Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
CONSEJO DIRECTIVO

RESOLUCIÓN 24/26/75-00
ACTA 1208/16/12/2024

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *AUDITORÍA INFORMÁTICA*, DE LA CARRERA LICENCIATURA EN CIENCIAS INFORMÁTICAS – PLAN 2023 DE LA FP-UNA"

VISTO: El Memorando DA/2437/2024 del Director Académico de la FP-UNA, Prof. MSc. Felipe Santiago Uzabal Escurra, con el cual remite el Memorando CCPTCC/036/2024 de la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado de la FP-UNA, en el que presenta la propuesta de Programas de Estudio de las Asignaturas de la Carrera Licenciatura en Ciencias Informáticas.

CONSIDERANDO: La Ley 4995/2013 de Educación Superior, el Estatuto de la Universidad Nacional de Asunción y las deliberaciones sobre el tema.

Que la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado, solicita la aprobación del Programa de Estudio de la asignatura **"Auditoría Informática"**, de la carrera Licenciatura en Ciencias Informáticas – Plan 2023, cuyo plan de estudio ya fue aprobado por el Consejo Superior Universitario.

EL CONSEJO DIRECTIVO DE LA FACULTAD POLITÉCNICA
RESUELVE:

24/26/75-01 APROBAR el Programa de Estudio de la Asignatura **"Auditoría Informática"**, de la carrera Licenciatura en Ciencias Informáticas – Plan 2023 de la FP-UNA, detallado en el ANEXO 67 de la presente Acta.

24/26/75-02 COMUNICAR, copiar y archivar.

Prof. Abg. Joel Arsenio Benítez Santacruz
Secretario

Prof. Ing. Silvia Teresa Leiva León, MSc.
Presidenta

TEL/FAX: +595 21 5887000 – C.C. 1130 (Asunción) – 2111 (San Lorenzo)
www.pol.una.py

DEPARTAMENTO DE ENSEÑANZA DE INFORMÁTICA
PROGRAMA DE ESTUDIO

I. IDENTIFICACIÓN

Asignatura	Auditoría Informática				
Carrera	**Plan**	**Sede/Filial**	**Carácter**	**Semestre**	**Prerrequisitos**
Licenciatura en Ciencias Informáticas	2023	Sede San Lorenzo / Filial Villarrica / Filial Coronel Oviedo	Obligatoria	Sexto	Seguridad Informática.
Horas semanales	4				
Total de horas teóricas semestral	36				
Total de horas prácticas semestral	36				
Total de horas semestral	72				
Valor en créditos académicos	La valoración en créditos académicos será comunicada en su oportunidad, ajustada al reglamento para la aplicación del Sistema Nacional de Créditos Académicos – Paraguay en la UNA; ajuste que se encuentra en proceso de elaboración conforme a las disposiciones de la Resolución CONES N° 221/2024, en su artículo N° 10.				
Actualización	Al egreso de la primera cohorte.				

II. FUNDAMENTACIÓN

La asignatura Auditoría Informática prepara a los estudiantes para desempeñar un papel importante en la evaluación y análisis de los sistemas de información, la infraestructura tecnológica y los controles internos de las organizaciones. Los auditores informáticos deben ser capaces de garantizar que los sistemas de información cumplan con los requisitos legales y reglamentarios, protejan los activos de información de la organización y mantengan la confidencialidad, integridad y disponibilidad de los datos. Estas competencias son relevantes en el entorno actual donde las tecnologías de la información y comunicación (TIC) son cada vez más estratégicas para el éxito organizacional.

Esta asignatura, además, enfatiza las competencias del auditor para evaluar la eficacia, eficiencia, integridad y seguridad de los sistemas y controles tecnológicos. Más allá de las auditorías formales, los estudiantes son introducidos a las habilidades necesarias para construir relaciones efectivas dentro de las organizaciones, lo que les permite agregar valor y aumentar la efectividad de sus funciones. Este enfoque alineado con los nuevos paradigmas de la auditoría destaca la importancia del rol estratégico del auditor como un agente de cambio que promueve la mejora continua en los procesos organizacionales.

