



Política de Seguridad de la Información

Versión: 0.0

Clasificación: Uso Interno

Aprobado por: Dirección General

Fecha de entrada en vigor: 26 /05 /2026

Versión	Fecha	Descripción de los cambios	Elaborado por	Revisado por	Aprobado por
0.0	26/05/2026	Emisión inicial del documento	Responsable Seguridad	Comité de Seguridad	Dirección MOTUM

Confidencialidad

Documento de uso interno propiedad de **MOTUM Technologies**, S.L. Su reproducción, modificación o comunicación a terceros requiere autorización, salvo obligación legal o contractual.

1. APROBACIÓN Y ENTRADA EN VIGOR	2
2. INTRODUCCIÓN	2
3. ALCANCE	2
4. MISIÓN	3
5. PRINCIPIOS RECTORES DE LA POLÍTICA	3
6. MARCO NORMATIVO	4
7. ORGANIZACIÓN DE LA SEGURIDAD: FUNCIONES Y RESPONSABILIDADES	5
8. PROCEDIMIENTO DE DESIGNACIÓN	8
9. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	8
10. TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD	8
11. GESTIÓN DE RIESGOS	9
12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	9
13. OBLIGACIONES DEL PERSONAL	9
14. TERCERAS PARTES / PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES	10
15. GESTIÓN DE INCIDENTES DE SEGURIDAD	10
16. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR	10

1. APROBACIÓN Y ENTRADA EN VIGOR

El presente texto fue aprobado el día 26 de mayo de 2026 por la Dirección de MOTUM Technologies, S.L.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

MOTUM Technologies, S.L. (en adelante, MOTUM Technologies), consciente de que la información manejada es un recurso con gran valor, ha establecido un Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con los requisitos establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el cumplimiento de los objetivos fijados.

El objetivo de disponer de un Sistema de Seguridad de la Información es garantizar la calidad de la información y la continuidad de los servicios prestados, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

El objetivo de la Política de Seguridad de la Información es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales, que puedan afectar a los sistemas de información necesarios para la prestación de los servicios, a la información de los clientes gestionada por MOTUM Technologies o a la información propia considerada como confidencial.

Para ello, deberán identificarse los riesgos que puedan afectar a los elementos que constituyen los sistemas que dan soporte a la actividad de MOTUM Technologies y que puedan comprometer la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas o información. Para cada riesgo identificado deberá determinarse la probabilidad de que se manifieste la amenaza, el nivel de vulnerabilidad de la organización frente a ésta, y el impacto que tendría su materialización.

Esta Política proporciona el marco de referencia para la mejora continua del SGSI y será de obligatorio cumplimiento para todo el personal participante en la prestación de los servicios ofrecidos por MOTUM Technologies y todo aquel que pueda acceder a los recursos de información relacionados con éstos.

3. ALCANCE

El alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) de MOTUM Technologies comprende los procesos, servicios, infraestructuras tecnológicas y personal que dan soporte a las actividades de consultoría IT, desarrollo y mantenimiento de software (ERP), firma electrónica, digitalización de procesos de negocio, integración tecnológica e identidad digital, dirigidos a clientes del sector público y privado.

El ámbito de aplicación se extiende a todos los miembros de MOTUM Technologies determinados dentro del alcance, así como a todo el personal contratado, subcontratado, colaboradores y demás personas físicas y jurídicas que actúen de forma autorizada en nombre o por cuenta de la organización.

Toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión está obligada al cumplimiento estricto de la Política de Seguridad.

4. MISIÓN

4.1. Presentación de la empresa y sus servicios

MOTUM Technologies, S.L. es una empresa de ingeniería tecnológica con sede en Sant Feliu de Llobregat (Barcelona), fundada en 2018. Opera en el sector de las tecnologías de la información prestando servicios de consultoría IT, desarrollo de software a medida, firma electrónica, digitalización de procesos empresariales e identidad digital, dirigidos tanto a clientes del sector público como privado.

