ECPD

IAITG

INSTITUTE
OF AUDIT &
IT-GOVERNANCE

El Instituto es una iniciativa que se ha posicionado como referente en el estudio y análisis de la realidad de las tecnologías de la información y su buen gobierno.

De manera especial, impulsa la investigación en el Gobierno de las Tecnologías de la Información (IT-Governance) desde una perspectiva interdisciplinar (Management, Tecnología y Derecho, en particular en protección de datos personales) con una vocación de centro de intercambio de mejores experiencias a nivel internacional.

El Instituto busca vincular a la Academia y en particular a la investigación universitaria con las necesidades de los actores sociales, tanto en la administración pública como empresas y asociaciones profesionales.

Así, en los últimos años ha centrado su actuación en formar especialistas en Auditoría, Control, Seguridad, Gobierno y Derecho de las Tecnologías de la Información y de las Comunicaciones a través de cursos, seminarios y másteres (maestrías), realizadas en colaboración con centros universitarios reconocidos internacionalmente.

De igual forma, el Instituto desarrolla proyectos de investigación y asesoría; diseña y organiza cursos, conferencias, diplomados, programas de formación y actualización entre otros, que sean de interés y que reporten un beneficio académico y práctico en materia de nuevas tecnologías.

El Instituto desarrolla la formación basándose en tres pilares:

La propuesta formativa

La propuesta formativa se desarrolla desde la triple perspectiva Tecnológica, Jurídica y Empresarial, sin olvidar la aplicación práctica de la misma y en particular el intercambio de buenas prácticas y experiencias en temas como la seguridad, la protección de datos personales y el gobierno de las nuevas tecnologías.

INTRODUCCIÓN

La información es uno de los bienes más importantes, tanto para una empresa como para la Administración Pública. Con el incremento de la complejidad en los sistemas de información y de los riesgos asociados, es necesario incrementar la capacitación para que encargados del manejo de los mismos cuenten con experiencia y conocimientos probados para identificar y evaluar los riesgos, y sepan minimizar las vulnerabilidades de estos sistemas, con apego estricto a la normativa nacional e internacional en la materia.

La capacidad que dan los nuevos sistemas de información para capturar, almacenar, analizar y procesar cantidades ingentes de datos, así como para intercambiarla con el entorno (clientes, proveedores, socios, ciudadanos...) ha hecho que las TIC hayan llegado a ser un componente crítico de gran parte de los procesos productivos y de toma de decisiones. Efectos residuales de la creciente utilización de las TIC son los igualmente crecientes presupuestos de TIC, los crecientes éxitos y fracasos y la creciente mentalización de la necesidad de controlar adecuadamente la utilización de estas tecnologías.

En la actualidad la seguridad de la información y asociada a ella, el tratamiento de datos de carácter personal, es una de las principales preocupaciones de las organizaciones y administraciones públicas.

Consciente de los crecientes riesgos de las nuevas tecnologías, tanto a nivel nacional como internacional existen nuevas normas sobre privacidad y protección de datos, las cuales son capitales en la gestión y gobierno de los sujetos obligados por las mismas, públicos y privados.

En este sentido, es primordial conocer la regulación de los diversos ámbitos de aplicación y de participación de las nuevas tecnologías, de la gestión de la información, de los procesos de control y de la gestión de riesgos en los diferentes ámbitos, en particular por lo que se refiere a la protección de datos personales.

Es imprescindible el conocimiento de las normas y su aplicación a fin de poder garantizar el respeto y cumplimiento y evitar la producción de resultados no deseados, así como para tomar consciencia de la traducción jurídica de los actos realizados u omitidos y de sus consecuencias.

Las propuestas de formación, en sus diferentes opciones, buscan responder a la necesidad de disponer de un número creciente de profesionales cualificados en la identificación y evaluación de los riesgos de los sistemas de información y en el diseño y evaluación independiente de los controles necesarios para asegurar la eficacia, eficiencia, legalidad y seguridad de los sistemas y de la información que se contiene en los mismos.

Se busca formar expertos multidisciplinares en el que a una base jurídica de privacidad, tanto nacional como internacional se le añada el componente tecnológico necesario en el mundo actual, independientemente de la formación profesional o el perfil de cada persona.

En algunas de las opciones de los programas de formación se busca además el adecuado reconocimiento certificable para demostrar la debida competencia profesional frente a terceros a nivel internacional.