La naturaleza de la asignatura es teórico-práctica, y combina el estudio de principios y marcos conceptuales con el desarrollo de habilidades prácticas mediante la utilización de herramientas especializadas y simulaciones de auditoría.

La relación entre los ejes temáticos y las unidades es la siguiente:

- Auditoría y control de TICs: se desarrolla en las unidades "Visión global de la Auditoría", donde se exploran los fundamentos de la auditoría y su importancia estratégica, y "Auditoría de controles a nivel corporativo", que detalla cómo los controles tecnológicos y organizacionales aseguran el cumplimiento de estándares. La unidad "Marcos de Trabajo y estándares" complementa este eje al introducir los *frameworks* reconocidos internacionalmente, como COBIT e ISO 27001, para el control de TIC.
- Utilización de técnicas y herramientas para auditar actividades informáticas: se relaciona principalmente con las unidades prácticas de auditoría, como "Auditoría de Sistemas Operativos Windows" y "Auditoría de Sistemas Operativos Unix y Linux", que enseñan el uso de herramientas específicas para verificar configuraciones y controles. También incluye las unidades "Auditoría de ruteadores, switches y firewalls" y "Auditoría de aplicaciones Web y Servidores Web", que abordan la evaluación técnica de infraestructuras críticas.
- Necesidades de auditar las TIC y herramientas disponibles: se desarrolla en las unidades "Visión global de la Auditoría", que establece el contexto de la auditoría en las organizaciones, y "Auditoría de computación en la nube y tercerización de operaciones", que analiza los riesgos y beneficios de la externalización tecnológica. Además, las unidades "Auditoría de Bases de Datos" y "Auditoría de Almacenamiento" exploran aspectos específicos de sistemas fundamentales para las operaciones informáticas.
- Técnicas de auditoría y desarrollo práctico de una auditoría: se vincula con la unidad "El proceso de la Auditoría", donde se presentan las etapas de una auditoría. También incluye las unidades "Auditoría de Aplicaciones", "Auditoría de entornos virtualizados" y "Auditoría de WLAN y dispositivos móviles", que enseñan la aplicación práctica de técnicas de auditoría en distintos entornos tecnológicos.
- Preparación de documento sobre el resultado de la auditoría: se consideran en la unidad "El proceso de la Auditoría".
- Normas de calidad y gestión de riesgos de las TIC: se presenta en las unidades "Auditoría de controles a nivel corporativo", donde se trata la planificación estratégica y la gestión de activos tecnológicos, y "Auditoría de centros de cómputos y recuperación de desastres", que enfatiza la continuidad operativa y la mitigación de riesgos. También en la unidad "Marcos de Trabajo y estándares", que proporciona guías normativas específicas.
- Controles sobre información y procesos TI (físicos y lógicos): se relaciona con las unidades "Auditoría de ruteadores, switches y firewalls", "Auditoría de sistemas operativos Windows y Unix/Linux" y "Auditoría de Aplicaciones". Estas unidades abordan los controles críticos necesarios para garantizar la seguridad, integridad y disponibilidad de la información en los sistemas informáticos.

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS

1. Seleccionar, utilizar y construir instrumentos innovadores asociados al ejercicio de las ciencias informáticas.
2. Planificar, proyectar, diseñar y ejecutar proyectos sostenibles e integrales para la resolución de problemas, la mejora y la innovación en el ámbito de las ciencias informáticas.
3. Aplicar en la práctica profesional los valores humanos, la ética y los mecanismos de seguridad laboral.

IV. ORGANIZACIÓN DE LA ASIGNATURA

Unidades	Contenidos	Resultados de aprendizaje
1. Visión global de la Auditoría.	1.1 La misión real de los departamentos de auditoría.	1 Explica el propósito y la misión de los departamentos de auditoría interna.

