



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Microsystem S.A.

Actualizado por: Jorge Armijo CISO	Revisado por: Jorge Armijo CISO	Aprobado por: Nicolás Andalaft González Gerente General Grupo Microsystem
--	---------------------------------------	--

SG-DG-PSI-013

ÍNDICE

1. INTRODUCCIÓN	3
2. PRINCIPIOS	3
3. COMPROMISO DE LA DIRECCIÓN	4
4. ROLES Y RESPONSABILIDADES	5
5. CUMPLIMIENTO DE NORMATIVA APLICABLE	9
6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE MICROSYSTEM	9
7. SANCIONES	11
8. CONTROL DE CAMBIOS	12

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

1. INTRODUCCIÓN

La Política de Seguridad de la Información de Microsystem tiene como finalidad adoptar una serie de medidas para preservar la confidencialidad, integridad y disponibilidad de la información, como componentes básicos y fundamentales de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001. Su objetivo principal es establecer los requisitos aplicables para la protección de la información que se almacena y procesa en sus equipos, servidores, plataformas de soporte y en sus dependencias, tanto de los clientes como propios de la organización que son utilizados para brindar la mayoría de sus procesos de negocio. La presente política representa el componente primordial del conjunto de documentos que conforman el SGSI de Microsystem.

Microsystem establece que la presente política es aplicable para todos los miembros de la organización que se encuentran ejecutando labores que se vean directa o indirectamente relacionadas con los Sistema de Protección de la Información propia y la de los clientes que se genera y se procesa como parte de la prestación de los servicios de Software as a Service y Servicios de Desarrollo de Software, además de los documentos físicos propios y de nuestros clientes que se custodian en bodegas administradas por el área KeeperBox.

2. PRINCIPIOS

La presente política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional de la Norma ISO 27001, así como al cumplimiento de la legislación chilena vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a la operación de Microsystem. Para lo anterior se establecen los siguientes principios básicos como directrices fundamentales de seguridad de la información para la operación diaria:

- ❖ Contar con el compromiso y apoyo de todos los niveles directivos de Microsystem con el objetivo de actuar de forma coordinada e integrada con la dirección estratégica de la organización.
- ❖ Integrar como un solo cuerpo los elementos fundamentales (técnicos, humanos, materiales, entre otros) para resguardar la seguridad de la información, evitando las

Fecha de impresión 03-06-2026	Página 3 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

amenazas críticas que obstaculicen la continuidad operacional diaria, dentro de los parámetros permitidos por las normativas, legislaciones, acuerdos contractuales, entre otros, que apliquen en su actuar.

- ❖ El análisis y gestión de riesgos en forma oportuna, eficiente y eficaz, son la pieza clave que permite el control de los riesgos manteniéndolos en niveles aceptables, reduciendo la posibilidad de eventos críticos. Las medidas para la protección, detección y recuperación deben ser proporcionales a los potenciales riesgos detectados y al nivel de criticidad y valor de la información y procesos afectados por ellos.
- ❖ Se planificarán, ejecutarán y controlarán medidas de seguimiento periódicos al SGSI tanto por personal interno como externo calificado, obteniendo retroalimentación de nuestras operaciones, que nos permiten mejorar continuamente la eficacia y eficiencia de nuestro sistema de gestión de seguridad de la información.
- ❖ Los sistemas deben diseñarse y configurarse con altas medidas de seguridad, con el objetivo de garantizar una seguridad por defecto acorde a las necesidades de las partes interesadas. Dada la importancia de este sistema, la presente política debe ser conocida, comprendida y cumplida por todos los miembros de la organización que son cubiertos con el alcance antes mencionado.