La Dirección General establece y documenta el SGSI conforme al Real Decreto 311/2022 (ENS), con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y protegerla de los riesgos derivados del amplio grupo de amenazas existentes.

4.2. Objetivos en materia de seguridad

Los objetivos en materia de seguridad que MOTUM Technologies pretende garantizar con la presente Política son:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y la continuidad en la prestación de los servicios.
- Identificar y evaluar los riesgos que afectan a los sistemas de información, implementando medidas de seguridad proporcionales al riesgo.
- Formar y concienciar a los integrantes de MOTUM Technologies respecto a la seguridad de la información.
- Implementar medidas de seguridad que permitan la trazabilidad de los accesos, respetando el principio de mínimo privilegio y el deber de confidencialidad.
- Garantizar la seguridad física de los activos de información en áreas protegidas y con controles de acceso adecuados.
- Proteger la información personal adoptando las medidas técnicas y organizativas necesarias conforme a la legislación en materia de protección de datos.
- Gestionar adecuadamente los incidentes de seguridad para su detección, contención, mitigación y resolución.
- Supervisar de forma continuada el SGSI, mejorando y corrigiendo las ineficiencias detectadas.

5. PRINCIPIOS RECTORES DE LA POLÍTICA

De conformidad con el artículo 5 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, la presente Política se basa en los siguientes principios rectores:

5.1. Alcance estratégico

La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente. La Dirección de MOTUM Technologies apoya activamente la implantación y el mantenimiento del SGSI.

5.2. Seguridad integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

5.3. Gestión de la seguridad basada en el riesgo

La gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas, serán proporcionales al riesgo que tratan y deberán estar justificadas. El Comité de Seguridad se compromete a establecer medidas que traten de reducir el nivel de riesgos de aquellos elementos del sistema que se sitúen por encima del nivel MEDIO o superior.

5.4. Prevención, detección, respuesta y conservación

MOTUM Technologies implementa acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas y evitando la materialización de las amenazas. Cuando estas se produzcan, se dará una respuesta ágil para restaurar la información o los servicios prestados, garantizando una conservación segura de la información.

5.5. Existencia de líneas de defensa

La estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad. Ninguna medida de seguridad se considera suficiente por sí sola; las distintas capas actúan de forma complementaria para garantizar la protección integral del sistema.

5.6. Vigilancia continua y reevaluación periódica

MOTUM Technologies implementa medios de detección y respuesta a actividades o comportamientos anómalos. Existirá un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

5.7. Seguridad por defecto y desde el diseño

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

5.8. Diferenciación de responsabilidades

Las funciones del Responsable de la Seguridad y del Responsable del Sistema están diferenciadas y son desempeñadas por personas distintas, garantizando la segregación de funciones requerida por el ENS.

6. MARCO NORMATIVO

El Sistema de Gestión de la Seguridad de la Información implantado en MOTUM Technologies debe dar respuesta a los requisitos establecidos en la legislación vigente aplicable a la actividad de la entidad, que tiene como referentes principales:

- REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley Orgánica 3/2018 (LOPDGDD): adapta el RGPD al ordenamiento jurídico español y regula derechos digitales y aspectos específicos del tratamiento de datos.
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad (Reglamento sobre la Ciberseguridad).

- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, estableciendo los principios y requisitos mínimos que deben cumplir los sistemas de información del sector público y de las entidades que se relacionan con él.

Asimismo, se tendrán en cuenta los requisitos de seguridad establecidos por clientes, proveedores y otras partes interesadas, siempre que hayan sido previamente analizados y aceptados por MOTUM Technologies.

La organización mantendrá un registro actualizado de los requisitos legales, regulatorios y contractuales aplicables, asegurando su revisión periódica y su adecuada integración en el sistema de gestión.

La Política de Seguridad de la Información estará a disposición de todos los miembros de la organización a través de la intranet corporativa.

