Empresa Municipal de Telecomunicaciones de Ipiales S.A. E.S.P.
NIT: 900292948-3

MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN "MIPG"

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

IPIALES, 2022

	UNIMOS EMPRESA MUNICIPAL DE TELECOMUNICACIONES DE IPIALES S.A. E.S.P.	
POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
Código:	POL-02	**Versión:** 1

ELABORÓ	**REVISÓ**	**APROBÓ**
Javier Salazar Betancourt	Jose David Lafaurie	Diana Isabel Obando Guerrero
Jefe Oficina de Operaciones Digitales	Jefe Oficina Asesora de Planeación	Gerente
FECHA	**FECHA**	**FECHA**
07/10/2022	14/10/2022	17/10/2022

REGISTRO DE MODIFICACIONES
Reestructuración de Políticas de acuerdo a los lineamientos y Gestión de el Plan de Gobierno Municipal “Hablamos con Hechos”.
Actualización vigencia de la política

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Empresa Municipal de Telecomunicaciones de Ipiales UNIMOS S.A. E.S.P. con el fin de lograr el cumplimiento normativo en los temas relacionados con la administración y protección de la información en cada una de sus dimensiones como la disponibilidad, integridad y confidencialidad, ha elaborado una serie de acciones para la implantación de un Subsistema de Gestión de Seguridad de la Información (SGSI) alineado con los objetivos estratégicos de la Entidad.

Es de este modo que, para asegurar el Modelo de Seguridad y Privacidad de la Información (MSPI) debe adoptar controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el Modelo.

Así entonces se describe la Política General de Seguridad y Privacidad de la Información, los lineamientos generales, los requerimientos legales y las responsabilidades tanto de la alta dirección como de los propietarios de los activos y en general todos los funcionarios, contratistas y terceros que intervengan en la generación, tratamiento y almacenamiento de la información.

2. DEFINICIONES

- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **S.I.G:** Sistema de Información Geográfica.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de información:** Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.
- **Integridad:** Hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.
- **Confidencialidad:** Es la necesidad de ocultar o mantener secreto sobre determinada información o recursos.
- **Disponibilidad:** Hace referencia a que la información debe permanecer accesible a elementos autorizados.
- **Incidente de seguridad:** es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura de información y tecnología de APC-Colombia (sistemas de cómputo, sistemas de información, sistemas de telefonía), como pueden ser: ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, crímenes definidos en la ley 1273 de 2009 u otras normas que cobijen a la entidad.
- **Código malicioso:** un gusano informático usa archivos compartidos para contaminar cientos de estaciones dentro de la entidad. La entidad recibe un reporte del vendedor de sus antivirus en donde alerta de un virus que se dispersa a gran velocidad mediante correo electrónico por Internet. El virus aprovecha una vulnerabilidad presente en los servidores de la entidad, basado en la experiencia de la entidad en otros incidentes se estima que el virus podría afectar a los equipos en un lapso de tres horas.

- **Acceso no autorizado:** un atacante utiliza una herramienta de explotación de vulnerabilidades para tener acceso al archivo de password de usuarios. Un perpetrador obtiene acceso no autorizado a nivel de administrador a un servidor y a la información confidencial que contiene y luego intimida a la víctima amenazando la de divulgar a la prensa a la información si no realiza el pago de un dinero.
- **Uso inapropiado:** un usuario entrega copias de software de la entidad a personas no autorizadas. Una persona amenaza a otra vía correo electrónico.
- **Seguridad de la Información:** Preservación de la confidencialidad, disponibilidad e integridad de la información (ISO/IEC 27000) independiente de su medio de conservación, transmisión o formato.