3. COMPROMISO DE LA DIRECCIÓN

La alta dirección de Microsystem, demuestra su liderazgo y compromiso con la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- ❖ Asegurarse de que se establezca la política y objetivos para el SGSI, siendo compatibles con el contexto y la dirección estratégica de la organización.
- ❖ Asegurar la integración de los requisitos del SGSI en los procesos de la organización.
- ❖ Asegurarse de que estén disponibles los recursos necesarios para el SGSI

Fecha de impresión 03-06-2026	Página 4 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

- ❖ Comunicar la importancia de una gestión de seguridad de la información eficaz y conforme con los requisitos del SGSI
- ❖ Asegurarse de que el SGSI logre los resultados previstos
- ❖ Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI
- ❖ Promover la mejora continua
- ❖ Apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo en la forma en la que aplique a sus áreas de responsabilidad

4. ROLES Y RESPONSABILIDADES

Con el objetivo de velar por el cumplimiento de la presente política y las medidas y controles establecidos en el SGSI, la Gerencia General dispone la conformación del Comité de Seguridad, el cual tiene como finalidad coordinar todas las acciones que se deben desarrollar en la aplicación de la norma y que verifica el cumplimiento de los procedimientos que se definan para ello.

El Comité de Seguridad debe ser informado por todas aquellas personas que desarrollen, administren o pongan en producción servicios, de cualquier modificación significativa a considerar en los mismos, a fin de que pueda verificar que se ajustan a las normas establecidas.

Las principales funciones del Comité de Seguridad son:

- ❖ Revisar y proponer al Gerente General del Grupo Microsystem, para su aprobación, la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- ❖ Revisar y establecer los requisitos de seguridad que se deben cumplir a nivel organizativo, de control de los sistemas y servicios, de disponibilidad y otros que permitan alcanzar los objetivos de seguridad identificados.
- ❖ Revisar y aprobar la Política de Seguridad de la Información, asegurando que se mantengan alineados con los objetivos de seguridad definidos y con la estrategia general del negocio.

Fecha de impresión 03-06-2026	Página 5 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

- ❖ Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- ❖ Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- ❖ Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
- ❖ Garantizar que la seguridad sea parte del proceso de planificación de la información.
- ❖ Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- ❖ Promover la difusión y apoyo a la seguridad de la información dentro de Microsystem y coordinar el proceso de administración de la continuidad de las actividades de la empresa.
- ❖ Definir sanciones adecuadas en el caso de que se vulnere las políticas definidas por la organización según la regulación de la empresa y la legislación vigente.
- ❖ Mantener contactos periódicos con grupos, otras entidades, foros etc. que resulten de interés en el ámbito de la seguridad compartiendo experiencias y conocimiento que ayuden a mejorar y mantener su seguridad
- ❖ Dado que los directores de la organización son integrantes del comité de seguridad es su obligación asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
- ❖ Designar responsables respecto de la Seguridad de la Información, en caso de que un miembro del comité esté imposibilitado de ejercer su rol; o bien delegar responsabilidades para trabajos específicos de la autoridad certificadora (AC).
- ❖ El comité de seguridad se debe pronunciar al menos una vez al año para aprobar, definir

Fecha de impresión 03-06-2026	Página 6 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

o aceptar temas relevantes levantados por el oficial de seguridad.

El comité de seguridad estará compuesto por

❖ **Gerente General del grupo Microsystem y Representante de la Dirección.**

Proporcionar dirección estratégica y liderazgo en lo que respecta a la seguridad de la información en toda la organización. Aprobar las políticas y estrategias de seguridad de la información propuestas por el Comité o el Oficial de Seguridad, asegurándose de que estén alineadas con los valores y las metas de Microsystem.

Proporcionar los recursos necesarios, tanto financieros como humanos, para implementar y mantener el programa de seguridad de la información de manera efectiva. Participar en la evaluación y gestión de riesgos relacionados con la seguridad de la información, tomando decisiones informadas sobre la aceptación, mitigación o transferencia de riesgos.

❖ **Ejecutiva Experiencia Cliente.** Asegurar que las políticas y procedimientos de seguridad de la información sean comunicados eficazmente a los clientes y usuarios finales.