7. ORGANIZACIÓN DE LA SEGURIDAD: FUNCIONES Y RESPONSABILIDADES

La implantación de la Política de Seguridad en MOTUM Technologies requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Los roles de seguridad definidos son los siguientes:

Rol	Descripción
Comité de Seguridad	Órgano de coordinación, asesoramiento y decisión en materia de seguridad para garantizar el cumplimiento normativo.
Responsable de Seguridad	Supervisión y verificación del cumplimiento de los requisitos del ENS.
Responsable del Sistema	Operación, mantenimiento y supervisión técnica de los sistemas de información.
Responsable del Servicio	Gobernanza, requisitos del servicio, continuidad y niveles de servicio.
Responsable de la Información	Gobernanza, custodia, clasificación y validación de la información del SGSI.
Delegado de Protección de Datos (DPD)	Supervisión del cumplimiento del RGPD y la LOPDGDD.

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles:

7.1. Comité de Seguridad

El Comité de Seguridad es el órgano responsable de la definición, supervisión y mejora continua de la seguridad de la información. La eficacia y aplicación del Sistema de Gestión es responsabilidad directa del Comité de Dirección, que ha delegado en el Comité de Seguridad la suficiente autoridad para desempeñar un papel activo en el SGSI. Sus funciones son:

- Actualización y revisión de la Política de Seguridad y de las responsabilidades principales, antes de su aprobación final por la Dirección.

- Definir e impulsar la estrategia y la planificación de la seguridad, proponiendo la asignación de presupuesto y recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de la información a las amenazas principales, así como del desarrollo e implantación de controles destinados a garantizar la seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la seguridad.
- Supervisión y seguimiento de las principales incidencias en la Seguridad de la Información, elaboración y actualización de planes de continuidad, y cumplimiento y difusión de la Política de Seguridad.

El Comité de Seguridad se reunirá con la periodicidad que se determine internamente y, en todo caso, cuando se produzcan incidentes graves o situaciones que así lo requieran.

7.2. Responsable de Seguridad

El Responsable de Seguridad es el rol encargado de la definición, supervisión y verificación del cumplimiento de los requisitos de seguridad de la información, de conformidad con el artículo 11 del Real Decreto 311/2022 (ENS). Sus funciones son:

- Establecer los requisitos en materia de seguridad de la información gestionada y los servicios prestados.
- Determinar los requisitos de seguridad aplicables y velar por su cumplimiento.
- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de la estrategia de seguridad y de las normas y procedimientos contenidos en la Política de Seguridad.
- Supervisar los incidentes de seguridad producidos.
- Difundir las normas y procedimientos contenidos en la Política de Seguridad de la Información, así como las funciones y obligaciones en materia de seguridad.
- Supervisar y colaborar en las auditorías internas y externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas.

7.3. Responsable del Sistema

El Responsable del Sistema es el rol encargado de la operación, mantenimiento y supervisión técnica de los sistemas de información, de conformidad con el artículo 12 del Real Decreto 311/2022 (ENS). Sus funciones son:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, desde sus especificaciones hasta la verificación de su correcto funcionamiento.
- Definir la topología y el sistema de gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles.
- Cerciorarse de que las medidas específicas de seguridad se integran adecuadamente dentro del marco general de seguridad definido por el Responsable de Seguridad.
- Seleccionar y establecer las funciones y obligaciones de los técnicos encargados de la gestión de la seguridad de los activos, conforme a la estrategia definida por el Responsable de Seguridad.
- Garantizar que la implantación de nuevos sistemas y los cambios en los existentes cumplen los requerimientos de seguridad establecidos.
- Establecer los procesos y controles de monitorización que permitan detectar incidencias y coordinar su investigación y resolución, informando al Responsable de Seguridad.
- Proponer la suspensión del manejo de información o de la prestación de servicios cuando se detecten deficiencias graves de seguridad, previa coordinación con el Responsable de Seguridad y los Responsables de la Información y del Servicio afectados.