PRESENTACIÓN

El Perú, en desarrollo del cumplimiento del artículo 6° numeral 2 de la Constitución Política, que aboga por garantizar el derecho fundamental a la protección de datos personales, ha promulgado la Ley N° 29733, Ley de Protección de Datos Personales (LPDP), y su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, que obliga a todas las organizaciones que almacenen y traten datos personales a dar un uso apropiado y correcto de los mismos, no solo para evitar sanciones derivadas de una equivocada o incompleta observancia de lo dispuesto por la LPDP y su reglamento, sino también con el objetivo de generar valor al interior de la organización debido al correcto y funcional uso de la tecnología de la información en lo que corresponde al tratamiento de datos personales.

OBJETIVOS

IAITG con el objetivo de esclarecer dudas y vacíos, y ofrecer soluciones reales a las necesidades tanto de las entidades del sector público como de otros sectores de la economía en lo que respecta a la Ley de Protección de Datos Personales (LPDP), el curso EXPERTO CERTIFICADO en PROTECCIÓN DE DATOS (ECPD), que ofrece la formación especializada legal, administrativa y técnica suficiente para el dominio completo sobre protección de datos personales, los riesgos de su incumplimiento y las oportunidades que la misma ofrece como generador de valor. Preparará a los asistentes para que lideren en el interior de sus organizaciones los procesos necesarios para adecuar a su entidad a las demandas y exigencias de la LPDP.

INFORMACIÓN

Duración y horario.

2 semanas

Lunes a viernes

De 6:30 pm a 9:30 pm

EXAMEN

Sábado de 10 am a 12 am.

Información y matrícula.

Institute of Audit & IT-Governance

inscripciones@iaitg.eu

Lugar de Impartición

Aula de Formación

Avda. Paseo de la República 3587, piso 9

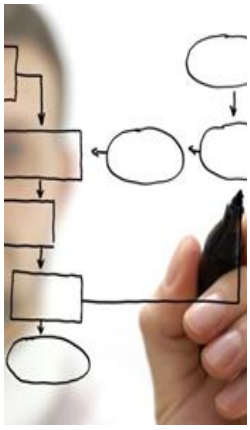
San Isidro. Lima

DERECHOS DE MATRÍCULA

IMPORTE DE LA MATRÍCULA: **1.500$ (USD) (*)**

(*) A dicho Importe se le añadirá el IGV

Incluye toda la documentación y materiales necesarios para el seguimiento del curso y los derechos de inscripción al examen de certificación.



PROGRAMA

- **Módulo 1 (5%)**: Fundamentos.
- **Módulo 2 (25%)**: Marco nacional.
- **Módulo 3 (10%)**: Marco europeo.
- **Módulo 4 (10%)**: Marco internacional.
- **Módulo 5 (15%)**: Protección de los activos de información.
- **Módulo 6 (10%)**: Gestión y respuesta ante incidentes.
- **Módulo 7 (15%)**: Control y auditoría de los sistemas de información.
- **Módulo 8 (10%)**: Gobierno de los sistemas de información.

Módulo 1: Fundamentos

INTRODUCCIÓN A LA PROTECCIÓN DE DATOS

- Marco de desarrollo de los derechos y libertades de las personas.
- La protección de datos personales como derecho fundamental.
- El derecho a la autodeterminación informativa de las personas.
- El artículo 2° numeral 6 de la Constitución.
- La Ley N° 29733 – Ley de Protección de Datos Personales.
- Reglamento de la Ley N° 29733 aprobado por Decreto Supremo N° 003-2013-JUS
- Directiva de Seguridad de la Información.

Módulo 2: Marco nacional

ÁMBITO DE APLICACIÓN

- Objeto y ámbito.
- Concepto de dato personal.
- Concepto de banco de datos y tratamiento.
- Datos sensibles.
- Datos de menores.
- Persona física identificable.
- La anonimización o disociación.
- Fuentes de acceso público.
- Ámbito de aplicación objetivo y subjetivo.
- Ámbito territorial.
- Tratamientos excluidos.
- Datos referidos a seguridad interna y nacional.
- Datos de información periodística.

LOS SUJETOS DE LA LPDP

- Responsable del tratamiento.
- Encargado del tratamiento.
- Relación entre responsable y encargado.
- Deberes.
- Subcontratación.

PRINCIPIO DE LEGALIDAD

- Legislación peruana.
- Derecho internacional.

