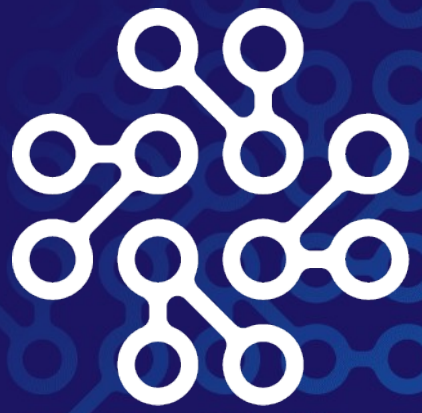


LAC4

Latin America and Caribbean Cyber Competence Centre

Funded by the European Union

GESTIÓN DE RIESGOS DE TERCEROS

Gabriela Reynaga Vargas

CRISC, CISA, CDPSE, GRCP, COBIT 5 & COBIT 2019 Accredited Trainer, LA ISO 37001:2016
Consejera Independiente Certificada

Gabriela Reynaga Vargas

CRISC, CISA, CDPSE, GRCP,
COBIT 5 & COBIT 2019 Accredited Trainer,
LA ISO 37001:2016
Consejera Independiente Certificada

Directora de Consultoría en Holistics GRC, Firma de Consultoría y Auditoría de procesos y GRC para las Tecnologías de Información y Operación.

Es Licenciada en Contaduría Pública y cuenta con 19+ años de experiencia como Auditor y Consultor en diferentes áreas.

Cuenta con experiencia en planeación, ejecución, supervisión y reportes de auditoría y consultoría de Tecnologías de Información en controles generales y controles automáticos de procesos de negocio, en ERP's, Ciberseguridad de sistemas SCADA/ICS.

- Board Member de ISACA 2018-2019, 2019-2020
- Chair del comité de Auditoría y Riesgos de ISACA 2019-2020
- Miembro del comité de Finanzas de ISACA 2018-2019
- Member of the Advisory Board of the GFCE (The Global Forum on Cyber Expertise) 2018-2020
- Presidente de ISACA Capítulo Guadalajara 2015-1018
- Presidente de la Comisión de TI de la Vicepresidencia del Sector Gubernamental del IMCP 2017-2019
- Miembro del Open Compliance and Ethics Group (OCEG).
- Miembro de Fundación Capa 8
- ISACA Evangelist
- Miembro del Comité Estratégico para Latinoamérica ISACA 2022

www.linkedin.com/in/gabrielareynaga

Funded by
the European Union

Outsourcing de TI

"es el uso de proveedores de servicios externos que posibilita de manera fácil y rápida contar con soluciones de infraestructura de TI, aplicaciones y procesos de negocio que permitan generar resultados comerciales"

Funded by the European Union

Razones de la subcontratación (algunas)

1. Reducción de costos
2. Uso de tecnologías y recursos innovadores
3. Falta de personal

Top 10 controles de seguridad que fallan los terceros en la evaluación inicial

Rank	Control	Security Domain	Suppliers Failing Control
1	Secure disposal or reuse of equipment	Physical and Environmental Security	52.8%
2	Information systems audit controls	Operations Security	50.6%
3	Policy on the use of cryptographic controls	Cryptography	49.5%
4	Management of technical vulnerabilities	Operations Security	46.1%
5	Removal or adjustment of access rights	Access Controls	32.9%
6	User access provisioning	Access Controls	26.4%
7	Unattended user equipment	Access Controls	26.3%
8	Screening	Human Resource Security	24.8%
9	Network controls	Network Security Management	24.6%
10	Policies for information security	Information Security Policies	22.2%

https://en.softtek.co/hubfs/images/landing-pages/Risk_Management/Report/State_of_Digital_Third-Party_Risk_Report.pdf