3. MARCO LEGAL

NORMA	DESCRIPCIÓN
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 679 de 2011	Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución
Ley 1273 de 2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la Información y de los Datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1221 de 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley 1403 de 2010	Por la cual se adiciona la Ley 23 de 1982, sobre Derechos de Autor, se establece una remuneración por comunicación pública a los artistas intérpretes o ejecutantes de obras y grabaciones audiovisuales o "Ley Fanny Mikey"
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 105 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Resolución 793 de 2019 de la ANE	Por la cual se adopta la Política del Sistema de Gestión de Seguridad y Privacidad de la información, Seguridad Digital y se definen lineamientos frente al uso de la información
Resolución 500 DE 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
CONPES 3854 de 2016	Política Nacional de Seguridad Nacional que tiene como objetivo fortalecer las capacidades de las múltiples Partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en el marco de cooperación, colaboración y asistencia, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social.
Norma técnica colombiana 27001de 2013	TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS
Norma técnica colombiana 27002 de 2015	Estándar para la seguridad de la información. Código de buenas prácticas para la gestión de la seguridad de la información.

4. OBJETIVOS

4.1. OBJETIVO GENERAL.

Establecer los lineamientos que conduzcan a la preservación de la confidencialidad, integridad, disponibilidad de la información, a partir del establecimiento de políticas, controles, procedimientos, promoción de la cultura de privacidad y seguridad, y mediante la gestión de los riesgos de seguridad de la información para brindar confianza a las partes interesadas y grupos de valor y contribuir al logro de los objetivos de UNIMOS Empresa Municipal de Telecomunicaciones de Ipiales S.A. E.S.P.

4.2. OBJETIVOS ESPECÍFICOS.

- ✓ Establecer las directrices y lineamientos requeridos para proteger la información y los sistemas de información donde se administra, produce, procesa y/o transforma la información de UNIMOS S.A. E.S.P. y usuarios, en los diferentes procesos, ante cualquier amenaza que pueda comprometer la confidencialidad, disponibilidad e integridad de dicha información.
- ✓ Gestionar los Riesgos de seguridad de la información de forma oportuna por medio de controles, ayudando a reducir los impactos negativos de su materialización.
- ✓ Reducir los Incidentes de Seguridad de la Información que afecten el normal funcionamiento de UNIMOS S.A. E.S.P.
- ✓ Fomentar una Cultura de Seguridad de la información en la entidad para que todos los Colaboradores tomen conciencia de sus deberes y responsabilidades frente al SGSI.
- ✓ Generar cultura de privacidad y seguridad de la información para las partes interesadas y grupos de valor demás grupos de interés, mediante la definición de una estrategia de uso y apropiación de la presente política y sus políticas relacionadas.

5. ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del UNIMOS S.A. E.S.P. y la ciudadanía en general.

6. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI de UNIMOS S.A. E.S.P.:

- UNIMOS S.A. E.S.P. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- UNIMOS S.A. E.S.P. protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- UNIMOS S.A. E.S.P. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- UNIMOS S.A. E.S.P. protegerá su información de las amenazas originadas por parte del personal.
- UNIMOS S.A. E.S.P. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- UNIMOS S.A. E.S.P. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- UNIMOS S.A. E.S.P. implementará control de acceso a la información, sistemas y recursos de red.

- UNIMOS S.A. E.S.P. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- UNIMOS S.A. E.S.P. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- UNIMOS S.A. E.S.P. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- UNIMOS S.A. E.S.P. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7. DESARROLLO DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de UNIMOS empresa Municipal de Telecomunicaciones de Ipiales S.A. E.S.P., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para UNIMOS S.A. E.S.P., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de UNIMOS S.A. E.S.P.
- Garantizar la continuidad del negocio frente a incidentes.
- UNIMOS S.A. E.S.P. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

7.1. LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Con base en lo anterior, establece los siguientes lineamientos para la implementación de la política de seguridad y privacidad del SGSI de UNIMOS S.A. E.S.P.

7.1.1. DISPOSITIVOS MÓVILES Y TELETRABAJO.

- Se debe garantizar la seguridad del teletrabajo y el uso de dispositivos móviles de la empresa y de los dispositivos móviles personales dentro de las instalaciones.