PRINCIPIO DE CONSENTIMIENTO

- Libre.
- Previo.
- Expreso.
- Informado.
- Inequívoco.

PRINCIPIO DE FINALIDAD

- Diferenciación de finalidades.
- Oposición y tratamiento otras finalidades.

PRINCIPIO DE PROPORCIONALIDAD

- Adecuado.
- Relevante.
- No excesivo.

PRINCIPIO DE CALIDAD

- Datos exactos, completos, pertinentes, correctos y actualizados.
- Conservación, Bloqueo y Destrucción.
- Pruebas de cumplimiento.

PRINCIPIO DE SEGURIDAD

- Alcance, Funciones, Factores, Acciones.
- Medidas Jurídicas, Técnicas y Organizativas.

PRINCIPIO DE DISPOSICIÓN DE RECURSO

PRINCIPIO DE NIVEL DE PROTECCIÓN ADECUADO

EL SISTEMA DE GARANTÍAS

- Deber de informar.
- Ejercicio de derechos.
- Restricciones.
- Medios y costos.
- Procedimientos.
- Decisiones sin intervención humana valorativa.
- Requisitos de la solicitud de protección de derechos.
- Tercero interesado.

TRANSFERENCIAS

- Alcance.
- Condiciones.
- Tipos de Transferencias.
- Nacionales e Internacionales.

COMPETENCIA Y FUNCIONES DE LA AUTORIDAD ADMINISTRATIVA

- La Autoridad Nacional de Protección de Datos.
- Registro Nacional de Protección de Datos.
- Tutela de Derechos.
- Inicio de procedimientos.
- Procedimiento fiscalizador.
- Procedimiento sancionador.

AUTORREGULACIÓN VINCULANTE

- Objeto y alcances.
- Objetivos específicos, incentivos.
- Certificación.

DIRECTIVA DE SEGURIDAD

- Objetivos, base legal, alcance y responsabilidad.
- Disposiciones generales.
    - Categoría.
    - Condiciones de seguridad.
    - Requisitos de seguridad e información complementaria.
- Disposiciones específicas.
    - Medidas de seguridad organizativas.
    - Medidas de seguridad jurídicas.
    - Medidas de seguridad técnicas.
- Procedimiento.
- Disposiciones complementarias.

CÓDIGO PENAL. LEY DE DELITOS INFORMÁTICOS.

LEY N° 30096 y LEY Nº 30171

- Finalidad y Objeto.
- Delitos contra datos y sistemas informáticos.
- Delitos informáticos contra la indemnidad y libertades sexuales.
- Delitos informáticos contra la intimidad y el secreto de las comunicaciones.
- Delitos informáticos contra el patrimonio.
- Circunstancias de agravación punitiva
- Modificaciones introducidas por la Ley Nº30171

Módulo 3: Marco europeo

INSTITUCIONES

- Las Instituciones Europeas
    - Parlamento Europeo
    - Consejo de la Unión Europea
    - Comisión Europea
    - Tribunal de Justicia
    - Tribunal de Cuentas
    - Organismos Interinstitucionales.
- La protección de datos en las instituciones europeas.
    - El Reglamento (CE) No 45/2001 de 18 de diciembre de 2000 sobre protección de datos por las instituciones europeas.
- El papel de la Comisión Europea en el desarrollo en Europa de la protección de Datos: la nueva Propuesta de Reglamento Europeo de Protección de Datos personales, antecedentes y planteamiento.

LEGISLACIÓN

- El Convenio 108 del Consejo de Europa y su proceso de reforma.
- La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- El Tratado de Lisboa. La Carta Europea de Derechos Fundamentales y la inclusión en su artículo 8 del derecho a la protección de los datos de las personas.
- La regulación de las comunicaciones electrónicas y el Mercado de las Telecomunicaciones.
- La Directiva sobre retención de datos.

ORGANISMOS

- Autoridades de control.
- European Data Protection Supervisor (EDPS).
- Europol.
- IWGDPT (International Working Group of Data Protection and Telecommunications).
- Grupo del artículo 29.

LA TRANSPARENCIA EN EUROPA.

- El Reglamento de Transparencia EC/1049/2001 y su influencia en la protección de datos en Europa.
- Aplicación práctica del Reglamento.

