso presentado.*					
	Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
		Cognitivos	Procedimental	Actitudinal		
	9	**Distingue** la evidencia digital: Características, Admisibilidad, relevancia.	**Investiga sobre** la evidencia digital: Características, Admisibilidad, relevancia	**Valora** la evidencia digital: Características, Admisibilidad, relevancia	**Expositiva** (Docente/Alumno) • Uso de tecnología digital • Medios y materiales de uso presencial **Debates** Monitoreados • Individuales • Grupales **Lecturas** • Uso de repositorio digital **Lluvia de ideas** • Expositivas	**Reúne** la evidencia digital: Características, Admisibilidad, relevancia
	10	**Comprende** las Guías RFC 3227, Guía de la IOCE, Electronic crime scene investigation a guide for first responders.	**Usa** las Guías RFC 3227, Guía de la IOCE, Electronic crime scene investigation a guide for first responders	**Usa** las Guías RFC 3227, Guía de la IOCE, Electronic crime scene investigation a guide for first responders		**Practica** las Guías RFC 3227, Guía de la IOCE, Electronic crime scene investigation a guide for first responders
	11	**Reconoce** las herramientas de la informática forense. Tipos de herramientas forenses	**Utiliza** las herramientas de la informática forense. Tipos de herramientas forenses	**Integra** las herramientas de la informática forense. Tipos de herramientas forenses		**Aplica** las herramientas de la informática forense. Tipos de herramientas forenses
	12	**Analiza** las herramientas forenses open source en la informática forense.	**Revisa** las herramientas forenses open source en la informática forense.	**Se interesa** por las herramientas forenses open source en la informática forense.		**Identifica** por las herramientas forenses open source en la informática forense.
		EVALUACIÓN DE LA UNIDAD DIDÁCTICA				
		EVIDENCIA DE CONOCIMIENTO	**EVIDENCIA DE PRODUCTO**		**EVIDENCIA DE DESEMPEÑO**	

		Estudios de Casos: Cuestionarios	Trabajos individuales y/o grupales, Soluciones a Ejercicios propuestos	Participación puntual en las clases, respondiendo las preguntas del docente.

Unidad Didáctica IV: ANÁLISIS DE EVIDENCIAS Y TÉCNICAS ANTIFORENSE

CAPACIDAD DE LA UNIDAD DIDÁCTICA IV: *Maneja técnicas y herramientas para el análisis forense.*

Semana	Contenidos			Estrategia didáctica	Indicadores de logro de la capacidad
	Cognitivos	Procedimental	Actitudinal		
13	**Reconoce** la recolección de la evidencia digital en una escena del crimen cibernético. ISO/IEC 27037.	**Experimenta** la recolección de la evidencia digital en una escena del crimen cibernético. ISO/IEC 27037.	**Adquiere el hábito** de la recolección de la evidencia digital en una escena del crimen cibernético. ISO/IEC 27037.	**Expositiva** (Docente/Alumno) • Uso de tecnología digital • Medios y materiales de uso presencial **Debates** Monitoreados • Individuales • Grupales **Lecturas** • Uso de repositorio digital **Lluvia de ideas** • Expositivas	**Demuestra** la recolección de la evidencia digital en una escena del crimen cibernético. ISO/IEC 27037.
14	**Identifica** las herramientas de Análisis de evidencias. Analizando fuente de evidencia.	**Aplica** las herramientas de Análisis de evidencias. Analizando fuente de evidencia.	**Aprecia** las herramientas de Análisis de evidencias. Analizando fuente de evidencia.		**Emplea** las herramientas de Análisis de evidencias. Analizando fuente de evidencia.
15	**Evalúa e**l informe pericial informático, objeto de la pericia, metodología.	**Desarrolla e**l informe pericial informático, objeto de la pericia, metodología.	**Acepta e**l informe pericial informático, objeto de la pericia, metodología.		**Prepara e**l informe pericial informático, objeto de la pericia, metodología.
16	**Clasifica** las Técnicas Antiforense, ingeniería reversa, consideraciones antes de iniciar la investigación.	**Investiga** las Técnicas Antiforense, ingeniería reversa, consideraciones antes de iniciar la investigación.	**Comparte** las Técnicas Antiforense, ingeniería reversa, consideraciones antes de iniciar la investigación.		**Identifica** las Técnicas Antiforense, ingeniería reversa, consideraciones antes de iniciar la investigación.