Recabar los comentarios y preocupaciones de los clientes sobre la seguridad de la información, ayudando a identificar áreas de mejora o nuevos riesgos que deben abordarse dentro del comité de seguridad de la información.

❖ **Oficial de Seguridad de la Información (CISO).** Debe coordinar las decisiones del Comité de Seguridad de la Información, desarrollar y ejecutar estrategias integrales de seguridad de la información para proteger los activos y datos de la organización contra amenazas internas y externas.

Debe contribuir en la identificación, evaluación y gestión de riesgos de seguridad de la información, y trabajar para implementar controles adecuados para mitigar estos riesgos.

Debe establecer políticas, procedimientos y estándares de seguridad de la información en toda la organización, asegurándose de que cumplan con las regulaciones y normativas aplicables.

Coordinar la respuesta a incidentes de seguridad, investigando y gestionando las brechas

Fecha de impresión 03-06-2026	Página 7 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

de seguridad cuando ocurren, y tomando medidas correctivas para evitar que se repitan.

Promover la concientización sobre seguridad de la información a los colaboradores.

Proporcionar información sobre el estado de la seguridad de la información, incluyendo riesgos identificados, incidentes de seguridad, cumplimiento normativo y eficacia de los controles.

- ❖ **Gerente General de Microsystem.** Fomentar una cultura de seguridad de la información en toda la organización, destacando la importancia de la seguridad y el cumplimiento de las políticas, procedimientos establecidos, obligaciones legales y regulatorias en este ámbito.

Debe proporcionar los recursos necesarios, tanto financieros como humanos, para implementar y mantener el programa de seguridad de la información de manera efectiva. Participar en la evaluación y gestión de riesgos relacionados con la seguridad de la información, tomando decisiones informadas sobre la aceptación, mitigación o transferencia de riesgos.

- ❖ **Gerente OPTI.** Velar por la seguridad de sus procesos conforme a los riesgos analizados. Efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases de su ciclo de vida. Además, debe garantizar el cumplimiento de las políticas, procedimientos y normativas de seguridad aplicables a dichos procesos.

- ❖ **Gerente MicroEdoc.** Garantizar la seguridad de los procesos de acuerdo con los riesgos evaluados para la autoridad certificadora. Asimismo, debe llevar a cabo las labores de desarrollo y mantenimiento para la AC, siguiendo una metodología de ciclo de vida de sistemas adecuada que incorpore medidas de seguridad en todas las etapas del proceso. Adicionalmente, debe asegurar el cumplimiento de la Ley 19.799, políticas, procedimientos y normativas de seguridad pertinentes para dichos procesos.

- ❖ **Encargado del SGC.** Asegurar que las iniciativas de seguridad se encuentren alineadas con las de calidad. Contribuye en la toma de decisiones asegurando la sostenibilidad y

Fecha de impresión 03-06-2026	Página 8 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

eficacia del SGI. Además, facilita la comunicación entre los equipos de calidad y seguridad de la información, promoviendo una cultura organizacional que valore tanto la calidad del servicio como la protección de la información. Su participación activa en el Comité de Seguridad de la Información es esencial para identificar sinergias, evitar redundancias y asegurar que el SGI funcione como un sistema cohesivo que cumple con los requisitos de ambas normas.

5. CUMPLIMIENTO DE NORMATIVA APLICABLE

La presente Política de Seguridad se ajusta dentro del marco legal vigente, utilizando como referencia los siguientes requisitos regulatorios:

- ❖ Decreto 142 de 2015. de la SUBTEL aplicable a la Ciberseguridad (<https://www.leychile.cl>)
- ❖ Ley N° 21.459 Establece norma sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objetivo de adecuar al convenio de Budapest
- ❖ Ley 17.336 Ley de propiedad intelectual
- ❖ Ley 19.628: Protección de la Vida Privada
- ❖ Ley 19.799: Ley sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma
- ❖ Ley 21.719: Ley regula la protección y el tratamientos de los datos personales
- ❖ Ley 21.663: Ley Marco de Ciberseguridad.