Módulo 4: Marco internacional

GOBERNANZA DE INTERNET A NIVEL INTERNACIONAL

- Asamblea General y el Consejo Económico y Social de la ONU.
- Derechos en línea/mundo virtual (online) mundo real (offline).
- Participación de actores no gubernamentales
- Internet Corporation for Assigned Names and Numbers (ICANN)

APERTURA Y DERECHOS CIBERNÉTICOS

- Resolución A/67/195 sobre "Tecnologías de la Información y las Comunicaciones para el Desarrollo"
- Resolución 20/8 (2012) del Consejo de Derechos Humanos.
- Resolución 2012/19 del ECOSOC
- Segunda Comisión (TICs para el desarrollo)
- Primera Comisión sobre Información y Telecomunicaciones en el contexto de la Seguridad Internacional (A/67/404).

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

- Transferencias internacionales de datos: concepto y aplicaciones prácticas.
- Binding Corporate Rules (BCRs).
- Safe Harbour
- Acuerdo SWIFT.
- Nivel adecuado de protección: las decisiones de adecuación.
- Los acuerdos PNR's sobre transmisión de datos de pasajeros a EE.UU.
- Cesiones de datos a Estados que no ofrecen un nivel equiparable de protección.

LA PROTECCIÓN DE DATOS EN ALGUNOS ESTADOS.

- La situación en España: la actuación de la Agencia Española y las agencias autonómicas.
- La propuesta de reglamento europea.
- El Garante italiano.
- La Comisión Nacional de la informática y las libertades francesa.

USA

- US-Consumer Privacy Bill of Rights.
- La aplicación de la normativa y su interpretación por la Federal Trade Commission.

CANADÁ

- Gobierno y sistema legal.

- Las Autoridades de Protección de Datos en Canadá.
- The Personal Information Protection and Electronic Documents Act.
- Model Code for the Protection of Personal Information.

LATINOAMÉRICA

- Red Iberoamericana.
- Las diferentes regulaciones en los países iberoamericanos

OTROS SISTEMAS:

- Asia Caribe
- Red de la Francofonía.

Módulo 5: Protección de los activos de información

GESTIÓN DE RIESGOS

- Conceptos Generales.
- Tipos de Riesgo.
- Análisis de Riesgos.
- Metodologías y Estándares.
- Elementos y Fases.
- Tecnologías.
- Outsourcing y SLA (Acuerdos de Nivel de Servicio).
- Implementación.
- Monitorización y Comunicación.

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

- Confidencialidad, Integridad y Disponibilidad.
- Inventario y clasificación de activos.
- Funciones y responsabilidades del personal.
- Concienciación y Formación.
- Componentes y Arquitectura Hardware.
- Arquitectura y Software de Sistemas de Información.
- Infraestructura de Redes de Sistemas de Información.

EXPOSICIONES Y ACCESOS

- Permisos de Acceso al Sistema.
- Riesgos y Controles de Acceso al Sistema.
- Seguridad de las redes de área local.
- Seguridad Inalámbrica.
- Seguridad en Internet.

CRIPTOGRAFÍA

- Sistemas de Clave Privada.
- Sistemas de Clave Pública.
- Infraestructura de Clave Pública.

FIRMA DIGITAL

- Concepto, regulación y clases.
- La identificación electrónica.
- La certificación digital.
- Los prestadores de servicio.

PLAN DE BACKUP

- Procedimientos periódicos de copias.
- Frecuencia y método de rotación.

Módulo 6: Gestión y respuesta ante incidentes

ANÁLISIS PREVIO

- BIA (Análisis del impacto en el negocio).
- PIA (Análisis del impacto en la Privacidad).

FUNCIONES

- Detección y Notificación.
- Jerarquización.
- Análisis.
- Respuesta.

PLANIFICACIÓN DE LA CONTINUIDAD

- Desastres y Otras Interrupciones.
- Punto de recuperación.
- Tiempo de recuperación.
- Estrategias de Recuperación.

Módulo 7: Control y auditoría de los sistemas de información

CONTROL

- Control Interno
- Control sobre el personal
- Control sobre los proveedores
- Control de las TIC
- COBIT (Objetivos de Control)
- Métricas
- Limitaciones del Control

AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

- Tipos de Auditoría.
- Metodologías.
- Riesgos de auditoría.
- Autoevaluación de Controles.
- Control y auditoría de la adquisición y mantenimiento de la infraestructura de SI.
- Control y auditoría de la operación de los SI.
- Control y auditoría de la adquisición, desarrollo y mantenimiento de las aplicaciones.
- Control y auditoría en las aplicaciones: Origen, entrada, procesos y salida.

