

MODALIDAD GRABADA

DIPLOMADO DE ALTA ESPECIALIZACIÓN

CIBERSEGURIDAD Y DELITOS INFORMÁTICOS EN LA ADMINISTRACIÓN PÚBLICA

Protege la información pública, prevén
delitos digitales y actúa con respaldo
legal ante incidentes cibernéticos.

INICIA AHORA

CERTIFICACIÓN UNIVERSITARIA



Universidad Nacional
SAN LUIS GONZAGA

✓ PRESENTACIÓN:

El diplomado en Ciberseguridad y Delitos Informáticos en la Administración Pública brinda a los participantes una visión práctica e integral de los principales riesgos digitales que enfrentan las entidades del Estado. A partir de casos reales del sector público, se abordan las amenazas más frecuentes, los delitos informáticos y sus implicancias legales, así como la protección de datos personales y la gestión de incidentes de seguridad. El programa enfatiza el rol del funcionario público en la prevención, detección y respuesta ante incidentes, fortaleciendo la cultura de seguridad y promoviendo buenas prácticas aplicables de manera inmediata en la gestión institucional.

✓ DIRIGIDO A:

- Funcionarios y servidores públicos de los gobiernos nacional, regional y local.
- Directivos, jefes, coordinadores y personal de áreas de TI, informática, sistemas, seguridad de la información y transformación digital.
- Personal de asesoría legal, control interno, gestión de riesgos, recursos humanos y atención al ciudadano.
- Responsables del manejo de bases de datos, expedientes, información sensible o servicios digitales.
- Profesionales del sector público interesados en fortalecer sus competencias en ciberseguridad, prevención de delitos informáticos y protección de datos personales.

✓ OBJETIVOS:

Fortalecer las capacidades de los servidores públicos para prevenir, identificar y responder a riesgos de ciberseguridad y delitos informáticos, asegurando el cumplimiento normativo, la protección de datos personales y la continuidad de los servicios públicos digitales.

✓ ¿POR QUÉ IPAPPG?

+10 años

**de experiencia como la
plataforma líder en
sector público**

+300 empresas

**han confiado en
nosotros para capacitar
a sus equipos**

+50mil alumnos

**trabajando en grandes
instituciones del Estado**

✓ INICIO

Clase 100% virtual	12 meses de acceso al aula virtual sin restricciones	
Nº DE SESIONES	MODALIDAD	HORARIO
6	Grabada	24/7
TÚ ELIGES CUANDO INICIAR Y FINALIZAR 		

✓ BENEFICIOS:



DOCENTES ESPECIALISTAS

- Expertos certificados con experiencia en el Sector público y privado.



VÁLIDO

- Para los concursos en la Administración Pública y Privada.
- Por 384 horas académicas.



CERTIFICACIÓN ADICIONAL CON

- IPAPPG Físico.
- Universidad Nacional San Luis Gonzaga de Ica.



CERTIFICACIÓN DIGITAL

- Obtenlo en corto tiempo.
- Con valor legal.

✓ PLANA DOCENTE:



MG. RÓMULO LOMPARTE ALVARADO

Actualmente es Presidente de ISACA Lima Chapter.

Magister en Dirección de Negocios y Licenciado en Computación. Fue responsable ejecutivo de Comando, Coordinación y Comunicaciones en los Juegos Panamericanos y Parapanamericanos de Lima.

Líder en tecnologías de información con sólida y amplia experiencia para el sector comercial y financiero en dirección de proyectos de TI, auditoría, seguridad, ciberseguridad y consultoría en las mismas áreas. Habilidad para el desarrollo de talento, optimización de procesos, manejo de situaciones críticas con recursos limitados. Experiencia en uso de COSO, CobiT y procesos de Certificación Sarbanes-Oxley.

✓ PLAN DE ESTUDIOS:

MÓDULO	CONTENIDOS
MÓDULO I	Contexto de la Ciberseguridad en la Administración Pública • Transformación digital del Estado y riesgos asociados • Activos de información en el sector público • Amenazas más frecuentes en entidades públicas: - Phishing institucional - Ransomware en municipalidades y hospitales - Fugas de información por errores humanos • Impacto: legal, reputacional, operativo y social • Ejemplos prácticos: - Caso de ataque ransomware a municipalidad: paralización de servicios - Suplantación de correos de ministerios para fraudes ciudadanos • Actividad breve: - Identificación de activos críticos en la propia entidad del participante

