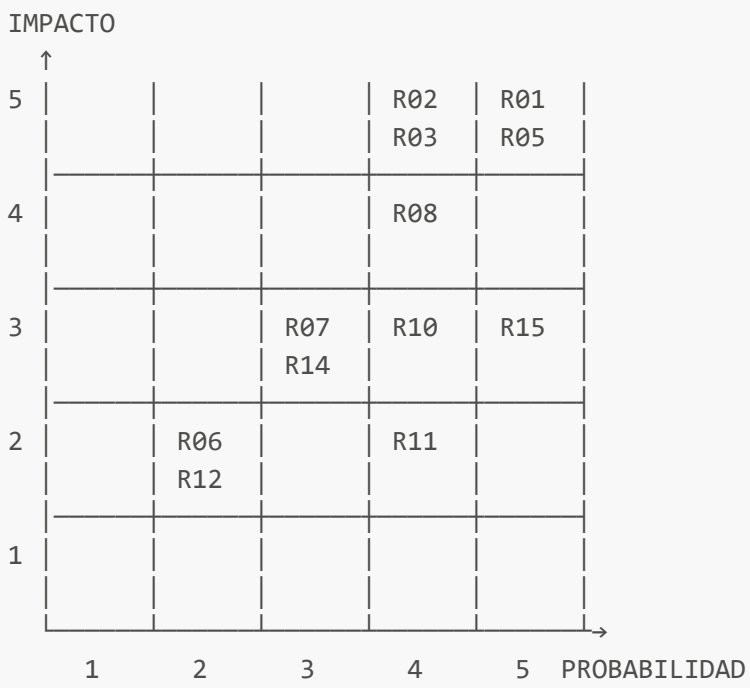
📊 MATRIZ DE RIESGOS DETALLADA - SISTEMA TESCHI

🎯 MAPA DE CALOR DE RIESGOS



CÓDIGO DE COLORES:
🔴 Rojo (20-25): Riesgo CRÍTICO
🟠 Naranja (15-19): Riesgo ALTO
🟡 Amarillo (10-14): Riesgo MEDIO
🟢 Verde (5-9): Riesgo BAJO
⚪ Blanco (1-4): Riesgo MUY BAJO

📋 TABLA COMPLETA DE RIESGOS

ID	Riesgo	Prob.	Imp.	Total	Nivel	Categoría	Prioridad
R01	Pérdida de datos BD	2	5	**10**	🟡	Datos	P2
R02	Pérdida de archivos	3	5	**15**	🟠	Almacenamiento	**P1**
R03	Acceso no autorizado	3	5	**15**	🟠	Seguridad	**P1**
R04	Virus/Malware	2	4	**8**	🟢	Seguridad	P3
R05	Falla del servidor	3	5	**15**	🟠	Disponibilidad	**P1**
R06	Expiración de token	4	2	**8**	🟢	Usabilidad	P3
R07	Pérdida conectividad	3	3	**9**	🟢	Red	P3

ID	Riesgo	Prob.	Imp.	Total	Nivel	Categoría	Prioridad
R08	Error validación docs	3	3	**9**	🟠	Proceso	P3
R09	Incumplimiento LGPD	2	5	**10**	🟡	Legal	P2
R10	Falta documentación	4	3	**12**	🟡	Mantenimiento	P2
R11	Incompatibilidad navegador	2	2	**4**	🟢	Compatibilidad	P4
R12	Error de usuario	4	2	**8**	🟠	Usabilidad	P3
R13	Rendimiento lento	3	2	**6**	🟠	Rendimiento	P3
R14	Falta capacitación	3	3	**9**	🟠	RRHH	P3
R15	Dependencia desarrollador	3	4	**12**	🟡	Recursos	P2

🟠 ANÁLISIS POR CATEGORÍA

1. SEGURIDAD (4 riesgos)

```
Categoría más crítica: 2 riesgos altos

R03 🟡 Acceso no autorizado        [P×I: 3×5 = 15]
R04 🟠 Virus/Malware               [P×I: 2×4 = 8]

Total exposición: 23 puntos
```

Recomendaciones:

