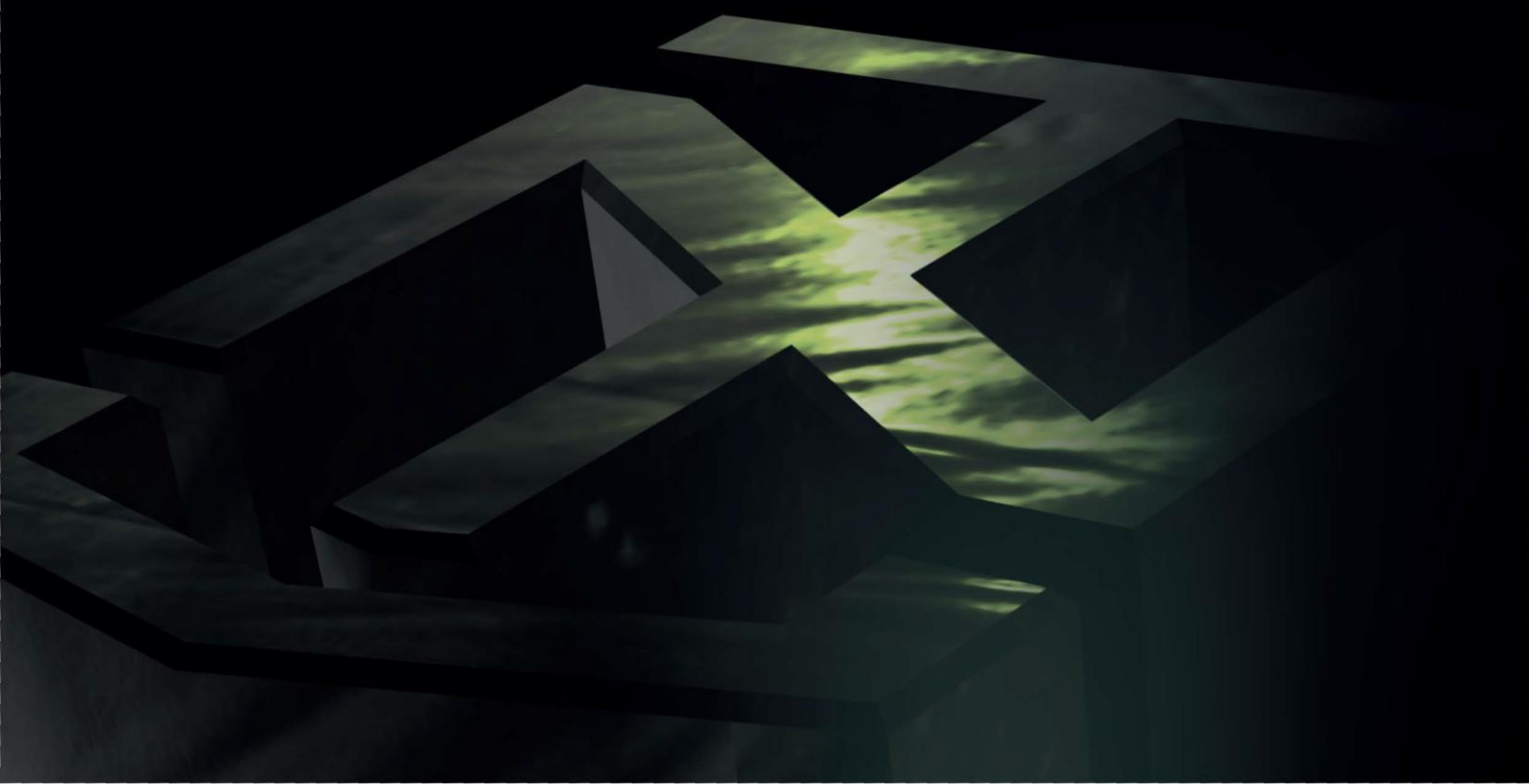
TUTOR NEGOTIA®

Investment Risk Management



**Modelo de Programa de Resiliencia Operativa en Ciberseguridad**
**Elaborado por: Tutor Negotia Fecha: 05 de febrero de 2026 Versión: 1.0 Confidencialidad:**

**Tabla de Contenidos**



## Introducción

(Nombre de empresa), como empresa dedicada a [insertar breve descripción de la empresa, ej.: servicios de telecomunicaciones y entretenimiento vía satélite], enfrenta un panorama de amenazas cibernéticas en constante evolución. La resiliencia operativa en ciberseguridad se define como la capacidad de la organización para anticipar, resistir, recuperarse y adaptarse a interrupciones causadas por incidentes cibernéticos, minimizando el impacto en las operaciones, la reputación y los stakeholders.

Este programa, elaborado por Tutor Negotia, establece un enfoque integral y proactivo para fortalecer la postura de seguridad cibernética de {nombre de la empesa] Se basa en mejores prácticas internacionales, adaptadas al contexto operativo de la empresa, con énfasis en la continuidad del negocio y la protección de datos sensibles.