	EVALUACIÓN DE LA UNIDAD DIDÁCTICA		
	EVIDENCIA DE CONOCIMIENTOS	**EVIDENCIA DE PRODUCTO**	**EVIDENCIA DE DESEMPEÑO**
	Estudios de Casos: Cuestionarios	Trabajos individuales y/o grupales, Soluciones a Ejercicios propuestos	Participación puntual en las clases, respondiendo las preguntas del docente.

VI. MATERIALES EDUCATIVOS Y OTROS RECURSOS DIDÁCTICOS

Los materiales educativos y recursos didácticos que se utilizaran en el desarrollo del presente curso:

1. MEDIOS ESCRITOS

- Materiales convencionales como separatas, guías de prácticas y pizarra
- Material de apoyo del curso.

2. MEDIOS VISUALES Y ELECTRÓNICOS

- Materiales audiovisuales como videos
- Presentaciones multimedia, animaciones y simulaciones interactivas.
- Servicios telemáticos: sitios web, correo electrónico, chats, foros.

3. MEDIOS INFORMÁTICOS

- Lap top con conexión a internet
- Programas informáticos (CD u on-line) educativos
- Uso de plataformas virtual con fines educativos

VII. EVALUACIÓN

La Evaluación es inherente al proceso de enseñanza aprendizaje y será continua y permanente. Los criterios de evaluación son de conocimiento, de desempeño y de producto.

1. Evidencias de Conocimiento.

La Evaluación será a través de pruebas escritas y orales para el análisis y autoevaluación. En cuanto al primer caso, medir la competencia a nivel interpretativo, argumentativo y propositivo, para ello debemos ver como identifica (describe, ejemplifica, relaciona, reconoce, explica, etc.); y la forma en que argumenta (plantea una afirmación, describe las refutaciones en contra de dicha afirmación, expone sus argumentos contra las refutaciones y llega a conclusiones) y la forma en que propone a través de establecer estrategias, valoraciones, generalizaciones, formulación de hipótesis, respuesta a situaciones, etc.

En cuanto a la autoevaluación permite que el estudiante reconozca sus debilidades y fortalezas para corregir o mejorar.

Las evaluaciones de este nivel serán de respuestas simples y otras con preguntas abiertas para su argumentación.

1. EVIDENCIA DE CONOCIMIENTO		PORCENTAJE	PONDERACION	INSTRUMENTOS
1	• Estudios de Casos • Cuestionarios	5%	0.05	Cuestionario
2	• Sustentación oral • Argumentación de la investigación	7%	0.07	Cuestionario
3	• Exposiciones de los trabajos, y argumentación	8%	0.08	Cuestionario
4	• Exposiciones de los trabajos, y argumentación	10%	0.1	Cuestionario/videos
Total Evidencia de Conocimiento		**30%**	**0.3**	

2. Evidencia de Desempeño.

Esta evidencia pone en acción recursos cognitivos, recursos procedimentales y recursos afectivos; todo ello en una integración que evidencia un saber hacer reflexivo; en tanto, se puede verbalizar lo que se hace, fundamentar teóricamente la práctica y evidenciar un pensamiento estratégico, dado en la observación en torno a cómo se actúa en situaciones impredecibles.

La evaluación de desempeño se evalúa ponderando como el estudiante se hace investigador aplicando los procedimientos y técnicas en el desarrollo de las clases a través de su asistencia y participación asertiva.

2. EVIDENCIA DEL DESEMPEÑO	PORCENTAJE	PONDERACION	INSTRUMENTOS
1. Presentación oportuna del trabajo	5%	0.05	Responsabilidad en la entrega de avances de los proyectos formativos
2. Formular un procedimiento para hacer el mejor planteamiento de la solución posibles.	15%	0.15	
3. Discriminar las soluciones posibles y propone una solución la que permite resolver el problema.	10%	0.1	
Total Evidencia del Desempeño	**30%**	**0.3**	

3. Evidencia de Producto.

Están implicadas en las finalidades de la competencia, por tanto, no es simplemente la entrega del producto, sino que tiene que ver con el campo de acción y los requerimientos del contexto de aplicación.

La evaluación de producto de evidencia en la entrega oportuna de sus trabajos parciales y el trabajo final.

Además, se tendrá en cuenta la asistencia como componente del desempeño, el 30% de inasistencia inhabilita el derecho a la evaluación.

