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.

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.

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 N°30171

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.

LEGISLACIÓN

- El Convenio 108 del Consejo de Europa y su proceso de reforma.
- La Directiva 95/46/CE.
- El Tratado de Lisboa. La Carta Europea de Derechos Fundamentales
- La regulación de las comunicaciones electrónicas y el Mercado de las Telecomunicaciones.
- La Directiva sobre retención de datos.
- Reglamento Europeo de Protección de Datos personales, antecedentes y planteamiento.

ORGANISMOS

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

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)

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.
- 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.

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.

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.

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.

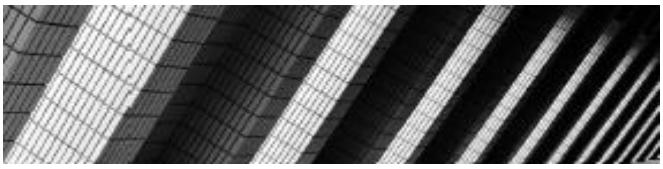
AUDITORÍA DE PRIVACIDAD

- 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



MODELOS DE IT-GOVERNANCE

- Comparativa de modelos
- Toma de decisiones

PLAN ESTRATÉGICO

- Definición de niveles de servicio.
- Arquitectura de la información.
- Dirección tecnológica.

PLAN DIRECTOR DE SEGURIDAD

- 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.

DIRECCIÓN

Antoni Bosch Pujol.

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

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).

Profesor de la Pacíifico Business School

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). Presidente Fundador ISACA-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. Ha sido el representante español en el subcomité ISO de IT-Governance (ISO 38500) y coordinador del subgrupo de IT-Governance.

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.