POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE GENERAL DE ALQUILER DE MAQUINARIA, S.A.

Fecha aprobación	28/07/2026
Órgano de aprobación	Consejo de Administración
Versión	Inicial (1.0)
Modificaciones	-

ÍNDICE

1. INTRODUCCIÓN

Este documento (en adelante, la "**Política**") recoge la política general de seguridad de la información aplicable a General de Alquiler de Maquinaria, S.A. ("**GAM**" o la "**Sociedad**") y su grupo consolidado (el "**Grupo GAM**").

De conformidad con lo establecido en el artículo 249 bis de la Ley de Sociedades de Capital (LSC) y en el artículo 5.1.a) del Reglamento del Consejo de Administración, corresponde a dicho órgano la aprobación de las políticas generales de la Sociedad. En ejercicio de dicha competencia, el Consejo de Administración de GAM adopta la presente Política con el fin de expresar el compromiso de la Sociedad y del Grupo GAM en el cumplimiento de la normativa aplicable y en el seguimiento de los estándares más exigentes en materia de seguridad de la información.

La Política se encuentra a disposición de los accionistas e inversores, empleados y demás grupos de interés en la página web de la Sociedad (www.gamrentals.com).

2. FINALIDAD DE LA POLÍTICA Y ALCANCE

Esta Política tiene como finalidad proporcionar un marco de principios generales aplicable al Grupo GAM para la implementación de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de aquella información propia y de terceros que se encuentre a disposición de la Sociedad y del Grupo GAM.

La presente Política tiene carácter obligatorio para todos los empleados del Grupo GAM, así como para el personal externo y los colaboradores que, en el ejercicio de sus funciones, accedan, gestionen o traten información, o utilicen los sistemas titularidad de la Sociedad o de cualquiera de las entidades que integran el Grupo GAM. A tal efecto, la Sociedad garantizará que esta Política se mantenga permanentemente disponible y accesible para todos los empleados, así como para el personal y colaboradores externos que interactúen con el Grupo GAM en el marco de cualquiera de sus procesos operativos, administrativos o de soporte.

El contenido de esta Política se somete a un proceso de revisión y actualización anual.

3. PRINCIPIOS GENERALES

Los principios que a continuación se recogen han sido definidos por el Consejo de Administración de la Sociedad en atención a la finalidad de esta Política y en línea con lo establecido en la legislación aplicable, las mejores prácticas de buen gobierno corporativo y la normativa interna de la Sociedad:

- Seguridad desde el diseño y por defecto: GAM declara su compromiso, desde la fase de diseño y establecimiento, con la operación, monitorización, mantenimiento, revisión y mejora continua de las medidas de seguridad de la información, con especial foco en la ciberseguridad dentro del Grupo GAM. En este sentido, se encomienda a la Dirección de Sistemas la definición de los objetivos y metas de la seguridad de la información, de cara a la protección de la confidencialidad, integridad y disponibilidad de esta.

- Legalidad, eficiencia, corresponsabilidad, cooperación y coordinación: La Sociedad y el Grupo GAM deberán cumplir con lo establecido en esta Política, con todos aquellos requerimientos legales, regulatorios y estatutarios que les sean de aplicación y con sus obligaciones contractuales. En particular, se garantizará el cumplimiento de la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

- Responsabilidad proactiva: GAM estará en disposición de acreditar el cumplimiento del Cuerpo Normativo de Seguridad, de forma que siempre existan evidencias suficientes para poder demostrar dicho cumplimiento.

- Prevención y mejora continua: GAM establece una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. En el transcurso de este ciclo de mejora continua, GAM mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

- Clasificación y minimización de la información: GAM clasifica la información para facilitar los procesos de control de acceso, custodia y monitorización. Según el nivel de clasificación, se establecen medidas y controles preventivos, siendo estos más restrictivos cuanto más sensible

se considere la información. La cantidad y el tipo de información compartida se restringirá al mínimo necesario para la finalidad para la que sea solicitada.

- Autenticidad y trazabilidad: La Sociedad garantizará que el origen y las identidades asociadas a la información sean verificables y que exista registro suficiente para determinar en todo momento quién accede a la información y qué actividad realiza sobre la misma, posibilitando el no repudio cuando proceda.

- Seguridad en la cadena de suministro: La Sociedad integrará requisitos y controles de seguridad en toda la cadena de suministro TIC, evaluando y monitorizando de forma continua a proveedores y subcontratistas críticos para asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los servicios externalizados.

- Limitación de acceso a la información, confidencialidad e integridad: Se limitará al máximo posible el acceso a la información, de manera que esta sea únicamente accesible para las personas debidamente autorizadas. La información será tratada y compartida garantizando su protección contra el acceso y uso no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

- Disponibilidad: La disponibilidad de la información deberá garantizarse mediante las medidas adecuadas de respaldo y continuidad de negocio.

- Formación y concienciación: El personal con responsabilidades en materia de seguridad de la información deberá disponer de la adecuada formación para ello. Asimismo, GAM realizará tareas de formación para concienciar a las personas de su equipo en el debido uso de la información y en el cumplimiento de las medidas de seguridad.

- Registro de incidentes: Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información deberá ser registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas.

- Cumplimiento de la legislación aplicable, recomendaciones de buen

gobierno y de la normativa interna de la Sociedad: La Sociedad velará porque se cumpla en todo momento con la legislación aplicable, las mejores prácticas de buen gobierno corporativo y la normativa interna de la Sociedad.

Los controles técnicos específicos en materia de seguridad de la información se desarrollan en los procedimientos internos que integran el Cuerpo Normativo de Seguridad, aprobados por la Dirección de Sistemas.

4. SUPERVISIÓN Y CONTROL DE LA POLÍTICA

La gestión e implementación de esta Política corresponde a la Dirección de Sistemas, a quien corresponderá asimismo la interpretación de las dudas que puedan surgir en su aplicación.

Por su parte, la Comisión de Auditoría y Control será el órgano competente para la supervisión periódica de la aplicación y el cumplimiento de esta Política, informando de todo ello al Consejo de Administración cuando corresponda y, en todo caso, con carácter anual.

La revisión de esta Política podrá efectuarse junto con la del resto de políticas corporativas de la Sociedad cuya supervisión corresponda a la Comisión de Auditoría y Control en un único informe anual de supervisión de políticas corporativas.

5. APROBACIÓN Y APLICACIÓN DE LA POLÍTICA

Esta Política es de aplicación desde el momento de su aprobación por el Consejo de Administración el día 28 de julio de 2026 a todo el Grupo GAM.

No obstante lo anterior, el Consejo de Administración podrá acordar la modificación de esta Política en cualquier momento durante su vigencia cuando lo considere necesario, para adecuarla a la realidad legal, social o económica de cada momento.

****