2025

Gestión de Riesgos de Ciberseguridad en la Cadena de Suministro:

Guía Legal para la Contratación de Servicios de Outsourcing

DOCIDO 02: GUÍAS IDÓNEA

idónea

Soluciones Legales para un Mundo Digital

CONTENIDO

Gestión de riesgos de ciberseguridad en la cadena de suministro: Guía para la contratación de servicios de Outsourcing

En el intrincado ecosistema empresarial actual, la externalización de servicios se ha consolidado como una estrategia operativa esencial. Si bien la promesa de eficiencia, flexibilidad y especialización es innegable, la subcontratación introduce una capa de complejidad en la gestión de riesgos de ciberseguridad, especialmente en lo que respecta a la cadena de suministro.

Esta guía, tiene como objetivo proporcionar un marco integral para la gestión de riesgos de cibersegurden la contratación de servicios de outsourcing. No se trata de enumerar amenazas abstractas, sino de ofrecer una hoja de ruta práctica y accionable para que las organizaciones puedan externalizar con seguridad, protegiendo sus activos de información y cumpliendo con las exigencias regulatorias.

LA CADENA
DE SUMINISTRO EN RIESGO:

UN ANÁLISIS DETALLADO DE LAS AMENAZAS DE LA EXTERNALIZACIÓN

La externalización, por su propia naturaleza, expande la superficie de ataque de una organización. Cada proveedor externo se convierte en un nuevo eslabón en la cadena de suministro, y cada eslabón representa una potencial vulnerabilidad. Comprender la naturaleza específica de estos riesgos es el primer paso para mitigarlos eficazmente. Entre las amenazas más relevantes, destacan:

1. Vulnerabilidades Estratégicas:

La ausencia de una estrategia de seguridad de la información robusta y específica para la externalización es un error fundamental. Sin una hoja de ruta clara, las medidas de seguridad se implementan de forma dispersa y descoordinada, dejando huecos críticos sin protección.

Una estrategia insuficiente para la externalización se identifica como la primera y fundamental amenaza. Si falta una estrategia clara, los aspectos de seguridad de la información no se tienen debidamente en cuenta en las diferentes fases del ciclo de vida de la externalización. Esto conduce a un nivel de seguridad insuficiente tanto en la propia institución como en los Proveedores de externalización. Las consecuencias pueden ser procesos comprometidos, fallos y la fuga de información a terceros no autorizados.

Desde el punto de vista legal, una estrategia de externalización clara es esencial para garantizar el cumplimiento de las leyes de protección de datos y otros requisitos regulatorios. Una estrategia deficiente puede considerarse como negligencia organizativa y, en caso de violación de la protección de datos, puede acarrear multas y reclamaciones por daños y perjuicios considerables. Las empresas deben poder demostrar que han seguido una estrategia meditada para minimizar los riesgos de la externalización.

2. Procesos Críticos en manos de Terceros:

La externalización de procesos críticos para la institución, que por su criticidad o necesidad de protección deberían permanecer en la empresa, representa otra amenaza significativa. Si la empresa pierde el control sobre estos procesos, puede provocar graves interrupciones en las operaciones comerciales.

Los fallos o interrupciones de los procesos pueden poner en peligro el funcionamiento normal del negocio y provocar pérdidas de control. Además, los Proveedores de externalización ganan una mayor influencia, lo que aumenta la dependencia de la empresa.

Desde una perspectiva legal, la externalización de procesos críticos conlleva el riesgo de que las empresas dejen de cumplir sus obligaciones legales y contractuales. Por ejemplo, los fallos en el procesamiento de datos pueden dar lugar a infracciones de las leyes de protección de datos. Además, la dependencia de un único proveedor de externalización puede poner en peligro la continuidad del negocio de la empresa en caso de crisis. Por lo tanto, un análisis cuidadoso de la criticidad de los procesos y una estrategia de externalización diferenciada son esenciales.

