CARBONELL FIGUERAS

NORMATIVA DE SEGURIDAD PARA TERCERAS PARTES

Contenido

1. Control de cambios

V	Fecha	Responsable	Cambios	Aprobado por
01	16/06/2025	Responsable SGSI	Versión inicial	Responsable SGSI

Texto aprobado el día 16/06/2025 por el Responsable del SGSI de Carbonell Figueras SA y Carbonell Figueras Construcciones Sostenibles SLU (en adelante, conjuntamente referidos como Carbonell Figueras).

Esta normativa es efectiva desde esa fecha y hasta que sea reemplazada por una nueva.

Este documento anula cualquier versión anterior.

El Responsable del SGSI de Carbonell Figueras se compromete a revisar esta normativa anualmente adaptándola a nuevas exigencias que puedan aparecer y la deja a disposición de las partes interesadas que lo requieran.

2. Introducción

La seguridad en las relaciones para terceras partes es un componente esencial del Sistema de Gestión de Seguridad de la Información (SGSI) de Carbonell Figueras. Esta normativa establece los requisitos mínimos de seguridad que deben cumplir los proveedores externos que traten información corporativa o tengan acceso a los sistemas.

3. Objetivo y alcance

Establecer los criterios para la selección, contratación, seguimiento y finalización de relaciones con terceros con el fin de proteger la información de Carbonell Figueras. Aplica a:

- Proveedores externos que accedan almacenen, procesen o transmitan información de Carbonell Figueras.
- Clientes, accionistas, inversores, reguladores y otras partes interesadas externas.
- Personal interno responsable de la gestión de proveedores.

4. Responsabilidades

Responsable del SGSI	• Supervisar el cumplimiento y actualizar esta normativa. • Gestionar y documentar las excepciones a la normativa. • Coordinar auditorías y revisiones de seguridad aplicables a proveedores. • Validar la eliminación segura de datos tras la finalización contractual. • Prestar soporte al equipo de Compras para evaluar riesgos de seguridad y establecer requisitos con los terceros.
Departamentos que gestionan compras	• Mantener un registro clasificado la categorización de proveedores por criticidad. • Aplicar los requisitos de seguridad en los procesos de adquisición. • Verificar que toda contratación relación con terceros incluya cláusulas de seguridad aplicables según el riesgo. • Coordinar con el SGSI la diligencia debida antes de la contratación.
Departamento Jurídico	• Validar contratos y acuerdos en materia de seguridad de la información. • Establecer las cláusulas legales específicas sobre protección de datos, seguridad de la información y derecho de auditoría.

Responsables de servicios	• Verificar el cumplimiento de la normativa por parte de los proveedores. • Supervisar la ejecución de los SLAs y KPIs relacionados con la seguridad. • Reportar incidentes o incumplimientos detectados durante la operación. • Apoyar en la clasificación de proveedores según criticidad.

5. Registro de proveedores

Las terceras partes que mantengan una relación contractual con Carbonell Figueras y que tengan acceso a activos de información, sistemas, redes, datos o instalaciones, serán dados de alta y registrados formalmente en los registros de terceros de Carbonell Figueras.

Este registro tendrá como objetivo centralizar, mantener y actualizar la información relevante sobre cada proveedor para facilitar la evaluación de riesgos, seguimiento de cumplimiento y auditorías internas o externas.

El registro debe contener, como mínimo, la siguiente información:

- **Nombre legal del proveedor**, razón social y datos de contacto actualizados.
- **Persona responsable de la relación contractual**.
- **Descripción de la relación o servicios contratados**.
- **Fecha de inicio y finalización del contrato.**
- **Criterios de clasificación:**
  - Tipo de servicio TI prestado
  - Nivel de Acceso
  - Tipo de información tratada
- **Clasificación del tercero** según su criticidad (alta, media, baja).

El registro deberá mantenerse actualizado ante cualquier cambio en la relación contractual, servicios prestados o condiciones de seguridad, y estará disponible para revisión por el Responsable del SGSI y/o auditores autorizados.

6. Gestión de riesgos de terceros

6.1. Clasificación de terceros en base a riesgo

Con el fin de aplicar un enfoque proporcional y basado en riesgos, todos los terceros de Carbonell Figueras deberán ser **clasificados según su nivel de criticidad**, tomando como referencia los siguientes criterios:

- Tipo de servicios TI prestados (estratégicos, operativos, auxiliares).
- Nivel de acceso a sistemas, redes, aplicaciones o instalaciones físicas.
- Tipo de información tratada (pública, interna, confidencial o datos personales).
- Impacto potencial sobre la continuidad del negocio o la reputación de la organización en caso de fallo o incidente.

