# IMPLEMENTACIÓN CONJUNTA PCI DSS 4.0.1 & ISO 27001:2022

SISTESEG CYBER AI

# Contenido

## Comparación Estratégica: ISO 27001:2022 vs PCI DSS 4.0.1 y Modelo de Implementación Integrada

**Introducción**

Las organizaciones que procesan pagos con tarjeta enfrentan el desafío de cumplir simultáneamente con múltiples marcos de seguridad. PCI DSS v4.0.1 se convirtió en el único estándar activo después del 31 de diciembre de 2024, mientras que ISO 27001:2022 continúa siendo el estándar internacional certificable más reconocido para sistemas de gestión de seguridad de la información.

Implementar estos estándares de manera aislada genera duplicación de esfuerzos, inconsistencias operacionales y costos innecesarios. Este artículo presenta un análisis exhaustivo de ambos marcos, identifica sus convergencias y divergencias, y proporciona una estrategia de implementación integrada optimizada por costos, complejidad técnica y tiempos de documentación. Todo lo anterior enmarcado en el ciclo del PHVA.

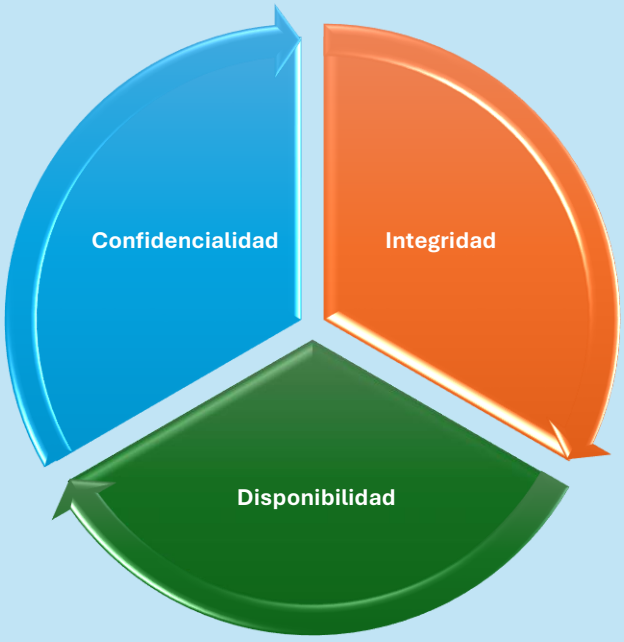
## Panorama General de Ambos Estándares

**ISO 27001:2022: Sistema de Gestión Integral**

ISO 27001:2022 es un estándar certificable que especifica requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Su característica distintiva es la flexibilidad: las organizaciones realizan evaluaciones de riesgo contextuales y seleccionan controles aplicables de un catálogo de 93 opciones organizadas en cuatro temas (Organizacionales, Personas, Físicos y Tecnológicos) para preservar la confidencialidad, integridad y disponibilidad.

**Características clave:**

- **Enfoque:** Gestión de riesgos de seguridad de la información en general
- **Alcance:** Toda la organización o partes definidas
- **Naturaleza:** Marco adaptable basado en riesgos
- **Certificación:** Certificable por terceros acreditados
- **Audiencia:** Todas las industrias
- **Ciclo de auditoría:** Anual (vigilancia) + cada 3 años (recertificación)



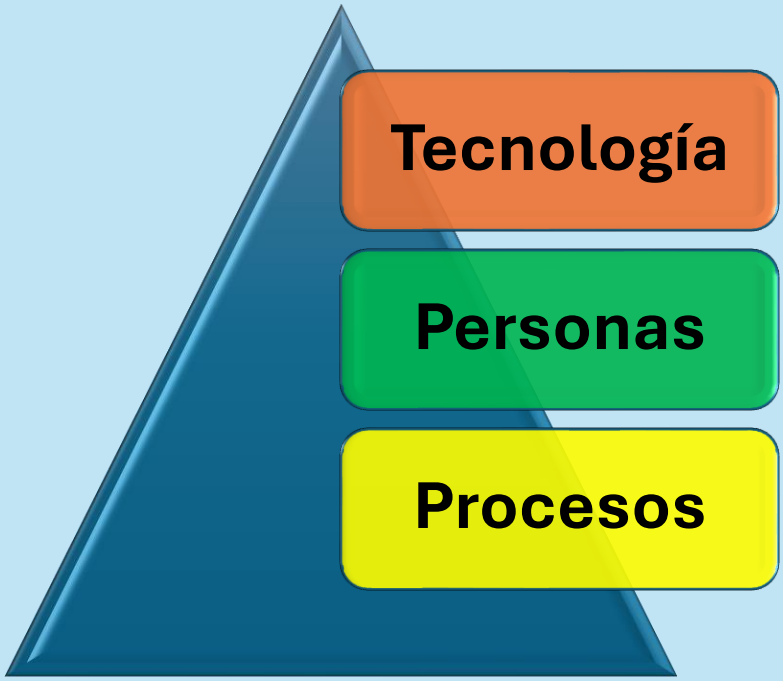
## PCI DSS 4.0.1: Requisitos Prescriptivos para Pagos

PCI DSS 4.0 entró en vigor el 31 de marzo de 2024 e introdujo 64 nuevos requisitos. La versión 4.0.1 no añadió nuevos requisitos sino que proporcionó clarificaciones, como la especificación de que solo las vulnerabilidades críticas deben parchearse en 30 días y considerar las personas, los procesos y la tecnología.

PCI DSS es prescriptivo: define exactamente qué debe implementarse para proteger datos de tarjetahabientes (CHD) y datos de autenticación sensibles (SAD). Consta de 12 requisitos principales agrupados en seis objetivos de control, con aproximadamente 400 sub-requisitos detallados.

**Características clave:**

- **Enfoque:** Protección específica de datos de tarjetas de pago
- **Alcance:** Entorno de datos de tarjetahabientes (CDE)
- **Naturaleza:** Requisitos prescriptivos obligatorios
- **Validación:** Validación anual por QSA (Qualified Security Assessor) o SAQ (Self-Assessment)
- **Audiencia:** Entidades que procesan, almacenan o transmiten CHD
- **Consecuencias de incumplimiento:** Multas de marcas de pago, pérdida de capacidad de procesar tarjetas



## Estructura Comparativa Detallada

**Los 12 Requisitos de PCI DSS 4.0.1**

**Objetivo 1: Construir y Mantener una Red Segura**

**Requisito 1:** Instalar y mantener configuraciones de seguridad de red para proteger datos de tarjetahabientes

- Firewalls y routers con reglas restrictivas
- Segmentación de red entre CDE y otras redes
- Documentación de flujos de datos y arquitectura de red