3. Dependencia Excesiva de los Proveedores:

La concentración de servicios en un único proveedor genera una dependencia que puede ser explotada. Esta dependencia reduce la capacidad de negociación, incrementa los riesgos operativos y puede llevar a condiciones contractuales desfavorables en materia de seguridad.

4. Estándares de Seguridad Insuficientes de los Proveedores:

Un nivel insuficiente de seguridad de la información en los Proveedores de externalización puede generar importantes brechas de seguridad. Si los Proveedores no mantienen ningún estándar de seguridad o solo uno insuficiente, surgen vulnerabilidades que pueden ser explotadas para ataques informáticos y pérdidas de datos. Las consecuencias pueden ser consecuencias legales, daños financieros y pérdidas de reputación para la empresa.

Legalmente, las empresas estarán obligadas a adoptar medidas técnicas y organizativas adecuadas para proteger los datos personales (nueva norma sobre datos personales). La selección de proveedores de externalización con un nivel de seguridad insuficiente puede considerarse como una infracción de estas obligaciones. Las empresas deben asegurarse de que sus socios de externalización tienen un nivel de seguridad adecuado y lo mantienen continuamente. Esto requiere auditorías y controles regulares de las medidas de seguridad de los Proveedores.

5. Falta de Supervisión y Control de la Gestión:

Una gestión deficiente de la externalización conduce a una gestión inadecuada de los procesos externalizados en curso. La transparencia disminuye o se pierde, y las empresas ya no pueden controlar ni gestionar adecuadamente a sus Proveedores de externalización. Esto pone en peligro la seguridad de la información y puede dar lugar a un tratamiento descuidado de la información por parte de los Proveedores.

Una gestión eficaz de la externalización es esencial desde el punto de vista legal para garantizar el cumplimiento de los contratos y los requisitos legales. Las empresas deben definir e implementar responsabilidades y procesos claros para la gestión de la externalización. Esto incluye el seguimiento regular del rendimiento de los proveedores de externalización, la realización de auditorías y la escalada de problemas. Una gestión deficiente de la externalización puede considerarse como negligencia organizativa en caso de responsabilidad.

6. Contratos Insuficientes en Materia de Seguridad:

Regulaciones contractuales insuficientes con los Proveedores de externalización pueden generar vulnerabilidades en la seguridad de la información a lo largo de todo el ciclo de vida de la externalización. Los contratos definen todo el proceso de externalización y son la base para las reclamaciones de la empresa. Los contratos defectuosos o incompletos pueden dar lugar a diversos problemas de seguridad, especialmente si las tareas, los parámetros de rendimiento o los gastos se describen de forma insuficiente o confusa. Esto puede hacer que no se apliquen medidas de seguridad, que no se cumplan los requisitos y obligaciones regulatorias o que no se respeten las obligaciones de información y las leyes. Si no se tiene en cuenta el aspecto de la seguridad de la información en la elaboración del contrato, los procesos y los datos pueden quedar insuficientemente protegidos.

La elaboración del contrato es un factor de éxito crítico para una externalización segura. Desde el punto de vista legal, los contratos deben contener regulaciones detalladas sobre la seguridad de la información, incluyendo estándares de seguridad, responsabilidades, derechos de auditoría, cuestiones de responsabilidad, disposiciones sobre protección de datos y regulaciones sobre la devolución de datos al final del contrato. Las cláusulas contractuales estándar a menudo no son suficientes; los contratos deben adaptarse individualmente a los riesgos y requisitos específicos del proyecto de externalización. Por lo tanto, es muy recomendable la participación de expertos legales y de seguridad en el proceso de elaboración del contrato.

7. Gestión Inadecuada de los Derechos de Acceso, Entrada y Autorización

Una gestión eficaz de la externalización es esencial desde el punto de vista legal para garantizar el cumplimiento de los contratos y los requisitos legales. Las empresas deben definir e implementar responsabilidades y procesos claros para la gestión de la externalización. Esto incluye el seguimiento regular del rendimiento de los proveedores de externalización, la realización de auditorías y la escalada de problemas. Una gestión deficiente de la externalización puede considerarse como negligencia organizativa en caso de responsabilidad.