La clasificación se realizará en una de las siguientes categorías:

- **Alta:** Terceros que tratan información confidencial o personal, prestan servicios esenciales o tienen acceso privilegiado a sistemas o infraestructuras críticas.
- **Media**: Terceros que tratan información interna o prestan servicios con dependencia operativa parcial.
- **Baja**: Terceros sin acceso a información sensible ni a entornos operacionales relevantes.

A continuación, se definen los criterios de clasificación:

Criterio	Clasificación Alta	Clasificación Media	Clasificación Baja
Tipo de servicios TI prestados	Estratégicos (servicios críticos para el negocio)	Operativos (soporte parcial de procesos de negocio)	Auxiliares (servicios de soporte no críticos)
Nivel de acceso	Acceso privilegiado a sistemas, redes, aplicaciones o instalaciones críticas	Acceso limitado a determinados sistemas o instalaciones no críticas	Sin acceso a sistemas, redes ni instalaciones relevantes
Tipo de información tratada	Confidencial o datos personales (incluyendo datos especialmente protegidos)	Información interna (no pública, pero no confidencial ni personal)	Información pública o sin sensibilidad aparente

Esta clasificación determinará:

- La intensidad y frecuencia de las auditorías o revisiones.
- Las cláusulas contractuales mínimas exigibles.
- Los requisitos de planes de continuidad.
- La necesidad de evaluación de riesgos específica

6.2. Establecimiento de requisitos de seguridad

Previo al inicio de cualquier relación contractual con una organización externa, Carbonell Figueras llevará a cabo un proceso de definición de requisitos en función del nivel del tercero según su clasificación:

Categoría de criticidad	Requisitos mínimos a exigir
Alta	• Contrato con cláusulas de confidencialidad estrictas • Acuerdo de nivel de servicio (SLA) detallado con penalizaciones • Evaluación de seguridad de la información previa a la contratación (due diligence) • Derecho de auditoría o inspección periódica • Asegurar la formación en ciberseguridad del personal del tercero • Plan de continuidad de negocio / recuperación ante desastres • Revisión periódica del cumplimiento y recertificación de requisitos de seguridad
Media	• Contrato con cláusulas básicas de confidencialidad • Acuerdo de nivel de servicio (SLA) con controles de calidad y tiempos de respuesta • Cuestionario de autoevaluación de seguridad y privacidad • Procedimientos de notificación de incidentes claros
Baja	• Contrato estándar con cláusula de confidencialidad • Información sobre cómo notificar incidencias • Verificación inicial de requisitos mínimos legales (por ejemplo, cumplimiento LOPD)

7. Obligaciones de los terceros

7.1. Evaluación de riesgos

Se espera que los terceros gestionen de forma proactiva los riesgos relacionados con el tratamiento de sus datos y servicios mediante las siguientes prácticas:

- **Evaluación y mitigación de riesgos:** Los terceros deben realizar evaluaciones de riesgos periódicas que evalúen las posibles amenazas, vulnerabilidades e impactos en los datos, sistemas y procesos de Carbonell Figueras. Los riesgos deben documentarse y se deben implementar medidas de mitigación efectivas para abordar estos riesgos.
- **Monitoreo y mejora continuos:** Los terceros deben mantener sistemas para monitorear continuamente nuevas vulnerabilidades o amenazas, y deben demostrar un enfoque proactivo para identificar y abordar los riesgos emergentes, incluido un sistema para realizar evaluaciones periódicas de vulnerabilidades y pruebas de penetración.

7.2. Control de acceso y autenticación

Para garantizar la seguridad e integridad de los datos y sistemas de Carbonell Figueras, los terceros deben implementar controles integrales de acceso y autenticación de usuarios. Estos controles son esenciales para proteger la información confidencial y evitar el acceso no autorizado. Las siguientes directrices describen los requisitos clave a los que deben adherirse los terceros:

- **Acceso de usuarios y administración de roles:** Los terceros deben implementar el control de acceso basado en roles (RBAC) para garantizar que los usuarios solo tengan acceso a los datos y sistemas necesarios para realizar sus tareas laborales específicas. Todos los controles de acceso deben revisarse a intervalos regulares (por ejemplo, anualmente).
- **Protocolos de autenticación:** El acceso a los sistemas, aplicaciones y datos de Carbonell Figueras debe protegerse mediante la autenticación multifactor (MFA) obligatoria, lo que garantiza una seguridad sólida más allá de las contraseñas. El acceso debe protegerse mediante una combinación de contraseñas seguras y factores de autenticación secundarios (por ejemplo, basados en tokens, basados en SMS o biométricos).
- **Privilegios de usuario:** Los derechos de acceso a los sistemas y datos críticos deben seguir el principio de privilegio mínimo, lo que garantiza que los usuarios y los sistemas solo tengan acceso a los datos mínimos necesarios para sus tareas. Este acceso debe revisarse periódicamente, y los derechos de acceso deben revocarse de inmediato cuando ya no sean necesarios (por ejemplo, durante cambios de rol de empleado o terminaciones de contratos).

