



Taller Fundamentos de Privacidad de Datos



Taller Fundamentos de Privacidad de datos

Objetivo:

El asistente aprenderá los conceptos fundamentales para la creación y fortalecimiento de habilidades para incorporación de la privacidad de datos en el diseño de soluciones tecnológicas, productos y procesos.

Dirigida a:

Personas interesadas en crear, implementar y evaluar soluciones técnicas de privacidad de datos que cuenten con conocimientos básico-intermedio en tecnologías de información.

Modalidad: Virtual (ZOOM)

Fecha: miércoles 18 y viernes 20 de septiembre, 2024

Sesiones: 2 Sesiones

Hora: 8:00 a.m. a 5:30 p.m.

Horas CPE's: 16 horas.

Curso Incluye:

- Material que brinde el expositor.
- Certificado de participación

Inversión:

Miembros ISACA: ₡ 115 000 colones

Convenios: ₡130 000 colones

Público General: ₡160 000 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.

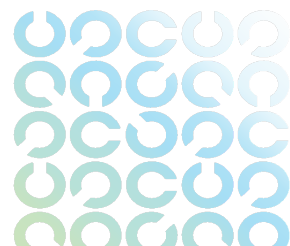
Cédula Jurídica: 3-002-045936

Cta. IBAN Colones -BCR CR69015201001013860853

Cta. IBAN Dólares - BCR CR96015201001022338943

Nota:

Enviar copia del depósito / comprobante de transferencia a la cuenta electrónica capacitacion@isacacr.org





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

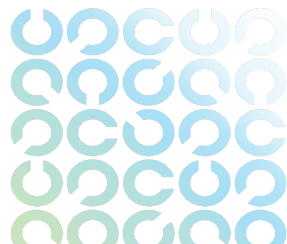
- 2.1. Pilas de tecnología
- 2.2. Servicios basados en la nube
- 2.3. Endpoints
- 2.4. Acceso remoto
- 2.5. Endurecimiento del sistema

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

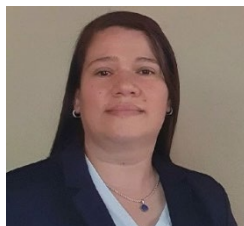
Sección A. Finalidad de los datos

- 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

Instructora:



Ing. Mariela Varela Campos

CRISC, CISA, CDPSE, CSXF, ITIL v4 Fundamentos, COBIT 5, SFPC - Fundamentos de Scrum

Mariela cuenta con una maestría en Administración de Empresas con énfasis en Finanzas, es Lic. en Ingeniería Industrial, con certificaciones en CRISC, CISA, CDPSE, CSXF, ITIL v4 Fundamentos, COBIT 5, SFPC - Fundamentos de Scrum. Con más de 11 años de experiencia en la gestión de servicios, riesgos y mejora de procesos utilizando las mejores prácticas existentes como: Six sigma, ISO 9001 Sistema de Gestión de Calidad, PMBOK Gestión de programas/proyectos, Seguridad de información y Ciberseguridad (Risk IT, NIST y familia ISO 27001 Sistema de Gestión de Seguridad de información), Gestión de riesgos empresariales (COSO ERM e ISO 31000 Sistema de Gestión de Riesgos), Gobierno corporativo, Gobierno de Información y Tecnología (COBIT), Riesgo Legal, Riesgo de Reputación y Lavado de capitales y financiamiento del terrorismo y diseño de armas de destrucción masiva, Cumplimiento regulatorio, Diseño y gestión de servicios (ISO 21000 Gestión de servicios, ITIL y VeriSM) y mejora de la Arquitectura Empresarial (TOGAF) y de TI (IT4IT).

