INSTITUTO KENNEDY
EDUCACIÓN VIRTUAL

PROGRAMA ACADÉMICO

CATEGORÍA: Informática

PERIODO LECTIVO: 2024

MODALIDAD: Distancia

CURSO: Diplomatura en Ciberseguridad

CURSO/S	Ciberseguridad	**N° 14**	**IDENTIFICACIÓN: IK00014**

CÁTEDRA:	**Duración**	**Régimen**	**Plan**	**Certificado**
Diplomatura en Ciberseguridad	4 meses	Curso de tarifa aplicable	2024	De aprobación

EQUIPO DOCENTE:

PROFESOR/ES | DISERTANTES	**CATEGORÍA**
Moreyra, Maximiliano Gabriel	Titular

1- FUNDAMENTOS DE LA CÁTEDRA

La **Diplomatura en Ciberseguridad** tiene como objetivo formar profesionales capaces de proteger la infraestructura tecnológica de las organizaciones ante ciberataques y vulnerabilidades. En un mundo cada vez más digitalizado, las amenazas a la seguridad informática han crecido exponencialmente, haciendo imprescindible el desarrollo de habilidades y conocimientos avanzados en ciberseguridad para prevenir, detectar y mitigar riesgos.

2- OBJETIVOS

Generales:

- ➔ Brindar a los estudiantes los conocimientos teóricos y prácticos necesarios para identificar, prevenir y gestionar amenazas de ciberseguridad en diferentes entornos.
- ➔ Desarrollar competencias para implementar soluciones de seguridad informática eficaces en redes, sistemas y aplicaciones.

Específicos:

- ➔ Formar en el uso de herramientas y técnicas de defensa contra ciberataques.
- ➔ Desarrollar habilidades en análisis forense digital para investigar incidentes de seguridad.
- ➔ Capacitar en la gestión de políticas y normativas de seguridad para asegurar el cumplimiento en entornos corporativos.

3- CONTENIDOS:

UNIDAD I: Fundamentos de Ciberseguridad

- Historia y evolución de la ciberseguridad.
- Principios básicos: confidencialidad, integridad y disponibilidad (CIA).
- Tipos de ciberataques: malware, phishing, ransomware, ataques DDoS.
- Modelos de seguridad informática.

UNIDAD II: Redes y Seguridad de la Información

- Introducción a redes de computadoras y protocolos.
- Seguridad en redes locales (LAN), redes inalámbricas y redes WAN.
- Firewalls, VPNs y sistemas de detección de intrusos (IDS).
- Segmentación de redes y políticas de acceso.

UNIDAD III: Criptografía y Protección de Datos

- Fundamentos de la criptografía: algoritmos simétricos y asimétricos.
- Protocolos de seguridad (SSL, TLS, HTTPS).
- Firma digital y certificados electrónicos.
- Cifrado de datos en tránsito y en reposo.

UNIDAD IV: Seguridad en Aplicaciones y Desarrollo Seguro

- Ciclo de vida de desarrollo seguro (SDLC).
- Vulnerabilidades comunes: inyección SQL, cross-site scripting (XSS), cross-site request forgery (CSRF).
- Seguridad en aplicaciones móviles y web.
- Implementación de prácticas seguras en el desarrollo de software.

UNIDAD V: Gestión de Incidentes y Respuesta a Ciberataques

- Modelos y procesos de gestión de incidentes.
- Plan de respuesta ante incidentes y recuperación de desastres.
- Técnicas de análisis forense digital: recopilación y preservación de pruebas.
- Herramientas y técnicas de monitoreo de seguridad.

UNIDAD VI: Auditoría de Seguridad y Cumplimiento Normativo

- Normas internacionales de seguridad (ISO/IEC 27001, GDPR, PCI DSS).
- Auditoría de seguridad de la información.
- Evaluación de vulnerabilidades y pruebas de penetración (pentesting).
- Gobernanza de TI y políticas de seguridad corporativa.