**Requisito 2:** Aplicar configuraciones seguras a todos los componentes del sistema

- Hardening de sistemas operativos, bases de datos, aplicaciones
- Eliminación de cuentas, servicios y protocolos innecesarios
- Gestión de configuraciones con líneas base documentadas

**Objetivo 2: Proteger los Datos de los Tarjetahabientes**

**Requisito 3:** Proteger datos almacenados de tarjetahabientes

- Minimización de datos: retener solo lo necesario
- Enmascaramiento de PAN (Primary Account Number) cuando se muestra
- Cifrado fuerte para CHD almacenado
- Gestión de claves criptográficas

**Requisito 4:** Proteger datos de tarjetahabientes con criptografía fuerte durante transmisión en redes públicas

- TLS 1.2 o superior para transmisiones
- Cifrado end-to-end
- Protección de claves de cifrado

**Objetivo 3: Mantener un Programa de Gestión de Vulnerabilidades**

**Requisito 5:** Proteger todos los sistemas y redes contra malware

- Antimalware en sistemas afectados por malware
- Actualizaciones automáticas de definiciones
- Escaneos periódicos
- Mecanismos anti-tampering

**Requisito 6:** Desarrollar y mantener sistemas y software seguros

- Gestión de vulnerabilidades con aplicación oportuna de parches
- Desarrollo seguro de software (SDLC seguro)
- Prevención de vulnerabilidades comunes (OWASP Top 10)
- Gestión de cambios
- Componentes de software inventariados

**Objetivo 4: Implementar Medidas Fuertes de Control de Acceso**

**Requisito 7:** Restringir acceso a datos de tarjetahabientes según necesidad de conocer del negocio

- Control de acceso basado en roles (RBAC)
- Principio de privilegio mínimo
- Acceso otorgado basado en clasificación de datos y trabajo

**Requisito 8:** Identificar usuarios y autenticar acceso a componentes del sistema

- Identificación única para cada usuario
- Autenticación multifactor (MFA) para acceso a CDE
- Gestión robusta de contraseñas
- Gestión de sesiones

**Requisito 9:** Restringir acceso físico a datos de tarjetahabientes

- Controles físicos para áreas con sistemas que procesan CHD
- Visitantes escoltados
- Destrucción segura de medios
- Dispositivos POI protegidos contra manipulación

**Objetivo 5: Monitorear y Probar Redes Regularmente**

**Requisito 10:** Registrar y monitorear todos los accesos a recursos de red y datos de tarjetahabientes

- Logging completo de eventos de seguridad
- Revisión diaria de logs
- Protección de logs contra alteración
- Retención mínima de 1 año (3 meses online)

**Requisito 11:** Probar la seguridad de sistemas y redes regularmente

- Escaneos de vulnerabilidades trimestrales por ASV aprobado

- Pruebas de penetración anuales (internas y externas)
- Sistemas de detección/prevención de intrusiones (IDS/IPS)
- Monitoreo de integridad de archivos críticos

**Objetivo 6: Mantener una Política de Seguridad de la Información**

**Requisito 12:** Apoyar la seguridad de la información con políticas y programas organizacionales

- Políticas de seguridad documentadas y publicadas
- Análisis de riesgos anual
- Programa de concientización de seguridad
- Gestión de proveedores de servicios
- Respuesta a incidentes
- Responsabilidades definidas

| PCI Data Security Standard – High Level Overview | |
|---|---|
| **Build and Maintain a Secure Network and Systems** | 1. Install and Maintain Network Security Controls.<br>2. Apply Secure Configurations to All System Components. |
| **Protect Account Data** | 3. Protect Stored Account Data.<br>4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks. |
| **Maintain a Vulnerability Management Program** | 5. Protect All Systems and Networks from Malicious Software.<br>6. Develop and Maintain Secure Systems and Software. |
| **Implement Strong Access Control Measures** | 7. Restrict Access to System Components and Cardholder Data by Business Need to Know.<br>8. Identify Users and Authenticate Access to System Components.<br>9. Restrict Physical Access to Cardholder Data. |
| **Regularly Monitor and Test Networks** | 10. Log and Monitor All Access to System Components and Cardholder Data.<br>11. Test Security of Systems and Networks Regularly. |
| **Maintain an Information Security Policy** | 12. Support Information Security with Organizational Policies and Programs. |

## Mapeo con ISO 27001:2022

La siguiente tabla mapea los requisitos de PCI DSS con controles relevantes de ISO 27001:2022 Anexo A:

| PCI DSS Req. | Descripción | Controles ISO 27001 Principales | Superposición |
|---|---|---|---|
| **1** | Seguridad de red | 8.20 Seguridad de Redes, 8.22 Segregación de Redes | **85%** |
| **2** | Configuraciones seguras | 8.9 Gestión de Configuración, 8.19 Instalación de Software | **90%** |
| **3** | Protección de datos almacenados | 8.10 Eliminación de Información, 8.11 Enmascaramiento, 8.24 Criptografía | **75%** |
| **4** | Protección en transmisión | 8.24 Uso de Criptografía, 5.14 Transferencia de Información | **80%** |
| **5** | Anti-malware | 8.7 Protección contra Malware | **95%** |
| **6** | Sistemas seguros | 8.8 Gestión de Vulnerabilidades, 8.25-8.29 Desarrollo Seguro, 8.32 Gestión de Cambios | **80%** |
| **7** | Control de acceso lógico | 5.15 Control de Acceso, 8.3 Restricción de Acceso | **85%** |
| **8** | Identificación/Autenticación | 5.16-5.18 Gestión de Identidades, 8.5 Autenticación Segura | **90%** |
| **9** | Acceso físico | 7.1-7.4 Controles Físicos, 7.10 Medios de Almacenamiento | **70%** |
| **10** | Logging/Monitoreo | 8.15 Registro, 8.16 Monitoreo, 8.17 Sincronización de Relojes | **85%** |
| **11** | Testing de seguridad | 8.8 Gestión de Vulnerabilidades, 8.29 Pruebas de Seguridad | **65%** |
| **12** | Políticas y procedimientos | 5.1 Políticas, 5.2 Roles, 6.3 Concientización, 5.24-5.27 Gestión de Incidentes | **90%** |

**Observaciones del mapeo:**

- **Superposición alta (>80%):** Requisitos 1, 2, 5, 6, 7, 8, 10, 12 tienen equivalencias muy fuertes
- **Superposición moderada (60-80%):** Requisitos 3, 4, 9, 11 tienen equivalencias parciales
- **Divergencias principales:** PCI DSS es más prescriptivo en pruebas de penetración externas, escaneos ASV y requisitos específicos de cifrado

## Convergencias Fundamentales

**1. Gestión de Riesgos como Fundamento**

Ambos estándares reconocen la gestión de riesgos como base:

- **ISO 27001:** Cláusulas 6.1.2 y 6.1.3 requieren evaluación y tratamiento de riesgos formal
- **PCI DSS 12.3:** Requiere análisis de riesgos anual que identifique amenazas, vulnerabilidades e impactos

**Sinergia:** Un proceso unificado de evaluación de riesgos puede satisfacer ambos requisitos. La evaluación ISO 27001 es más amplia (toda la información), mientras PCI DSS enfoca en CHD, pero la metodología puede ser común.

