# Una Guía para Desarrollar su Programa Principal de Gestión de Riesgos de Terceros

## Diligencia Básica y la Transición al TPRM Periódico

## Del Caos al Control

Este manual es su guía definitiva para lanzar y evolucionar un programa estructurado de Gestión de Riesgos de Terceros (TPRM). Está diseñado para organizaciones que operan en la etapa de Diligencia Básica, que es un punto de partida común y práctico donde los equipos dependen de revisiones ad hoc y herramientas ligeras para ponerse en marcha.

Desde este punto de partida fundamental, existe una valiosa oportunidad para construir mayor consistencia, visibilidad e impacto. Esta guía se enfoca en ayudarle a progresar hacia un enfoque de TPRM Periódico mediante la introducción de políticas y flujos de trabajo más definidos, y fortaleciendo las prácticas básicas que desbloquean una gestión de riesgos más proactiva y escalable a lo largo del tiempo.

> *"El panorama de proveedores de la cadena de suministro se está multiplicando rápidamente, y la IA está acelerando el ritmo de las amenazas. ¿Sigue confiando en prácticas de gestión de riesgos de los años 90?"*
>
> Estado de la Ciberseguridad en la Cadena de Suministro 2026

# El Público Objetivo y el Valor

Esta guía de solución está diseñada específicamente para organizaciones que inician su proceso formal de TPRM y buscan pasar de una **etapa de Diligencia Básica** a una **etapa de TPRM Periódico** con un marco repetible.

Las organizaciones en esta etapa suelen definirse por las siguientes características:

| Área | Característica de la Diligencia Básica |
|---|---|
| **Estructura del Equipo** | Las responsabilidades de TPRM están fragmentadas y frecuentemente distribuidas entre profesionales generalistas de TI o Seguridad de la Información. |
| **Estado del Proceso** | Dependencia de procesos manuales e ineficientes (p. ej., hojas de cálculo) que generan una carga administrativa significativa. |
| **Uso de Tecnología** | Herramientas y tecnología adoptadas mínimas, lo que conduce a procesos de gestión de riesgos desarticulados e incompletos. |
| **Necesidad Principal** | Simplificar las revisiones de seguridad durante la contratación para que la incorporación de proveedores pueda avanzar. |

Esta etapa se define por el paso de revisiones de seguridad ad hoc durante la contratación a un programa estructurado y orientado por políticas que utiliza la clasificación de proveedores y evaluaciones anuales recurrentes para mantener el cumplimiento.

| Enfoque | Descripción |
|---|---|
| **Objetivo de Madurez** | Establecer un programa estructurado y orientado al cumplimiento que mantenga un rastro de auditoría mediante ciclos de evaluación recurrentes |
| **Público Objetivo** | CISO, Líder de TI, Responsable de TPRM, Operaciones de TI |
| **Desafío Principal** | Creciente acumulación de evaluaciones manuales causada por un número fijo de personal que intenta mantener el ritmo con un inventario de proveedores en crecimiento y ciclos de revisión anual recurrentes |
| **Resultado Empresarial** | Lograr la preparación para auditorías y la escala operativa reemplazando las revisiones ad hoc con un programa estructurado que elimine los atrasos en evaluaciones y acelere la incorporación. |

# Resultados e Impacto Esperados

### Establecer una cultura de riesgo

Pasar de las verificaciones de contratación "puntuales" a un programa orientado por políticas que garantice la preparación para auditorías mediante un ciclo de vida de evaluación repetible.

### Priorizar los riesgos de proveedores

Implementar la clasificación de proveedores para enfocar la experiencia en los socios críticos mientras se evita que los proveedores de bajo riesgo colapsen el proceso de evaluación.