7.3. Protección de datos y privacidad

Los terceros están obligados a implementar medidas integrales y rigurosas de protección de datos y privacidad para garantizar la seguridad de la información confidencial. Esto incluye:

- **Cifrado de datos:** Los terceros deben aplicar el cifrado de extremo a extremo para todos los datos confidenciales (incluida la PII) tanto en reposo (en almacenamiento) como en tránsito (durante la transmisión). El cifrado debe cumplir con los estándares de la industria, como AES-256.

- **Enmascaramiento de datos y anonimización:** Cuando sea posible, los terceros deben utilizar técnicas de enmascaramiento de datos o anonimización para ofuscar los datos confidenciales durante el procesamiento o el análisis. Esto ayuda a minimizar la exposición durante las tareas de procesamiento de datos.
- **Localización y transferencias de datos:** Los terceros no deben almacenar ni procesar ningún dato de Carbonell Figueras fuera de la jurisdicción especificada sin el consentimiento explícito y previo por escrito de Carbonell Figueras. Cualquier transferencia de datos transfronteriza debe realizarse de conformidad con las normas de protección de datos, como el RGPD, y el Tercero debe asegurarse de que se implementen las salvaguardias adecuadas.
- **Retención y destrucción de datos:** Los datos de Carbonell Figueras solo deben conservarse durante el tiempo que sea necesario para cumplir con el contrato o los requisitos legales. Los terceros deben garantizar la destrucción segura de los datos cuando ya no sean necesarios, utilizando métodos de borrado de datos reconocidos.

7.4. Respuesta de gestión de incidentes

Se requiere que los terceros establezcan medidas integrales para detectar y responder a incidentes de seguridad que involucren los datos y sistemas de Carbonell Figueras. Esto implica:

- **Detección e informes de incidentes:** Los terceros deben crear y mantener un plan de respuesta a incidentes (IRP) para identificar, informar y mitigar rápidamente cualquier violación o incidente de seguridad. Este plan debe incorporar sistemas de monitoreo en tiempo real para detectar actividades sospechosas y posibles violaciones de datos. El IRP debe detallar los procedimientos para la detección de incidentes, la evaluación inicial, la contención, la erradicación, la recuperación y la presentación de informes.
- **Notificación de incidentes:** En caso de violación de seguridad o pérdida de datos, los terceros deben notificar a Carbonell Figueras de inmediato y, a más tardar, 24 horas después del descubrimiento del incidente. La notificación debe incluir:
    - Información detallada sobre la violación o incidente, incluidos los sistemas afectados, los datos y el alcance del incidente.
    - Acciones tomadas para contener y mitigar el incidente, incluidas las medidas inmediatas implementadas para evitar daños mayores.
    - Medidas que se están tomando para evitar que se repita el incidente, incluidos los planes de corrección a largo plazo y las mejoras de seguridad.
- **Análisis y corrección de la causa raíz:** Después de cada incidente, los terceros deben realizar un análisis exhaustivo de la causa raíz (RCA) para identificar las causas subyacentes del incidente. Deben proporcionar a Carbonell Figueras un informe completo que detalle los hallazgos de la RCA, las acciones tomadas para abordar el incidente y cualquier acción correctiva necesaria para evitar que ocurran en el futuro. Este informe debe incluir los plazos, las partes responsables y cualquier cambio en las políticas o procedimientos que se implementarán como resultado del incidente.

7.5. Recursos Humanos y seguridad

Los terceros deben implementar medidas integrales de recursos humanos y seguridad para garantizar que el personal que maneja los datos y sistemas de Carbonell Figueras sea confiable y esté adecuadamente capacitado. Esto incluye:

- **Verificaciones de antecedentes:** Los terceros deben asegurarse de que todos los empleados, contratistas y subcontratistas involucrados en el procesamiento de los datos de Carbonell Figueras se sometan a verificaciones de antecedentes exhaustivas, incluidas las de antecedentes penales y verificación de identidad. Estas comprobaciones deben realizarse antes de que el personal tenga acceso a información o sistemas confidenciales.
- **Capacitación y concienciación:** Los terceros deben proporcionar capacitación periódica y programas de concientización sobre seguridad para su personal para garantizar la comprensión de los requisitos de protección de datos, las prácticas seguras de manejo de datos y los procedimientos de notificación de incidentes. La capacitación debe llevarse a cabo en el momento de la contratación y, a partir de entonces, a intervalos regulares.
- **Políticas de seguridad para el personal:** Los terceros deben aplicar estrictas políticas de conducta de los empleados que aborden cuestiones como la seguridad de la información, la confidencialidad y la protección de datos. Todo el personal debe firmar acuerdos de confidencialidad antes de que se otorgue acceso a los datos confidenciales de Carbonell Figueras.