AUDITORÍA DE PRIVACIDAD

- Marco legal.
- Metodologías.
- Papeles de trabajo.
- Informe final.
- Archivos temporales y definitivos.

EL DATA PROTECTION OFFICER (Experto Certificado en Protección de Datos Personales)

- Funciones y responsabilidades.
- Marco europeo e internacional.
- Competencia profesional.

Módulo 8: Gobierno de los sistemas de información

PLAN ESTRATÉGICO

- Definición de niveles de servicio.
- Arquitectura de la información.
- Dirección tecnológica.
- Organización de TI.
- Gestión de personal de TI.
- Gestión de servicios externos.
- Gestión económica de TI.
- Gestión de la capacidad y el rendimiento.

PLAN DIRECTOR DE SEGURIDAD

- Privacy by design
- Recursos: Humanos, tecnológicos y procesos.
- Restricciones.
- Hoja de ruta.
- Plan de implementación

ADMINISTRACIÓN ELECTRÓNICA

- El procedimiento administrativo y el uso de las nuevas tecnologías.
- Las nuevas tecnologías y los procesos electorales (el voto electrónico).
- e-Negocios y e-Gestión.
- Comunidades virtuales.

ESTÁNDARES

- ISO 38500
- ISO 20000
- ISO 27000
- Estándares de Privacidad

(ECPD)
EXPERTO CERTIFICADO EN PROTECCIÓN DE DATOS

El profesional que quiera optar al título de:

Experto Certificado en Protección de Datos deberá cumplir dos requisitos:

1. Asistir al menos al 80% de las clases
2. Segundo: Acreditar sus conocimientos en las materias impartidas

Características de la Prueba teórica:

- 100 preguntas con una sola respuesta válida de 4 posibles.
- No hay puntos negativos.
- Distribución de las preguntas de acuerdo al peso relativo de los 8 dominios.

A todos los alumnos que asistan al menos al 80% de las clases al curso se les otorgará un diploma de **Experto en Protección de Datos**

Para obtener el de **Experto Certificado en Protección de Datos**, deberán además superar la Prueba Teórica.

ACUERDOS INSTITUCIONALES

Universidad Autónoma de Madrid en el que se realiza el primer máster multidisciplinar en Auditoría, Seguridad, Gobierno y Derecho de las TIC conjuntamente con la Escuela Politécnica Superior, La Facultad de Derecho y la Facultad de Ciencias Económicas.

Escuela de negocios CEU San Pablo con el máster en IT-Governance, el máster en Auditoría y Privacidad, curso de mediación y resolución de ciberconflictos con menores, curso de Estrategia e Innovación TIC, curso de Prevención de delitos económicos e informáticos, etc.

Universidad Autónoma de Barcelona acuerdo de colaboración para investigación y desarrollo en IT-Governance, así como el máster en Auditoría y protección de datos, la aplicación sectorial, realizado con el soporte de la Agencia Española de Protección de Datos y de la Agencia Catalana.

Escuela de Administración de Empresas-EAE cursos de Auditoría de sistemas de gestión de seguridad de la información, Auditoría de sistemas de la información, IT Governance, Firma digital, documento electrónico y factura electrónica, Responsabilidad civil y nuevas tecnologías, Governance, outsourcing y protección de datos personales.

Organización Médica Colegial de España con el que se realizan periódicamente cursos de capacitación en Creación y preservación de valor a través de las TICS, cursos de privacidad, cursos de responsabilidad penal y civil, etc.

ISACA con los cursos de preparación al CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT).

ASOBANCARIA con los cursos de preparación al ECPD Talleres Prácticos en Protección de Datos en Colombia.

EAFIT con los cursos de preparación al ECPD en Colombia.

Escuela Superior de Guerra de Colombia con el convenio marco de colaboración académica

CLAUSTRO DOCENTE

Dirección:

Antoni Bosch Pujol.

Director General del Institute of Audit & IT-Governance (IAITG).

Presidente Fundador ISACA-Barcelona. Director del Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC (Universidad Autónoma de Madrid con Escuela Politécnica Superior, Facultad de Derecho y Facultad de Ciencias Económicas).

Licenciado en Ciencias Físicas (Universidad de Barcelona), Diplomado en Alta Dirección de Empresas (ESADE), Máster en Auditoría Informática, Auditor Certificado en Sistemas de Información (CISA), Técnico Superior en Prevención de Riesgos Laborales (UOC), Director Certificado en Seguridad de la Información (CISM), Diplomado en Managing Information Technology (Center for Information Systems Research-MIT Sloan School), Certified in the Governance of Enterprise IT (CGEIT).