### Crear eficiencias operativas

Reducir drásticamente los tiempos de ciclo "envío a cierre", permitiendo que un número fijo de personal gestione un inventario de proveedores en crecimiento sin aumentar el atraso.

| Área | Resultado Esperado | Impacto Empresarial |
|---|---|---|
| **Cultura de Riesgo y Cumplimiento** | Infraestructura lista para auditoría: Establece un programa formal y orientado por políticas con un ciclo de vida repetible. | Protección legal y regulatoria: Satisface los requisitos legales, de seguros y regulatorios al tiempo que traslada la responsabilidad documentada al tercero. |
| **Priorización de Proveedores** | Gestión de riesgos escalonada: Categorización estratégica de socios en función de la criticidad empresarial. | Asignación optimizada de recursos: Garantiza que el personal técnico de alto valor se concentre en los riesgos más críticos en lugar de quedar sepultado en el "ruido" de bajo riesgo. |
| **Eficiencia Operativa** | Tiempos de ciclo acelerados: Pasando de meses a una ventana estándar de 2 semanas de "envío a cierre". | Crecimiento escalable: Permite a la empresa gestionar un inventario de proveedores más amplio sin aumentar la plantilla ni ralentizar la incorporación. |

# Principios Rectores Esenciales de TPRM

A medida que mejora su programa base, estos tres principios fundamentales deben guiar sus esfuerzos iniciales:

**Defina su marco de gobernanza de riesgos**

Determine qué estándares de cumplimiento (como SOC 2 o ISO) serán necesarios y asegúrese de tener un sistema de registro listo para auditoría para almacenar las evaluaciones históricas.

**Establecer una metodología de clasificación**

Categorice su población de proveedores antes de lanzar nuevas evaluaciones definiendo qué constituye un proveedor “Crítico” frente a uno de “Bajo Riesgo” según el impacto empresarial.

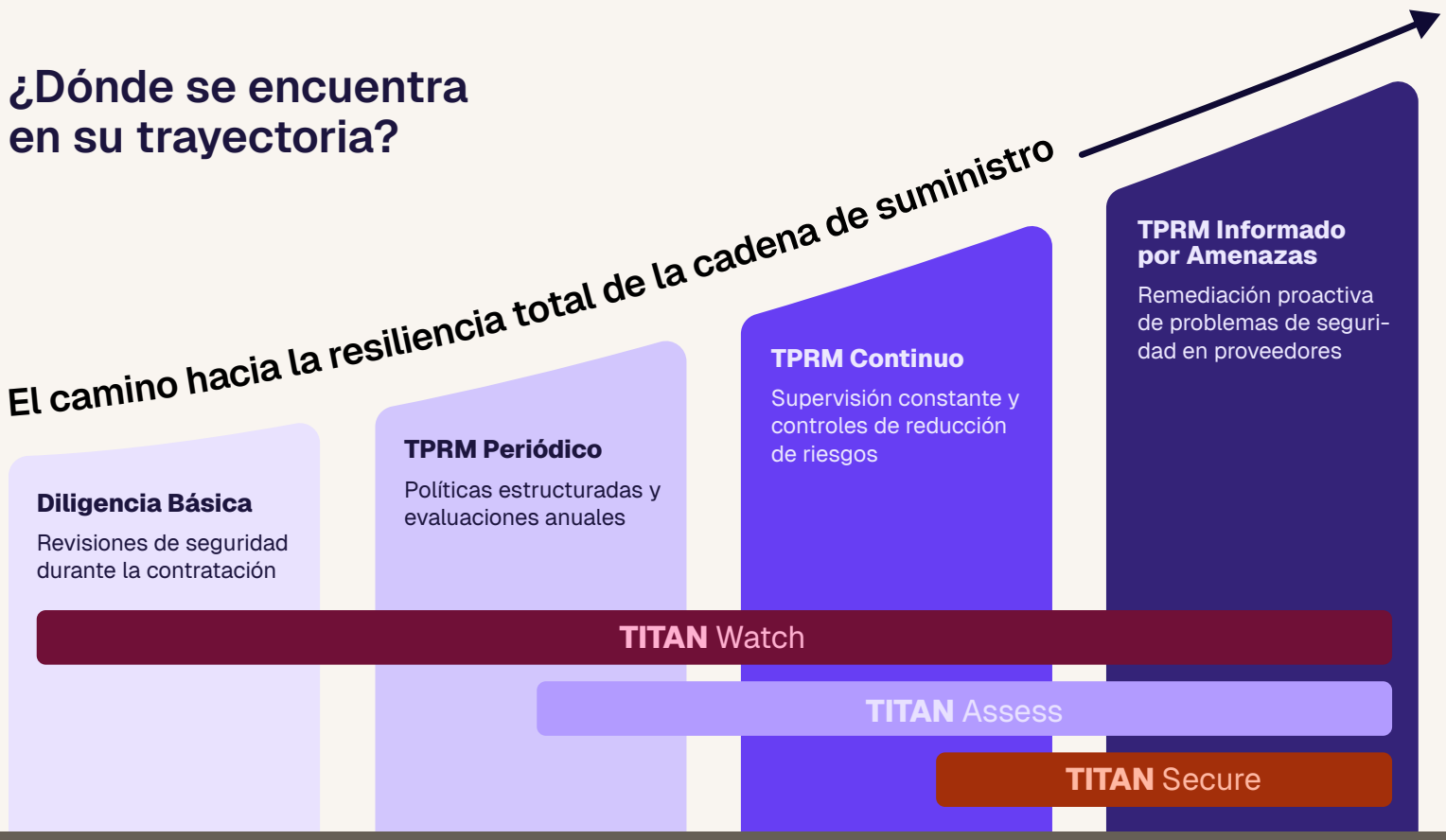
**Estandarizar el flujo de trabajo de evaluación**