MÓDULO II	Delitos Informáticos: Tipologías y Responsabilidad Legal • Concepto de delito informático • Principales tipos: - Acceso ilícito - Interceptación de datos - Fraude informático - Suplantación de identidad - Manipulación de sistemas • Responsabilidad penal, administrativa y civil • Rol del funcionario público como: - Víctima - Facilitador involuntario - Responsable por negligencia • Marco legal (Perú – ajustar si aplica): - Ley de Delitos Informáticos (Ley 30096 y modificatorias) - Código Penal - Ley de Protección de Datos Personales • Ejemplos prácticos: - Funcionarios que comparten credenciales - Uso indebido de bases de datos institucionales • Actividad: - Análisis de escenarios: ¿es delito?, ¿falta administrativa?, ¿ambos?
MÓDULO III	Protección de Datos y Seguridad de la Información en el Estado • Principios de protección de datos personales • Datos sensibles en el sector público • Medidas organizativas y técnicas mínimas: - Control de accesos - Gestión de contraseñas - Clasificación de información • Relación entre: - Seguridad de la información - Protección de datos - Continuidad de servicios públicos • Normativas y marcos: - Ley 29733 y su Reglamento - ISO/IEC 27001 (visión gerencial) - Lineamientos de la PCM / Secretaría de Gobierno Digital • Ejemplos: - Padrón electoral - Historias clínicas - Registros tributarios y sociales • Actividad: - Mapeo simple de datos personales en un proceso público típico

MÓDULO IV	Gestión de Incidentes y Evidencia Digital • ¿Qué es un incidente de seguridad? • Fases: - Detección - Contención - Notificación - Recuperación • Cadena de custodia y evidencia digital • Coordinación con: - Oficina de TI - Oficina Legal - Autoridad Nacional de Protección de Datos - Fiscalía / Policía • Errores comunes en entidades públicas: - Borrar evidencias - No reportar oportunamente - Comunicar sin control • Ejemplos: - Filtración de base de datos - Ataque de malware en PCs de atención al público • Actividad: - Simulación básica de manejo de incidente (qué hacer en las primeras 24 h)
MÓDULO V	Prevención, Cultura de Seguridad y Buenas Prácticas Institucionales • Factores humanos como principal vector de ataque • Cultura de ciberseguridad en el Estado • Políticas mínimas recomendadas: - Uso aceptable de recursos - Manejo de información - Teletrabajo seguro • Rol de la alta dirección y mandos medios • Integración con control interno y gestión de riesgos • Ejemplos: - Campañas internas de concientización - Simulacros de phishing • Actividad: - Diseño de acciones de mejora para la propia entidad

MÓDULO VI

Diagnóstico Básico de Riesgos de Ciberseguridad y Delitos Informáticos en una Entidad Pública

- Descripción del proceso crítico
 - Ejemplo: atención al ciudadano, gestión de expedientes, recaudación, salud, educación
- Identificación de activos de información
 - Sistemas
 - Bases de datos
 - Documentos
- Principales riesgos de ciberseguridad
 - Técnicos
 - Humanos
 - Organizacionales
- Posibles delitos informáticos asociados
 - Tipificación legal aproximada
- Medidas de prevención recomendadas
 - Organizativas
 - Tecnológicas
 - Capacitación
- Procedimiento básico de respuesta ante incidente

✓ **Pago (S/)**



COMPRA EL PROGRAMA AQUÍ

PAGO EN LÍNEA

   

*Aceptamos todas las tarjetas

DEPÓSITO BANCARIO

TRANSFERENCIA BANCARIA

**CUENTA DE AHORRO
/ CUENTAS CORRIENTES**



Nº de ahorro en soles:
Nº: 04-052-191772



Nº de cuenta corriente:
Nº: 193-2260106-0-52



Nº de cuenta corriente:
Nº: 0011-0147-0100076128



Nº de cuenta corriente:
Nº: 0004029593



Nº de cuenta corriente:
Nº: 087-300126963-6

Código de cuenta interbancario:
CCI: 00219300226010605212

✓ **Comunícate con un asesor**

CORREO COMERCIAL



informes@ipappg.edu.pe

CORREO ACADÉMICA



academica@ipappg.edu.pe

HORARIO DE ATENCIÓN

**Lunes a Viernes:
9:00 am a 6:00 pm**

HORARIO DE ATENCIÓN

**Lunes a Viernes:
2:00 pm a 10:00pm**