Director del IT-Governance Think-Tank Group de Barcelona. Director y creador de los cursos de Experto Certificado en Protección de Datos (ECPD) en España, Colombia, Perú, México. Director del Máster en Auditoría y Protección de Datos (Universidad San Pablo CEU-EN), Director del Máster en IT-Governance (Universidad San Pablo CEU-Escuela de Negocios), Director del Máster en Auditoría y Privacidad (Universidad Autónoma de Barcelona), Director del Máster Interuniversitario en Auditoría y Seguridad de los Sistemas de Información (Universidad de Barcelona-Universidad Autónoma de Barcelona).

Director de los Posgrados y cursos en Aula Digital, Formación de profesorado en el uso de las TIC. Directos de los cursos de Data Privacy Officer. Director de los cursos de preparación al CISA, CISM y CGEIT. Director de los cursos de Mediación y Resolución de Ciberconflictos con Menores (Universidad San Pablo CEU-Escuela de Negocios). Director de los cursos de Prevención de Fraude Informático (Universidad San Pablo CEU-Escuela de Negocios). Director de los cursos de Estrategia e Innovación TIC (Organización Médica Colegial de España). Director de los cursos de Ciberseguridad y Privacidad (Organización Médica Colegial de España). Director de los cursos de Derecho Penal de las TIC (UNOAC).

Director y ponente en numerosos cursos, jornadas y seminarios en materias de seguridad, ITIL, ISO 20000, IT-Governance, Auditoría de Sistemas de Información y seguridad, Control Interno, Protección de Datos Personales, etc. Asesor de diversas empresas y administraciones públicas. Profesional con más de 30 años de experiencia en el mundo de las TIC.

Sus áreas de expertise incluyen el desarrollo de estándares y políticas TIC, IT-Governance, análisis y gestión de riesgos tecnológicos, ITIL, ISO 20000, ISO 27000, ISO 38500, evaluaciones de controles, gestión de niveles de servicio, protección de datos, gestión de incidentes, planes de continuidad de negocio, gestión de proyectos, asesoría de seguridad, planes estratégicos TIC.

Miembro del SC7/GT 25 de AENOR y coordinador del subgrupo de IT-Governance. Ha sido el representante español en el subcomité ISO de IT-Governance (ISO 38500).

Miembro Académico del European Corporate Governance Institute, Coordinador de la comunidad de IT-Governance en epractice.eu, Coordinador del grupo de Profesionales de Privacidad en linkedin.

Ha sido entre otros: Fundador de la Asociación Profesional Española de Privacidad (APEP) y creador de la primera Certificación Profesional española en la materia, Fundador y Secretario General del Club Kiwanis de Catalunya, Secretario General de La Agrupación Empresarial Independiente, Fundador y Presidente de la Asociación de Auditores Informáticos de Cataluña, Director de IT-Governance del Instituto de Derecho y Tecnología de la Universidad Autónoma de Barcelona, Director del Centro de Auditoría y Gestión de Riesgos Tecnológicos de la Universidad Autónoma de Barcelona así como profesor de la UAB en el departamento de Ingeniería de la Información y de las Comunicaciones responsable de las asignaturas de Auditoría y Control de los sistemas de información y IT-Governance.

Profesorado:

José Álvaro Quiroga León.

Abogado por la Pontificia Universidad Católica del Perú. Presidente de la Comisión Multisectorial que elaboró el Reglamento de la Ley de Protección de Datos Personales.

Ha sido Director de la Autoridad Nacional de Protección de Datos Personales.

Experto Certificado en Protección de Datos (ECPD)

Ha sido Director Nacional de Justicia, docente en Derecho Procesal, Contratos y Obligaciones en la Pontificia Universidad Católica del Perú. Tiene estudios de Maestría en Derecho Civil y Diplomados en "Diseño de Políticas Públicas" e "Instituciones Jurídicas del Mercado". Es Árbitro de los centros del Colegio de Abogados de Lima, de la Cámara de Comercio de Lima y del Centro de Arbitraje Empresarial y expositor sobre Protección de Datos Personales en Perú, México, Uruguay y Colombia. Ha publicado en libros revistas y diarios escritos sobre la Abogacía Derecho Civil, Procesal Civil, y Protección de Datos Personales.

