EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Información del Documento

- **Organización:** Mi Empresa de Prueba
- **Fecha de Creación:** 15 de marzo de 2025
- **Versión:** 1.0

1. Introducción

Este documento presenta los resultados de la evaluación de riesgos de seguridad de la información para Mi Empresa de Prueba, identificando y analizando los riesgos que podrían afectar a los activos de información de la organización.

2. Metodología

La metodología utilizada para la evaluación de riesgos se basa en la norma ISO 27005 e incluye los siguientes pasos:

1. Identificación de activos de información
2. Identificación de amenazas y vulnerabilidades
3. Evaluación de probabilidad e impacto
4. Determinación del nivel de riesgo
5. Tratamiento de riesgos

3. Criterios de Evaluación

3.1 Niveles de Probabilidad

- **Alto (3):** Es probable que ocurra múltiples veces en un período de 12 meses
- **Medio (2):** Es probable que ocurra al menos una vez en un período de 12 meses
- **Bajo (1):** Es improbable que ocurra en un período de 12 meses

3.2 Niveles de Impacto

- **Alto (3):** Impacto significativo en la operación, finanzas o reputación
- **Medio (2):** Impacto moderado en la operación, finanzas o reputación
- **Bajo (1):** Impacto mínimo en la operación, finanzas o reputación

3.3 Matriz de Riesgo

- **Alto (7-9):** Requiere atención inmediata y controles robustos
- **Medio (4-6):** Requiere medidas de mitigación planificadas
- **Bajo (1-3):** Puede ser aceptable con monitoreo

4. Inventario de Activos de Información

Los siguientes activos de información han sido identificados:

- Base de datos de clientes
- Información de tarjetas de pago
- Sitio web
- Plataforma de procesamiento de pagos

- Catálogo de productos
- Análisis de mercado

5. Amenazas Identificadas

Las siguientes amenazas han sido identificadas:

- Violación de datos personales
- Fraude de tarjetas
- Ataques DDoS
- Inyección SQL
- Suplantación de identidad (phishing)

6. Vulnerabilidades Identificadas

Las siguientes vulnerabilidades han sido identificadas:

- Cifrado insuficiente
- Validación de entrada inadecuada
- Capacidad limitada de infraestructura
- Controles de acceso inadecuados
- Falta de parches de seguridad

7. Controles Existentes

Los siguientes controles ya están implementados:

- Cifrado de datos sensibles
- Firewall de aplicaciones web
- Capacidad de escalado en la nube
- Auditorías de seguridad periódicas
- Cumplimiento PCI-DSS

8. Análisis de Riesgos

R01	Base de datos de	Violación de datos	Cifrado insuficiente	Alto	Alto	Alto
R03	Sitio web de pago	Ataques	Capacidad inadecuada	Medio	Medio	Medio
R05	Catálogo de pagos	SQL	Suplantación de identidad (phishing)	Controles inadecuados	Alto	Medio	Alto

9. Plan de Tratamiento de Riesgos

Riesgos de Nivel

	Alto (Prioridad Inmediata)

Riesgo R01: Base de datos de clientes - Violación de datos personales

- **Opción de tratamiento:** Mitigar
- **Controles recomendados:** Implementar controles técnicos adecuados, Establec
- **Responsable:** y procedimientos, Realizar revisiones periódicas [A definir]
- **Fecha límite:** [A definir]

Riesgo R05: Catálogo de productos - Suplantación de identidad (phishing)

- **Opción de tratamiento:** Mitigar
- **Controles recomendados:** Implementar filtrado de correo avanzado, Realizar fo
- **Responsable:** concienciación en seguridad, Implementar autenticación multifactor [A definir]
- **Fecha límite:** [A definir]

Riesgos de Nivel Medio (Planificación a Corto Plazo)

Riesgo R02: Información de tarjetas de pago - Fraude de tarjetas

- **Opción de tratamiento:** Mitigar
- **Controles recomendados:** Implementar controles técnicos adecuados, Establec
- **Responsable:** y procedimientos, Realizar revisiones periódicas [A definir]
- **Fecha límite:** [A definir]

Riesgo R03: Sitio web - Ataques DDoS

- **Opción de tratamiento:** Mitigar
- **Controles recomendados:** Implementar controles técnicos adecuados, Establec
- **Responsable:** y procedimientos, Realizar revisiones periódicas [A definir]
- **Fecha límite:** [A definir]

Riesgo R04: Plataforma de procesamiento de pagos - Inyección SQL

- **Opción de tratamiento:** Mitigar
- **Controles recomendados:** Implementar controles técnicos adecuados, Establec
- **Responsable:** y procedimientos, Realizar revisiones periódicas [A definir]
- **Fecha límite:** [A definir]

10. Conclusiones y Recomendaciones

Basado en la evaluación de riesgos realizada, se recomienda:

1. Priorizar la implementación de controles para los riesgos de nivel alto
2. Establecer un cronograma para la implementación de controles para riesgos de nivel medio
3. Monitorear los riesgos de nivel bajo
4. Revisar y actualizar esta evaluación de riesgos al menos una vez al año
5. Capacitar al personal en concienciación de seguridad

11. Aprobación

Aprobado por:
Nombre:
Cargo:
Fecha:
Firma: