Diplomatura en Ciberseguridad

I. PRESENTACIÓN

La Unidad de Posgrado de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, consciente con su compromiso con el desarrollo del país, viene aplicando estrategias y propuestas para fomentar, propiciar y promover la investigación que nutra la formación de los nuevos profesionales en sistemas e informática

En ese sentido, la Dirección y el Comité Directivo de la UPG FISI, con la colaboración de docentes, grupo de interés han realizado diversas actividades conducentes a la creación de la Diplomatura en Ciberseguridad en modalidad no presencial.

La ciberseguridad cada día es más importante. El funcionamiento de las sociedades modernas depende de la tecnología y esta es una tendencia que, al parecer, irá en aumento. Previo a la pandemia, ya vivíamos en un mundo digitalizado, pero ahora más que nunca ha aumentado el uso de Internet y las herramientas digitales.

Hoy en día, vemos una gran cantidad de empresas implementando el teletrabajo, universidades ofreciendo cursos a distancia y un sinfín de personas que han migrado a un entorno digital. Aunque esta forma de hacer las cosas ha generado oportunidades, también ha provocado un aumento en los ciberdelitos.

Si a esto sumamos al auge de los servicios en la nube, el Internet de las Cosas y los teléfonos inteligentes, nos damos cuenta del gran desafío al que se enfrentan los países en todo el mundo. Para estar preparados, echemos un vistazo general a la ciberseguridad, en qué consiste y cómo podemos protegernos.

En esta Diplomatura en Ciberseguridad aprenderemos todo lo necesario sobre las amenazas digitales, a prevenir ciberataques y a responder ante riesgos de manera más rápida y eficiente. El Programa de Diplomatura en Ciberseguridad, regirá a partir del semestre 2023-2.

II. VISIÓN DE LA FACULTAD Y/O DE LA UPG

Ser reconocidos como una facultad de excelencia en la formación profesional e investigación en el área de Computación e Informática comprometidos con la responsabilidad social y el desarrollo sostenible de la sociedad.

III. MISIÓN DE LA FACULTAD Y/O DE LA UPG

Generar y difundir conocimiento científico y tecnológico, formando profesionales e investigadores en el área de Computación e Informática, con valores y respetuosos de la diversidad cultural, promotores de la identidad nacional basada en una cultura de calidad y responsabilidad social para contribuir al desarrollo sostenible del país y la sociedad.

IV. LÍNEAS DE INVESTIGACIÓN

Objetivos de desarrollo (n=8)	Líneas de Investigación (n=8)	
ODS3: Salud y Bienestar	1	Ciberseguridad
	2	Computación Gráfica e Imágenes
	3	Gobierno y Gestión de TIC
	4	Ingeniería de Software
	5	Procesamiento Digital de Señales
	6	Sistemas Inteligentes
ODS4: Educación de Calidad	1	Ciberseguridad
	2	Computación Gráfica e Imágenes
	3	Gobierno y Gestión de TIC
	4	Ingeniería de Software
	5	Sistemas Inteligentes
ODS5: Igualdad de género	1	Computación Gráfica e Imágenes
	2	Gobierno y Gestión de TIC
	3	Ingeniería de Software
	4	Sistemas Inteligentes
ODS7: Energía asequible y no contaminante	1	Computación Gráfica e Imágenes
	2	Sistemas Inteligentes
ODS8: Trabajo decente y crecimiento económico	1	Gobierno y Gestión de TIC
	2	Ingeniería de Software
ODS9: Industria, Innovación e Infraestructura	1	Ciberseguridad
	2	Computación Gráfica e Imágenes
	3	Gobierno y Gestión de TIC
	4	Ingeniería de Software
	5	Internet de las Cosas
	6	Redes TIC
	7	Sistemas Inteligentes
ODS16: Paz, Justicia e Instituciones sólidas	1	Ciberseguridad
	2	Computación Gráfica e Imágenes
	3	Gobierno y Gestión de TIC
	4	Ingeniería de Software
	5	Sistemas Inteligentes
ODS17: Alianzas para lograr los objetivos	1	Ciberseguridad
	2	Gobierno y Gestión de TIC
	3	Ingeniería de Software
	4	Procesamiento Digital de Señales
	5	Redes TIC
	6	Sistemas Inteligentes

V. PERFILES:

1. Perfil del ingresante al Programa

- Bachilleres de universidades públicas y privadas, nacionales o extranjeras de las áreas de ciencias, Ingenierías que desempeñen una función o actividad relacionada con las Tecnologías de la Información y Comunicaciones. Con actitudes y valores (honestidad solidaridad, proactividad); y capacidades y habilidades (Aprendizaje, razonamiento, liderazgo, adaptación a cambios tecnológicos).
- Y otro tipo de profesionales que demuestren experiencia relacionada con el campo de la seguridad informática o de la Ciberseguridad.