- Se debe documentar e implementar procedimientos medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

7.1.2. SEGURIDAD DEL RECURSO HUMANO.

- Se debe asegurar que los colaboradores comprenden sus responsabilidades y son idóneos para el desempeño de sus funciones u obligaciones contractuales.
- Se debe llevar a cabo una verificación de antecedentes alineada con los requisitos legales que apliquen para cada colaborador.
- Los acuerdos contractuales con los colaboradores deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.
- La alta dirección debe exigir a todos los colaboradores la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por el UNIMOS S.A. E.S.P.
- Se debe establecer y ejecutar un programa de sensibilización en seguridad y privacidad de la información, acorde con las políticas y procedimientos pertinentes de la empresa, teniendo en cuenta la información que se debe proteger, y los controles que se han implementado.
- Se debe definir, comunicar a los colaboradores y hacer cumplir las responsabilidades y los deberes de seguridad de la información que permanecen válidos aún después de la terminación contrato o cambio de empleo.

7.1.3. ACTIVOS DE INFORMACIÓN.

- Se debe mantener un inventario de activos de información actualizado, alineado con los requisitos legales y regulatorios, en donde se registren los propietarios, responsables, custodios y clasificación de los mismos.
- Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por UNIMOS S.A. E.S.P.

- Se debe documentar e implementar procedimientos para que los colaboradores realicen la devolución de todos los activos que sean de propiedad de la empresa, al terminar su contrato, acuerdo o retiro de la Entidad.
- Se debe disponer en forma segura de los medios de almacenamiento de información cuando ya no se requieran, utilizando procedimientos formales.

7.1.4. CONTROL DE ACCESO.

- Se deben documentar e implementar políticas que permitan limitar el acceso a información y a instalaciones de manejo de información, que permita el acceso a las redes, sistemas y servicios para los que tengan autorización formal previa, con especial atención a los accesos privilegiados, implementando un procedimiento formal de registro, ajuste, cancelación y revisión periódica de accesos.
- UNIMOS S.A. E.S.P. debe implementar mecanismos de autenticación adecuada para los ingresos seguros a sistemas o aplicaciones, las credenciales de acceso deben mantenerse en secreto por parte de los colaboradores, de igual forma serán personales y de uso exclusivo.

7.1.5. CONTROLES CRIPTOGRÁFICOS.

- Se debe contemplar el uso apropiado y eficaz de la criptografía en los sistemas y aplicaciones para proteger la confidencialidad, autenticidad e integridad de la información.

7.1.6. SEGURIDAD FÍSICA Y DEL ENTORNO.

- Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
- Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.
- Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

- Se deben realizar acciones para prevenir la pérdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la organización; los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.
- Todos los funcionarios y contratistas de la empresa deben bloquear los equipos de cómputo cuando estén desatendidos, cerrar las sesiones de las aplicaciones o servicios de red cuando ya no se necesiten, adoptar la política de escritorio limpio de papeles y medios de almacenamiento removibles y tener la pantalla del computador despejada, libre de archivos o accesos directos a los programas.

7.1.7. SEGURIDAD DE LAS OPERACIONES.

La Empresa UNIMOS S.A. E.S.P. para brindar seguridad de las operaciones debe:

- Asegurar las operaciones de las instalaciones de procesamiento de información; los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
- Controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- Separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
- Implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada de los colaboradores, para proteger a UNIMOS S.A. E.S.P. contra códigos maliciosos.
- Realizar copias de respaldo (Backup) de la información, software e imágenes de los sistemas, y probarlas regularmente de acuerdo con una política de copias de respaldo definida.