3. EVIDENCIA DEL PRODUCTO	PORCENTAJE	PONDERACION	INSTRUMENTOS
1. Presentación del primer avance del proyecto formativo.	5%	0.05	Trabajo impreso de acuerdo al formato establecido
2. Contenido de forma y fondo	20%	0.2	
3. Aportes hechos al trabajo	15%	0.15	
Total Evidencia del Producto	**40%**	**0.4**	

VARIABLES	PONDERACIONES	UNIDADES DIDÁCTICAS DENOMINADAS MÓDULOS
Evaluación de Conocimiento	30 %	El ciclo académico comprende 4
Evaluación de Producto	35%	
Evaluación de Desempeño	35 %	

Siendo el promedio final (PF), el promedio simple de los promedios ponderados de cada módulo (PM1, PM2, PM3, PM4)

$$PF = \frac{PM1 + PM2 + PM3 + PM4}{4}$$

CRONOGRAMA ACADEMICO

EVALUACIONES DEL SEMESTRE ACADÉMICO	DEL	AL
Módulo I	14/04/2025	18/04/2025
Módulo II - I PARCIAL (Plan por Objetivos)	12/05/2025	16/05/2025
Módulo III	09/06/2025	13/06/2025
Módulo IV - II PARCIAL (Plan por objetivos)	07/07/2025	11/07/2025
Examen Sustitutorio (Plan por Objetivos)	11/07/2025	
INGRESO DE NOTAS AL SISTEMA	**DEL**	**AL**
Módulo I	21/04/2025	27/04/2025
Módulo II - I PARCIAL (Plan por objetivos)	19/05/2025	25/05/2025
Módulo III	16/06/2025	22/06/2025
Módulo IV - II PARCIAL (Plan por objetivos)	14/07/2025	20/072025
FINALIZAR Y GENERAR ACTA POR EL DOCENTE RESPONSABLE DEL CURSO A CARGO	**14/07/2025**	**25/07/2025**
IMPRESIÓN Y FIRMA DE ACTAS POR PARTE DE: ORAA Y DOCENTE DE CURSO	**14/07/2025**	**25/07/2025**
Al finalizar cada Módulo y/o Parcial el Director de Escuela Profesional Informa al Decano el incumplimiento de los docentes sobre el ingreso de notas al sistema, en sus dos modalidades.		
Inicio y término de clases	**24/03/2025**	**11/07/2025**

VIII. BIBLIOGRAFÍA Y REFERENCIAS WEB

UNIDAD DIDACTICA I:

Cano, J.(2006). Introducción a la informática forense: Una disciplina técnico – legal. Revista 96. Recuperado de https://acis.org.co/archivos/Revista/96/dos.pdfMinisterio de Justicia y Derechos humanos(2022). Ciberdelincuencia Reporte de

Diario El Peruano.(2019). Convenio obre la ciberdelincuencia.Editora Peru.Recuperado de https://dataonline.gacetajuridica.com.pe/gaceta/admin/elperuano/2292019/22-09-2019_CONVENIO.pdf

UNIDAD DIDÁCTICA II:

Lazaro, F.(2013). Introducción a la informática forense.España. Grupo Editorial RA-MA

Lopez, O.; Amaya, H & León, R.(2001). Informática forense : generalidades, aspectos técnicos y herramientas. Universidad de Los Andes.Recueprado de https://urru.org/papers/rrfraude/informaticaforense_ol_ha_rl.pdf

UNIDAD DIDACTICA III:

Lopez, L.(s.f).Informatica Forense.Grupo ANDINA.Recuperado de https://digitk.areandina.edu.co/bitstream/handle/areandina/1942/RP_eje1.pdf?sequence=1&isAllowed=y

Palacios, A.(2010).Metodología para el análisis forense informático en sistemas de redes y equipos de computo personal.Instituto Politecnico Nacional.Recuperado de https://tesis.ipn.mx/bitstream/handle/123456789/17759/Metodologia%20para%20el%20analisis%20forense%20informatico%20en%20sistemas%20de%20redes%20y%20equipos%20de%20computo.pdf

UNIDAD DIDACTICA IV:

Cajamarca, A.(2016). Implementación de un laboratorio de Informática Forense en el Órgano Rector del Sistema de Inteligencia Nacional.Universidad Sam Ignacio de Loyola.Recuperado de https://repositorio.usil.edu.pe/server/api/core/bitstreams/aba2f5e1-7135-4a8c-86eb-ca5f40526790/content

Palacios, A.(2010).Metodología para el análisis forense informático en sistemas de redes y equipos de computo personal.Instituto Politecnico Nacional.Recuperado de https://tesis.ipn.mx/bitstream/handle/123456789/17759/Metodologia%20para%20el%20analisis%20forense%20informatico%20en%20sistemas%20de%20redes%20y%20equipos%20de%20computo.pdf

Huacho, 29 de marzo 2026

Ing. Jorge Luis Barrozo Guillen
Docente Principal