UNIDAD VII: Ciberseguridad en la Nube y Tecnologías Emergentes

- Seguridad en entornos de computación en la nube (cloud security).
- Retos de la ciberseguridad en la era de la inteligencia artificial y el IoT.
- Blockchain y su aplicación en la seguridad informática.
- Protección de la privacidad y seguridad de los datos en la nube.

4- METODOLOGÍA DE TRABAJO - ESTRATEGIAS DE ENSEÑANZA Y DE APRENDIZAJE

La metodología que se llevará a cabo será teórica y práctica, con clases expositivas y participativas. Para desarrollar el programa se utilizarán materiales didácticos como los módulos correspondientes a cada unidad, bibliografía digitalizada, video clases, materiales para lectura complementaria y recomendaciones de páginas webs para consultar. Se promoverá la participación de los estudiantes en los distintos foros con el fin de que realicen aportes significativos para la gestión de la enseñanza y del aprendizaje.

Cada clase tendrá una actividad para realizar en foro, y autoevaluaciones. Como así también se realizarán trabajos prácticos, todas las actividades tendrán una devolución escrita por el docente, y alguna retroalimentación grupal si la actividad lo requiriera. La interacción entre el docente y el alumno se realizará mediante la plataforma a medida que se vayan desarrollando los módulos y al terminar cada unidad, mediante foros de debates.

Se realizarán clases sincrónicas, el día y horario serán publicados en el foro de novedades. Con respecto al chat en vivo podrán contactarse con el docente en los días y horarios previamente informados en el foro de novedades.

5- EVALUACIÓN

Criterios de Evaluación:

- ➔ Capacidad reflexiva y análisis crítico.
- ➔ Participación constructiva en los foros.
- ➔ Habilidad para la resolución de problemas y creatividad.
- ➔ Capacidad para manejar información y transmitirla en forma ordenada y coherente.

Instrumentos de evaluación:

- Foros.
- Actividades prácticas obligatorias.
- Examen al final de cada unidad
- Examen integrador final para finalizar el curso

Condición para regularizar la materia:

- ➔ Participaciones obligatorias en foros de debates/ reflexión/otros.
- ➔ Aprobar los Trabajos prácticos obligatorios. Deberá contar con un 80% del total de los trabajos prácticos aprobados.
- ➔ Aprobar el Trabajo integrador final. que deberán ser aprobados con un puntaje mínimo de 60/100

Condiciones para aprobar la asignatura:

- ➔ Cumplir con las condiciones de regularización.
- ➔ Aprobar el examen final.

Alumnos libres: Deberán rendir un examen integrador de todos los módulos y un informe final que consistirá en el análisis profundo de un sistema productivo designado por el docente. El alumno deberá aprobar el trabajo final con un puntaje superior a 7 siete. Una vez aprobado el trabajo integrador podrá acceder al examen final.

6 - RECURSOS DIDÁCTICOS

- ➔ Estará a disposición para los alumnos bibliografía básica digitalizada, como así también bibliografía complementaria.
- ➔ Se utilizarán sitios de internet, específicos los cuales serán debatidos en foros de consultas.
- ➔ Recursos audiovisuales (video clases) de temas claves para la materia.
- ➔ Respecto a la plataforma de e-learning se disponen de herramientas de comunicación como foros, mensajería interna y salas de chats.
- ➔ Trabajos grupales a través de las wikis (estrategia de trabajo grupal cooperativo y colaborativo entre los miembros de un curso).
- ➔ Encuentros online sincrónicos con los alumnos

7- BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA			
AUTOR	**TÍTULO**	**EDITORIAL**	**LUGAR Y AÑO DE EDICIÓN**
Stallings, William	Cryptography and Network Security: Principles and Practice	Pearson	Londres, Reino Unido 2020

FIRMA DE RESPONSABLE: Moreyra, Maximiliano Gabriel

Fecha: 11 de octubre de 2024