7.4. Responsable del Servicio

El Responsable del Servicio es el rol encargado de determinar los requisitos del servicio, garantizar su disponibilidad y calidad, y velar por la continuidad de la actividad de MOTUM Technologies, de conformidad con el artículo 11 del Real Decreto 311/2022 (ENS). Sus funciones son:

- Determinar los requisitos del servicio prestado por MOTUM Technologies en materia de disponibilidad, continuidad y niveles de servicio (SLA), trasladando dichos requisitos al Responsable de Seguridad y al Responsable del Sistema.
- Elaborar, mantener actualizado y supervisar el BIA (Análisis de Impacto en el Negocio), asegurando que los tiempos de recuperación (RTO) y los puntos de recuperación (RPO) se ajustan a las necesidades del servicio.
- Participar en la gestión de incidentes que afecten a la disponibilidad o continuidad del servicio, coordinando las acciones de respuesta y recuperación.
- Aceptar o rechazar los riesgos residuales del servicio, previo informe del Responsable de Seguridad, elevando al Comité de Seguridad aquellos riesgos que superen el umbral definido.
- Aprobar los acuerdos de nivel de servicio con proveedores y terceras partes, verificando que incluyen las cláusulas de seguridad exigidas.

7.5. Responsable de la Información

El Responsable de la Información tiene como función principal revisar, validar y dar seguimiento a los elementos del SGSI elaborados por el Responsable de Seguridad, velando por su conformidad con los requisitos del ENS y el sistema de gestión de la organización. Sus funciones son:

- Establecer los requisitos en materia de seguridad de la información gestionada.
- Determinar los niveles de seguridad de la información (asesorado por el Responsable de Seguridad).
- Revisar y validar la documentación elaborada en el marco del SGSI (políticas, procedimientos, controles, informes), comprobando su coherencia y adecuación normativa.
- Verificar que los requisitos definidos en la Declaración de Aplicabilidad (SoA) se aplican correctamente y se reflejan en los procedimientos y controles implantados.
- Validar los informes de resultados de auditorías internas, análisis de riesgos y revisiones por la dirección.
- Informar al Comité de Seguridad sobre el estado de revisión del SGSI y la conformidad global del sistema con los requisitos normativos.

7.6. Delegado de Protección de Datos (DPD)

El Delegado de Protección de Datos (DPD) es el rol responsable de supervisar el cumplimiento del RGPD y la LOPDGDD. Conforme al artículo 38 del RGPD, el DPD actúa con independencia funcional del responsable de seguridad y no puede recibir instrucciones respecto al ejercicio de sus funciones. Sus funciones son:

- Informar y asesorar a MOTUM Technologies y a sus empleados sobre las obligaciones que les incumben en virtud del RGPD y demás normativa de protección de datos aplicable.
- Supervisar el cumplimiento del RGPD, la LOPDGDD y las políticas internas de protección de datos.
- Mantener actualizado el Registro de Actividades de Tratamiento (RAT).
- Gestionar y coordinar la respuesta ante brechas de seguridad que afecten a datos personales, asegurando la notificación a la AEPD en los plazos legalmente establecidos (72 horas) cuando proceda.
- Actuar como punto de contacto con la AEPD y con los interesados en el ejercicio de sus derechos (acceso, rectificación, supresión, portabilidad, oposición y limitación del tratamiento).
- Asesorar en la realización de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD/DPIA).

8. PROCEDIMIENTO DE DESIGNACIÓN

La designación del Responsable de Seguridad, del Responsable del Sistema, del Responsable del Servicio, del Delegado de Protección de Datos (DPD) y del Responsable de la Información será realizada por la Dirección de MOTUM Technologies o por los órganos en quienes esta delegue.

En ningún caso una misma persona podrá ostentar simultáneamente los roles de Responsable de Seguridad y Responsable del Sistema, ni los de Responsable de Seguridad y Delegado de Protección de Datos, al objeto de garantizar la segregación de funciones exigida por el ENS y el RGPD.