- 🔧 Implementar 2FA inmediatamente
- 🔧 Integrar ClamAV para antivirus real
- 🔧 Auditoría de seguridad externa
- 🔧 Penetration testing

---

2. DATOS Y ALMACENAMIENTO (2 riesgos)

```
Incluye el riesgo más alto del sistema

R01 🟡 Pérdida de datos BD         [P×I: 2×5 = 10]
R02 🟠 Pérdida de archivos         [P×I: 3×5 = 15] ⚠

Total exposición: 25 puntos
```

Recomendaciones:

- 🔧 **URGENTE:** Sistema de backup automático

- 🔧 Migrar archivos a cloud storage
- 🔧 Replicación de base de datos
- 🔧 Snapshots diarios

---

3. DISPONIBILIDAD Y RENDIMIENTO (2 riesgos)

```
Crítico durante período de reinscripción

R05 🟠 Falla del servidor          [P×I: 3×5 = 15] ⚠
R13 🟠 Rendimiento lento           [P×I: 3×2 = 6]

Total exposición: 21 puntos
```

Recomendaciones:

- 🔧 Servidor de respaldo (hot standby)
- 🔧 Pruebas de carga
- 🔧 Monitoreo 24/7
- 🔧 Plan de contingencia

---

4. LEGAL Y CUMPLIMIENTO (1 riesgo)

```
Alto impacto potencial

R09 🟠 Incumplimiento LGPD         [P×I: 2×5 = 10]

Total exposición: 10 puntos
```

Recomendaciones:

- 🔧 Aviso de privacidad
- 🔧 Consentimiento de estudiantes
- 🔧 Implementar derechos ARCO
- 🔧 Consultoría legal

---

5. USABILIDAD Y PROCESO (3 riesgos)

```
Riesgos menores pero frecuentes

R06 🟠 Expiración token            [P×I: 4×2 = 8]
R08 🟠 Error validación            [P×I: 3×3 = 9]
R12 🟠 Error de usuario            [P×I: 4×2 = 8]

Total exposición: 25 puntos
```

Recomendaciones:

- 🔧 Mejorar UX con más validaciones
- 🔧 Confirmaciones en acciones críticas
- 🔧 Tutorial interactivo

📅 CRONOGRAMA DE MITIGACIÓN (6 MESES)

MES 1 - ENERO 2025: Seguridad de Datos

```
☑ Backups
  □ Configurar pg_dump diario
  □ Configurar backup de uploads/
  □ Probar restauración

☑ Monitoreo
  □ Implementar logging de accesos
  □ Configurar alertas básicas
```

MES 2 - FEBRERO 2025: Seguridad de Acceso

```
☑ Autenticación
  □ Implementar 2FA para admins
  □ Política de contraseñas estricta

☑ Auditoría
  □ Análisis de vulnerabilidades
  □ Actualizar dependencias
```

MES 3 - MARZO 2025: Disponibilidad

```
☑ Infraestructura
  □ Configurar servidor de respaldo
  □ Implementar load balancer

☑ Testing
  □ Pruebas de carga (500 usuarios)
  □ Plan de contingencia documentado
```

MES 4 - ABRIL 2025: Cumplimiento Legal

```
☑ LGPD
   □ Aviso de privacidad publicado
   □ Consentimientos implementados
   □ Derechos ARCO habilitados

☑ Documentación
   □ Políticas de privacidad
   □ Términos y condiciones
```

MES 5 - MAYO 2025: Mejora Continua

```
☑ Malware Protection
   □ ClamAV instalado y configurado
   □ Actualización automática de firmas

☑ Performance
   □ Implementar Redis para caché
   □ Optimizar queries lentas
```

MES 6 - JUNIO 2025: Capacitación y Consolidación

```
☑ Equipo
   □ Manual de usuario completo
   □ Capacitación a administradores
   □ Videos tutoriales

☑ Revisión
   □ Revisión trimestral de riesgos
   □ Actualizar matriz de riesgos
```

🎓 RIESGOS ESPECÍFICOS DEL TESCHI

R16 - Período de Reinscripción Masivo

Atributo	Valor
Probabilidad	5 - Muy Alta
Impacto	4 - Alto
Riesgo	**20 - 🟤 CRÍTICO**

Descripción: Durante el período de reinscripción (típicamente 2-3 semanas), todos los estudiantes del TESCHI suben documentos simultáneamente.