Juan Dávila Ramírez

Presidente ISACA Perú.

MBA por ESAN e Ingeniero Industrial por la Universidad Nacional del Callao. Tiene las certificaciones CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager) y CRISC (Certified in Risk and Information Systems Control) por ISACA, además de ISO/IEC 27001 Lead Auditor e ISO/IEC 22301 Lead Auditor por BSI (British Standards Institution). Es trainer acreditado de COBIT 5 Foundation por APMG International.

Consultor en gestión de riesgos y mejora de procesos. Fue responsable de Auditoría de TIC (arquitectura e infraestructura de TI y de voz fija&móvil) en Telefónica del Perú en el período 2000-2015, gestionando la planificación anual de auditoría, gestión de riesgos en procesos de negocio y esquemas de cumplimiento legal y regulatorio. Anteriormente, trabajó para firmas consultoras en proyectos de procesos y TI relacionados con BCP, DRP, BI, SDLC, BBDD, SSOO, redes y comunicaciones, Gestión de Servicios, Seguridad de Información, entre otros.

Instructor en cursos de preparación de los exámenes de certificación para CISA, CISM y CRISC en el Capítulo de ISACA Lima, desde 2008. Profesor en cursos y conferencista en eventos sobre Seguridad, Auditoría, Gobierno y Riesgos de TI, en Puerto Rico, Colombia, España, Brasil, Chile, Uruguay y Perú, incluyendo el Latin CACS 2011 (San Juan), 2012 (Bogotá) y 2013 (Medellín), y el CIGRAS 2014 (Montevideo).

Miembro del capítulo de ISACA en Lima desde septiembre de 2004. Past Presidente del Capítulo en los períodos 2009-2011 y 2011-2013, en los que se obtuvo el premio K.Wayne Snipes 2011 (Mejor Capítulo a nivel América Latina) y 2012 (Mejor Capítulo a nivel global). Miembro del MGRC

Profesional con más de 20 años de experiencia en planificación estratégica, auditoría, gobierno y seguridad de TI. Especializado en la gestión de riesgos en procesos de negocios y de TI.

Gino Fernández Canorio

Responsable de División de Consultoría en el Institute of Audit & IT Governance (IAITG - PERÚ).

Ingeniero de Sistemas de la Universidad Nacional Mayor de San Marcos, con estudios de postgrado en Implantación de Sistemas de Gestión de Seguridad de la Información y Continuidad del Negocio (ESAN).

Experto Certificado en Protección de Datos Personales (ECPD) por IAITG, cuenta además con las certificaciones CISM (Certified Information Security Manager) de ISACA, Information Security based on ISO 27002 de EXIN e ITILv3 de PeopleCert.

Cuenta con amplia experiencia en adecuaciones de empresas públicas y privadas a estándares internacionales de Seguridad de la Información y Gobierno de TI. Responsable del proyecto de implementación del Sistema Gestión de Seguridad de la Información basado en la Norma Técnica Peruana 27001:2008 en el Ministerio de Economía y Finanzas. Gestor del Componente Alineamiento Normativo TIC en el Proyecto de Reingeniería y Automatización de Procesos de la Oficina de Normalización Previsional - ONP. Responsable en IAITG de las consultorías para la adecuación de empresas de gran envergadura a la Ley 29733 - Ley de Protección de Datos Personales, en alianza con el Estudio Benites, Forno y Ugaz.

Pedro José Fernández García

Director General de AENOR Perú

Licenciado en Administración y Dirección de empresas con campo de orientación en dirección internacional de la Universidad de Cádiz. Máster en Gestión Internacional de la Empresa en la Fundación CECO del Instituto de Comercio Exterior de España (ICEX) en Madrid. Complementó su formación en el International Business Program en la Universidad de Ciencias Aplicadas Georg Simon Ohm de Nuremberg (Alemania).

Ha desarrollado su carrera profesional en empresas multinacionales en países como Suiza, Brasil, Países Bajos y Vietnam en los campos de finanzas, el control de gestión y el desarrollo de herramientas de gestión.

Juan Carlos Medina Carruitero

Ingeniero Industrial de la Pontificia Universidad Católica del Perú y catedrático universitario, en la misma universidad, en materias de Elaboración y Evaluación de Proyectos de inversión, Control de Gestión e Ingeniería Económica.