Unidades	Contenidos	Resultados de aprendizaje
	1.2 El concepto de independencia y como evitar mal utilizarlos. 1.3 Cómo agregar valor más allá de las auditorías formales. Educa. 1.4 Cómo incrementar la efectividad construyendo relacionamientos. 1.5 El rol de la auditoría de TICs y cómo elegir el foco correcto. 1.6 Cómo construir y mantener un equipo de auditoría.	2 Analiza el concepto de independencia en auditoría. 3 Evalúa cómo los departamentos de auditoría pueden agregar valor más allá de las auditorías formales. 4 Justifica el rol de la auditoría de TICs en la organización. 5 Diseña estrategias para construir y mantener equipos de auditoría efectivos.
2. El proceso de la Auditoría.	2.1 El proceso de auditoría. 2.2 Elección de puntos a auditar. 2.3 Fases iniciales de una auditoría. 2.3.1 Planificación. 2.3.2 Trabajo de campo y documentación 2.3.3 Descubrimiento y validación. 2.3.4 Desarrollo de la solución. 2.3.5 Elaboración del informe y su remisión. 2.3.6 Seguimiento a observaciones.	1. Explica los controles internos en el contexto de auditoría. 2. Identifica criterios para seleccionar los puntos a auditar. 3. Describe las etapas del proceso de auditoría. 4. Analiza las fases iniciales de una auditoría, incluyendo planificación, trabajo de campo y documentación. 5. Evalúa las actividades de descubrimiento, validación y desarrollo de soluciones. 6. Elabora informes de auditoría y propone estrategias para el seguimiento de observaciones.
3. Auditoría de controles a nivel corporativo	3.1 Planificación estratégica y hoja de ruta en tecnología. 3.2 Indicadores de rendimiento y métricas. 3.3 Aprobación de proyectos y proceso de monitoreo. 3.4 Políticas, estándares y procedimientos. 3.5 Administración de RRHH. 3.6 Administración de activos y capacidades tecnológicas. 3.7 Configuración de sistemas y administración de cambios.	1. Explica los principios de planificación estratégica y elaboración de hojas de ruta en tecnología. 2. Analiza indicadores de rendimiento y métricas utilizados en la auditoría corporativa. 3. Evalúa el proceso de aprobación y monitoreo de proyectos tecnológicos. 4. Describe políticas, estándares y procedimientos aplicados en los controles corporativos. 5. Analiza la administración de recursos humanos en el contexto de la gestión tecnológica. 6. Evalúa la administración de activos y capacidades tecnológicas en una organización. 7. Describe la configuración de

Unidades	Contenidos	Resultados de aprendizaje
		sistemas y los procesos de administración de cambios.
4. Auditoría de centros de cómputos y recuperación de desastres.	4.1 Seguridad física y controles ambientales. 4.2 Operaciones del centro de cómputos. 4.3 Continuidad del Sistema y del centro de cómputos. 4.4 Preparación para desastres.	1. Evalúa los controles de seguridad física y ambientales en centros de cómputos. 2. Analiza las operaciones realizadas en un centro de cómputos. 3. Describe los principios de continuidad del sistema y del centro de cómputos. 4. Diseña estrategias de preparación para la recuperación ante desastres.
5. Auditoría de ruteadores, switches y firewalls.	5.1 Introducción a la complejidad del equipamiento de redes. 5.2 Controles críticos de las redes 5.3 Revisión de controles específicos de ruteadores, switches y firewalls.	1. Explica la complejidad del equipamiento de redes y su importancia en la infraestructura tecnológica. 2. Analiza los controles críticos necesarios para garantizar la seguridad y operatividad de las redes. 3. Evalúa los controles específicos implementados en ruteadores, switches y firewalls.
6. Auditoría de Sistemas Operativos Windows	6.1 Configuración y controles generales. 6.2 Auditoría de Servidores Windows. 6.3 Herramientas para auditar Servidores Windows. 6.4 Auditoría de cuentas y control de contraseñas. 6.5 Herramientas para editar archivos encriptados de contraseñas. 6.6 Seguridad de Redes y Controles. 6.7 Auditoría de estaciones de trabajo Windows. 6.8 Evaluación del firewall del S. O. 6.9 Software antivirus 6.10 Actualización de parches del S. O. 6.11 Instalación de Service Packs. 6.12 Evaluación de controles de seguridad física.	1. Evalúa la configuración, controles generales y seguridad de sistemas operativos Windows, incluyendo servidores y estaciones de trabajo. 2. Analiza cuentas, contraseñas y herramientas relacionadas con su auditoría y encriptación. 3. Verifica la seguridad de redes, firewalls, antivirus y controles de actualizaciones en Windows. 4. Examina los controles de seguridad física asociados a sistemas Windows.
7. Auditoría de Sistemas Operativos Unix y	7.1 Comandos básicos para moverse en el entorno *nix 7.2 Cómo auditar sistemas	1. Describe comandos básicos para interactuar con el entorno Unix y Linux.