Predefina sus conjuntos de cuestionarios y la cadencia de seguimiento automatizado para garantizar que pueda alcanzar de forma realista un tiempo de ciclo de 2 semanas a medida que aumenta la cobertura de proveedores

## ¿SABÍA QUE?

La investigación muestra que las organizaciones en la etapa de Diligencia Básica típicamente enfrentan tiempos de ciclo de cuestionarios de 1 a 3 meses. Al implementar los flujos de trabajo escalonados y orientados por políticas de este manual, los equipos comprimen esa ventana de “envío a cierre” a solo 2 semanas, una reducción del 80% que acelera el negocio sin sacrificar la seguridad.

## ¿Dónde se encuentra en su trayectoria?




**APROVECHAMIENTO DE LA IA PARA OPTIMIZAR Y MEJORAR LOS FLUJOS DE TRABAJO**

# TPRM Periódico: Cómo establecer un programa repetible y escalable

Esta sección describe una transición en tres pasos desde verificaciones de seguridad manuales y ad hoc hacia un programa maduro de Gestión de Riesgos de Terceros (TPRM) mediante gobernanza formal, clasificación basada en riesgos y flujos de trabajo digitales estandarizados.

## PASO 1

### Formalizar la Gobernanza de Riesgos

Transición de las verificaciones de seguridad manuales y ad hoc a un programa documentado y repetible regido por una política formal de TPRM y un sistema de registro listo para auditoría.

| ACCIÓN | EXPLICACIÓN DETALLADA |
|---|---|
| **Redactar documentación de política** | Definir los desencadenantes de las evaluaciones, los tipos de datos requeridos (SOC 2, ISO) y la frecuencia de las revisiones recurrentes. |
| **Centralizar los datos de proveedores** | Trasladar los datos de proveedores de hojas de cálculo planas a una plataforma GRC o TPRM centralizada para mantener un rastro de auditoría histórico. |
| **Estandarizar el lenguaje contractual** | Estandarizar el lenguaje legal en los contratos que obligue a los proveedores a participar en revisiones de seguridad periódicas. |

**MEJOR PRÁCTICA**

**“Mapeo Retroactivo de Auditoría”**

Diseñe sus flujos de trabajo de evaluación basándose en lo que sus auditores internos o proveedores de seguros requerirán como prueba de diligencia debida 12 meses a partir de ahora.

**HITO DE MADUREZ: LA RATIFICACIÓN DE LA POLÍTICA**

La finalización se marca cuando el equipo directivo aprueba una política formal de TPRM que exige evaluaciones para todos los proveedores, no solo los nuevos.

