IDENTIFICACIÓN DE LA MATERIA

Programa académico: Maestría en Ciberseguridad y Ciberdefensa
Nombre de la materia: Gestión de la Ciberseguridad
Código: 020TR
Área de formación: Profesional
Número de créditos: 3
Intensidad horaria: 36 horas
Gestor de la materia: Jaider Ospina Navas
Docente(s): Jaider Ospina Navas
Dependencia: Maestría en Ciberseguridad y Ciberdefensa

2. PROPÓSITO FORMATIVO

Propósito general de la materia:

Potencializar en los estudiantes las habilidades y competencias para crear estrategias de ciberseguridad en organizaciones e infraestructuras cibernéticas críticas. Mediante la protección de los activos críticos y respondiendo adecuadamente ante incidentes de ciberseguridad y su aseguramiento basado en estándares internacionales y buenas prácticas de la industria.

3. COMPETENCIAS (referidas al PEP)

COMPETENCIA GENERAL: Desarrolla habilidades y competencias que le permitan proteger los activos críticos y responder adecuadamente ante la creación de estrategias de Ciberseguridad en organizaciones e infraestructuras críticas cibernéticas.

COMPETENCIAS ESPECÍFICAS:

- Gestiona de manera efectiva las estrategias de ciberseguridad, minimizando las consecuencias y tomando medidas preventivas para que no vuelva a ocurrir estos aspectos.
- Aplica metodologías de auditoría, monitoreo y mantenimiento de sistemas y tecnologías (activos digitales o de la información).
- Determina las características para la Identificación de amenazas y vulnerabilidades en sistemas informáticos.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

4. RESULTADOS DE APRENDIZAJE

- R1. Comprende y explica los principales frameworks de arquitectura y gestión de la ciberseguridad, incluyendo SABSA, Zachman, NIST CSF y MITRE.
- R2. Integra marcos normativos y estándares internacionales como ISO 27001:2022 y NIST SP 800-53 para fortalecer el sistema de gestión de seguridad de la información.
- R3. Analiza el contexto cibernético de la organización para alinear la estrategia de ciberseguridad con los objetivos y prioridades del negocio.
- R4. Evalúa y gestiona riesgos cibernéticos empleando metodologías reconocidas, determinando el apetito de riesgo y aplicando controles adecuados según normatividad vigente.
- R5. Diseña e implementa estrategias y políticas de ciberseguridad y ciberdefensa basadas en prácticas internacionales y frameworks especializados.
- R6. Utiliza herramientas y matrices, como MITRE ATT&CK, para identificar amenazas, mejorar la detección y establecer salvaguardas efectivas en infraestructuras críticas.

5. CONTENIDOS TEMÁTICOS

Contenido temático 1: Contexto y conceptos de la construcción de la Gestión de la Ciberseguridad.

- **Contexto cibernético:** Entorno digital global de sistemas, redes y datos donde interactúan tecnologías, usuarios y procesos de información.
- **Alineación del modelo de ciberseguridad a la estrategia del negocio:** Integración de la ciberseguridad con los objetivos y prioridades empresariales para proteger activos y apoyar la misión corporativa

***Horas*: 10**

***Resultado de aprendizaje específico*:**
Comprensión de los fundamentos de la gestión de la ciberseguridad y su encuadramiento en el contexto cibernético.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

***Actividades*:** Exposiciones, lecturas dirigidas, análisis de casos.

***Bibliografía*:**

- White Paper Enterprise Security Architecture John Sherwood, Andrew Clark & David Lynas. (https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-down-approach)
- https://www.nist.gov/cyberframework
- Architecture PMBOK Guide Fifth Edition Bringing the PMBOK guide to life. https://repository.dinus.ac.id/docs/ajar/PMBOKGuide_5th_Ed.pdf. capítulo 11 (pag 309-353).
- Framework. Lori DeLooze . Copyright SANS Institute 2021. (https://www.sans.org/reading-room/whitepapers/modeling/applying-security-enterprise-zachman-framework-367).
- Gestión de la exposición en ciberseguridad, https://www.researchgate.net/publication/384473232_Gestion_de_la_exposicion_en_ciberseguridad

Contenido temático 2: Planificación y gestión de la seguridad informática, buenas prácticas y estándares. Modelos de Gestión de seguridad.

- **Framework de SABSA:** Metodología para diseñar arquitecturas de seguridad empresarial alineadas a objetivos de negocio.
- **Framework de Zachman:** Estructura para organizar y visualizar arquitecturas empresariales con perspectivas y niveles detallados.
- **ISACA:** Asociación global que desarrolla normas y certificaciones en auditoría, control y gobierno de TI.
- **NIST CSF:** Marco de referencia para gestionar y mejorar la ciberseguridad en organizaciones, basado en buenas prácticas y estándares

Horas: 14
***Resultado de aprendizaje específico*:** Define el plan de gestión de la Ciberseguridad desde un Proyecto Gerencial.