Funded by
the European Union

TPRM - Gestión de Riesgos de Terceros

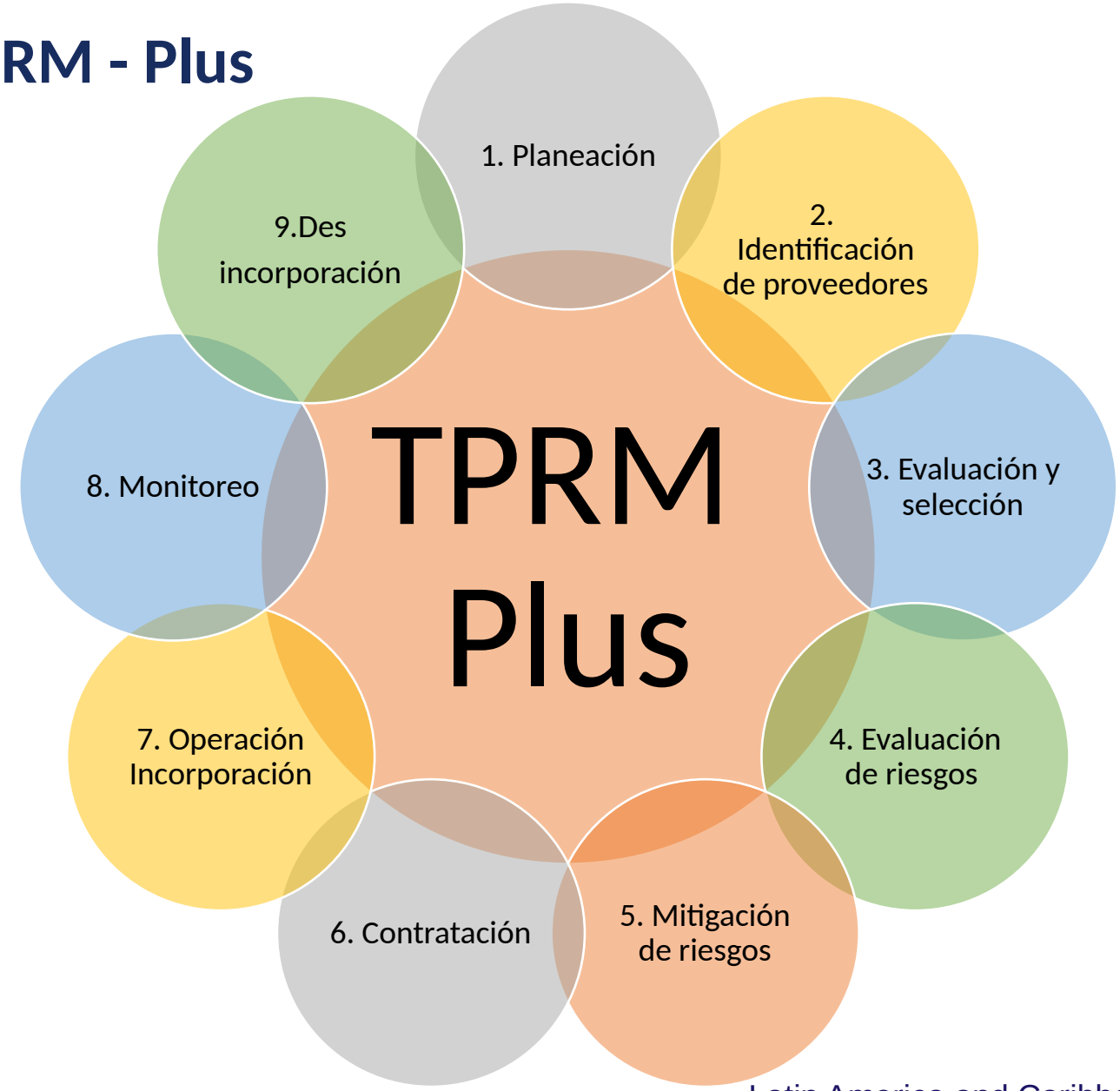
Es el **proceso** de **analizar** y **minimizar** los riesgos asociados a la subcontratación de terceros vendedores o proveedores de servicios.