- Elaborar, conservar y revisar regularmente los registros acerca de actividades de los usuarios, operadores y administradores, excepciones, fallas y eventos de seguridad de la información y protegerlos contra alteración y acceso no autorizado.
- Sincronizar todos los relojes de los sistemas de procesamiento de información con una única fuente de referencia de tiempo.
- Controlar la instalación y actualización de aplicaciones o servicios en los servidores.
- Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
- El Grupo de Gestión de Sistemas e Informática a través de la mesa de ayuda, son los únicos autorizados para instalar o desinstalar cualquier tipo de programa de los equipos de los colaboradores propendiendo por el cumplimiento legal en materia de derechos de autor.

7.1.8. SEGURIDAD DE LAS COMUNICACIONES.

- Se debe asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información, documentar y hacer cumplir acuerdos de confidencialidad o no divulgación de información de UNIMOS S.A. E.S.P.

7.1.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

- Se debe incluir la seguridad de la información como parte integral de los sistemas de información durante todo su ciclo de vida, como requisito para nuevos sistemas de información o mejoras a los mismos, estableciendo y aplicando reglas para el desarrollo de software o sistemas.
- Documentar y aplicar procedimientos formales para el control de cambios en los sistemas de información, contar con ambientes de desarrollo, pruebas y producción separados y seguros.

7.1.10. RELACIONES CON LOS PROVEEDORES.

- Se deben documentar y acordar los requisitos de seguridad de la información para mitigar los riesgos asociados con los activos de información a los que tengan acceso o suministren los proveedores.
- Se debe hacer seguimiento, revisión y auditoria a la prestación de servicios de los proveedores en cuanto a términos y condiciones de seguridad de la información.

7.1.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

- Se debe establecer las responsabilidades y procedimientos de gestión para una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- Todos los colaboradores deben reportar los incidentes de seguridad de la información a la mesa de ayuda del Grupo de Sistemas e Informática tan pronto como tengan conocimiento del mismo o sospechen de alguno.
- Se definir y aplicar procedimientos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para ser usado en la reducción de la posibilidad o el impacto de incidentes futuros.
- Se deben definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información de los incidentes de seguridad de la información que pueda servir como evidencia.

7.1.12. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO.

- UNIMOS S.A. E.S.P. debe establecer, documentar, implementar y mantener procesos, procedimientos y controles donde se determinen sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas.
- Se debe verificar por lo menos anualmente los controles establecidos para la continuidad de la gestión de la seguridad de la información para asegurar que son válidos y eficaces.

- Las instalaciones de procesamiento de información se deben implementar con redundancia en cumplimiento de los requisitos de disponibilidad.

7.1.13. CUMPLIMIENTO.

- Se debe garantizar el cumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
- Se debe definir e implementar una política de privacidad, tratamiento y protección de información de datos personales.
- El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de UNIMOS S.A. E.S.P., incluyendo lo establecido en las normas que competen al Gobierno Nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.
- La presente Política se debe publicar y socializar a las partes interesadas de UNIMOS S.A. E.S.P., debe esta soportada en las políticas específicas de seguridad y privacidad de la información, las cuales serán parte integral del presente documento y se deberá revisar mínimo una vez al año.

7.2. PRINCIPIOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A continuación se establecen 12 principios de seguridad que soportan el SGSI de UNIMOS S.A. E.S.P.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- UNIMOS S.A. E.S.P. protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- UNIMOS S.A. E.S.P. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- UNIMOS S.A. E.S.P. protegerá su información de las amenazas originadas por parte del personal.
- UNIMOS S.A. E.S.P. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- UNIMOS S.A. E.S.P. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- UNIMOS S.A. E.S.P. implementará control de acceso a la información, sistemas y recursos de red.
- UNIMOS S.A. E.S.P. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- UNIMOS S.A. E.S.P. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- UNIMOS S.A. E.S.P. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- UNIMOS S.A. E.S.P. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7.3. FASES DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

7.4. IMPORTANCIA DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN.

Para las entidades es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

BIBLIOGRAFIA

- MinTIC (2018). *Elaboración de la política general de seguridad y privacidad de la información*. MinTIC.
- https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0500_2021.htm.