POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código del documento:	POL-14
Versión:	2.1
Fecha entrada en vigor:	03/02/2023
Tipo de seguridad:	Información pública

Norma aprobada por el Consejo de Administración de Lorca Telecom Bidco, S.A. en su reunión del 3 de febrero de 2023

Elaborado	**Revisado**	**Aprobado**
Idoia Uriarte	Miguel Santos	Consejo
CISO	CTO	de Administración

ÍNDICE

1. OBJETO

La información, los servicios y los sistemas gestionados por Grupo MASMOVIL (en adelante, Grupo) son un activo fundamental que constituye un elemento estratégico y necesario para el desarrollo de sus actividades, y como tal sus mandos y empleados son responsables de su protección y salvaguarda. Por este motivo, la presente Política de Seguridad de la Información se basa en las recomendaciones del Estándar Internacional ISO/IEC 27001, y las buenas prácticas establecidas por la norma UNE-ISO/IEC 27002, así como los principios y requisitos del ENS (Esquema Nacional de Seguridad), el cumplimiento de la legislación vigente en materia de protección de datos personales, seguridad de las redes y sistemas de información, sociedad de la información, comercio electrónico, ciberseguridad y telecomunicaciones con el fin de mantener la seguridad e integridad de la información, estableciendo, en cada punto, los controles y medidas adecuados para protegerla del acceso o difusión no autorizados, de su modificación, destrucción o no disponibilidad por causas accidentales o intencionadas.

La presente Política tiene por objetivo definir los principios generales para regular y garantizar la seguridad de la información que genera, procesa y almacena el Grupo, así como de los sistemas y aplicaciones que la soportan, incluyendo la red de telecomunicaciones que soporta los servicios a los clientes del Grupo.

Del mismo modo, se persigue la aplicación de un conjunto de acciones destinadas a preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, que constituyen las tres componentes generales de la seguridad de la información.

2. ALCANCE

La presente Política obliga a todas las áreas, departamentos y equipos de trabajo del Grupo, tanto en sus relaciones internas como con terceras entidades. Es de aplicación a todas nuestras actividades, servicios y sistemas.

Todos los usuarios de los recursos informáticos y/o Sistemas de Información del Grupo deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Política.

3. DESARROLLO

3.1. Principios de la Política de Seguridad de la Información

La presente Política y su desarrollo deben ser comunicados a todas las personas del Grupo, tanto al personal propio como al de entidades colaboradoras, y estar a disposición de las partes interesadas.

La seguridad de la información incumbe a todo el personal del Grupo. Este principio, debe ser conocido, comprendido y asumido por todos los niveles de la Organización.

En el desarrollo de sus actividades, el Grupo aplicará criterios de acción preventiva, tanto a los activos existentes como a los cambios que en ellos se realicen:

- Planificando la prevención de riesgos.
- Identificando y evaluando los riesgos.
- Gestionando los riesgos identificados.
- Diseñando planes de mitigación de los riesgos identificados.
- Realizando un seguimiento y evaluación de la eficacia de los planes de mitigación de riesgos, buscando la mejora continua y la minimización de los riesgos corporativos en cada momento.

3.2. Organización de la Seguridad de la Información

Ciberseguridad impulsará el desarrollo e implantación de la seguridad de la información en el Grupo.

Se establecerá una estructura de la seguridad con la finalidad de:

- Garantizar la implementación de controles adecuados al tipo de información tratada.
- Comprometer la cooperación y apoyo de colaboradores.
- Verificar la efectividad de la presente norma y de las que se aprueben en desarrollo de la misma.

La asignación y delimitación de responsabilidades para asegurar que se implanta y satisfacen los objetivos propuestos en la presente política requieren el establecimiento de unas determinadas funciones encargadas de los aspectos generales de gestión de la seguridad de la información. Para ello, el Grupo ha establecido y documentado las funciones y responsabilidades en materia de seguridad de la información.

Se deberá mantener la seguridad de la información frente a accesos de terceras partes. Los controles deben ser acordados y definidos en un contrato de acceso por terceros en conjunto con el departamento de Ciberseguridad. Si además dichos terceros acceden a datos de carácter personal, deberá firmarse un contrato de Encargo de Tratamiento, de conformidad con los modelos establecidos por la Delegada de Protección de Datos.

La seguridad de la información deberá garantizarse y mantenerse, cuando la responsabilidad del tratamiento de la misma sea delegada a otra organización.