7.6. Continuidad del negocio y recuperación ante desastres

Todos los terceros deben garantizar la resiliencia y confiabilidad de los servicios, los terceros deben implementar medidas integrales de continuidad del negocio y recuperación ante desastres. Esto incluye:

- **Plan de Continuidad del Negocio (BCP):** Los terceros deben desarrollar y mantener un Plan de Continuidad del Negocio (BCP) para garantizar que los servicios permanezcan ininterrumpidos durante desastres o fallos del sistema. El BCP debe identificar las funciones críticas del negocio, esbozar estrategias para mantener las operaciones e incluir procedimientos para la comunicación, la asignación de recursos y la recuperación. Las pruebas y actualizaciones periódicas del BCP son esenciales para garantizar su eficacia.
- **Plan de recuperación ante desastres (DRP):** Los terceros deben implementar un plan de recuperación ante desastres (DRP) que detalle los pasos para restaurar datos y sistemas críticos después de una interrupción. El DRP debe incluir procedimientos para la recuperación de datos, la restauración del sistema y la reconstrucción de la infraestructura. También debe especificar las funciones y responsabilidades, los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO). Se deben realizar simulacros y simulaciones regulares para validar el DRP y garantizar la preparación.
- **Copia de seguridad y redundancia de datos:** Los terceros deben asegurarse de que los datos se respalden regularmente y se almacenen de forma segura en ubicaciones geográficamente separadas para evitar la pérdida de datos. Los procedimientos de copia de seguridad deben incluir copias de seguridad periódicas y automatizadas, almacenamiento seguro de los medios de copia de seguridad y pruebas periódicas de la integridad de la copia de seguridad. Se deben contar con sistemas e infraestructuras redundantes para proporcionar capacidades de conmutación por error y minimizar el tiempo de inactividad en caso de fallo del sistema.

7.7. Seguridad en la nube

Para garantizar la seguridad e integridad de los datos de Carbonell Figueras en entornos en la nube, los terceros deben implementar medidas sólidas de seguridad en la nube. Esto incluye:

- **Marco de seguridad en la nube:** Los terceros deben adherirse a los marcos de seguridad en la nube establecidos, como ISO 27017. Estos marcos proporcionan directrices completas para implementar controles de seguridad en entornos de nube, que abarcan aspectos como la protección de datos, la gestión del acceso y la respuesta a incidentes. El cumplimiento de estos marcos garantiza que los servicios en la nube cumplan con los estándares de la industria para la seguridad y la gestión de riesgos.

8. Finalización del contrato

La finalización de una relación contractual con un proveedor externo —ya sea por vencimiento, terminación anticipada o decisión unilateral— debe gestionarse de forma controlada para evitar riesgos de fuga de información, accesos indebidos o pérdida de activos.

Una vez concluido el vínculo contractual, se deberán ejecutar las siguientes acciones:

- **El proveedor deberá emitir un certificado de eliminación segura de los datos** proporcionados por Carbonell Figueras o generados durante la prestación del servicio. Esta destrucción debe realizarse conforme a métodos reconocidos (por ejemplo, sobreescritura segura, borrado criptográfico o destrucción física), y se aplicará tanto a soportes físicos como digitales.
- **Revocación de accesos**: Todos los accesos lógicos a sistemas, plataformas, bases de datos, VPN, herramientas colaborativas o servicios cloud, así como accesos físicos a instalaciones, deberán ser deshabilitados o eliminados por el área de IT o quien corresponda.
- **Devolución o recuperación de activos corporativos:** El proveedor debe devolver en perfecto estado todos los equipos, dispositivos, tokens, credenciales físicas o materiales entregados por Carbonell Figueras. La entrega se registrará formalmente y, de ser necesario, se verificará su integridad.
- **Cláusula de continuidad de obligaciones**: Las obligaciones contractuales relacionadas con confidencialidad, protección de datos y uso de información continuarán vigentes incluso tras la finalización del contrato.
- **Actualización del Registro de Proveedores**: La baja del proveedor deberá reflejarse en el registro, dejando constancia de la fecha de finalización, las acciones ejecutadas y cualquier documentación relacionada (actas, certificados, comprobantes).

Carbonell Figueras podrá realizar auditorías de salida para verificar que todas las obligaciones derivadas de la terminación han sido debidamente cumplidas.

9. Cumplimiento de la normativa

El incumplimiento de esta normativa podrá implicar sanciones contractuales, acciones disciplinarias o legales, según corresponda. El cumplimiento será verificado mediante auditorías, revisiones y controles de seguimiento.

10. Excepciones

Cualquier excepción a esta norma debe ser debidamente justificada, documentada y autorizada por el responsable de seguridad de Carbonell Figueras.