POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

En la presente política se establecen criterios básicos para proteger los datos, las telecomunicaciones, el hardware y el software de la organización en cualquiera de sus medios, físico o digital, así como la transferencia de estos.

En esta política se definen y relacionan las normas y procedimientos que deben seguir los usuarios del Sistema de Información, para preservar la confidencialidad, integridad y disponibilidad de la información de la organización. Para lograrlo, se seleccionan y establecen controles apropiados para proteger los recursos físicos, financieros, el buen nombre, la posición legal, los empleados y otros activos tangibles e intangibles. Esta política deberá seguir un proceso de actualización periódica, de acuerdo con los cambios organizacionales relevantes, tales como: crecimiento de la planta de personal, cambios en la infraestructura computacional, desarrollo de nuevos servicios, requerimientos de entes de control o de nuevas legislaciones.

OFICIAL

El objetivo de este documento es establecer las políticas en seguridad de la información de mutualser eps, con el fin de regular la gestión de la seguridad de la información al interior y exterior de la organización.

2. DESTINATARIOS DE LA POLÍTICA

Esta política es de carácter obligatorio para todo el personal de la organización, aplican también para los terceros que tengan alguna relación de transferencia o acceso autorizado a los activos de la información de la organización.

3. RESPONSABLE(S)

- Comité de Seguridad de la Información.
- Gerente de Tecnologías de la Información.
- Gerente de Experiencia y Fidelización del Cliente (Director de Gestión Documental, Director de Comunicaciones, Director Dpto. de Gestión Humana y Coordinador de Seguridad y Salud en el Trabajo).

- Oficial de Cumplimiento de Seguridad de la Información.

4. NORMATIVIDAD

4.1 Ley 1712 de 2014.
4.2 Ley 1581 de 2012.
4.3 NTC ISO 27001: 2022.

5. DEFINICIONES

5.1 Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

5.2 Activo de información: Es el elemento de información que la organización recibe o produce en el ejercicio de sus funciones.

5.3 Acuerdo de Confidencialidad: Documento en los que los funcionarios del mutualser eps o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la organización.

5.4 Cifrado: Transformación de los datos mediante el uso de la criptografía para producir datos no legibles y asegurar su confidencialidad.

5.5 Confidencialidad: Entendida como la garantía del acceso a la información únicamente de los usuarios autorizados.

5.6 Disponibilidad: Garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

5.7 Integridad: Se refiere a la exactitud y consistencia de los datos a lo largo de su ciclo de vida.

OFICIAL

5.8 Perfiles de usuario: Grupos de permisos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los activos de información.

5.9 Registros de Auditoría: Archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la organización.

5.10 Sistema de información: Conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas.

5.11 Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la organización.

5.12 Vulnerabilidades: Son las debilidades o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la organización (amenazas), las cuales se constituyen en fuentes de riesgo.

OFICIAL

6. ALCANCE DE LA POLÍTICA

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con mutualser eps, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada a todos los procesos de la organización.

7. LINEAMIENTOS DE LA POLÍTICA

7.1 Política Global y de Cultura de Seguridad de la Información: mutualser eps considera la información un activo fundamental y se compromete a proteger su confidencialidad, integridad y disponibilidad como parte de su estrategia de continuidad del negocio y administración de riesgos. Se fomenta una cultura de seguridad que exige la adopción obligatoria de estas directrices por parte de todo el personal, proveedores y terceros con acceso a la información.

7.2 Marco de Gobernanza y Revisión de Políticas: La Junta Directiva y la Alta Dirección son responsables de la aprobación y promoción activa de estas políticas, las cuales se revisan anualmente o ante cambios significativos. Un Comité de Seguridad de la Información se encarga del mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, con roles y responsabilidades claramente definidos para todas las áreas.

7.3 Gestión de Activos de Información: Es mandatorio identificar, clasificar y valorar los activos de información, reconociéndolos como valiosos e irremplazables para la identidad de la compañía. Se mantiene un inventario actualizado anualmente que asigna responsables para velar por su protección, garantizando la confidencialidad, integridad y disponibilidad. Se asegura la correcta devolución de activos y la eliminación irrecuperable de información al finalizar contratos o reasignar equipos.