**2. Control de Acceso y Gestión de Identidades**

Principios compartidos:

- Identificación única de usuarios
- Autenticación fuerte (MFA)
- Principio de privilegio mínimo
- Control de acceso basado en roles
- Revisiones periódicas de accesos

**Sinergia:** Implementar una solución IAM/PAM robusta (Identity and Access Management / Privileged Access Management) satisface PCI DSS Req. 7-8 e ISO 27001 controles 5.15-5.18 y 8.2-8.5 simultáneamente.

**3. Protección contra Malware**

Ambos requieren:

- Soluciones anti-malware en endpoints y servidores
- Actualizaciones automáticas
- Escaneos regulares
- Protección en tiempo real

**Sinergia:** Una plataforma EDR (Endpoint Detection and Response) moderna cumple ambos requisitos sin duplicación.

**4. Gestión de Vulnerabilidades y Parches**

Requisitos convergentes:

- Inventario de activos de software
- Identificación sistemática de vulnerabilidades

- Priorización basada en severidad
- Aplicación oportuna de parches
- Validación post-parche

**Diferencia clave:** PCI DSS 4.0.1 requiere parches de vulnerabilidades críticas en 30 días, mientras ISO 27001 deja la temporalidad a evaluación de riesgos.

**Sinergia:** Herramienta de gestión de vulnerabilidades unificada con políticas que satisfacen el requisito más estricto (PCI DSS).

**5. Logging, Monitoreo y Respuesta a Incidentes**

Elementos comunes:

- Generación de logs de eventos de seguridad
- Protección de logs contra alteración
- Revisión regular de logs
- Capacidad de respuesta a incidentes
- Documentación de incidentes

**Diferencia:** PCI DSS especifica revisión diaria de logs y retención mínima (1 año), ISO 27001 es más flexible.

**Sinergia:** Implementar SIEM (Security Information and Event Management) con reglas de correlación y retención según PCI DSS satisface ambos estándares.

**6. Desarrollo Seguro de Software**

Principios compartidos:

- Requisitos de seguridad en fase de diseño
- Revisiones de código
- Pruebas de seguridad antes de producción
- Gestión de cambios
- Separación de ambientes

**Sinergia:** Pipeline DevSecOps con SAST/DAST/SCA integrado satisface PCI DSS Req. 6 e ISO 27001 controles 8.25-8.32.

**7. Políticas, Procedimientos y Concientización**

Elementos comunes:

- Políticas de seguridad documentadas y aprobadas

- Definición de roles y responsabilidades
- Capacitación anual de personal
- Revisiones periódicas de políticas

**Sinergia:** Marco de políticas unificado que cumple requisitos de ambos estándares, con anexos específicos de PCI DSS donde necesario.

## Divergencias Críticas

**1. Alcance de Aplicación**

**ISO 27001:**

- Alcance flexible definido por la organización
- Puede incluir toda la empresa o unidades específicas
- Enfoca en todos los activos de información

**PCI DSS:**

- Alcance obligatorio: Entorno de Datos de Tarjetahabientes (CDE)
- Incluye sistemas que procesan, almacenan o transmiten CHD
- Sistemas conectados al CDE también en alcance
- Reducción de alcance mediante segmentación de red

**Implicación estratégica:** El alcance PCI DSS puede estar completamente contenido dentro del alcance ISO 27001, permitiendo implementación del SGSI completo con énfasis adicional en CDE.

**2. Pruebas Externas Mandatorias**

**PCI DSS especifica:**

- Escaneos de vulnerabilidades trimestrales por ASV (Approved Scanning Vendor)
- Pruebas de penetración anuales (internas y externas) por personal calificado
- Pruebas de segmentación de red

**ISO 27001:**

- Control 8.8 requiere gestión de vulnerabilidades pero no especifica frecuencia
- Control 8.29 requiere pruebas de seguridad pero sin mandato de terceros

**Implicación de costos:** PCI DSS genera costos anuales recurrentes por ASV ($2,000-$10,000) y pentests ($15,000-$50,000) no necesariamente requeridos por ISO 27001.

**3. Cifrado Prescriptivo**

**PCI DSS:**

- Especifica algoritmos mínimos (AES, RSA con longitudes clave específicas)
- Requiere cifrado de PAN cuando se almacena
- TLS 1.2+ obligatorio para transmisiones en redes públicas
- Gestión de claves con procedimientos detallados

**ISO 27001:**

- Control 8.24 requiere política de uso de criptografía
- No prescribe algoritmos específicos
- Decisiones basadas en evaluación de riesgos

**Implicación:** Las implementaciones PCI DSS automáticamente satisfacen requisitos ISO 27001 de cifrado, pero no viceversa.

**4. Gestión de Proveedores**

**PCI DSS 12.8:**

- Requisitos muy específicos para proveedores de servicios
- Validación anual de cumplimiento PCI DSS de proveedores
- Responsabilidad compartida documentada
- Registros de proveedores con acceso a CHD

**ISO 27001 5.19-5.22:**

- Requisitos generales de seguridad en contratos
- Monitoreo de proveedores
- Flexibilidad en implementación

**Implicación:** Programas de gestión de terceros deben incluir componente específico PCI DSS para proveedores con acceso a CHD.

**5. Destrucción de Medios y Retención de Datos**

**PCI DSS:**

- Minimización de datos: retener solo CHD necesario
- Procedimientos específicos de destrucción (trituración, desmagnetización)
- Logs retenidos 1 año mínimo (3 meses online)

**ISO 27001:**

- Controles 8.10 (Eliminación) y 5.33 (Protección de Registros) más generales
- Retención basada en requisitos legales y de negocio

**Implicación:** Políticas de retención y destrucción deben incorporar requisitos específicos PCI DSS para CHD mientras mantienen flexibilidad para otra información.