## PASO 2

### Implementar Clasificación Basada en Riesgos

Resuelva el cuello de botella operativo de las revisiones “de talla única” categorizando a los proveedores según su potencial impacto empresarial y acceso a datos.

| ACCIÓN | EXPLICACIÓN DETALLADA |
|---|---|
| **Evaluar el riesgo inherente** | Desarrollar un cuestionario corto de “alcance” para que los propietarios del negocio interno evalúen la criticidad del proveedor antes de la revisión de seguridad. |
| **Asignar niveles a los proveedores** | Establecer 3 a 4 niveles (p. ej., Crítico, Alto, Medio, Bajo) que dicten la profundidad y frecuencia de la evaluación de seguridad requerida. |
| **Asignar recursos técnicos** | Destine su expertise técnico limitado a los proveedores “Críticos” mientras utiliza validación automatizada para los niveles de riesgo “Bajo”. |

**MEJOR PRÁCTICA**

**Alcance Contextual**

Nunca envíe un cuestionario hasta saber si el proveedor maneja PII o tiene acceso a la red; esto evita la “sobrevaluación” de proveedores de bajo riesgo.

**HITO DE MADUREZ: EL INVENTARIO CLASIFICADO**

La finalización se marca cuando el 100% del portafolio de proveedores actual tiene asignado un nivel de riesgo, que dicta su ruta de evaluación específica.

PASO 3

# Estandarizar el Flujo de Trabajo de Evaluación

Elimine el atraso de evaluaciones reemplazando los seguimientos manuales con un flujo de trabajo digital estructurado de “envío a cierre”.

| ACCIÓN | EXPLICACIÓN DETALLADA |
|---|---|
| **Adoptar estándares de la industria** | Alejarse de los requisitos personalizados hacia conjuntos estándar de la industria (como SIG o CAIQ) que los proveedores puedan mapear fácilmente a sus datos existentes. |
| **Automatizar los seguimientos** | Configurar una cadencia basada en lógica para recordatorios a los proveedores, reduciendo la “persecución” administrativa que realiza el personal habitualmente. |
| **Formalizar la gestión de excepciones** | Crear un proceso estándar para marcar y rastrear las brechas de seguridad que los proveedores deben remediar antes de que se otorgue un “aprobado”. |

MEJOR PRÁCTICA

**Gestión de Disponibilidad**

Trate el ancho de banda de su equipo como un calendario; permita solo un número determinado de evaluaciones activas a la vez para evitar la acumulación de atrasos.

**HITO DE MADUREZ: TIEMPO DE CICLO DE DOS SEMANAS**

La madurez se logra cuando el tiempo promedio de “envío a cierre” de un cuestionario alcanza consistentemente el plazo de 14 días.

VISTA PREVIA DEL FLUJO DE TRABAJO CLAVE

# Evaluaciones de Riesgo de Proveedores

Una vez que haya realizado con éxito la transición de la Diligencia Básica al TPRM Periódico, su flujo de trabajo de evaluación pasa de un proceso manual y ad hoc a un motor de alta velocidad orientado por políticas.

| FASE | ACCIÓN | DETALLE DEL PROCESO |
|---|---|---|
| 1. **Incorporación y Clasificación** | **Categorizar la Solicitud** | Ante una nueva solicitud de proveedor, el propietario del negocio completa una evaluación de riesgo inherente. El sistema asigna automáticamente un Nivel (Crítico, Alto, Medio, Bajo) según el acceso a datos y el impacto empresarial. |
| 2. **Lanzamiento Focalizado** | **Implementar Revisión a Medida** | En lugar de una evaluación “de talla única”, se activa un cuestionario específico por nivel (p. ej., un SIG Core para proveedores Críticos frente a una versión Lite para proveedores de Bajo riesgo) para reducir la fricción del proveedor. |
| 3. **Comunicación Automatizada** | **Gestionar el Cronograma** | Todos los seguimientos se gestionan mediante una cadencia basada en lógica. Su equipo ya no “persigue” a los proveedores; los recordatorios automatizados garantizan que se mantenga el objetivo de 14 días de “envío a cierre”. |
| 4. **Análisis y Revisión** | **Marcar Excepciones de Política** | El personal técnico solo revisa las respuestas fuera de política marcadas por el sistema. Al centrarse únicamente en las brechas en lugar de cada respuesta individual, el “tiempo en evaluación” disminuye. |
| 5. **Determinación** | **Emitir Aprobación de Riesgo** | Se genera una postura de riesgo final. Si existen problemas críticos, se rastrean en un plan de remediación; si está claro, el proveedor pasa a la cola “Periódica” para su próxima revisión anual. |
| 6. **Archivo de Auditoría** | **Registrar la Instantánea** | La evaluación completada y toda la evidencia (SOC 2, certificados ISO) se archivan automáticamente en su Sistema de Registro, creando un rastro de auditoría permanente y listo para reguladores. |