7.4 Política de Gestión de Accesos, Privilegios y Autenticación Segura: La creación, modificación, bloqueo y retiro de cuentas se gestiona de acuerdo con las funciones del personal. Se promueve el uso responsable de los recursos y la asignación de contraseñas seguras, personales e intransferibles que deben cambiarse periódicamente. Toda actividad que implique acceso a la infraestructura tecnológica y sistemas de información debe tener roles, responsabilidades y niveles de acceso claramente definidos, incluyendo la segregación de funciones para sistemas críticos. Los usuarios finales no deben tener privilegios de administrador en sus equipos, excepto el personal técnico de TI. Las aplicaciones corporativas y equipos de cómputo deben implementar procesos de inicio de sesión seguros (ej., no mostrar información del sistema antes de la validación, ocultar contraseñas, no transmitirlas en texto plano) y contar con cierre automático de sesiones inactivas.

7.5 Política de Seguridad de Redes, Recursos en la Nube y Acceso Remoto: Las redes de datos y los recursos en la nube deben estar protegidos contra accesos no autorizados mediante firewalls, monitoreo de tráfico anómalo e inspección de correo electrónico. Se exige el cifrado en las integraciones expuestas a internet. La conexión inalámbrica y el acceso remoto están permitidos solo a personal autorizado, utilizando equipos asignados por la organización y medios proporcionados por la Gerencia de TI. Se restringe el almacenamiento de información clasificada en dispositivos personales y el uso de redes públicas inseguras.

7.6 Política de Uso Aceptable de Activos de Información: Los equipos, software, hardware y sistemas de información de la organización deben ser utilizados

OFICIAL

exclusivamente para fines institucionales. Se prohíbe el uso personal, la modificación o divulgación no autorizada de información, el acceso a sitios web inseguros o inapropiados, y cualquier acción ilegal sobre la información. Se establece que el acceso implica monitoreo y el uso del correo electrónico es para fines organizacionales. Los usuarios son responsables de sus credenciales y del contenido de sus comunicaciones.

7.7 **Política de Seguridad Física de Activos y Equipos de Cómputo**: Las áreas que custodian información sensible y equipos críticos (ej., archivos, cuartos de telecomunicaciones y procesamiento de datos) deben estar protegidas con controles de acceso (cerraduras, biometría, tarjetas) y perímetros de seguridad sólidos. El ingreso de terceros a estas áreas debe estar debidamente autorizado y supervisado. La Gerencia de Tecnología de la Información es responsable de la instalación, mantenimiento y ubicación de todos los equipos. Los usuarios deben mantenerlos en condiciones adecuadas, apagarlos al finalizar la jornada y reportar fallas de inmediato. Se prohíbe la manipulación de hardware o software sin la autorización previa de la Gerencia de TI. Los equipos de cómputo de la organización no deben ser dejados desatendidos en lugares públicos o vehículos. En caso de pérdida o robo, se debe informar de inmediato a la Gerencia de TI y a la autoridad competente. Se exige mantener los escritorios y pantallas limpios, lo que implica guardar bajo llave documentos y dispositivos cuando no se usan y bloquear las sesiones al abandonar el puesto de trabajo.

OFICIAL

7.8 **Política de Protección de Datos. Antimalware, Cifrado y Copias de Respaldo:** Se debe instalar y mantener actualizado el aplicativo de detección y prevención de software malicioso en todos los equipos, y la organización prohíbe la conexión de equipos no conformes a su red de datos. Toda la información sensible o confidencial debe ser cifrada en medios digitales, tanto durante su transferencia como en su almacenamiento. Se asegura la generación y almacenamiento de copias de respaldo de la información crítica en ubicaciones seguras y diferentes a las instalaciones principales. El uso de medios de almacenamiento removibles está restringido y controlado por herramientas tecnológicas y requiere autorización previa del dueño de la información y la Gerencia de TI, con técnicas de cifrado obligatorias.

7.9 **Política de Monitoreo de Eventos, Gestión de Vulnerabilidades y Pruebas de Seguridad:** mutualser eps realiza un monitoreo permanente del uso de la plataforma tecnológica y sistemas de información. Se garantiza la custodia de los registros de auditoría y el análisis de sus resultados para identificar eventos de seguridad, con una configuración horaria exacta para los servidores. La Gerencia de Tecnología y el equipo

de Arquitectura de TI son responsables de realizar pruebas periódicas de vulnerabilidades y hacking ético, generando lineamientos y planes de acción para la mitigación de las debilidades detectadas.