## Análisis de Costos Comparativo

**Costos de Certificación/Validación**

**ISO 27001:**

- Auditoría de certificación inicial: $15,000 - $50,000 (según tamaño y complejidad)
- Auditorías de vigilancia anuales: $8,000 - $25,000
- Recertificación cada 3 años: $15,000 - $45,000
- **Total anual promedio:** $13,000 - $35,000

**PCI DSS:**

- Nivel 1 (>6M transacciones/año): QSA ROC $30,000 - $100,000+ anual
- Nivel 2 (1-6M transacciones): SAQ + escaneo ASV $10,000 - $30,000 anual
- Nivel 3-4 (<1M transacciones): SAQ + escaneo ASV $5,000 - $15,000 anual
- **Total anual promedio:** $5,000 - $100,000 (según nivel)

**Costos de Implementación Tecnológica**

**Infraestructura Compartida (satisface ambos):**

- Firewall enterprise: $20,000 - $100,000
- SIEM: $30,000 - $200,000 anual (según volumen logs)
- EDR/Antimalware: $20 - $50 por endpoint/año
- Solución IAM/PAM: $50,000 - $300,000
- Gestión de vulnerabilidades: $15,000 - $80,000 anual
- Backup/DR: $30,000 - $150,000
- **Subtotal:** $165,000 - $830,000 inicial + $45,000 - $280,000 anual

**Específico PCI DSS:**

- Tokenización/Cifrado de CHD: $50,000 - $200,000
- Segmentación de red adicional: $20,000 - $100,000
- Pruebas de penetración anuales: $15,000 - $50,000
- Escaneos ASV trimestrales: $2,000 - $10,000 anual
- **Subtotal:** $87,000 - $360,000 inicial + $17,000 - $60,000 anual

**Específico ISO 27001:**

- Consultoría para SGSI: $30,000 - $80,000 (opcional)

- Herramientas de gestión de riesgos: $5,000 - $20,000
- **Subtotal:** $35,000 - $100,000 (mayormente uno-vez)

## Costos de Personal

**Roles Necesarios:**

- **CISO/Responsable de Seguridad:** $120,000 - $250,000/año (o CISOaaS $60,000 - $120,000)
- **Analista de Seguridad (SOC):** $60,000 - $100,000/año por FTE (necesario 2-3)
- **Especialista en Cumplimiento:** $70,000 - $120,000/año
- **Personal de auditoría interna:** 0.5-1 FTE $50,000 - $80,000/año

**Total personal:** $310,000 - $650,000/año para implementación robusta

**Costos de Documentación y Mantenimiento**

**ISO 27001:**

- Desarrollo inicial de políticas: 200-400 horas ($20,000 - $60,000)
- Actualizaciones anuales: 80-120 horas ($8,000 - $18,000)
- Evaluaciones de riesgo: 120-200 horas ($12,000 - $30,000 anual)

**PCI DSS:**

- Documentación inicial (diagramas de red, flujos de datos): 100-200 horas ($10,000 - $30,000)
- Mantenimiento trimestral: 40-60 horas ($16,000 - $30,000 anual)
- Remediación pre-auditoría: 80-160 horas ($8,000 - $24,000 anual)

**Superposición:** 60-70% de documentación puede unificarse, ahorrando $15,000 - $40,000 anualmente.

## Costos Totales Proyectados (3 años)

**Implementación Separada:**

- ISO 27001: $450,000 - $1,200,000
- PCI DSS: $350,000 - $900,000
- **Total:** $800,000 - $2,100,000

**Implementación Integrada:**

- Infraestructura compartida: $300,000 - $900,000

- Complementos específicos: $150,000 - $400,000
- Auditorías/validaciones: $120,000 - $400,000
- Personal (sinergias 20-30%): $700,000 - $1,500,000
- **Total:** $1,270,000 - $3,200,000

**Ahorro potencial:** 20-35% ($200,000 - $700,000) mediante implementación integrada.

**Análisis de Complejidad**

**Complejidad Técnica**

## Elementos de Alta Complejidad Compartidos:

1. **Segmentación de red robusta (PCI Req. 1 / ISO 8.20-8.22)**
    - Requiere rediseño de arquitectura de red
    - Implementación de VLANs, firewalls internos, ACLs
    - Documentación exhaustiva de flujos
    - **Duración:** 3-6 meses
    - **Expertise:** Arquitectos de red especializados
2. **SIEM con correlación avanzada (PCI Req. 10 / ISO 8.15-8.16)**
    - Integración de múltiples fuentes de logs
    - Desarrollo de reglas de correlación
    - Configuración de alertas y dashboards
    - Ajuste continuo para reducir falsos positivos
    - **Duración:** 4-8 meses hasta madurez operacional
    - **Expertise:** Analistas SOC, ingenieros SIEM
3. **Desarrollo Seguro Completo (PCI Req. 6 / ISO 8.25-8.29)**
    - Transformación cultural de equipos desarrollo
    - Integración de herramientas en pipeline CI/CD
    - Capacitación de desarrolladores
    - Establecimiento de SLAs de remediación
    - **Duración:** 6-12 meses
    - **Expertise:** Especialistas AppSec, DevSecOps

**Elementos de Complejidad Moderada:**

- Gestión de identidades y acceso (IAM): 3-5 meses
- Anti-malware enterprise: 2-3 meses
- Gestión de vulnerabilidades: 2-4 meses
- Controles físicos: 1-3 meses (según instalaciones)

**Elementos de Baja Complejidad:**

- Políticas y procedimientos: 1-2 meses
- Programa de concientización: 1-2 meses

- Inventario de activos inicial: 1-2 meses

**Complejidad Organizacional**

**Alta Complejidad:**

1. **Cambio cultural hacia seguridad**
    - Resistencia de unidades de negocio
    - Equilibrio seguridad vs usabilidad
    - Modificación de procesos establecidos
    - **Mitigación:** Patrocinio ejecutivo, comunicación continua, quick wins
2. **Coordinación multi-departamental**
    - TI, Desarrollo, Operaciones, Legal, Compliance, Finanzas
    - Diferentes prioridades y lenguajes
    - **Mitigación:** Comité de gobierno con representación ejecutiva
3. **Gestión de proveedores críticos**
    - Evaluaciones de seguridad de múltiples proveedores
    - Negociación de cláusulas contractuales
    - **Mitigación:** Priorización basada en riesgo, templates de contratos

**Complejidad Documental**

**ISO 27001 requiere:**

- Alcance del SGSI
- Política de seguridad
- Objetivos de seguridad
- Evaluaciones de riesgo
- Declaración de Aplicabilidad (SOA) con justificaciones
- Procedimientos obligatorios (9 documentados explícitamente)
- Registros de evidencia (auditorías, incidentes, capacitación, revisiones)
- **Volumen estimado:** 500-2,000 páginas según complejidad

**PCI DSS requiere:**

- Diagramas de flujo de datos de CHD
- Diagramas de arquitectura de red

- Inventario de componentes en alcance
- Políticas y procedimientos específicos (12 áreas)
- Registros de pruebas (penetración, escaneos ASV)
- Evidencias de cumplimiento continuo
- **Volumen estimado:** 300-1,000 páginas

**Superposición documental:** 50-60% de políticas, procedimientos e inventarios pueden unificarse con referencias cruzadas.