Unidades	Contenidos	Resultados de aprendizaje
Linux.	Unix y Linux enfocándose en las siguientes áreas principales: 7.3 Administración de cuentas y control de contraseñas. 7.4 Controles y seguridad de archivos 7.5 Controles y Seguridad de red. 7.6 Logs de auditoría. 7.7 Monitoreo de seguridad y controles generales. 7.8 Herramientas y recursos para fortalecer las auditorías *nix.	2. Evalúa sistemas Unix y Linux en áreas clave como cuentas, contraseñas, seguridad de archivos y redes. 3. Analiza logs de auditoría y monitoreo de seguridad en sistemas Unix y Linux. 4. Utiliza herramientas y recursos especializados para fortalecer las auditorías en entornos *nix.
8. Auditoría de aplicaciones Web y Servidores Web.	8.1 Principios básicos de auditoría web 8.2 Auditoría de componentes web 8.2.1 Auditoría del sistema operativo (host) 8.2.2 Auditoría de servidores web 8.2.3 Auditoría de aplicaciones web 8.2.4 Auditoría avanzada de aplicaciones web 8.2.5 Uso de herramientas y tecnología 8.3 Gestión del conocimiento 8.4 Listado de verificación principal	1. Explica los principios básicos de auditoría web. 2. Realiza auditorías en sistemas operativos, servidores web y aplicaciones web utilizando pasos específicos. 3. Analiza controles avanzados en aplicaciones web. 4. Utiliza herramientas tecnológicas para realizar auditorías web. 5. Documenta y gestiona el conocimiento generado durante el proceso de auditoría. 6. Aplica una checklist estructurada para verificar aspectos clave en auditorías web.
9. Auditoría de Bases de Datos.	9.1 Aspectos esenciales para auditar Bases de Datos 9.2 Marcas comunes de Bases de Datos 9.3 Componentes de las Bases de Datos. 9.4 Pasos para auditar Bases de Datos. 9.5 Configuración y controles generales. 9.6 Seguridad del Sistema Operativo. 9.7 Administración de cuentas y permisos de acceso. 9.8 Encripción de datos. 9.9 Monitoreo y Administración. 9.10 Herramientas y tecnología: Herramientas de auditoría	1. Analiza los aspectos críticos para la auditoría de bases de datos. 2. Evalúa la configuración, controles generales y medidas de seguridad en bases de datos. 3. Aplica técnicas de auditoría para revisar cuentas, permisos de acceso y encriptación de datos. 4. Utiliza herramientas especializadas para auditar y monitorear bases de datos.

