



Taller Fundamentos de Privacidad de Datos



Taller Fundamentos de Privacidad de datos

Objetivo:

Brindar a los participantes los **conceptos fundamentales y las mejores prácticas** para desarrollar y fortalecer habilidades orientadas a la **incorporación de la privacidad de datos desde el diseño** (*privacy by design*) en soluciones tecnológicas, productos y procesos organizacionales.

Al finalizar el curso, el participante contará con una **base sólida** para identificar, integrar y evaluar controles de privacidad de datos en entornos tecnológicos, alineados con marcos y estándares reconocidos.

Dirigida a:

Profesionales y personas interesadas en **crear, implementar y evaluar soluciones técnicas de privacidad de datos**, que cuenten con **conocimientos básicos a intermedios en tecnologías de información**.

Este curso es ideal para perfiles en TI, seguridad de la información, cumplimiento, riesgos, desarrollo de sistemas y gobierno de datos.

Curso Incluye:

Material que brinde el expositor.

Certificado de participación

Modalidad: Virtual (ZOOM)

Fecha: 13 al 17 de abril

Sesiones: 5 Sesiones

Hora: 5:30 p.m. a 9:00 p.m.

Horas CPE's: 16 horas.

¿Por qué Matricular este curso?

La **privacidad de los datos** se ha convertido en una **competencia crítica para las organizaciones**, siendo uno de los pilares más relevantes dentro de la **gestión de la seguridad de la información y el cumplimiento regulatorio**.

Este curso le permitirá:

- Comprender la **privacidad como un habilitador estratégico**, no solo como un requisito legal
- Desarrollar criterios para **integrar la privacidad en el diseño de soluciones, procesos y tecnologías**
- Fortalecer la capacidad organizacional para **proteger la información, gestionar riesgos y generar confianza**
- Alinear sus prácticas con **estándares y mejores prácticas internacionales**

Matricular este curso es invertir en **conocimiento clave, aplicable y altamente demandado** en el entorno profesional actual.





Contenido:

Dominio 1: Gobierno de la privacidad

Parte A. Gobernanza

- 1.1. Información y datos personales.
- 1.2. Leyes y estándares de privacidad en todas las jurisdicciones.
- 1.3. Documentación de privacidad.
- 1.4. Propósito legal, consentimiento e interés legítimo
- 1.5. Derechos del interesado

Sección B: Gestión

- 1.6. Roles y responsabilidades relacionadas con los datos.
- 1.7. Capacitación y concienciación sobre la privacidad.
- 1.8. Gestión de proveedores y terceros.
- 1.9. Proceso de auditoría.
- 1.10. Gestión de incidentes de privacidad

Sección C: Gestión de riesgos

- 1.11. Proceso de gestión de riesgos.
- 1.12. Evaluación de impacto en la privacidad (PIA).
- 1.13. Amenazas, ataques y vulnerabilidades relacionados con la privacidad.

Dominio 2: Arquitectura de privacidad


Sección A: Infraestructura

- 2.1. Pilas de tecnología
- 2.2. Servicios basados en la nube
- 2.3. Endpoints
- 2.4. Acceso remoto
- 2.5. Endurecimiento del sistema

Sección B: Aplicaciones y software

- 2.6. Ciclo de vida de desarrollo seguro
- 2.7. Aplicaciones y refuerzo de software
- 2.8. API y servicios
- 2.9. Tecnologías de seguimiento





Sección C: Controles técnicos de privacidad

- 2.10. Protocolos de comunicación y transporte
- 2.11. Cifrado, hash y desidentificación
- 2.12. Gestión de claves
- 2.13. Monitoreo y registro
- 2.14. Gestión de identidades y accesos

Dominio 3: Ciclo de datos

Sección A. Finalidad de los datos

- 3.1. Inventario y clasificación de datos
- 3.2. Calidad de los datos
- 3.3. Diagramas de uso y flujo de datos
- 3.4. Limitación del uso de datos
- 3.5. Análisis de datos

Sección B. Persistencia de datos

- 3.6. Minimización de datos
- 3.7. Migración de datos
- 3.8. Almacenamiento de datos
- 3.9. Almacenes de datos
- 3.10. Retención y archivado de datos
- 3.11. Destrucción de datos





Instructor:



Luis Gorgona Solís
Socio de Consultoría y Auditoría – RSM Central America

🔒 Especialista en Ciberseguridad y Seguridad de la Información, con amplia trayectoria en el sector público y privado, tanto a nivel nacional como internacional.

📄 Certificaciones:

- CISA – Certified Information Systems Auditor (ISACA)
- CDPSE – Certified Data Protection Solutions Engineer (ISACA)

🏛️ Experiencia destacada:

- Exdirector de Seguridad de la Información en Casa Presidencial de Costa Rica (2006–2010)
- Instructor en ciberseguridad para el CICTE y REMJA de la OEA
- Líder de proyecto para la primera implementación de ISO 27001 en Centros de Datos de Hewlett Packard (EE.UU., 2011)
- Oficial de Seguridad para la certificación ISO 27001 en el CenAm Center (Costa Rica–Panamá)

🌐 Trayectoria internacional:

- Responsable de Gobernanza, Riesgo y Cumplimiento (GRC) para la región AMERICAS en McKinsey & Company (2015–2017)
- Encargado de la certificación ISO 27001 para el Centro de Datos de McKinsey en New Jersey (EE.UU.)
- Director de Consultoría en Ciberseguridad en la firma boutique Knogin (2017–2019)

🎤 Expositor:

- Ponente en conferencias regionales de ISACA y en diversos congresos del capítulo Costa Rica





Inversión:

Miembros ISACA: ₡ 190.000 colones

Convenios: ₡200.000 colones

Público General: ₡220. 000 colones

**Precios Incluyen IVA*

Formas de pago:

- Transferencia o Depósito a la cuenta de Asociación Costarricense de Auditores en Informática.
- Link de pago.

A Nombre de la Asociación Costarricense de Auditores en Informática.

Cédula Jurídica: 3-002-045936

Cta. IBAN Colones -BCR CR69015201001013860853

Cta. IBAN Dólares - BCR CR96015201001022338943

Nota:

Enviar copia del depósito / comprobante de transferencia al correo capacitacion@isacacr.org