**Estrategia de Implementación Integrada**

**Principios Rectores**

1. **Segmentación de CDE como prioridad:** Reduce alcance PCI DSS y simplifica cumplimiento
2. **Infraestructura compartida primero:** Maximiza ROI de inversiones tecnológicas
3. **Quick wins tempranos:** Genera momentum y justifica inversiones continuas
4. **Documentación unificada:** Un marco de políticas con anexos específicos
5. **Enfoque por fases iterativo:** No "big bang" sino sprints de 3-4 meses

**Fase 0: Preparación y Scoping (Mes 1-2)**

**Objetivo:** Definir alcances, realizar gap analysis, obtener compromiso ejecutivo.

**Actividades Clave:**

1. **Definición de Alcance Dual**
    - Identificar sistemas que procesan CHD (alcance PCI DSS)
    - Definir alcance SGSI (típicamente más amplio)
    - Documentar justificación de alcances
2. **Gap Analysis Integrado**
    - Evaluar estado actual contra ambos estándares
    - Identificar controles existentes aprovechables
    - Cuantificar brechas y esfuerzo de remediación
    - **Herramienta sugerida:** Matriz de mapeo con scoring
3. **Business Case y Presupuesto**
    - Proyección de costos 3 años (integrado vs separado)
    - Análisis de riesgos de no-cumplimiento

- Presentación a C-level con recomendación

4. **Formación de Equipos**
    - Nombrar CISO o responsable
    - Identificar campeones en áreas clave
    - Definir estructura de gobierno (comité directivo)

## Entregables:

- Documento de alcance dual
- Gap analysis con priorización
- Roadmap de implementación
- Presupuesto aprobado
- Estructura de gobierno

**Recursos:** 0.5-1 FTE + consultor externo (opcional) **Costo:** $20,000 - $50,000

**Fase 1: Fundamentos y Segmentación (Mes 3-6)**

**Objetivo:** Establecer controles base y reducir alcance PCI DSS mediante segmentación.

**Track 1: Segmentación de Red (Crítico para PCI DSS)**

- Diseñar arquitectura segmentada: CDE, zona interna, DMZ
- Implementar firewalls y ACLs entre segmentos
- Configurar VLANs y subnetting
- Documentar flujos de datos (diagramas detallados)
- Realizar pruebas de segmentación
- **Controles satisfechos:** PCI Req. 1, ISO 8.20-8.22
- **Duración:** 3-4 meses
- **Costo:** $40,000 - $150,000

**Track 2: Políticas y Gobierno**

- Desarrollar política maestra de seguridad (ISO 5.1 / PCI 12.1)
- Definir roles y responsabilidades (ISO 5.2 / PCI 12.4)
- Crear marco de 12 políticas específicas mapeadas a ambos estándares
- Establecer comité de seguridad con reuniones mensuales
- **Controles satisfechos:** ISO 5.1-5.2, PCI 12.1-12.4
- **Duración:** 2 meses
- **Costo:** $15,000 - $40,000 (consultoría documental)

**Track 3: Inventarios y Clasificación**

- Inventario completo de activos de TI (ISO 5.9)
- Inventario específico de componentes en CDE (PCI requisito de documentación)

- Esquema de clasificación de información (ISO 5.12)
- Identificación de CHD/SAD en organización
- **Controles satisfechos:** ISO 5.9-5.13, fundamento PCI
- **Duración:** 2 meses
- **Costo:** $10,000 - $30,000

**Track 4: Evaluación de Riesgos Inicial**

- Metodología unificada de evaluación de riesgos
- Assessment de riesgos para alcance ISO 27001
- Assessment específico de riesgos para CDE (PCI 12.3)
- Priorización de tratamientos
- **Controles satisfechos:** ISO 6.1.2-6.1.3, PCI 12.3
- **Duración:** 2 meses
- **Costo:** $20,000 - $50,000

**Entregables Fase 1:**

- Red segmentada con CDE aislado
- Suite de políticas aprobadas (12-15 documentos)
- Inventario de activos en herramienta
- Evaluación de riesgos documentada
- Roadmap de tratamiento de riesgos

**Recursos Fase 1:** 2-3 FTE + arquitecto de red + consultor **Costo Total Fase 1:** $85,000 - $270,000
**Tiempo:** 4 meses

**Fase 2: Protección y Control de Acceso (Mes 7-11)**

**Objetivo:** Implementar controles técnicos fundamentales de protección.

**Track 1: Gestión de Identidades y Acceso (IAM/PAM)**

- Implementar Active Directory limpio o solución IAM cloud
- Configurar SSO donde aplicable
- Desplegar MFA para acceso remoto y CDE (obligatorio PCI 8.4-8.5)
- Solución PAM para cuentas privilegiadas (ISO 8.2 / PCI 8.6)
- Control de acceso basado en roles (RBAC)

- Procedimientos de alta/baja/modificación de usuarios
- **Controles satisfechos:** ISO 5.15-5.18, 8.2-8.5 / PCI Req. 7-8 completo
- **Duración:** 4-5 meses
- **Costo:** $80,000 - $350,000

**Track 2: Hardening y Gestión de Configuración**

- Líneas base de configuración segura (CIS Benchmarks)
- Hardening de sistemas operativos, bases de datos, aplicaciones
- Eliminación de servicios/cuentas innecesarios (PCI 2.2)
- Gestión de configuración con herramienta (Ansible, Chef, Puppet)
- Change management formal (ISO 8.32 / PCI 6.5)
- **Controles satisfechos:** ISO 8.9, 8.19, 8.32 / PCI Req. 2, 6.5
- **Duración:** 3-4 meses
- **Costo:** $40,000 - $120,000

**Track 3: Criptografía**

- Política de uso de criptografía (ISO 8.24)
- Cifrado de CHD en almacenamiento (PCI 3.5-3.6)
- Cifrado de CHD en transmisión - TLS 1.2+ (PCI 4.2)
- Implementar tokenización o cifrado FPE donde viable
- Gestión de claves criptográficas (PCI 3.6-3.7)
- **Controles satisfechos:** ISO 8.24, 5.14 / PCI Req. 3-4 completo
- **Duración:** 3-4 meses
- **Costo:** $60,000 - $250,000 (tokenización aumenta costo)

**Track 4: Anti-Malware**

- Despliegue de EDR/antimalware enterprise
- Configuración de actualizaciones automáticas
- Escaneos periódicos y en tiempo real
- Protección en servidores críticos (PCI 5.2)
- Mecanismos anti-tampering
- **Controles satisfechos:** ISO 8.7 / PCI Req. 5 completo

- **Duración:** 2-3 meses
- **Costo:** $30,000 - $80,000

**Entregables Fase 2:**

- IAM/PAM operacional con MFA
- Sistemas hardenizados según baselines
- CHD cifrado en almacenamiento y transmisión
- Antimalware en 100% de sistemas en alcance
- Procedimientos de gestión de cambios formales