Estimaciones:

- Estudiantes TESCHI: ~2,000-3,000
- Documentos por estudiante: 3
- Total documentos: 6,000-9,000
- Período: 2-3 semanas
- Pico estimado: 200-300 usuarios simultáneos

Mitigaciones:

- 🔧 **CRÍTICO:** Pruebas de carga con 500 usuarios
- 🔧 Escalamiento horizontal durante período crítico
- 🔧 CDN para archivos estáticos
- 🔧 Caché agresivo
- 🔧 Horarios escalonados por carrera

R17 - Conexión a Internet del TESCHI

Atributo	Valor
Probabilidad	3 - Media
Impacto	4 - Alto
Riesgo	**12 - 🟠 MEDIO**

Descripción: Falla en el enlace de internet del TESCHI impide acceso al sistema.

Mitigaciones:

- 🔧 Enlace de internet redundante (ISP backup)
- 🔧 Servidor dentro del campus para acceso local
- 🔧 Modo offline parcial
- 🔧 Coordinación con proveedor de internet

💼 MATRIZ DE RESPONSABILIDADES

Riesgo	Responsable	Apoyo	Revisión
R01-R02	Admin. Sistemas	Desarrollador	Mensual
R03-R04	Seguridad TI	Admin. Sistemas	Mensual
R05	Infraestructura	Hosting Provider	Semanal
R06-R08	Desarrollador	UX Designer	Bimestral
R09	DPO / Jurídico	Dirección	Trimestral
R10	Desarrollador	Documentador	Mensual
R11-R13	Desarrollador	QA Tester	Trimestral
R14-R15	RRHH / TI	Capacitación	Semestral

Riesgo	Responsable	Apoyo	Revisión
R16-R17	Coord. TI	Dirección	Continuo

📈 INDICADORES DE RIESGO (KRIs)

Indicadores de Seguridad

```
□ Intentos de login fallidos / día        (Meta: < 50)
□ Archivos con virus detectados / mes     (Meta: 0)
□ Accesos no autorizados bloqueados / mes (Meta: 0)
□ Vulnerabilidades críticas abiertas      (Meta: 0)
```

Indicadores de Disponibilidad

```
□ Uptime del sistema                      (Meta: > 99.5%)
□ Tiempo de respuesta promedio            (Meta: < 2 seg)
□ Incidentes de caída / mes               (Meta: 0)
□ Tiempo de recuperación ante falla       (Meta: < 1 hora)
```

Indicadores de Datos

```
□ Backups exitosos / semana               (Meta: 7/7)
□ Tiempo de restauración de backup        (Meta: < 30 min)
□ Espacio en disco disponible             (Meta: > 30%)
□ Integridad de archivos (hash check)     (Meta: 100%)
```

Indicadores de Proceso

```
□ Documentos revisados en < 48h           (Meta: > 90%)
□ Errores de usuario reportados / mes     (Meta: < 10)
□ Tiempo promedio de reinscripción        (Meta: < 10 min)
□ Satisfacción de usuarios                (Meta: > 4/5)
```

🔍 ANÁLISIS DE ESCENARIOS

ESCENARIO 1: Falla Total del Servidor Durante Reinscripción

Probabilidad: Media (3) **Impacto:** Crítico (5) **Riesgo:** 15 - 🟠 ALTO

Secuencia de Eventos:

```
Día 1, 10:00 AM - Inicio de reinscripciones
                  500 estudiantes acceden simultáneamente
                  ↓
Día 1, 10:30 AM - Servidor se sobrecarga
                  Timeouts y errores 500
                  ↓
Día 1, 11:00 AM - Servidor se cae completamente
                  Sistema inaccesible
                  ↓
IMPACTO:
- 500 estudiantes afectados
- Proceso de reinscripción detenido
- Pánico y quejas masivas
- Reputación dañada
```