***Actividades*:** Exposiciones, lecturas dirigidas, análisis de casos.

***Bibliografía*:**

- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- ISACA. (2020). IT Audit Framework (ITAF™) (4th ed.). ISACA. https://www.famu.edu/administration/audit/pdf/standards/ITAF-4th-Edition.pdf
- Ejemplo del plano técnico de NIST SP 800-53 (https://docs.microsoft.com/es-es/azure/governance/blueprints/samples/nist-sp-800-53-r4).
- Effective Security Metrics A Guide to Effective Security Metrics,2017 (https://www.educause.edu/focus-areas-and-initiatives/policy-and-

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

security/cybersecurity-program/resources/information-security-guide/toolkits/effective-security-metrics).

Contenido temático 3: Modelos y estándares de gestión de riesgos en el contexto cibernético y sus ámbitos de aplicación.

- **ISO 27001:2022:** Norma internacional para gestionar la seguridad de la información mediante un sistema de gestión y controles sobre riesgos.
- **CSF - NIST:** Marco que ayuda a organizaciones a identificar, proteger, detectar, responder y recuperar ante riesgos de ciberseguridad.
- **NIST SP 800-53:** Catálogo de controles para proteger sistemas federales, centrándose en seguridad y privacidad de la información.
- **MITRE matrix:** Matriz que organiza y visualiza tácticas y técnicas usadas por atacantes durante ciberataques, facilitando defensa y detección

Horas: 12.

***Resultado de aprendizaje específico*:** Identifica brechas y controles en estrategias de resiliencia cibernética para sectores de infraestructura crítica y organizacionales.

***Actividades*:** Exposiciones, lecturas dirigidas, análisis de casos.

***Bibliografía*:**

- Apriany, A. (2024). Analysis of the implementation of ISO 27001:2022 and KAMI Index in information security management. Indonesian Journal of Computing and Cybernetics Systems, 18(3), 419-431. https://jurnal.ugm.ac.id/ijccs/article/download/100385/40369
- Papamartzivanos, D., Iliadis, J., Katsarakis, S., Tsihrintzis, G. A., & Kambourakis, G. (2021). Assessing MITRE ATT&CK risk using a cyber-security culture framework. Sensors, 21(10), 3294. https://pmc.ncbi.nlm.nih.gov/articles/PMC8125987/
- Definition of Cybersecurity – Gaps and overlaps in standardisation v1.0 | December 2015 (https://www.enisa.europa.eu/publications/definition-of-cybersecurity).
- The MITRE Corporation. (2024). Enterprise Matrix – MITRE ATT&CK® (Framework version v15, current as of April 2024). https://attack.mitre.org/matrices/enterprise/

6. ESTRATEGIA DIDÁCTICA

Estrategia de la Materia:

Se adopta la metodología de seminario, complementada con conferencias múltiples, talleres, simulaciones estratégicas y

- **Métodos:** Estudio de caso, exposición crítica, Aprendizaje basado en problemas.
- **Técnicas:** Lectura dirigida, trabajo colaborativo, simulaciones.

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."

• **Recursos didácticos:** BlackBoard, textos doctrinales, documentos institucionales, herramientas de gamificación.

AI7. EVALUACIÓN DEL APRENDIZAJE

Tipos de evaluación: Diagnóstica, formativa y sumativa

Instrumentos y técnicas: Examen escrito, desarrollo de estrategia hipotética, aprendizaje basado en retos.

Distribución porcentual:

***- Primer 30%:** Examen escrito. – Participación en clase.*

***- Segundo 30%:** Trabajo en clase (20 %), Quiz(s) en clase (10%).*

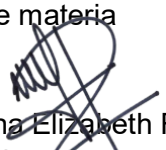
***- Tercer 40%:** Reto de aprendizaje – Modelo de gestión en ciberseguridad – Caso aplicado-.*

Momentos de evaluación: Parcial (Modulo 1), Intermedia (Modulo 2), Final (Modulo 3)

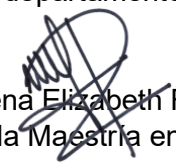
8. VALIDACIÓN ACADÉMICA



Jaider Ospina Navas
Gestor de materia



TC. Milena Elizabeth Realpe Díaz
Jefe del departamento



TC. Milena Elizabeth Realpe Díaz
Jefe de la Maestría en Ciberseguridad y Ciberdefensa



CR. Oscar Otoniel Torres Conde
Vicedirector Académico

Archivado en: 12303 Maestría en Ciberseguridad y Ciberdefensa 2025

"Documento propiedad SIG - ESDEG. Versión vigente en la Suite Visión Empresarial SVE. Se autoriza impresión total o parcial, como documento no controlado."