Dentro de la categoría de riesgos de terceros:

Riesgos financieros, medioambientales, de reputación y de seguridad.

Funded by the European Union

TPRM - Plus



Funded by the European Union

TPRM - Plus

1. Planeación

Desarrollar un plan para evaluar el nivel y la complejidad del riesgo inherente que presenta cada actividad, segmento para identificar las actividades críticas o de alto riesgo, y establecer los recursos necesarios.

- Servicio
- Volumen de actividad
- Naturaleza de los riesgos
- Interacciones con el equipo, clientes, autoridades, etc.
- Requerimientos regulatorios
- Presupuesto
- Modelo de abastecimiento

2. Identificación de proveedores

Proveedores disponibles de maneral local, nacional, internacional

- ¿Son proveedores únicos?
- ¿Hay sustitutos?
- ¿Quiénes son?
- ¿Tiempo en el mercado?
- Cumplimiento y gestión de riesgos
- Situación financiera y capacidad de recuperación
- Experiencia y reputación
- Directivos de la empresa
- Seguridad de la información y sistemas
- Gestión y notificación de incidentes
- Gestión de los recursos humanos
- Conflictos de intereses

Funded by the European Union

TPRM - Plus

3. Evaluación y selección

Llevar a cabo el proceso de evaluación de acuerdo a las características de los servicios que requerimos y procesos de selección de proveedores aplicables.

- Cumple o no cumple
- % de cumplimiento

4. Evaluación de riesgos

Evaluar riesgos de la selección de posibles proveedores

- Financieros
- Reputacionales
- Operativos
- Modelo de abastecimiento

Funded by the European Union

TPRM - Plus

5. Mitigación de riesgos

Es bueno pero…

- Acciones de remediación
- Tiempo para resolverlas
- Riesgos residuales
- Procesos de monitoreo (frecuencia, responsable, etc.)
- Seguimiento a la remediación

6. Contratación

Proceso de contratación

- Indicadores clave de rendimiento (KPI)
- Gestión de la información/comunicación
- Derechos de auditoría y supervisión
- Requisitos de cumplimiento
- Uso de la información, la propiedad intelectual y la tecnología
- Confidencialidad e integridad
- Conflictos de intereses
- Requisitos de los subcontratistas
- Condiciones de rescisión
- Convenios

Funded by the European Unic

TPRM - Plus

7. Operación Incorporación

- Ejecución de los planes y servicios contratados en el día a día
- Personal de operación
- Personal estratégico
- Supervisión efectiva en diversos niveles
- Integración, cultura y estilo

8. Monitoreo

- Auditoría
- Verificación de cumplimiento de contrato
- Otras actividades de supervisión

Funded by the European Union

TPRM - Plus

9. Des incorporación

- Evidencia
- Justificación
- Nuestra información
- Convenios de confidencialidad
- Multas y/o sanciones
- Contrato

Funded by the European Union

Algo para llevar

1. Llevar a cabo supervision operativa y ejecutiva
2. Mantener una base de datos de proveedores
3. Asignar un nivel de confianza a cada uno de ellos
4. Evaluar siempre la seguridad y el control en la gestión
5. Validar el nivel de confianza
6. Supervisar e informar

ITIL, ISO/IECS 20000, OCEG, Cibersecurity Maturity Platform de CMMI

7. COBIT 2019

Funded by
the European Union

Funded by
the European Union

¿Preguntas?

Contact us:

eucybernet@ria.ee

https://www.lac4.eu/

www.lac4.com

Funded by
the European Union

Gracias!

Gabriela Reynaga Vargas
CRISC, CISA, CDPSE, GRCP,
COBIT 5 & COBIT 2019 Accredited Trainer,
LA ISO 37001:2016
Consejera Independiente Certificada

Contact us:

eucybernet@ria.ee

https://www.lac4.eu/

www.lac4.com