

# Formación en la Norma PCI DSS

Código: PCI-DSS

**Propuesta de Valor:** OTROS CURSOS DE CAPACITACIÓN TECNOLÓGICA

**Duración:** 16 Horas



Este curso, compuesto de 3 módulos, incluye desde una introducción a las normas del PCI SSC (PCI Security Standards Council) hasta el conocimiento exhaustivo de cada uno de los requerimientos de la norma PCI DSS.

Gracias a la experiencia acumulada en proyectos relacionados con las normas de seguridad de datos de tarjeta en proyectos de implantación y auditoría, así como en la gestión y análisis de incidentes, ofrecemos una formación del más alto nivel.

## AUDIENCIA

- Personal de Empresas de comercio donde se realice pago electrónico o presencial y que gestionen la información de tarjetas o los sistemas, seguridad, comunicaciones, aplicaciones y desarrollos, etc.
- Personal de Proveedores de Servicios relacionados con el tratamiento, almacenamiento o transmisión de datos de tarjetas.
- Personal de departamentos de Auditoría, Seguridad, Tecnología, Sistemas, etc. de empresas afectadas por las normas.

## PRE REQUISITOS

- Conocimientos sobre los procesos de pago con tarjeta, conocimientos de seguridad en TI o experiencia en el desarrollo de sistemas y software.

## OBJETIVOS

- Conocer las normas de PCI.
- Realizar análisis de requerimientos PCI DSS.

## CERTIFICACIÓN DISPONIBLE

## **CONTENIDO**

### 1. INTRODUCCIÓN

#### 1.1. LAS NORMAS DE PCI (DSS, PA-DSS, PTS):

1.1.1. CAMBIOS EN PCI DSS y PA-DSS VERSIÓN 3.2

1.1.2. NORMAS PCI: PCI DSS, PA-DSS, PCI PIN, P2PE, PCI PTS (PCI PED)

#### 1.2. ¿EN QUÉ CONSISTE LAS NORMAS?

#### 1.3. ¿A QUÉ APLICAN CADA UNA?

#### 1.4. ¿CÓMO SE INTERRELACIONAN?

#### 1.5. HOMOLOGACIONES DE AUDITORES: QSA, PA-QSA, P2PE (QSA/PA-QSA), QPA Y ASV

#### 1.6. COMERCIOS, PROVEEDORES DE SERVICIO Y ENTIDADES ADQUIRIENTES:

1.6.1. CLASIFICACIÓN DE LAS EMPRESAS POR LAS MARCAS DE TARJETAS

1.6.2. RESPONSABILIDADES DE CADA AFECTADO

#### 1.7. LOS PROGRAMAS DE SEGURIDAD DE VISA Y MASTERCARD

1.7.1. EMV, SNCP Y PCI DSS

### 2. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

#### 2.1. ANÁLISIS DE REQUERIMIENTOS PCI DSS

2.1.1. ANÁLISIS DE LOS REQUERIMIENTOS 1 A 12

#### 2.2. ABORDANDO UNA IMPLANTACIÓN DE PCI DSS

2.2.1. IDENTIFICACIÓN DE PROCESOS

2.2.1.1. TRANSMITIR, PROCESAR Y ALMACENAR

2.2.1.2. IDENTIFICACIÓN DE PERSONAS Y TI

#### 2.3. APROXIMACIÓN PRIORIZADA DEL PCI SSC

2.3.1. CREACIÓN DEL PLAN DE ACCIÓN

2.3.2. IMPORTANCIA DE LA PRIORIZACIÓN DE PROYECTOS

#### 2.4. PROYECTO "CERO": REDUCCIÓN DEL ÁMBITO DE PCI DSS

#### 2.5. SEGREGACIÓN DEL ENTORNO

2.5.1. ¿QUÉ ES VÁLIDO EN LA SEGMENTACIÓN Y QUÉ NO?

2.5.2. LA IMPORTANCIA DEL NEED-TO-KNOW PARA REDUCIR EL ENTORNO

2.5.3. CIFRADO Y ENMASCARAMIENTO

#### 2.6. TAREAS RUTINARIAS PARA EL CUMPLIMIENTO

2.6.1. ESCANEOS DE VULNERABILIDADES, TEST DE INTRUSIÓN, ETC.

2.6.2. TODO LO DEMÁS

#### 2.7. CONTROLES COMPENSATORIOS

2.7.1. ALINEAMIENTO DEL MARCO NORMATIVO

2.7.2. SECURIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN

2.8. REPORTANDO EL CUMPLIMIENTO DE PCI DSS: SAQ O AUDITORÍA

2.8.1. SAQ, SELF ASSESSMENT QUESTIONAIRE

2.8.2. ¿CÓMO ELEGIR EL SAQ ADECUADO?

2.8.3. ¿CÓMO CUMPLIMENTAR CORRECTAMENTE EL CUESTIONARIO?

2.8.4. ERRORES HABITUALES EN LA CUMPLIMENTACIÓN DEL SAQ

2.9. AUDITORÍA DE UN QSA

2.9.1. EXIGENCIAS A LOS QSA

2.9.2. PROCEDIMIENTO DE AUDITORÍA

2.9.3. PRINCIPALES PROBLEMAS PARA SUPERAR UNA AUDITORÍA

2.10. MANTENIMIENTO DE LA CERTIFICACIÓN PCI DSS

2.10.1. ¿CÓMO MANTENGO LA CERTIFICACIÓN PCI DSS?

2.10.2. TAREAS INTERNAS

2.10.3. TAREAS EXTERNAS

### 3. INCIDENTES

3.1. GESTIÓN Y RESPUESTA ANTE INCIDENTES CON DATOS DE TARJETAS

3.1.1. PROCEDIMIENTOS EXIGIDOS POR LAS MARCAS

3.1.1.1. QUALIFIED INCIDENT RESPONSE ASSESSOR(QIRA) / PCI FORENSIC INVESTIGATOR (PFI)

3.1.2. COSTE DE UN INCIDENTE

---

## ★ BENEFICIOS

- Al finalizar el curso, tendrás conocimientos y habilidades en gestión y respuesta ante incidentes con datos de tarjetas.