3.3. Clasificación y control de la información a efectos de seguridad

El objetivo es proteger la información de manera proporcionada asegurando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad durante todo su ciclo de vida de acuerdo a su nivel de criticidad:

- Confidencialidad: característica que previene contra la divulgación o acceso no autorizados de la información.
- Integridad: característica que asegura que la información está completa, frente a su alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta, y que no ha sido modificada ni ha sufrido variaciones en su procesamiento.
- Disponibilidad: característica referida al acceso y uso autorizado de la información en el lugar, forma y tiempo determinados.
- Autenticidad: característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad: característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

La información se clasificará por su propietario tomando en consideración los siguientes criterios:

Nivel de Clasificación	Personas aut.	Descripción general
Secreta	1 / 2	Información crítica o altamente sensible, destinada a personas muy concretas de la organización. Es información que si se ve comprometida podría ocasionar daños graves o muy graves al Grupo, ocasionando pérdida abrupta de negocio o sanciones severas. El acceso a esta información está muy limitado y sólo se concede a personas nominativas. El responsable de la información deberá garantizar unas medidas de seguridad extraordinarias que ayuden a proteger su confidencialidad dentro de la organización, limitando por completo su acceso y distribución al exterior.

Restringida	n < 30	Información confidencial de alto valor o sensibilidad, destinada a un grupo muy limitado y controlado de personas. Es información que si se ve comprometida podría ser altamente perjudicial para los intereses del Grupo, sus clientes o terceras partes interesadas con las que colabora, ocasionando la pérdida de ventajas competitivas, aumentar el fraude directo, impacto directo elevado en las cuentas de resultados, etc. El acceso a esta información está restringido a determinadas personas de la organización y deberá estar controlado y ser expresamente autorizado por el responsable de la información. El responsable de la información deberá garantizar unas medidas de seguridad adecuadas que ayuden a proteger su confidencialidad tanto fuera como dentro de la organización, limitando su acceso y distribución a un grupo controlado de personas, que cumplan estrictamente el principio de necesidad de conocer.
Confidencial	Grupo limitado	Información destinada a un grupo limitado y controlado de personas. Es información que si se ve comprometida podría ser perjudicial para los intereses del Grupo, sus clientes o terceras partes interesadas con las que colabora. El acceso a esta información está limitado a determinadas personas de la organización y deberá estar controlado por el responsable de la información. El responsable de la información deberá garantizar unas medidas de seguridad adecuadas que ayuden a proteger su confidencialidad tanto fuera como dentro de la organización, limitando su acceso y distribución a un grupo controlado de personas, que cumplan estrictamente el principio de necesidad de conocer.
Interna	Grupo MM	Información destinada únicamente para su uso dentro de la organización, ya sea por el personal interno del Grupo MASMOVIL o por terceras partes que se determinen, sin perjuicio de su carácter confidencial, autorizadas por un tiempo acotado para su acceso y bajo la supervisión del responsable de la información. En general, es información que si se ve comprometida no causaría una disrupción o daño reputacional significativo para el Grupo o terceras partes interesadas. Precisa de medidas de seguridad que limiten su acceso por parte del personal ajeno al Grupo que no requiera de dicha información para cumplir los objetivos de su colaboración con el Grupo. Esta será la clasificación por defecto para la información del Grupo no clasificada previamente.
Pública	∞	Información abierta internamente a todo el personal del Grupo MASMOVIL y externamente al público en general. En general, se trata de información que concierne o no específicamente al Grupo, que puede ser divulgada o publicada a través de los canales oficiales y no requiere limitaciones de acceso. No precisa de medidas de seguridad específicas, puesto que la información está destinada a su publicación y/o divulgación sin restricciones ni limitaciones de acceso.

Las medidas de seguridad a aplicar en el tratamiento de la información tendrán directa relación con sus niveles de clasificación según las normas y procedimientos sobre la gestión de la información que la definen y clasifican.

3.4. Seguridad ligada al personal del Grupo

Todos los empleados y usuarios externos con acceso a información clasificada deberán firmar un acuerdo de confidencialidad y no revelación de la información.

Todos los empleados y colaboradores del Grupo deberán recibir una formación y concienciación adecuada en materia de seguridad de la información, a través de la cual se sensibilice a los mismos acerca de sus responsabilidades en materia de seguridad. Así mismo, se mantendrá a los usuarios al corriente de las amenazas existentes en materia de seguridad de la información, de forma que estén capacitados para respaldar la Política en materia de seguridad de la Organización, en el transcurso de sus tareas normales.