Dichas designaciones deberán recaer en personas con la cualificación y experiencia adecuadas para el desempeño de sus funciones. Las designaciones se revisarán periódicamente, al menos cada dos años o cuando se produzcan cambios organizativos relevantes o vacantes en los puestos.

Se garantizará la continuidad de las funciones mediante la designación de sustitutos o mecanismos equivalentes en caso de ausencia, cese o imposibilidad de desempeño de las funciones asignadas. Los nombramientos serán realizados por la Dirección a propuesta del Comité de Seguridad.

La estructura del comité y las designaciones de los roles de seguridad se encuentran formalizadas en las actas de constitución y designación de roles del SGSI, donde se identifican las personas asignadas a cada rol, sus responsabilidades y la fecha de designación.

9. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de Seguridad de la Información será revisada y, en su caso, actualizada al menos una vez al año, o cuando se produzcan cambios significativos en la organización, en los sistemas de información o en el marco normativo aplicable.

La revisión de la Política será responsabilidad del Comité de Seguridad, que propondrá, en su caso, las modificaciones oportunas para su aprobación final por la Dirección de MOTUM Technologies.

Una vez aprobada, la Política será comunicada a todo el personal y a aquellas terceras partes a las que resulte de aplicación, garantizando su adecuada difusión a través de la intranet corporativa, quedando registro de dicha comunicación.

10. TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD

En aplicación del principio de responsabilidad proactiva establecido en el RGPD, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

El tratamiento de los datos personales deberá realizarse de acuerdo con la normativa vigente en materia de protección de datos, garantizando en todo momento su confidencialidad, integridad y disponibilidad. Se adoptarán las medidas técnicas y organizativas necesarias para asegurar la protección de los datos personales, teniendo en cuenta la naturaleza de los datos, el contexto del tratamiento y los riesgos asociados.

En caso de producirse incidentes de seguridad que afecten a datos personales, estos deberán ser gestionados conforme a los procedimientos establecidos, garantizando su adecuada evaluación, registro y, en su caso, notificación a la AEPD y a los interesados cuando proceda.

MOTUM Technologies evaluará los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado, con el asesoramiento y supervisión del Delegado de Protección de Datos.

11. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos.

La gestión de riesgos quedará documentada en el ANÁLISIS DE RIESGOS POR ACTIVOS.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información se desarrollará por medio de normativa de seguridad, y se complementa e integra junto con otras políticas de MOTUM Technologies en diferentes materias, como el Código Telemático y la Política de Protección de Datos.

Las políticas estarán disponibles en la intranet corporativa para todos los miembros de la organización que necesiten conocerla, y en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

13. OBLIGACIONES DEL PERSONAL

Todos y cada uno de los usuarios de los sistemas de información son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales.

Todo el personal de MOTUM Technologies tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad relacionada, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de MOTUM Technologies atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, de acuerdo con la normativa interna aplicable, sin perjuicio de las responsabilidades legales correspondientes.

14. TERCERAS PARTES / PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando MOTUM Technologies preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. El Responsable de Seguridad actuará como punto de contacto.

Cuando MOTUM Technologies utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política y de la Normativa de Seguridad que atañe a dichos servicios o información. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la Información y los Responsables de los servicios afectados, antes de seguir adelante.

15. GESTIÓN DE INCIDENTES DE SEGURIDAD

MOTUM Technologies dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales, como la de protección de datos personales, para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad del Estado o los juzgados.

16. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisar anualmente. En caso de que los cambios supongan una modificación sustancial de los principios o responsabilidades asignadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados por la Dirección de MOTUM Technologies.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la Dirección de MOTUM Technologies, de lo que se informará adecuadamente a los interesados a través de la intranet corporativa.

Sant Feliu de Llobregat, 26 de mayo de 2026

Director General MOTUM Technologies, S.L. _____	Responsable de Seguridad MOTUM Technologies, S.L. _____	Responsable del Sistema MOTUM Technologies, S.L. _____
--	--	---