**Recursos Fase 2:** 3-4 FTE (administradores sistemas, seguridad) **Costo Total Fase 2:** $210,000 - $800,000 **Tiempo:** 5 meses

**Fase 3: Detección y Respuesta (Mes 12-17)**

**Objetivo:** Capacidad de detectar, monitorear y responder a incidentes.

**Track 1: Logging y SIEM**

- Identificar fuentes de logs críticos (ISO 8.15 / PCI 10.2)
- Desplegar colectores de logs
- Implementar SIEM (Splunk, QRadar, ELK, Sentinel)
- Desarrollar reglas de correlación (PCI 10.6)
- Configurar retención 1 año (PCI 10.7)
- Protección de logs contra alteración (PCI 10.5)
- Sincronización de relojes con NTP (ISO 8.17 / PCI 10.4)
- **Controles satisfechos:** ISO 8.15-8.17 / PCI Req. 10 completo
- **Duración:** 5-6 meses
- **Costo:** $100,000 - $300,000 (SIEM) + $30,000-$100,000/año (licencias)

**Track 2: Gestión de Vulnerabilidades**

- Herramienta de escaneo de vulnerabilidades (Nessus, Qualys, Rapid7)
- Escaneos internos mensuales mínimo (PCI 11.2)
- Contratar ASV para escaneos externos trimestrales (PCI 11.3)
- Proceso de priorización y remediación
- SLA: críticas 30 días, altas 60 días (PCI 6.3.1)

- **Controles satisfechos:** ISO 8.8 / PCI Req. 6.3, 11.2-11.3
- **Duración:** 3-4 meses
- **Costo:** $25,000 - $90,000 + $2,000-$10,000/año (ASV)

**Track 3: IDS/IPS y Monitoreo de Red**

- Desplegar IDS/IPS en perímetros críticos (PCI 11.4)
- Configurar alertas de actividad anómala
- Monitoreo de tráfico hacia/desde CDE
- File Integrity Monitoring (FIM) en sistemas críticos (PCI 11.5)
- **Controles satisfechos:** ISO 8.16 / PCI 11.4-11.5
- **Duración:** 3-4 meses
- **Costo:** $50,000 - $150,000

**Track 4: Gestión de Incidentes**

- Establecer CSIRT o capacidad de respuesta (ISO 5.24-5.27 / PCI 12.10)
- Desarrollar playbooks de respuesta
- Herramientas forenses (FTK, EnCase, o alternativas)
- Plan de comunicación de incidentes
- Simulacros trimestrales
- Procedimiento de recopilación de evidencia (ISO 5.28)
- **Controles satisfechos:** ISO 5.24-5.28 / PCI 12.10
- **Duración:** 3-4 meses
- **Costo:** $40,000 - $100,000

**Track 5: Testing de Seguridad**

- Pruebas de penetración internas y externas (PCI 11.3)
- Contratar pentester calificado (anuales)
- Pruebas de segmentación de red (PCI 11.3.4)
- Testing de aplicaciones web (PCI 6.4.4)
- **Controles satisfechos:** ISO 8.29 / PCI 11.3-11.4
- **Duración:** Recurrente anual
- **Costo:** $20,000 - $60,000/año

**Entregables Fase 3:**

- SIEM operacional con SOC o monitoreo managed
- Programa de gestión de vulnerabilidades maduro
- IDS/IPS y FIM desplegados
- Capacidad de respuesta a incidentes probada
- Primera prueba de penetración completada

**Recursos Fase 3:** 3-5 FTE (analistas SOC, especialistas detección) **Costo Total Fase 3:** $235,000 - $700,000 inicial + $50,000-$170,000/año **Tiempo:** 6 meses

**Fase 4: Desarrollo Seguro y Controles Avanzados (Mes 18-24)**

**Objetivo:** Madurar capacidades de desarrollo seguro y optimizar controles.

**Track 1: Secure SDLC**

- Integrar seguridad en metodología desarrollo (Agile/DevOps)
- Requisitos de seguridad en fase diseño (ISO 8.26 / PCI 6.4.1)
- Code reviews con checklist seguridad (PCI 6.4.2)
- SAST (análisis estático) en pipeline CI/CD (PCI 6.4.3)
- DAST (análisis dinámico) pre-producción (PCI 6.4.4)
- SCA (análisis de componentes) para librerías terceros (PCI 6.4.3)
- Capacitación desarrolladores en secure coding (PCI 6.4.2)
- **Controles satisfechos:** ISO 8.25-8.29 / PCI Req. 6.4 completo
- **Duración:** 6-8 meses (transformación cultural)
- **Costo:** $80,000 - $250,000

**Track 2: Controles Físicos**

- Evaluación de instalaciones físicas (ISO 7.1-7.4 / PCI 9.1-9.3)
- Control de acceso físico con badges (PCI 9.2)
- CCTV en áreas sensibles (PCI 9.1.2)
- Política de visitantes con registro (PCI 9.2)
- Protección de dispositivos POI si aplicable (PCI 9.9)
- Destrucción segura de medios (ISO 7.10, 8.10 / PCI 9.8)
- **Controles satisfechos:** ISO Tema 3 completo / PCI Req. 9

- **Duración:** 2-4 meses
- **Costo:** $30,000 - $120,000 (varía según instalaciones)

**Track 3: Gestión de Terceros**

- Inventario de proveedores con acceso a CHD o sistemas
- Evaluaciones de seguridad de proveedores (ISO 5.19-5.22 / PCI 12.8)
- Validación anual de cumplimiento PCI DSS de service providers (PCI 12.8.5)
- Cláusulas de seguridad en contratos (ISO 5.20)
- Responsabilidades definidas (shared responsibility matrix)
- **Controles satisfechos:** ISO 5.19-5.23 / PCI 12.8
- **Duración:** 3-4 meses inicial + ongoing
- **Costo:** $25,000 - $80,000

**Track 4: Continuidad y Respaldos**

- Análisis de Impacto de Negocio (BIA) (ISO requisito)
- Plan de Continuidad de Negocio (BCP) (ISO 5.29-5.30)
- Plan de Recuperación ante Desastres (DRP)
- Respaldos automatizados con cifrado (ISO 8.13 / PCI 12.3.1)
- Pruebas de restauración trimestrales
- Redundancia para sistemas críticos (ISO 8.14)
- **Controles satisfechos:** ISO 5.29-5.30, 8.13-8.14 / PCI elementos de 12.3
- **Duración:** 4-5 meses
- **Costo:** $60,000 - $200,000

**Track 5: Concientización y Capacitación**

- Programa de concientización anual para todo el personal (ISO 6.3 / PCI 12.6)
- Capacitación especializada por roles (ISO 6.3 / PCI 12.6.1)
- Simulacros de phishing trimestrales
- Capacitación en respuesta a incidentes
- Medición de efectividad (tests post-capacitación)
- **Controles satisfechos:** ISO 6.3 / PCI 12.6
- **Duración:** Ongoing, setup 1-2 meses