Los incidentes que afecten a la seguridad de la información deberán ser comunicados, tan pronto como sea posible, mediante los canales y procedimientos establecidos. Se deberá informar a empleados y terceras partes que pudieran encontrarse implicadas, acerca de los procedimientos para la comunicación de los diferentes tipos de incidentes en materia de seguridad, así como de los procedimientos a seguir en caso de que el incidente afecte a datos de carácter personal.

En el caso de que algún usuario (interno, externo, proveedor, etc. que preste algún tipo de servicio al Grupo) incurra en conductas contrarias a lo descrito en la presente Política o en su normativa interna de desarrollo, las mismas deberán ser puestas en conocimiento del canal ético por los cauces establecidos en el *Estatuto del Compliance Officer y de funcionamiento del canal ético*.

3.5. Seguridad física

Los espacios físicos donde se procese o almacene información clasificada o que contengan datos de carácter personal deberán ser adecuadamente protegidos mediante perímetros de seguridad definidos y controles de acceso apropiados. La protección suministrada deberá ser siempre proporcional al riesgo.

Las medidas de seguridad deberán garantizar la protección de la información contra pérdida, robo, acceso, divulgación, copia y distribución no autorizada de la información. Los empleados deberán ser conscientes de la necesidad de proteger la confidencialidad de la información. Las medidas adoptadas deben ser tales que manteniendo la disponibilidad de la información eviten el acceso no autorizado.

3.6. Seguridad en las comunicaciones y en la explotación de la información

Se deberán establecer procedimientos de rutina para garantizar la integridad y disponibilidad de los servicios de procesamiento, almacenamiento y comunicaciones, llevando a cabo la estrategia de resguardo definida, realizando copias de seguridad de los datos y ensayando su restablecimiento oportuno.

Se deberán establecer los procedimientos necesarios e implantar las soluciones necesarias para garantizar la confidencialidad de la información corporativa, considerando los requisitos de los niveles de clasificación existentes en la Organización, así como las medidas necesarias establecidas para cada uno de ellos.

Se deberá garantizar la seguridad de las redes telemáticas y la protección de la infraestructura de apoyo. Es de suma importancia la administración de seguridad sobre redes e infraestructuras situadas fuera del perímetro de la organización, y en especial los casos de infraestructuras de recursos compartidos, como es el caso de soluciones Cloud o en la nube. Se deberá garantizar que se aplican los controles suficientes por parte de proveedores de redes, infraestructuras y servicios en nube, sobre la información que es transmitida y/o alojada por estos. Las actividades deben estar estrechamente coordinadas para garantizar que los controles se aplican uniformemente en toda la infraestructura de procesamiento de datos de la Organización, ya se encuentre ésta dentro del perímetro corporativo o proporcionada por terceros mediante soluciones en nube.

Se deberá garantizar la seguridad de la información tanto en la comunicación como en el almacenamiento de la misma en dispositivos personales no pertenecientes al Grupo, en caso de que estuviera permitido.

Se deberán aplicar los controles suficientes para garantizar la seguridad de la información cuando cualquier dispositivo de trabajo (portátiles, teléfonos móviles o similares), ya sea personal o corporativo, procese información del Grupo a través de redes externas no controladas por el mismo. Se deberán establecer normas específicas para el uso específico de estos dispositivos que recojan las medidas de seguridad que estos dispositivos deben implementar para cumplir con los objetivos de seguridad del Grupo.

Deberán controlarse los intercambios de información y software entre organizaciones, siendo consecuentes con la legislación aplicable y los acuerdos existentes. Se deberán establecer procedimientos y estándares para proteger la información y los activos tanto en reposo como en tránsito, considerando principalmente la necesidad de reducir los riesgos de seguridad creados por la salida de información fuera del perímetro o sistemas del Grupo.

Deberán existir mecanismos adecuados para el control de vulnerabilidades y software malicioso.

3.7. Control de accesos

En los sistemas donde sea posible y así sea exigido por el negocio, deberán establecerse controles de acceso basado en segregación de funciones, aplicando el principio de mínimo privilegio específicamente para las funciones necesarias, evitando en la medida de lo posible el uso de usuarios con privilegios excesivos o innecesarios. Se deberá realizar una administración y mantenimiento de accesos ante cambios o modificaciones en las funciones.

El acceso no autorizado a los sistemas y activos de información deberá ser evitado, implementando controles apropiados para la gestión de los derechos de acceso a los usuarios.

El acceso a los servicios o sistemas del Grupo, tanto internos como externos, deberá ser controlado, garantizando la implantación de interfaces adecuadas con las redes públicas, mecanismos de autenticación robustos y controles de acceso apropiados.