2. Perfil del egresado del Programa

Al finalizar el programa, el egresado tendrá las siguientes competencias:

a) Implementa una estrategia de ciberseguridad alineada a la visión estratégica del negocio.

b) Gestiona un programa de ciberseguridad y proponer métricas para incrementar el nivel de madurez de una organización alineados a las buenas prácticas de ciberseguridad.

c) Previene, detecta y responde ante cualquier ataque informático malicioso contra empresas y organizaciones.

d) Detecta y responde a los incidentes de seguridad de la información.

e) Supervisa y monitorea la utilización y comportamiento de los activos.

f) Realiza auditorías y revisiones de los mecanismos y procedimientos relacionados con los procesos, la tecnología y las personas en el ámbito de la seguridad de la información.

VI. PLAN DE ESTUDIOS

PLAN DE ESTUDIOS 2023			
N°	**Código**	**Asignatura**	**Créditos**
Primer Ciclo			
1.		Sistema de gestión de seguridad de la información (SGSI)	4.0
2.		Fundamentos y marcos de trabajo para ciberseguridad.	4.0
3.		Interpretación e implementación de la norma ISO 27110.	4.0
		Subtotal	**12.0**
Segundo Ciclo			
4.		Gestión de riesgos aplicada a ciberseguridad	4.0
5.		Ciberseguridad defensiva	4.0
6.		Taller práctico de implementación de ciberseguridad en las organizaciones	4.0
		Subtotal	**12.0**
		Total	**24.0**

VII. SUMILLAS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Asignatura que corresponde al periodo de profundización, es de naturaleza teórico – práctica y de modalidad no presencial.

Tiene como propósito el establecer la estructura y prácticas que deben considerar las organizaciones para la implementación de un Sistema de Gestión de Seguridad.

Las unidades son:

I. Conceptos base de Seguridad de la Información en base a la familia de normas ISO 27000 y el framework del NIST de EE.UU.
II. Interpretación e implementación de la norma ISO 27001.
III. Revisión y consideraciones de implementación de la norma ISO 27002.

FUNDAMENTOS Y MARCOS DE TRABAJO PARA CIBERSEGURIDAD

Asignatura que corresponde al periodo de profundización, es de naturaleza teórico – práctica y de modalidad no presencial.

Tiene como propósito tener un claro entendimiento de los fundamentos de la Ciberseguridad y revisar los principales marcos de trabajo existentes para su implementación.

Las unidades son:

I. Fundamentos de CiberSeguridad.
II. Familia de Normas ISO 27000 para Ciberseguridad.
III. Marco de Trabajo para CiberSeguridad del NIST.

Diplomatura en Ciberseguridad

INTERPRETACIÓN E IMPLEMENTACIÓN DE LA NORMA ISO 27110.

Asignatura que corresponde al periodo de perfeccionamiento, es de naturaleza teórico – práctica y de modalidad no presencial.

Tiene como propósito el entendimiento, interpretación y consideraciones de implementación de la norma ISO 27110:2021 “Guía de desarrollo de un marco de trabajo para Ciberseguridad”.

Las unidades son:

I. Revisión completa de la norma.
II. Interpretación de la norma.
III. Consideraciones para la implementación de la norma.

GESTIÓN DE RIESGOS APLICADA A CIBERSEGURIDAD

Asignatura que corresponde al periodo de profundización, es de naturaleza teórico – práctica y de modalidad no presencial.

El propósito es desarrollar un claro entendimiento de las amenazas, vulnerabilidades y su mitigación, en el contexto de la utilización del denominado Ciberespacio.

Las unidades son:

I. Identificación de amenazas provenientes del ciberespacio.
II. Identificación de vulnerabilidades en los sistemas de servicios digitales.
III. Mitigación de riesgos.
IV. Implementación de un proceso de Gestión de Riesgos para la utilización de servicios a través del Ciberespacio.

CIBERSEGURIDAD DEFENSIVA

Asignatura que corresponde al periodo de profundización, es de naturaleza teórico – práctica y de modalidad no presencial.

Tiene como propósito entender cómo se producen los ataques en el denominado ciberespacio y desarrollar respuestas de ciberseguridad defensivas.

Las unidades son:

I. Explorar los escenarios de ciberataques y desglosar los diferentes tipos de amenazas y vulnerabilidades.
II. Entender como actividades maliciosas producto de actividades humanas.
III. Explorar técnicas de IA aplicables a Ciberseguridad.
IV. Desarrollar un marco de trabajo de respuestas a incidentes de Ciberseguridad.

TALLER PRÁCTICO DE IMPLEMENTACIÓN DE CIBERSEGURIDAD EN LAS ORGANIZACIONES

Asignatura que corresponde al periodo de perfeccionamiento, es de naturaleza teórico – práctica y de modalidad no presencial. Tiene como propósito simular actividades de ataques de ciberseguridad y de desarrollo de las correspondientes medidas defensivas.

Las unidades son:

I. Revisión de herramientas de ciberseguridad.
II. Simulación de ataques de ciberseguridad.
III. Simulación de respuestas ante ataques.