Además, estará alineada a los siguientes estándares:

- ❖ Norma ISO 9001
- ❖ Norma ISO 27001
- ❖ Norma ISO 27701

Fecha de impresión 03-06-2026	Página 9 de 13
-------------------------------	----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE MICROSYSTEM

Microsystem establece por medio del Sistema de Gestión de Seguridad de la Información (SGSI) las siguientes políticas de seguridad de la información que todos los miembros deben cumplir en función del puesto que desempeñan y su nivel de acceso a la información. Estas políticas están alineadas con la norma ISO 27001 (versión vigente) y las regulaciones aplicables:

1. **Protocolo de dispositivos:** Siguiendo la norma **TI-NOR-NUA Normativa Uso Aceptable de Activos**, todos los dispositivos personales utilizados para acceder a los sistemas y datos de la empresa deben cumplir con los estándares de seguridad establecidos. Esto incluye, pero no se limita a el uso de software antivirus actualizado, contraseñas seguras y la activación de cifrado en el dispositivo.
2. **Normas para la gestión y clasificación de activos de información:** Los activos de información deben ser clasificados de acuerdo a su nivel de sensibilidad y criticidad, en base al procedimiento **TI-PR-CINF Clasificación de la Información**. Se deben establecer controles adecuados para proteger estos activos según su clasificación (e.j., información pública, interna, confidencial y restringida).
3. **Normas para la gestión y control de accesos:** El acceso a los sistemas y datos de la empresa debe ser controlado mediante mecanismos de autenticación y autorización, basándose en el **TI-PR-CAC Control de Acceso**. Solo el personal autorizado debe tener acceso a la información según su rol y responsabilidad.
4. **Normas para la gestión de riesgos:** La gestión de riesgos debe ser un proceso continuo que incluye la identificación, evaluación y tratamiento de los riesgos de seguridad de la información, siguiendo los pasos del documento **SG-PR-GAR Gestión y Análisis de Riesgo**. Las medidas de protección, detección y recuperación deben ser proporcionales a los riesgos identificados.

Fecha de impresión 03-06-2026	Página 10 de 13
-------------------------------	-----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

5. **Protocolo para la gestión de incidentes de seguridad:** Los incidentes de seguridad deben ser reportados, registrados y gestionados de acuerdo con el procedimiento **TI-PR-II Incidencias Internas**. Esto incluye la identificación de la causa raíz, la contención del incidente y la implementación de acciones correctivas y preventivas.
6. **Normas para la gestión del ciclo de vida de la información:** La información debe ser gestionada de manera segura durante todo su ciclo de vida, desde su creación hasta su eliminación, en base al documento **TI-PR-IPTI Implementación Proyectos TI**. Esto incluye el almacenamiento seguro, la transmisión protegida y la disposición final segura de la información.
7. **Protocolo de copias de seguridad:** Las copias de seguridad deben realizarse regularmente y almacenarse de manera segura (**TI-PR-RESP Procedimiento de Respaldo**). Se deben realizar pruebas periódicas de restauración para asegurar la disponibilidad de la información en caso de pérdida o corrupción de datos.
8. **Normas sobre gestión de la privacidad de la información:** La información personal debe ser gestionada de acuerdo con las leyes de protección de datos aplicables. Se deben implementar medidas para asegurar que la información personal se maneje de manera confidencial y se proteja contra accesos no autorizados.
9. **Normas para la prevención de fuga de información:** Se deben implementar controles para prevenir la fuga de información, incluyendo la monitorización de sistemas, la protección contra el malware y la sensibilización de los empleados sobre la importancia de la seguridad de la información (**CS-PR-PFD Prevención de Fuga de Datos**).
10. **Normas para el teletrabajo:** Los empleados que trabajen de manera remota deben seguir las políticas de seguridad de la información de la empresa. Esto incluye el uso de redes seguras, dispositivos autorizados y la protección de la información contra accesos no autorizados (**TI-NOR-NUA Normativa Uso Aceptable de Activos**).
11. **Realización de auditorías y mejora continua del SGSI:** El SGSI debe ser auditado regularmente para asegurar su eficacia y cumplimiento con la norma ISO 27001. Se deben

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

implementar acciones de mejora continua basadas en los resultados de las auditorías y el monitoreo de la seguridad de la información (**SG-PR-AI Procedimiento Auditoría interna**).