Presidente del Comité de Prevención del Lavado de Activos y del Financiamiento del Terrorismo (COPLAFT) de la Federación Latinoamericana de Bancos (FELABAN). Presidente del Comité de Cumplimiento de la Asociación de Bancos del Perú (ASBANC). Vicepresidente de la Asociación de Egresados de MBA de EGADE Business School – Tecnológico de Monterrey, Sede Perú.

Ha sido Gerente de División de Cumplimiento del Banco Financiero del Perú.

MBA en EGADE Business School – Tecnológico de Monterrey. Especialista en Finanzas por la Universidad ESAN en Lima, Perú. Diplomado Internacional en Administración del Riesgo Financiero por el Tecnológico de Monterrey. Diplomado Internacional en "Técnicas de gestión para el control y monitoreo de los riesgos inherentes al lavado de dinero y financiamiento del terrorismo en los sistemas financieros" por el Instituto Bancario Internacional (Asociación Bancaria de Panamá) y la Universidad Católica Santa Maria La Antigua de Panamá.

Con certificación profesional (CPAML) por la Florida International Bankers Association (FIBA) y la Florida International University (FIU). Expositor internacional y experiencia en banca, y en empresas de servicios, en labores de control, auditoria, planeamiento, fraudes y riesgos; y en docencia universitaria, en áreas de gestión, proyectos, ingeniería y finanzas. Miembro del Instituto de Auditores Internos del Perú y de la Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS), organización antilavado de activos de alcance mundial.

María Cecilia Chumbe

Abogada por la Universidad Femenina del Sagrado Corazón - UNIFE, con estudios concluidos de Maestría en Derecho de la Empresa en la Escuela de Postgrado de Derecho de la Universidad Nacional Mayor de San Marcos.

Ha sido Directora (e) de Normatividad y Asistencia Legal de la Autoridad Nacional de Protección de Datos Personales – APDP del Ministerio de Justicia y Derechos Humanos.

Ex Secretaria Técnica de la Comisión Multisectorial que elaboró el proyecto de Reglamento de la Ley de Protección de Datos Personales.

Capacitada en protección de datos personales por el Programa de Derecho y Bienes Públicos de la Facultad Latinoamericana de Ciencias Sociales -FLACSO- y por la Agencia Española de Protección de Datos (Madrid).

Experta Certificada en Protección de Datos por el Institute of Audit & IT-Governance y la Asociación Española de Normalización y Certificación - AENOR PERU.

Ha participado en eventos internacionales de protección de datos personales que incluyen los encuentros de la Red Iberoamericana de Protección de Datos

Expositora en eventos académicos y docente en curso de especialización en protección de datos personales en Lima.

Andrea Pulgar

Responsable del Área de Nuevas Tecnologías y Protección de Datos Personales del Estudio Grau.

Experta Certificada en Protección de Datos (ECPD)

Abogada por la Universidad de Piura, docente en Derecho Procesal en la Universidad de Piura campus Lima. Tiene estudios de Maestría en Derecho de la Empresa con Especialidad en Gestión Empresarial por la Pontificia Universidad Católica del Perú (candidata), Master en Auditoría, Seguridad, gobierno y Derecho de las TIC (candidata) y Diplomado en "Arbitraje Internacional" por Amcham Perú.

Jesús Andrés Vega Gutierrez

Jefe del Área de Protección de Datos Personales del Estudio Benites Forno & Ugaz.

Abogado por la Pontificia Universidad Católica del Perú. Estudios concluidos de Maestría en Derecho Administrativo Económico - Instituto Universitario de Investigación Ortega y Gasset adscrito a la Universidad Complutense de Madrid, en convenio con la Escuela de Postgrado de la Universidad Continental. Diploma de Especialista en Derecho Administrativo - Escuela de Postgrado de la Universidad Continental. Master en Auditoría, Seguridad, Gobierno y Derecho de las TICs - Universidad Autónoma de Madrid-Institute of Audit & IT-Governance.

Experto Certificado en Protección de Datos Personales (ECPD) - Institute of Audit & It Governance (IAITG).

Docente de la Facultad de Derecho de la Universidad Nacional Mayor de San Marcos y Escuela de Postgrado de la Universidad Continental. Se ha desempeñado como Especialista Jurídico del Tribunal del Servicio Civil (SERVIR) y como abogado externo de los Estudios Martin Consultores Abogados y Linares Consultores Abogados.

IAITG

INSTITUTE
OF AUDIT &
IT-GOVERNANCE

Más información

www.iaitg.eu

Info@iaitg.eu