Plan de Respuesta:

```
INMEDIATO (0-15 min):
1. Detectar falla (monitoreo automático)
2. Notificar a equipo técnico
3. Comunicar a estudiantes vía redes sociales

CORTO PLAZO (15-60 min):
4. Reiniciar servidor
5. Verificar logs para identificar causa
6. Activar servidor de respaldo si es necesario
7. Restaurar servicio

MEDIANO PLAZO (1-24 horas):
8. Analizar causa raíz
9. Implementar corrección permanente
10. Extender fecha límite de reinscripción

LARGO PLAZO (1-7 días):
11. Documentar incidente
12. Actualizar matriz de riesgos
13. Implementar mejoras preventivas
```

ESCENARIO 2: Brecha de Seguridad - Acceso a Documentos

Probabilidad: Media (3) **Impacto:** Crítico (5) **Riesgo:** 15 - 🟠 ALTO

Secuencia de Eventos:

```
Un atacante encuentra vulnerabilidad XSS
                  ↓
Obtiene token JWT de un administrador
                  ↓
```

```
Descarga documentos de todos los estudiantes
                  ↓
IMPACTO:
- Violación de privacidad de 2,000+ estudiantes
- Datos personales expuestos
- Denuncia ante INAI
- Multas económicas
- Daño reputacional severo
```

Plan de Respuesta:

```
INMEDIATO (0-2 horas):
1. Detectar el ataque (revisar logs)
2. Bloquear IP del atacante
3. Invalidar todos los tokens JWT
4. Cambiar secretos de JWT
5. Forzar re-login de todos los usuarios

CORTO PLAZO (2-24 horas):
6. Análisis forense completo
7. Identificar vulnerabilidad explotada
8. Aplicar parche de seguridad
9. Notificar a autoridades (INAI)
10. Preparar comunicado oficial

MEDIANO PLAZO (1-7 días):
11. Notificar a estudiantes afectados
12. Ofrecer medidas compensatorias
13. Auditoría de seguridad completa
14. Implementar mejoras de seguridad

LARGO PLAZO (1-3 meses):
15. Denuncia penal si aplica
16. Revisión de políticas de seguridad
17. Capacitación en seguridad a equipo
18. Certificación de seguridad (ISO 27001)
```

ESCENARIO 3: Pérdida Total de Backups

Probabilidad: Baja (2) **Impacto:** Crítico (5) **Riesgo:** 10 - 🟡 MEDIO

Secuencia de Eventos:

```
Falla del disco donde están los backups
                  ↓
Al mismo tiempo, falla el servidor principal
                  ↓
No hay backup disponible para restaurar
```

```
                    ↓
IMPACTO:
- Pérdida permanente de datos
- Sistema debe reconstruirse desde cero
- Estudiantes deben reinscribirse manualmente
- Caos administrativo completo
```

Plan de Prevención:

```
ESTRATEGIA 3-2-1:
- 3 copias de los datos (original + 2 backups)
- 2 medios diferentes (disco local + nube)
- 1 copia offsite (ubicación remota)

IMPLEMENTACIÓN:
1. Backup local diario (servidor)
2. Backup en nube diario (AWS S3 / Azure)
3. Backup semanal a disco externo (guardado offsite)
```

🎯 PLAN DE MITIGACIÓN PRIORIZADO

PRIORIDAD 1 - INMEDIATO (1-2 semanas)

Acción	Mitiga Riesgo	Esfuerzo	Impacto
Backup automático de BD	R01	Bajo	Alto
Backup automático de uploads/	R02	Bajo	Alto
Prueba de restauración	R01, R02	Bajo	Alto
Documentar procedimientos críticos	R10, R15	Medio	Alto

PRIORIDAD 2 - CORTO PLAZO (1 mes)

Acción	Mitiga Riesgo	Esfuerzo	Impacto
Implementar 2FA	R03	Medio	Alto
Integrar ClamAV	R04	Medio	Medio
Pruebas de carga	R05	Medio	Alto
Aviso de privacidad	R09	Bajo	Alto

PRIORIDAD 3 - MEDIANO PLAZO (3 meses)