7. SANCIONES

Microsystem establece que en caso de incumplir la presente política y las normativas y procedimientos que la acompañan, la organización tiene la libertad de aplicar procesos disciplinarios adecuados como corrección y de forma alineada con el reglamento interno. Este proceso puede ser desde un llamado de atención, anotación a la hoja de vida del trabajador, carta a la dirección del trabajo, hasta la desvinculación inmediata del trabajador, según la gravedad del incumplimiento.

La gravedad de dicho incumplimiento debe ser analizada por el Comité de Seguridad, en conjunto con la jefatura directa y el área de Recursos Humanos, para validar su gravedad y no incumplir en otras normativas legales laborales.

8. CONTROL DE CAMBIOS

Versión	Fecha	Responsable	Modificaciones
02	25-07-2014	Paulina Pinto	Gerente Servicio al Cliente Incluye Párrafo 8.5
03	08-03-2016	Paulina Pinto	Se modifica el 2do objetivo de la política, ya que antes sólo mencionaba la protección para nuestros clientes: "Garantizar la protección de la información propia y confiada por nuestros clientes en términos de su confidencialidad e integridad"
04	21-12-2016	Paulina Pinto	Se elimina punto de criterios de aceptación del riesgo ya que estos se incorporan en el procedimiento de gestión y Análisis de Riesgo Se define periodicidad de revisión de la Política Se agrega objetivo de seguridad asociado al plan de riesgo

Fecha de impresión 03-06-2026	Página 12 de 13
-------------------------------	-----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Código:SG-DG-PSI Versión: 013
---	--	----------------------------------

05	11-12-2017	Paulina Pinto	Se agrega el Decreto 142 de 2015. de la SUBTEL y se detalla artículos de la ley 19223
06	19-12-2018	Paulina Pinto	Se agrega como punto Principal de la Política nuestra filosofía de orientación al cliente
07	22-04-2021	Jorge Armijo	Se actualiza integrantes del comité de seguridad
08	23-06-2021	Jorge Armijo	Se agrega la asignación de responsabilidades.
09	18-08-2022	Jorge Armijo	En el punto 8 de actualizar la Ley N° 21.459 Establece norma sobre delitos informáticos, deroga la Ley N° 19.223 se agrega punto 9 de referencias
010	28-02-2024	Oficial de Seguridad	- Se agrega en el alcance las instalaciones de KeeperBox y se revisa documentos, también se agrega sello de agua al documento. - Se agrega nuevo miembro al comité de Seguridad de Información el cual corresponde al Gerente de MicroEdoc. - Se realiza actualización de las responsabilidades de los miembros del comité.
011	17-07-2024	Oficial de Seguridad	- Reestructuración del documento en su totalidad
012	09-06-2025	Oficial de Seguridad	- En el punto 5 se agrega Ley 21.719: Ley regula la protección y el tratamientos de los datos personales - Se agrega punto número 9 con respecto Normas para la prevención de fuga de información; - Se agrega la ISO 27701 con respeto al manejo de la gestión de la información de privada
013	03-06-2026	CISO	- Se agrega registro de control para la versión 02 y 03 que no estaban y se encuentran en la incidencia ISOQMD-337 - Se realiza actualización de logo corporativo - Se agrega Ley 21.663 en el ítem 5

Fecha de impresión 03-06-2026	Página 13 de 13
-------------------------------	-----------------

NOTA: Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.