Desde el punto de vista legal, un control estricto de los derechos de acceso es esencial para garantizar la confidencialidad e integridad de los datos. Las empresas deben definir e implementar directrices y procesos claros para la concesión, gestión y supervisión de los derechos de acceso. Se debe aplicar sistemáticamente el principio de mínima concesión de derechos (Least Privilege). También son importantes las revisiones periódicas de los derechos de acceso y la revocación oportuna de los derechos cuando los empleados se marchan. Un sistema de gestión de identidades y accesos (IAM) puede facilitar considerablemente la gestión de los derechos de acceso en el entorno de la externalización.

8. Pérdida de Control y Gestión por Subcontrataciones

La subcontratación de partes de procesos de negocio o actividades a subproveedores por parte de los Proveedores de externalización entraña el riesgo de pérdida de control y gestión. Debido a los participantes adicionales, el proceso de externalización se vuelve más complejo e intransparente. Las empresas ya no pueden controlar ni gestionar adecuadamente los procesos externalizados. Además, los Proveedores de externalización pueden omitir exigir el nivel mínimo de seguridad de la información requerido por la empresa al subproveedor. La consecuencia es que los aspectos de seguridad de la información acordados no se implementan completamente por los subproveedores.

Desde el punto de vista legal, las empresas deben asegurarse de que los requisitos de seguridad se cumplen no solo por su socio de externalización directo, sino también en toda la cadena de subcontratistas. Por lo tanto, son esenciales las regulaciones contractuales sobre la subcontratación. Las empresas deben reservarse un derecho de aprobación para la contratación de subproveedores y asegurarse de que se aplican estándares de seguridad iguales o superiores también a los subproveedores. Los derechos de auditoría también deben extenderse a los subproveedores. Una cadena de suministro transparente es crucial para minimizar los riesgos de la subcontratación.

9. Instrumentos de Medición y Control Insuficientes e Inadecuados:

La falta de instrumentos o instrumentos inadecuados para la gestión de los Proveedores de externalización impide que las empresas verifiquen si los procesos externalizados se implementan correctamente. Además de los acuerdos, las empresas necesitan instrumentos como indicadores clave de rendimiento (KPIs) cualitativos y cuantitativos para medir y supervisar el rendimiento de los Proveedores de externalización. La falta de instrumentos hace que los Proveedores no puedan ser controlados y gestionados adecuadamente. Ya no se puede verificar ni rastrear el cumplimiento de los requisitos de seguridad.

Desde el punto de vista legal, la medición del rendimiento de los Proveedores de externalización es importante para verificar el cumplimiento de los contratos y los SLAs y, en caso de litigio, poder presentar reclamaciones. En los contratos deben definirse KPIs y métodos de medición claros. Se requieren informes y revisiones periódicas para supervisar el rendimiento y, en su caso, tomar medidas. Los derechos de auditoría permiten a las empresas verificar el cumplimiento de los requisitos de seguridad y la exactitud de los datos de rendimiento.

10. Planificación Deficiente de la Finalización del Contrato:

Regulaciones insuficientes para la finalización de una relación de externalización pueden causar problemas, especialmente en la devolución de hardware, datos y accesos. Las regulaciones faltantes o poco claras pueden hacer que la devolución de datos no se lleve a cabo correctamente o que los accesos no se bloqueen a tiempo.

Desde el punto de vista legal, deben acordarse regulaciones de salida claras en los contratos para garantizar una transición sin problemas al final del contrato. Esto incluye regulaciones sobre migración de datos, borrado de datos, devolución de hardware y software, bloqueo de accesos y entrega de documentación. También deben existir planes de contingencia para la finalización imprevista del contrato. También deben tenerse en cuenta las obligaciones legales de conservación de datos al final del contrato.