Unidades	Contenidos	Resultados de aprendizaje
	y Herramientas de monitoreo.	
10. Auditoría de Almacenamiento.	10.1 Componentes clave de medios de almacenamiento 10.2 Pasos para auditar medios de almacenamiento 10.2.1 Configuración y controles generales 10.2.2 Administración de cuentas 10.2.3 Administración de medios de almacenamiento 10.2.4 Controles de seguridad adicionales	1. Analiza los componentes clave de los medios de almacenamiento desde una perspectiva de auditoría. 2. Evalúa la configuración, controles generales y medidas de seguridad en medios de almacenamiento. 3. Revisa la administración de cuentas y medios de almacenamiento en auditorías específicas. 4. Aplica controles de seguridad adicionales en la auditoría de sistemas de almacenamiento.
11. Auditoría de entornos virtualizados.	11.1 Proyectos comerciales y Libres 11.2 Aspectos de auditoría de entornos virtuales 11.3 Pasos para auditar entornos virtuales. 11.4 Configuración y controles generales. Altas y Bajas de cuentas y recursos. Buscar sinónimos de los términos	1. Analiza proyectos comerciales y de código abierto en entornos virtualizados. 2. Evalúa los aspectos clave de la auditoría en entornos virtuales. 3. Aplica procedimientos para auditar entornos virtualizados. 4. Revisa la configuración, controles generales y gestión de usuarios y recursos en sistemas virtualizados.
12 Auditoría de WLAN y dispositivos móviles.	12.1 Aspectos de auditoría en WLAN y dispositivos móviles. 12.1.1 Auditoría técnica de dispositivos móviles. 12.1.2 Auditoría operacional de dispositivos móviles. 12.1.3 Consideraciones adicionales. 12.1.4 Herramientas y tecnología 12.2 Gestión del conocimiento 12.3 Listado de verificación principal	1. Evalúa los aspectos clave de auditoría en redes WLAN y dispositivos móviles. 2. Aplica auditorías técnicas y operacionales en dispositivos móviles. 3. Analiza herramientas y tecnologías utilizadas en auditorías de WLAN y dispositivos móviles. 4. Gestiona el conocimiento generado durante las auditorías. 5. Utiliza un listado de verificación estructurado para evaluar redes WLAN y dispositivos móviles.
13 Auditoría de Aplicaciones	13.1 Pasos para auditar aplicaciones 13.2 Controles de entrada de datos 13.3 Controles de Interfaces de aplicaciones. 13.4 Tablas de auditoría 13.5 Controles de acceso	1. Aplica pasos específicos para auditar aplicaciones. 2. Evalúa controles de entrada de datos, interfaces y modificación de aplicaciones. 3. Revisa tablas de auditoría, controles de acceso y copias de respaldo y restauración.

Unidades	Contenidos	Resultados de aprendizaje
	13.6 Controles de modificación de aplicaciones 13.7 Copias de respaldo y restauración. 13.8 Retención de datos y clasificación 13.9 Controles de S.O., BD y otros activos de infraestructura. 13.10 Gestión del conocimiento 13.11 Listado de verificación principal.	4. Analiza políticas de retención de datos, clasificación y seguridad de infraestructura. 5. Gestiona el conocimiento generado durante auditorías de aplicaciones. 6. Utiliza un listado de verificación para asegurar la revisión completa de aplicaciones.
14 Auditoría de computación en la nube y tercerización de operaciones	14.1 Tercerización de Sistemas e Infraestructura de TICs. 14.2 Tercerización de Servicios de TICs. 14.3 Reportes SAS70 14.4 Pasos para auditar computación en la nube y operaciones tercerizadas. 14.5 Pasos preliminares y visión de conjunto 14.6 Selección del Vendedor y Contratos 14.7 Seguridad de Datos 14.8 Operaciones 14.9 Consideraciones legales y cumplimiento normativo	1. Analiza los aspectos clave de la tercerización de sistemas, infraestructura y servicios de TIC. 2. Evalúa reportes SAS70 en el contexto de auditorías de operaciones tercerizadas. 3. Aplica pasos específicos para auditar computación en la nube y operaciones tercerizadas. 4. Revisa criterios para la selección de proveedores y contratos asociados. 5. Evalúa la seguridad de datos, operaciones y cumplimiento normativo en entornos tercerizados.
15 Marcos de Trabajo y estándares.	15.1 Introducción a los controles internos de TICs, marcos de trabajo y estándares. 15.2 COSO 15.3 COBIT 15.4 ITIL 15.5 ISO 27001	1. Explica los fundamentos de los controles internos de TIC y los principales marcos de trabajo y estándares. 2. Analiza la aplicación del marco COSO en auditorías de TIC. 3. Evalúa el uso de COBIT como marco para la gobernanza y gestión de TIC. 4. Describe la implementación de buenas prácticas mediante ITIL. 5. Examina los principios y requisitos de seguridad establecidos en ISO 27001.