Acción	Mitiga Riesgo	Esfuerzo	Impacto
Servidor de respaldo	R05	Alto	Alto

Acción	Mitiga Riesgo	Esfuerzo	Impacto
Migrar a cloud storage	R02	Alto	Alto
Auditoría de seguridad	R03	Alto	Medio
Capacitación personal	R14	Medio	Medio

PRIORIDAD 4 - LARGO PLAZO (6 meses)

Acción	Mitiga Riesgo	Esfuerzo	Impacto
Certificación ISO 27001	R03, R09	Muy Alto	Alto
Redundancia de ISP	R17	Alto	Medio
Sistema de caché (Redis)	R13	Medio	Medio

💰 ESTIMACIÓN DE COSTOS

Inversión en Mitigación (Primer Año)

Concepto	Costo Estimado (MXN)	Prioridad
Servidor de respaldo	$20,000 - $40,000	P3
Almacenamiento en nube (AWS S3)	$500 - $2,000/mes	P2
Software antivirus (ClamAV)	Gratis (open source)	P2
Auditoría de seguridad	$30,000 - $50,000	P2
Capacitación personal	$10,000 - $20,000	P3
Monitoreo (Datadog/New Relic)	$1,000 - $3,000/mes	P2
Disco de backup externo	$3,000 - $5,000	P1
Consultoría legal (LGPD)	$15,000 - $30,000	P2
Certificación ISO 27001	$80,000 - $150,000	P4
———	———	———
TOTAL PRIMER AÑO	**~$200,000 - $400,000 MXN**	

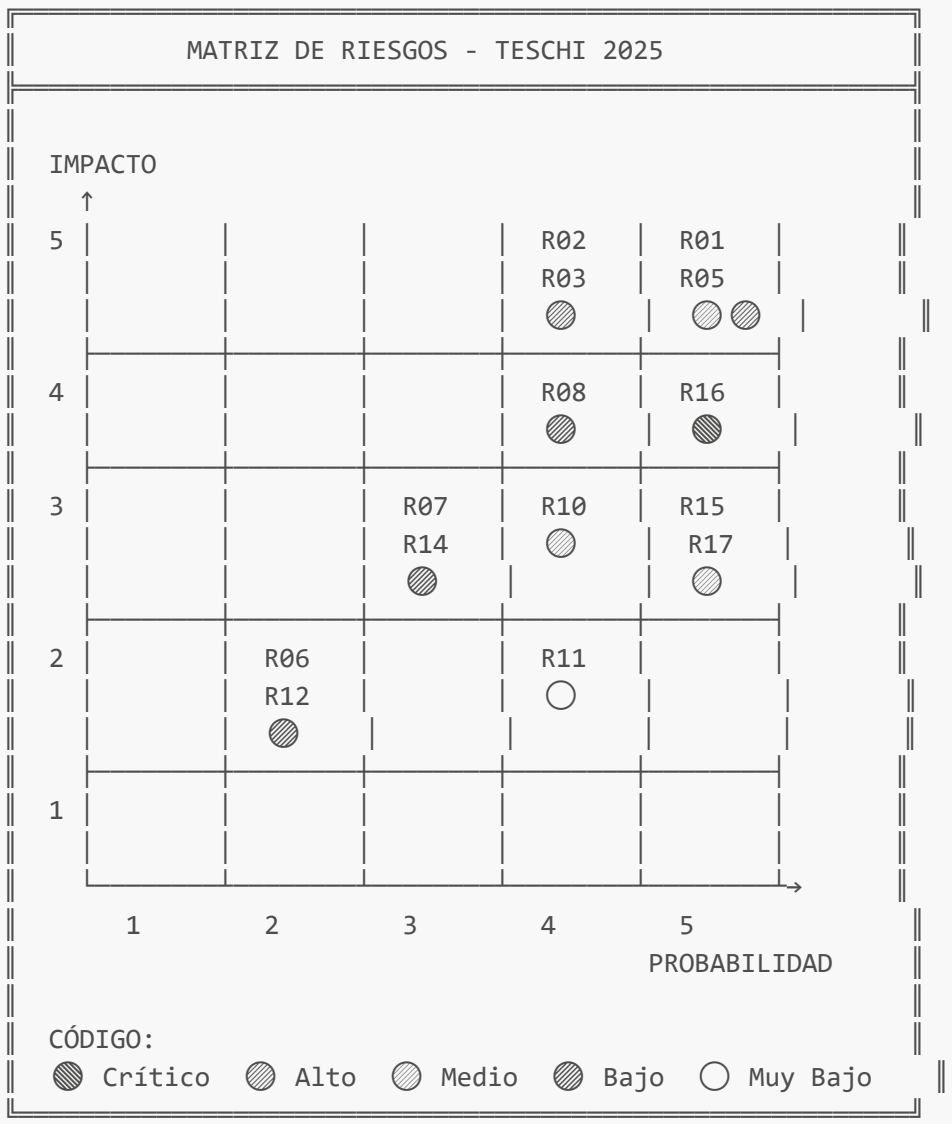
Retorno de Inversión (ROI)