11. Concepto de emergencia Inadecuado:

Un entendimiento insuficiente de lo que significa una emergencia, puede provocar, en caso de fallo, ciberataque o crisis, que los procesos externalizados fallen. Una previsión de emergencias insuficiente pone en peligro la continuidad del negocio de la empresa y puede provocar importantes daños económicos. No solo la propia empresa, sino también las instituciones conectadas pueden verse afectadas. Los efectos en cascada a través de los proveedores de servicios ascendentes y descendentes pueden intensificar los efectos.

Desde el punto de vista legal, las empresas están obligadas a tomar medidas de contingencia adecuadas para garantizar la disponibilidad de sus sistemas y datos críticos. Por lo tanto, es esencial un concepto de emergencia integral también incluya los procesos de externalización. El concepto de emergencia debe definir responsabilidades claras, procesos de escalada, vías de comunicación y planes de recuperación. Son importantes los ejercicios de emergencia regulares con los Proveedores de externalización para verificar y mejorar la eficacia del concepto de emergencia.

CONSTRUYENDO UNA FORTALEZA DE CIBERSEGURIDAD:

La mitigación eficaz de estos riesgos exige la implementación de un marco de seguridad robusto y estructurado, que abarque medidas fundamentales en tres niveles:

Requisitos Esenciales

1 De cumplimiento obligatorio

Requisitos Estándar

2 Buenas prácticas recomendadas

Requisitos Mejorados

3 Para información altamente sensible

REQUISITOS ESENCIALES (DE CUMPLIMIENTO NECESARIO):

Estos requisitos son la base indispensable de cualquier proyecto de externalización segura y deben ser implementados de forma imperativa:

- Definición de Perfiles de Requisitos de Seguridad por Proceso: Elaborar perfiles detallados para cada proceso externalizado, especificando la función, los datos que maneja, las interfaces y una evaluación de criticidad en términos de seguridad de la información.
- Implementación de un Enfoque de Gestión de Riesgos: Realizar una evaluación de riesgos exhaustiva antes de externalizar cualquier proceso, considerando la criticidad de la información, la probabilidad de incidentes y el impacto potencial en el negocio.
- Evaluación Rigurosa de la Idoneidad de los Proveedores: Llevar a cabo una diligencia debida exhaustiva de los proveedores potenciales, verificando su experiencia en seguridad, su reputación y su solvencia financiera.
- Inclusión de Cláusulas de Seguridad Contractuales Estándar: Incorporar en los contratos de externalización cláusulas específicas sobre seguridad de la información, incluyendo niveles de servicio, responsabilidades, derechos de auditoría y protocolos de respuesta a incidentes.
- Garantía de Capacidad Multi-Cliente Segura (si aplica): Si el proveedor atiende a múltiples clientes, exigir y verificar la implementación de medidas robustas de separación lógica y física de datos y entornos, garantizando la confidencialidad de la información.
- Desarrollo e Implementación de un Concepto de Seguridad Integral: Crear un concepto de seguridad específico para cada proyecto de externalización, alineado con estándares reconocidos y que defina claramente las responsabilidades de la organización cliente y del proveedor en materia de seguridad.
- Establecimiento de Protocolos de Finalización del Contrato: Definir procedimientos claros y detallados para la finalización del contrato, tanto planificada como imprevista, incluyendo la repatriación de datos, la revocación de accesos y la gestión de la transición.

REQUISITOS ESTÁNDAR (BUENAS PRÁCTICAS RECOMENDADAS):

Estos requisitos, aunque no esenciales, representan las mejores prácticas para elevar significativamente el nivel de seguridad en la externalización:

