1. Política General de la Información

Microsystem, comprendiendo la importancia de la seguridad de la información que mantiene de sus clientes, se compromete a implementar un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001, que permita mantener una adecuada gestión de la seguridad en términos de la confidencialidad, integridad y disponibilidad de la Información que administra.

1. Con el propósito de aplicar activamente la filosofía de orientación al cliente, todo el quehacer de Microsystem se focaliza en satisfacer sus necesidades. En especial, el tratamiento de la información sensible que los clientes confían a Microsystem, debe ser resuelto con altos estándares de seguridad.
2. La información es un activo valioso para el negocio de Microsystem.
3. Se debe evaluar y gestionar los posibles riesgos a los que estos estén expuestos nuestros activos de Información, de acuerdo a su sensibilidad, valor y criticidad.
4. Nuestra administración se compromete a revisar y verificar que se cumpla con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad de la información y continuidad del negocio.
5. La seguridad de la Información es responsabilidad de todos los empleados de Microsystem
6. Microsystem se compromete a entrenar constantemente a su personal comunicando instrucciones con respecto a la seguridad de la información.
7. Esta Política y todas las políticas, procedimientos y normativas asociadas a la Seguridad de la Información que se deriven de la misma, se aplican a todo el personal de la Empresa y su incumplimiento constituye una falta grave que será sancionada según la regulación de la empresa y la legislación vigente.
8. La revisión de la seguridad de la información debe ser realizado por organismos independientes.

2. Canales de Comunicación

Se utilizaran los canales de comunicación definidos por Microsystem tales como:

- Plataforma de Gestión de Documentos
- Correo Electrónico
- Documentos físicos
- Portal del Colaborador
- Reuniones periódicas con las áreas definidas en el alcance.

3. Objetivos de Seguridad

1. Cumplir con los SLAs definido con nuestros clientes en sus contratos
2. Garantizar la protección de la información propia y confiada por nuestros clientes en términos de su confidencialidad e integridad.
3. Cumplir con la legislación aplicable en materia de seguridad de la información
4. Mantener a sus colaboradores entrenados en materia de seguridad de la información.

5. Mejorar la eficacia y eficiencia de la organización mediante la valoración y el tratamiento del riesgo de la seguridad de la Información

4. Alcance

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 a Service y Servicios de Desarrollo de Software

El compromiso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), según la norma ISO 27001 se circunscribirá inicialmente a los sistemas de información que soportan los servicios prestados desde la Casa Central.

5. Organización de la Seguridad

La Organización dispone de un Comité de Seguridad, entendido dentro del ámbito de la Política de este documento, que coordina todas las acciones que se tengan que desarrollar en la aplicación de las normas de ésta y que verifica el cumplimiento de los procedimientos que se definan para satisfacer dichas normas.

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.

La responsabilidad general y última de la presente Política de Seguridad recae sobre el Comité de Seguridad, con las funciones principales en cuanto a ella:

- Revisar y proponer al Gerente General de 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 todas las políticas, procedimientos y normativas de seguridad, para garantizar que están alineadas con la política de seguridad y los objetivos del negocio.
- 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 este imposibilitado de ejercer su rol; o bien delegar responsabilidades para trabajos específicos de la autoridad certificadora (AC).

El comité de seguridad estará compuesto por

- **Gerente General y Representante de la Dirección**. Serán los responsables de la implementación de esta Política de Seguridad de la Información Gerente Servicio al Cliente. Cumplirá la función velar por la seguridad de sus procesos conforme a los riesgos analizados.

- **Ejecutiva Servicio al Cliente**. Cumplirá la función velar por la seguridad de susprocesos conforme a los riesgos analizados.

- **Oficial de Seguridad de la Información**. Será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política. También cumplirá funciones relativas a la seguridad de los sistemas de información de Microsystem, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

- **Gerente de Servicios Digitales**. Cumplirá la función velar por la seguridad de sus procesosconforme a los riesgos analizados. cambiar

- **Gerente TI**. Velará por la seguridad de sus procesos conforme a los riesgos analizados. Por otra parte, tendrá la función de 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, garantizará el cumplimiento de las políticas, procedimientos y normativas de seguridad aplicables a dichos procesos.

El comité de seguridad se debe pronunciar al menos una vez al año para aprobar, definir o aceptar temas relevantes levantados por el oficial de seguridad.

6. CLAUSULA DE REVISION

La aprobación de este documento se realizará conforme al procedimiento Control de Documentos de la ISO 9001

Adicionalmente, y a solicitud del comité de seguridad, este documento puede ser revisado ante la detección de nuevos riesgos de seguridad asociados a los servicios provistos por la empresa o cambios tecnológicos u organizativos que puedan afectar a los sistemas de información y, por ende, a su seguridad.
La revisión de la Política de seguridad de la información se realizara en cada reunión gerencial, para definir si sigue vigente la misma o si se realiza algún cambio frente a nuevos procesos o servicios.

7. CLÁUSULA DE APROBACIÓN

La aprobación de este documento se realizará conforme al procedimiento Control de Documentos de la ISO 9001.

8. 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 Nº 19.223** Figuras penales relativas a la Informática.
    - Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
    - Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio
    - Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
    - Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."

- 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

Además, estará alineada a los siguientes estándares:
- Norma ISO 9001
- Norma ISO 27001

Sobre esta política se sustentarán el resto de las políticas, procedimientos, instructivos, etc. de la seguridad de la información.

9. CONTROL DE CAMBIOS

Versión	Fecha	Responsable	Modificaciones
4	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 Politica Se agrega objetivo de seguridad asociado al plan de riesgo
5	11-12-2017	Paulina Pinto	Se agrega el Decreto 142 de 2015. de la SUBTEL y se detalla artículos de la ley 19223
6	19-12-2018	Paulina Pinto	Se agrega como punto Principal de la Política nuestra filosofía de orientación al cliente
7	22-04-2021	Jorge Armijo	Se actualiza integrantes del comité de seguridad
8	23-06-2021	Jorge Armijo	Se agrega la asignación de responsabilidades.

Nicolás Andalaft G.
Gerente General
Microsystem S.A.