## Objetivos del Programa

- Anticipar amenazas: Identificar y mitigar riesgos cibernéticos antes de que se materialicen.
- Resistir incidentes: Implementar controles robustos para limitar el impacto de ataques.
- Recuperarse rápidamente: Asegurar la restauración de operaciones en el menor tiempo posible.
- Adaptarse y mejorar: Fomentar una cultura de aprendizaje continuo para evolucionar frente a nuevas amenazas.
- Cumplir normativas: Alinear con regulaciones locales (ej.: Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México) e internacionales (ej.: GDPR, NIST).

## Alcance y Aplicabilidad

Este programa aplica a todas las operaciones de [empresa], incluyendo:

- Sistemas de TI y OT (tecnología operativa).
- Datos de clientes, empleados y proveedores.
- Infraestructura en la nube, on-premise y remota.
- Todas las ubicaciones, con enfoque en Hermosillo, Sonora, MX como sede principal.

Exclusiones: Actividades no relacionadas con ciberseguridad, como operaciones financieras puras (aunque se integran en riesgos cibernéticos).

## Marco Normativo y Referencias

- Normas internacionales: NIST Cybersecurity Framework (CSF), ISO 27001, COBIT.
- Regulaciones locales:.
- Mejores prácticas: CIS Controls, MITRE ATT&CK Framework.

## Componentes del Programa

**Gobierno y Liderazgo**
Establecer un Comité de Ciberseguridad liderado por el CISO (Chief Information Security Officer), con representación de todas las áreas. Responsabilidades:

- Definir políticas de seguridad.
- Aprobar presupuestos anuales.
- Realizar revisiones trimestrales.

**Evaluación de Riesgos**

- Realizar análisis de riesgos anuales utilizando metodologías como OCTAVE o FAIR.
- Identificar activos críticos (ej.: servidores de transmisión satelital).
- Evaluar vulnerabilidades mediante escaneos regulares (mensuales).

**Controles de Seguridad**
Implementar capas de defensa:

- Acceso: Autenticación multifactor (MFA), principio de menor privilegio.
- Protección de datos: Encriptación AES-256 para datos en reposo y tránsito.
- Red: Firewalls de próxima generación (NGFW), segmentación de red.
- Endpoint: Antivirus con IA, EDR (Endpoint Detection and Response).

**Detección y Respuesta a Incidentes**

- Establecer un SOC (Security Operations Center) 24/7.
- Desarrollar un Plan de Respuesta a Incidentes (IR Plan) con escenarios como ransomware o DDoS.
- Integrar herramientas como SIEM (Security Information and Event Management) para alertas en tiempo real.

**Recuperación y Continuidad**

- Crear planes de continuidad de negocio (BCP) y recuperación de desastres (DRP).
- Realizar backups diarios con estrategia 3-2-1 (3 copias, 2 medios, 1 offsite).
- Pruebas de recuperación semestrales.

**Capacitación y Concientización**

- Programa anual de entrenamiento para todos los empleados, incluyendo simulacros de phishing.
- Cursos especializados para equipos de TI.
- Campañas mensuales de awareness vía email y talleres.

**Monitoreo y Mejora Continua**

- Métricas clave: Tiempo medio de detección (MTTD), tiempo medio de respuesta (MTTR).
- Auditorías internas anuales y externas bianuales.
- Actualización del programa basada en lecciones aprendidas de incidentes.

**Responsabilidades**

| Rol | Responsabilidades Principales |
|---|---|
| **CISO** | Liderazgo general, reporte al CEO. |
| **Equipo de TI** | Implementación técnica de controles. |
| **Recursos Humanos** | Capacitación y cumplimiento ético. |
| **Empleados** | Reportar incidentes sospechosos. |
| **Auditores Externos** | Validación independiente. |

**Recursos Requeridos**

Presupuesto: Estimado en $500,000 USD anuales (ejemplo) (herramientas, entrenamiento, consultorías).
Personal: 5 especialistas en ciberseguridad adicionales.
Herramientas: Licencias para SIEM, EDR, y plataformas de capacitación (ej.: KnowBe4).

**Cronograma de Implementación**

| Fase | Actividades | Plazo |
|---|---|---|
| **Fase 1: Planificación** | Evaluación inicial de riesgos, aprobación de políticas. | Meses 1-3 |
| **Fase 2: Implementación** | Despliegue de controles y entrenamiento. | Meses 4-6 |
| **Fase 3: Pruebas** | Simulacros y auditorías. | Meses 7-9 |
| **Fase 4: Monitoreo** | Operaciones continuas y revisiones. | Mes 10 en adelante |

**Anexos**

- Anexo A: Plantilla de Política de Seguridad Cibernética.
- Anexo B: Matriz de Riesgos Ejemplo.
- Anexo C: Glosario de Términos (ej.: MFA, SIEM).

Este programa se revisará anualmente o tras incidentes mayores. Para consultas, contactar a Tutor Negotia a contacto@tutornegotia.com].

**Fin del Documento**