- Elaboración de una Estrategia de Externalización Documentada: Desarrollar una estrategia formal y documentada para la externalización, definiendo objetivos, alcance, criterios de selección de proveedores y principios de seguridad.
- Creación de una Política de Externalización: Establecer una política de externalización formal, que defina los procedimientos, responsabilidades y controles de seguridad para todos los proyectos de externalización.
- Designación de un Responsable de la Gestión de la Externalización: Asignar un responsable o equipo dedicado a la gestión de la externalización, con la función de coordinar la seguridad, supervisar a los proveedores y gestionar los riesgos.
- Mantenimiento de un Registro de Externalización Centralizado: Crear y mantener un registro actualizado de todos los proyectos de externalización, incluyendo información detallada de los proveedores, contratos, evaluaciones de riesgo y medidas de seguridad implementadas.
- Generación Periódica de Informes de Externalización: Producir informes periódicos sobre el estado de los proyectos de externalización, incluyendo métricas de rendimiento, incidentes de seguridad y riesgos identificados, para informar a la dirección y facilitar la toma de decisiones.
- Diseño de Contratos con Participación Multidisciplinar: Involucrar a expertos legales, de seguridad y operativos en el diseño y revisión de los contratos de externalización, garantizando una cobertura integral de todos los aspectos relevantes.
- Implementación de Controles de Acceso a la Red Estrictos: Establecer controles de acceso a la red robustos y granulares, limitando el acceso de los proveedores únicamente a los sistemas y datos estrictamente necesarios para la prestación del servicio.
- Realización de Auditorías de Seguridad Periódicas a los Proveedores: Llevar a cabo auditorías de seguridad periódicas e independientes a los proveedores, verificando el cumplimiento de los estándares de seguridad contractuales y la efectividad de las medidas implementadas.

- Verificación de Antecedentes y Fiabilidad del Personal del Proveedor: Implementar procesos de verificación de antecedentes y fiabilidad para el personal del proveedor que acceda a información sensible de la organización cliente.

- Revisión Periódica de Acuerdos y Contratos: Establecer ciclos de revisión periódica de los acuerdos y contratos de externalización, adaptándolos a la evolución del panorama de amenazas y a los cambios en las necesidades del negocio.

- Desarrollo de Planes de Contingencia para Proveedores Alternativos: Elaborar planes de contingencia para la transición a proveedores alternativos en caso de incumplimiento contractual, problemas de seguridad o finalización del contrato, reduciendo la dependencia y garantizando la continuidad del servicio.

- Integración de Proveedores en el Plan de Respuesta a incidentes:: Incorporar a los proveedores de externalización en el plan de respuesta a incidentes de la organización, definiendo roles, responsabilidades y protocolos de comunicación para incidentes de seguridad.

REQUISITOS MEJORADOS (PARA INFORMACIÓN ALTAMENTE SENSIBLE):

Para organizaciones que manejan información especialmente sensible o que operan en sectores regulados, se recomiendan medidas de seguridad adicionales y reforzadas:

Firma de Acuerdos tipo Escrow para Software Crítico: Establecer acuerdos de depósito para el código fuente de software crítico de proveedores, garantizando el acceso y la continuidad del servicio en caso de quiebra o incumplimiento del proveedor.

Realización de Ejercicios Conjuntos de Respuesta a Emergencias y Crisis: Organizar simulacros de incidentes de seguridad conjuntos con los proveedores, validando los planes de respuesta y mejorando la coordinación y la comunicación en situaciones de crisis.

Implementación Obligatoria de Cifrado Robusto de Datos Sensibles: Exigir el cifrado robusto de datos sensibles tanto en tránsito como en reposo, utilizando algoritmos de cifrado reconocidos y gestionando las claves de forma segura.

Verificación Exhaustiva del Personal del Proveedor: Realizar verificaciones exhaustivas de antecedentes y evaluaciones de fiabilidad para el personal del proveedor que acceda a información altamente confidencial, incluyendo investigaciones y acreditaciones de seguridad si fuera necesario.

Utilización de Entornos Sandbox para la Validación de Datos y Software del Proveedor: Implementar entornos sandbox o “zonas seguras” para analizar y validar datos y software provenientes de proveedores externos, minimizando el riesgo de introducción de malware o vulnerabilidades en los sistemas de la organización.

idónea

Cuéntanos sobre ti

info@idonea.cl

www.idonea.cl

Idónea Consultores