Costos evitados al mitigar riesgos:

- Multa por violación de datos: $500,000 - $2,000,000 MXN
- Pérdida de datos sin backup: Incalculable
- Demandas legales: $100,000 - $500,000 MXN
- Daño reputacional: $200,000 - $1,000,000 MXN

ROI estimado: 300-500% en primer año

MATRIZ DE RIESGOS VISUAL



REGISTRO DE INCIDENTES

Fecha	Riesgo Materializado	Severidad	Tiempo Resolución	Lecciones Aprendidas
-	-	-	-	Sin incidentes registrados

CHECKLIST DE SEGURIDAD MENSUAL

```
MES: _____    RESPONSABLE: _____

□ Backups funcionando correctamente
□ Restauración probada exitosamente
```

```
□ Logs revisados sin anomalías
□ Actualizaciones de seguridad aplicadas
□ Espacio en disco suficiente (>30%)
□ Tiempos de respuesta aceptables (<2 seg)
□ Sin intentos de acceso sospechosos
□ Antivirus actualizado
□ Certificados SSL vigentes
□ Contraseñas de admin rotadas
□ Usuarios inactivos deshabilitados
□ Matriz de riesgos revisada

FIRMA: _____  FECHA: _____
```

📞 PLAN DE COMUNICACIÓN DE CRISIS

NIVEL 1 - Incidente Menor 🟢

```
Afectación: < 10 usuarios
Duración: < 1 hora

COMUNICACIÓN:
- Email a usuarios afectados
- Post-mortem interno
```

NIVEL 2 - Incidente Moderado 🟡

```
Afectación: 10-100 usuarios
Duración: 1-4 horas

COMUNICACIÓN:
- Aviso en sistema
- Email masivo
- Post en redes sociales
- Reporte a dirección
```

NIVEL 3 - Incidente Mayor 🔴

```
Afectación: > 100 usuarios
Duración: > 4 horas

COMUNICACIÓN:
- Comunicado oficial
- Conferencia de prensa (si aplica)
- Reporte a autoridades educativas
- Plan de contingencia activado
```

NIVEL 4 - Crisis 🟤

```
Afectación: Todo el sistema
Duración: > 24 horas

COMUNICACIÓN:
- Comunicado oficial TESCHI
- Notificación a SEP
- Notificación a INAI (si hay brecha de datos)
- Medios de comunicación
- Plan de compensación a estudiantes
```

🎓 RIESGOS ESPECÍFICOS POR MÓDULO

MÓDULO: Autenticación

```
R03 🟠 Acceso no autorizado        [15]
R06 🟠 Expiración de token         [8]

PRIORIDAD: Alta
ESTADO: Requiere 2FA
```

MÓDULO: Subida de Documentos

```
R02 🟠 Pérdida de archivos         [15]
R04 🟠 Virus/Malware               [8]
R07 🟠 Pérdida de conectividad     [9]

PRIORIDAD: Alta
ESTADO: Requiere mejor antivirus y backups
```

MÓDULO: Revisión de Documentos

```
R08 🟠 Error en validación         [9]

PRIORIDAD: Baja
ESTADO: Aceptable con mejoras UX
```