- **Costo:** $20,000 - $60,000 anual

**Entregables Fase 4:**

- Pipeline DevSecOps con SAST/DAST/SCA
- Controles físicos auditables
- Programa de terceros operacional
- BCP/DRP probados
- Programa de concientización maduro

**Recursos Fase 4:** 3-4 FTE (AppSec, continuidad, capacitación) **Costo Total Fase 4:** $215,000 - $710,000 **Tiempo:** 6-7 meses

**Fase 5: Auditoría, Certificación y Mejora Continua (Mes 25-30)**

**Objetivo:** Obtener certificaciones y establecer ciclo de mejora.

**Track 1: Pre-auditoría y Remediación**

- Auditoría interna completa ISO 27001 (ISO 9.2)
- Auto-evaluación PCI DSS (SAQ o preparación ROC)
- Identificación de gaps residuales
- Remediación urgente de no conformidades
- Simulacro de auditoría externa
- **Duración:** 2-3 meses
- **Costo:** $30,000 - $80,000 (auditoría interna + remediation)

**Track 2: Certificación ISO 27001**

- Selección de organismo certificador acreditado
- Auditoría Stage 1 (revisión documental)
- Remediación de hallazgos Stage 1
- Auditoría Stage 2 (implementación)
- Obtención de certificado
- **Duración:** 3-4 meses proceso
- **Costo:** $20,000 - $60,000

**Track 3: Validación PCI DSS**

- Completar cuestionario de auto-evaluación (SAQ) o

- Contratar QSA para Report on Compliance (ROC) si Nivel 1
- Escaneos ASV trimestrales (ongoing)
- Attestation of Compliance (AOC)
- Envío a marcas de pago (Visa, Mastercard, etc.)
- **Duración:** 2-3 meses
- **Costo:** $10,000 - $100,000 (según nivel)

**Track 4: Establecer Mejora Continua**

- Ciclo de revisión trimestral de métricas
- Revisión por la dirección semestral (ISO 9.3)
- Actualizaciones de evaluación de riesgos
- Programa de auditorías internas periódicas
- Seguimiento de KPIs de seguridad
- **Duración:** Ongoing
- **Costo:** $40,000 - $100,000 anual

**Entregables Fase 5:**

- Certificado ISO 27001:2022
- AOC (Attestation of Compliance) PCI DSS
- Dashboard de métricas de seguridad
- Plan de vigilancia y mejora continua

**Recursos Fase 5:** 2-3 FTE (compliance, auditoría) **Costo Total Fase 5:** $100,000 - $340,000 **Tiempo:** 6 meses

## Resumen Financiero de Implementación Integrada (30 meses)

**Inversión por Fase**

| Fase | Duración | Costos Directos | Recursos (FTE) | Total Estimado |
|---|---|---|---|---|
| 0 - Preparación | 2 meses | $20K - $50K | 0.5-1 | $20K - $50K |
| 1 - Fundamentos | 4 meses | $85K - $270K | 2-3 | $145K - $370K |
| 2 - Protección | 5 meses | $210K - $800K | 3-4 | $335K - $1,000K |
| 3 - Detección | 6 meses | $235K - $700K | 3-5 | $395K - $1,000K |
| 4 - Avanzados | 7 meses | $215K - $710K | 3-4 | $360K - $910K |
| 5 - Certificación | 6 meses | $100K - $340K | 2-3 | $175K - $440K |
| **TOTAL 30 meses** | - | **$865K - $2,870K** | - | **$1,430K - $3,770K** |

**Costos Recurrentes Anuales Post-Implementación**

| Categoría | Costo Anual |
|---|---|
| Personal (CISO, 3-4 analistas, compliance) | $310K - $650K |
| Licencias de herramientas (SIEM, EDR, etc.) | $80K - $200K |
| Auditorías (ISO vigilancia + PCI validación) | $25K - $135K |
| Pentests y escaneos ASV | $22K - $70K |
| Capacitación y concientización | $20K - $60K |
| Consultoría y soporte (10% bugs, mejoras) | $30K - $100K |
| **TOTAL ANUAL** | **$487K - $1,215K** |

**Comparación Integrada vs Separada (3 años)**

| Enfoque | Año 1 | Año 2 | Año 3 | Total 3 años |
|---|---|---|---|---|
| **Separado** | $800K | $650K | $650K | **$2,100K** |
| **Integrado** | $900K | $550K | $500K | **$1,950K** |
| **Ahorro** | -$100K | $100K | $150K | **$150K (7%)** |

*Nota: Año 1 integrado es más alto por inversión inicial concentrada, pero años subsecuentes son más eficientes.*

## Timeline Visual de Implementación

| Mes: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 |
|---|
| \|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\|--\| |
| Fase 0: Prep \|==\| |
| Fase 1: Fund \|========\| |
| Fase 2: Protec \|==========\| |
| Fase 3: Detect \|==========\| |
| Fase 4: Avanz \|==========\| |
| Fase 5: Audit \|==========\| |

Hitos Críticos:

▼ M2: Aprobación de presupuesto

▼ M6: CDE segmentado y operacional

▼ M11: MFA desplegado, cifrado CHD completo

▼ M17: SIEM operacional, primera pentest

▼ M24: DevSecOps pipeline completo

▼ M28: Pre-auditorías completadas

▼ M30: Certificaciones obtenidas

**Métricas de Éxito y KPIs**

**KPIs de Cumplimiento**

**ISO 27001:**

- % de controles aplicables implementados: Objetivo 100% a M24
- Hallazgos de auditoría interna: Reducción 30% interanual
- Tiempo medio de cierre de no conformidades: <30 días
- Participación en revisiones por dirección: 100% C-level

**PCI DSS:**

- Resultado escaneos ASV: 0 vulnerabilidades críticas/altas
- Resultado pentests: 0 hallazgos críticos sin remediar

- Tiempo de remediación vulnerabilidades críticas: <30 días (mandatorio)
- % de componentes CDE en alcance: Reducción continua (segmentación)

## KPIs Operacionales

**Detección y Respuesta:**

- Mean Time to Detect (MTTD): <4 horas para incidentes críticos
- Mean Time to Respond (MTTR): <24 horas para contención inicial
- Falsos positivos SIEM: <10% de alertas generadas
- Disponibilidad de sistemas críticos: >99.9%

**Gestión de Vulnerabilidades:**

- Tiempo medio de parche crítico: <15 días (objetivo más estricto que PCI)
- Cobertura de escaneos: 100% de activos en alcance
- Vulnerabilidades críticas/altas pendientes: <5 en cualquier momento

**Concientización:**

- % de empleados que completan capacitación anual: >95%
- Tasa de clics en simulacros de phishing: <10%
- Incidentes de seguridad por error humano: Reducción 40% en 2 años