# Medición y Próximos Pasos

## Métricas Clave (KPIs) a Seguir

Mida el progreso reportando estas métricas alineadas con el negocio:

### TIEMPO DEDICADO POR EVALUACIÓN

Identifica el “costo humano” de su programa

### COMPLETACIÓN DE CLASIFICACIÓN DE INVENTARIO

Asegura que su metodología basada en riesgos se esté aplicando realmente

### TIEMPO DE CICLO DEL CUESTIONARIO (ENVÍO A CIERRE)

Mide la velocidad de su motor de evaluaciones

### HALLAZGOS DE AUDITORÍA RELACIONADOS CON EL RIESGO DE TERCEROS

Demuestra que está cumpliendo los mandatos regulatorios y de cumplimiento

### TASA DE RESPUESTA A CUESTIONARIOS

Rastrea el compromiso de proveedores y la salud de sus relaciones en la cadena de suministro

CONCLUSIÓN

# De las Casillas de Verificación a la Gobernanza de Riesgos Escalable

Al realizar la transición de la Diligencia Básica al TPRM Periódico, su organización supera la revisión de seguridad “puntual” y establece un programa defendible y orientado por políticas. Este cambio garantiza que, a medida que crece su ecosistema de proveedores, la supervisión de riesgos siga siendo coherente, auditable y operativamente eficiente.

## El Impacto de Su Progreso

### ENFOQUE EN EL RIESGO ESPECÍFICO

Deja de tratar a todos los proveedores igual, lo que permite a su equipo enfocar su expertise en los socios que más importan para el negocio.

### GANANCIAS DRÁSTICAS DE EFICIENCIA

Al implementar la clasificación y los flujos de trabajo estandarizados, comprime el ciclo “envío a cierre” mientras reduce el tiempo de revisión manual.

### PREPARACIÓN CONTINUA PARA AUDITORÍAS

Reemplaza las hojas de cálculo fragmentadas con un sistema formal de registro, creando un rastro permanente que satisface los mandatos de cumplimiento.

SU PRÓXIMO PASO

# Transición del TPRM Periódico al TPRM Continuo

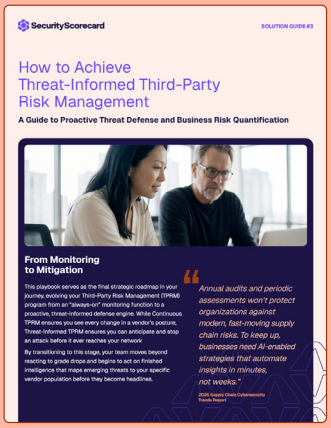
La próxima evolución en su trayectoria lo lleva de instantáneas “puntuales” a visibilidad en tiempo real. Mientras que el TPRM Periódico construye la base de gobernanza, el TPRM Continuo garantiza que nunca sea sorprendido por regresiones de seguridad que ocurran entre revisiones anuales. En el próximo manual, aprenderá cómo:

- **Cerrar la “Brecha de Visibilidad”:** Descubra cómo lograr visibilidad de 365 días sobre el riesgo de proveedores, alejándose del modelo de evaluación anual de “configurar y olvidar”.
- **Escalar la Cobertura al 100% de su Inventario de Proveedores:** Aprenda las estrategias para expandir el alcance de su programa desde un subconjunto de proveedores críticos hasta toda su cadena de suministro.
- **Iniciar el Compromiso Colaborativo de Riesgos:** Aprenda a activar asociaciones con proveedores alertándolos sobre cambios en sus exposiciones de riesgo, garantizando responsabilidad y remediación inmediatas.

GUÍA DE SOLUCIÓN #1


GUÍA DE SOLUCIÓN #2


GUÍA DE SOLUCIÓN #3




SecurityScorecard