IV. ESTRATEGIAS DIDÁCTICAS

En el desarrollo del programa se aplicarán estrategias didácticas conducentes a la apropiación teórica y la ejecución práctica de procesos y procedimientos, a saber:

- **Debate:** exposición por parte del docente de los conceptos básicos por unidad, con materiales de lectura y ejemplos orientados a la enseñanza de las competencias específicas de la asignatura. El docente asume el rol de expositor y buscará generar el debate a través de preguntas sobre lo expuesto y desde la participación de los estudiantes.

- **Aprendizaje basado en problemas:** estrategia de enseñanza donde se busca resolver un problema a través del conocimiento que adquirió en el aula, el estudiante toma liderazgo de su aprendizaje e identifica la importancia de su aprendizaje y el conocimiento.

- **Aprendizaje basado en proyectos:** metodología donde el estudiante participa activamente en su aprendizaje, desarrollando diferentes habilidades para solucionar un problema a través de un proyecto, y que pueda implementarse para la mejora del contexto.

La elección particular de la estrategia didáctica aplicada será explícita en el plan de clases, de acuerdo con el perfil de los estudiantes, los recursos disponibles y el contexto educativo.

V. ESTRATEGIAS EVALUATIVAS

Procesos de evaluación grupales e individuales, pruebas orales y/o escritas durante el desarrollo de las unidades, análisis y evaluación de casos prácticos de auditoría. Todos estos serán valorados y en su conjunto aportarán a la calificación y promoción, aplicándose según las normativas institucionales.

Con fines de calificación y promoción se aplicará la normativa sobre evaluación vigente en la institución que prevé valoraciones de proceso y final.

VI. MEDIOS AUXILIARES

Aula virtual, pizarrón, proyector, marcadores, ordenadores, conexión a internet.

VII. BIBLIOGRAFÍA

- Davis, C., Schiller, M., & Wheeler, K. (2019). IT auditing: Using controls to protect information assets (3ra ed.). McGraw Hill
- Piattini, M., del Peso, E., & otros. (2000). Auditoría informática: Un enfoque práctico (2ª ed.). RA-MA.
- Nava, F. (n.d.). Apuntes de auditoría informática. Servicio de Publicaciones de la Universidad Rey Juan Carlos.
- Derrien, Y. (1995). Técnicas de la auditoría informática. Alfaomega, Marcombo.
- Echenique García, J. A. (2000). Auditoría en informática. McGraw-Hill.
- Echenique García, J. A. (2003). Auditoría en informática (2ª ed.). McGraw-Hill.
- Gómez Vieites, Á. (2013). Auditoría de seguridad informática. Ediciones de la U.
- Jiménez Alzate, Á. I. (2009). Una visión sistemática de la auditoría informática. Universidad Santiago de Cali.
- Li, D. H. (1997). Auditoría en centros de cómputo: Objetivos, lineamientos y procedimientos. Trillas.
- Piattini Velthuis, M. G., & del Peso Navarro, E. (2001). Auditoría informática: Un enfoque práctico (2ª ed.). Alfaomega, RA-MA.
- PiattiniVelthuis, M. G., del Peso Navarro, E., & del Peso, M. (2008). Auditoría de tecnologías y sistemas de información. Alfaomega, RA-MA