**KPIs Financieros**

- Costo por activo protegido: Benchmark contra industria
- ROI de programa de seguridad: Medido por incidentes evitados
- Costo de cumplimiento como % de revenue: <1.5% para medianas empresas
- Reducción de primas de ciberseguro: Objetivo 15-25% con certificaciones

**Riesgos de la Implementación Integrada**

**Riesgos Técnicos**

**1. Complejidad de Segmentación de Red**

- **Probabilidad:** Alta
- **Impacto:** Crítico (retrasa PCI DSS)
- **Mitigación:**
    - Contratar arquitecto de red experimentado en PCI DSS
    - Realizar POC en ambiente de lab antes de producción
    - Documentación exhaustiva pre y post implementación
    - Buffer de 4-6 semanas en timeline

**2. Integración de SIEM**

- **Probabilidad:** Media
- **Impacto:** Alto (afecta detección y cumplimiento)
- **Mitigación:**
    - Seleccionar SIEM con conectores pre-construidos para sistemas clave
    - Fase piloto con sistemas críticos antes de full deployment
    - Contratar servicios profesionales del vendor
    - Considerar SOC as a Service durante maduración

**3. Resistencia de Aplicaciones Legacy a Controles**

- **Probabilidad:** Media-Alta
- **Impacto:** Alto (puede impedir certificación)
- **Mitigación:**
    - Inventario temprano de aplicaciones legacy
    - Controles compensatorios documentados
    - Roadmap de modernización o reemplazo
    - Aislamiento adicional de aplicaciones problemáticas

**Riesgos Organizacionales**

**1. Falta de Compromiso Ejecutivo Sostenido**

- **Probabilidad:** Media
- **Impacto:** Crítico (todo el programa)
- **Mitigación:**
    - Dashboard ejecutivo con métricas de negocio (no solo técnicas)
    - Revisiones trimestrales con C-level
    - Comunicación de quick wins y ROI temprano
    - Inclusión en balanced scorecard corporativo

**2. Rotación de Personal Clave**

- **Probabilidad:** Media
- **Impacto:** Alto (pérdida de conocimiento)
- **Mitigación:**

    - Documentación exhaustiva y accesible
    - Cross-training entre miembros del equipo
    - Retención mediante compensación competitiva y desarrollo profesional
    - Backup de consultores externos para roles críticos

**3. Fatiga de Compliance**

- **Probabilidad:** Alta (en fases 3-4)
- **Impacto:** Medio (ralentiza progreso)
- **Mitigación:**
    - Automatización máxima de tareas repetitivas
    - Celebración de hitos intermedios
    - Variedad en asignaciones del equipo
    - Comunicación clara de beneficios más allá de compliance

**Riesgos de Cronograma**

**1. Subestimación de Remediación**

- **Probabilidad:** Alta
- **Impacto:** Medio (retrasos)
- **Mitigación:**
    - Gap analysis conservador con buffers 20-30%
    - Revisiones bimensuales de timeline
    - Identificación temprana de blockers
    - Escalation path definido

**2. Dependencias de Terceros**

- **Probabilidad:** Media
- **Impacto:** Medio-Alto
- **Mitigación:**
    - Contratos con SLAs específicos y penalidades
    - Proveedores alternativos identificados
    - Evaluación de vendors antes de compromiso
    - Project manager dedicado a gestión de terceros

## Optimizaciones para Diferentes Tamaños de Organización

**Pequeñas Empresas (<100 empleados, <$10M revenue)**

**Ajustes de Alcance:**

- ISO 27001: Implementar solo controles de alta prioridad (40-50 controles)
- PCI DSS: Si nivel 3-4, enfocarse en SAQ y reducción agresiva de alcance

**Optimizaciones de Costos:**

- CISO as a Service (parte tiempo): $60K-$90K/año vs $150K+ tiempo completo
- SOC as a Service / MSSP: $2K-$5K/mes vs equipo interno
- Herramientas cloud/SaaS: Reducen CAPEX 60-80%
- Consultoría puntual vs recursos dedicados

**Timeline Extendido:**

- 36-42 meses para implementación completa (vs 30 meses)
- Foco en quick wins: MFA, antimalware, respaldos primeros 6 meses

**Presupuesto Estimado:**

- Inicial (Año 1): $150K - $350K
- Recurrente: $180K - $350K/año
- Total 3 años: $660K - $1,400K

**Medianas Empresas (100-1,000 empleados, $10M-$100M revenue)**

**Alcance Estándar:**

- ISO 27001: Implementación completa de 93 controles
- PCI DSS: Típicamente nivel 2-3, puede requerir QSA

**Equipo Recomendado:**

- CISO (1 FTE)
- Analistas de seguridad (2-3 FTE)
- Especialista compliance (0.5-1 FTE)
- Soporte de equipo IT existente

**Timeline Estándar:**

- 30-36 meses según modelo presentado

**Presupuesto Estimado:**

- Inicial (Año 1): $600K - $1,200K
- Recurrente: $450K - $900K/año
- Total 3 años: $1,500K - $3,000K

**Grandes Empresas (>1,000 empleados, >$100M revenue)**

**Alcance Extendido:**

- ISO 27001: Múltiples sitios, potencialmente múltiples certificados
- PCI DSS: Típicamente nivel 1, requiere QSA ROC

**Equipo Extendido:**

- CISO + equipo de 8-12 personas (SOC, AppSec, GRC, Arquitectura)
- Especialistas por dominio (cloud, OT, IoT según aplique)
- Equipos regionales si operaciones globales

**Complejidades Adicionales:**

- Múltiples CDE o ecosistemas de pago
- M&A: Integración de adquisiciones en SGSI
- Regulaciones adicionales (SOX, GDPR, sector-específicas)

**Presupuesto Estimado:**

- Inicial (Año 1): $1,500K - $3,500K
- Recurrente: $1,200K - $2,500K/año
- Total 3 años: $3,900K - $8,500K

**Lecciones Aprendidas de Implementaciones Reales**

**Factores de Éxito Consistentes**

1. **Patrocinio Ejecutivo Visible y Sostenido**
    - CEO/CFO comunican importancia en all-hands
    - Seguridad en agenda de board trimestralmente
    - Presupuesto protegido incluso en recortes
2. **Quick Wins Comunicados Ampliamente**
    - MFA desplegado en 2 meses → comunicar reducción de riesgo 70%
    - Segmentación completada → comunicar reducción de alcance PCI 40%
    - Crea momentum y justifica inversiones continuas

3. **Automatización Agresiva desde Inicio**
    - Infrastructure as Code para configuraciones
    - CI/CD con gates de seguridad automatizados
    - Orquestación de respuesta a incidentes (SOAR)
    - Libera recursos para tareas de mayor valor