MÓDULO: Base de Datos

```
R01 🟢 Pérdida de datos            [10]

PRIORIDAD: Media
ESTADO: Requiere backups automáticos
```

🛡️ CONTROLES DE SEGURIDAD IMPLEMENTADOS

Controles Preventivos

```
☑ Autenticación JWT
☑ Autorización por roles
☑ Validación de entrada (Joi)
☑ Rate limiting
☑ Helmet.js (security headers)
☑ CORS configurado
☑ Prisma ORM (previene SQL injection)
☑ Validación de tipos de archivo
☑ Límite de tamaño de archivo
☑ Escaneo básico de virus
```

Controles Detectivos

```
☑ Logs de aplicación (Winston)
⚠ Logs de acceso (parcial)
❌ Monitoreo en tiempo real (NO implementado)
❌ Alertas automáticas (NO implementado)
❌ IDS/IPS (NO implementado)
```

Controles Correctivos

```
⚠ Backups (NO automatizados)
❌ Plan de recuperación ante desastres (NO documentado)
❌ Procedimientos de respuesta a incidentes (NO definidos)
```

📈 EVOLUCIÓN ESPERADA DE RIESGOS

Después de Implementar Mitigaciones (6 meses)

Riesgo	Nivel Actual	Nivel Esperado	Reducción
R02	🟢 15	🟢 6	↓ 60%

Riesgo	Nivel Actual	Nivel Esperado	Reducción
R03	🟠 15	🟡 9	↓ 40%
R05	🟠 15	🟡 9	↓ 40%
R09	🟠 10	🟡 5	↓ 50%
R10	🟠 12	🟡 4	↓ 67%
R15	🟠 12	🟡 6	↓ 50%
R16	🔴 20	🟠 10	↓ 50%

Reducción promedio de riesgo: 51%

📝 CONCLUSIONES Y RECOMENDACIONES

Estado Actual del Sistema

```
🟠 FORTALEZAS:
- Arquitectura sólida (React + Node.js + PostgreSQL)
- Autenticación robusta (JWT)
- Validaciones implementadas
- Código limpio y mantenible

🟠 DEBILIDADES:
- Sin backups automatizados (CRÍTICO)
- Sin servidor de respaldo
- Antivirus básico
- Falta de monitoreo 24/7
- Sin cumplimiento completo de LGPD
```

Recomendaciones Principales

CRÍTICAS (Implementar en 30 días)

1. ☑ Sistema de backup automático (BD + archivos)
2. ☑ Probar restauración de backups
3. ☑ Implementar 2FA para administradores
4. ☑ Documentar procedimientos de emergencia

IMPORTANTES (Implementar en 90 días)

5. ☑ Integrar ClamAV para antivirus real
6. ☑ Configurar servidor de respaldo
7. ☑ Pruebas de carga antes de reinscripción
8. ☑ Aviso de privacidad y ARCO

DESEABLES (Implementar en 180 días)

9. ☑ Migrar archivos a AWS S3 o Azure
10. ☑ Auditoría de seguridad externa
11. ☑ Monitoreo 24/7 con alertas
12. ☑ Capacitación completa del equipo

ANEXOS

ANEXO A: Glosario de Términos

- **JWT:** JSON Web Token
- **2FA:** Two-Factor Authentication
- **LGPD:** Ley General de Protección de Datos Personales
- **INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- **ARCO:** Acceso, Rectificación, Cancelación y Oposición (derechos)
- **DPO:** Data Protection Officer
- **RAID:** Redundant Array of Independent Disks

ANEXO B: Normatividad Aplicable

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Lineamientos del INAI
- NOM-151-SCFI-2016 (Comercio electrónico)
- OWASP Top 10
- ISO 27001:2013

Documento Controlado

Versión	Fecha	Autor	Cambios
1.0	Enero 2025	Sistema TESCHI	Versión inicial

Aprobación Requerida:

- ☐ Coordinador de TI
- ☐ Dirección General
- ☐ Responsable de Protección de Datos

Tecnológico de Estudios Superiores de Chimalhuacán Documento Confidencial - Uso Interno