Se establecerán sistemas de monitorización a fin de comprobar la eficacia de los controles adoptados y detectar las desviaciones respecto de la normativa interna de control de accesos.

Deberá garantizarse la seguridad de la información en el uso de dispositivos móviles e instalaciones de trabajo remotas. La protección requerida será proporcional al riesgo que implique la modalidad del trabajo.

3.8. Desarrollo, Adquisición y mantenimiento de aplicaciones

Se desarrollarán directrices para garantizar que la seguridad es incorporada en el diseño, desarrollo, adquisición, mantenimiento y puesta en explotación de nuevos proyectos a fin de prevenir pérdidas, modificación o usos no autorizados de la información.

Los requerimientos de seguridad deberán ser identificados y aprobados por el departamento de Ciberseguridad en la etapa de diseño de los sistemas de información.

Para el establecimiento de los requerimientos de seguridad se tendrán en cuenta los requisitos del negocio, el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento de la información, así como los requisitos de la legislación vigente en función de la aplicabilidad de la misma a cada proyecto.

Deberá desarrollarse un análisis de seguridad y riesgos en cada nuevo proyecto y en las modificaciones sustanciales a fin de identificar las amenazas y riesgos que están expuestos, pudiendo así decidir el tratamiento o asunción de los mismos.

3.9. Continuidad de negocio

La continuidad de las actividades críticas de la organización estará garantizada mediante la implantación de directrices y controles preventivos y correctivos por el departamento de Continuidad de Negocio a fin de proteger los procesos críticos de los negocios de los efectos de fallos significativos o desastres.

El plan de contingencia para la información automatizada debe desarrollarse e implementarse para asegurar que los procesos críticos de negocio pueden restablecerse en el tiempo requerido, incluyendo controles para identificar y reducir los riesgos, limitar las consecuencias de los incidentes que afectan negativamente, y asegurar el tiempo de respuesta de las operaciones esenciales.

3.10. Tratamiento de datos personales

Todo tratamiento de datos personales debe apoyarse en una base que lo legitime. Entre los puntos a tener en cuenta, destacan:

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

El tratamiento de datos personales está bajo una protección regulatoria especial por lo que se deberá aplicar medidas y controles para garantizar su Seguridad y cumplimiento con la regulación vigente.

Cualquier tratamiento de datos de carácter personal por parte de terceros, deberá ser revisado por el área Delegada de Protección de Datos y firmarse un contrato de Encargo de Tratamiento en conformidad con los modelos establecidos.

3.11. Planificación de Seguridad de la Información

Anualmente se establecerán los objetivos de seguridad atendiendo a las necesidades del negocio o a la identificación de los riesgos que hubieran sido detectados.

El establecimiento de los objetivos y proyectos de seguridad contemplará además el resultado de los análisis de riesgos desarrollados.

3.12. Gestión de riesgos

Se deberán aplicar criterios de acción preventiva sobre los activos de información junto con el departamento de Ciberseguridad identificando los riesgos existentes y evaluando su impacto, con el fin de establecer las medidas de seguridad adecuadas, a fin de combatir los riesgos en su origen siguiendo el procedimiento de Gestión de riesgos.

Se deberán verificar la eficacia de los controles y medidas de seguridad implantadas mediante la monitorización continua y la realización de auditorías.

3.13. Control y auditorías de Seguridad de la Información

Para controlar y evaluar el cumplimiento de los requerimientos legales y procedimientos internos se realizarán las acciones de supervisión y auditorías internas y externas necesarias con la periodicidad que se establezcan, respetando en todo caso los criterios legalmente establecidos.

Los resultados obtenidos se tendrán en cuenta en la revisión y evaluación que Seguridad de la Información debe realizar periódicamente sobre la implantación de esta Política.

4. RESPONSABILIDADES

- Es responsabilidad de todo el personal del Grupo MASMOVIL asegurarse de que tienen acceso, conocen y aplican las versiones vigentes de la la Política de seguridad de la información.
- Los responsables de la elaboración de los documentos son los responsables de realizar la comunicación de la disponibilidad de dicha documentación en la organización y revisar su contenido como mínimo anualmente.

5. REGISTRO DE REVISIONES

Versión actual	*2.1*		
Historial de Cambios	Fecha	**Versión**	
	05/02/2020	*1.0*	*Creación del documento*
	29/09/2022	*2.0*	*Unificación políticas Grupo y actualización*
	05/01/2023	*2.1*	*Adaptación requisitos ENS*