7.10 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información: Se establecen directrices para garantizar la integridad de los sistemas de información desde su adquisición y desarrollo. Esto incluye la especificación de cláusulas de confidencialidad y derechos de autor en contratos con desarrolladores externos, y la implementación de métodos de desarrollo de software seguro. Se exige la separación física o virtual de ambientes. La seguridad en los sistemas de información debe evaluarse rigurosamente, prohibiéndose el uso de datos sensibles en ambientes de prueba. Se prohíbe estrictamente el uso y/o la introducción de información no validada y/o ficticia en los ambientes productivos de los sistemas de información de la organización. Se gestiona la baja de software obsoleto.

7.11 Política de Relaciones con Terceros: Todos los proveedores y terceros con acceso a los activos de información deben firmar acuerdos de confidencialidad y compromiso con el cumplimiento de las políticas de seguridad. Se deben definir acuerdos de niveles de servicio (SLA) y establecer las condiciones de conexión para sus equipos a la red de la organización. La organización y cada gerencia de área velarán por mantener los niveles acordados de seguridad y prestación de servicios con los proveedores.

OFICIAL

7.12 Política de Cumplimiento Legal, Normativo y Gestión de Incidentes: mutualser eps garantiza el cumplimiento irrestricto de la normativa vigente en protección de datos personales (Ley 1581 de 2012) y los derechos de autor del software utilizado, manteniendo inventarios de software autorizado y prohibiendo instalaciones no autorizadas. Se establecen directrices para la gestión de incidentes de seguridad, asegurando su identificación y tratamiento oportuno para minimizar daños y evitar propagación. Se incluyen lineamientos de seguridad aplicables a la gestión humana, como la selección de personal idóneo y acuerdos de confidencialidad para empleados y el proceso de retiro. Además, la organización promueve la concientización y formación en seguridad de la información para todo el personal y establece un régimen de sanciones para las violaciones a las políticas.

7.13 Política de Uso Adecuado y Ético de la Inteligencia Artificial (IA): mutualser eps reconoce el potencial de las tecnologías de Inteligencia Artificial para la mejora de sus servicios. Es importante destacar que esta política se formula en base a los principios generales de seguridad de la información, uso aceptable de activos, cumplimiento legal

y gestión de riesgos documentados en las políticas precedentes. El uso, desarrollo y adquisición de sistemas de IA deben adherirse estrictamente a los principios de Confidencialidad, Integridad y Disponibilidad de la información. Se exige un uso ético y responsable de la IA, garantizando que su implementación se alinee con los objetivos institucionales y prohíba cualquier actividad ilegal, discriminatoria o contradictoria de los valores y principios corporativos. Se debe asegurar la responsabilidad sobre las decisiones o acciones derivadas de sistemas de IA. La implementación de IA debe considerar la gestión de riesgos y vulnerabilidades específicas que estas tecnologías puedan introducir, y asegurar la trazabilidad y auditabilidad de sus operaciones y resultados. Se prohíbe la introducción de datos confidenciales en herramientas diferentes a las suministradas por la organización.

8. DOCUMENTOS DE REFERENCIA

No aplica.

OFICIAL

9. VIGENCIA

El presente compendio de políticas de seguridad de la información rige a partir del 27 de septiembre de 2019, fecha en que fue aprobada por la Junta Directiva de mutualser eps, teniendo en cuenta modificación o sustitución de los lineamientos a que sea sujeto el presente documento.

10. CONTROL DE CAMBIOS

VERSIÓN ANTERIOR	FECHA DE APROBACIÓN	VERSIÓN ACTUAL	DESCRIPCIÓN DEL CAMBIO
N/A	24/08/2018	01	Creación del documento.
01	27/09/2019	02	Aprobación general de la documentación por parte de la Junta Directiva y adopción a la nueva plantilla institucional.
02	30/04/2020	03	Actualización y ajuste de redacción del Manual de Políticas de la Seguridad de

			la Información y se adicionan nuevas políticas.
03	02/01/2025	04	Se incorporó el rol de CISO como responsable en varias secciones y se actualizó el año de la norma ISO 27001 a 2022 en todo el documento. Se ajustaron definiciones claves (integridad, integralidad, criticidad, hacking ético, perfiles de usuario, y trabajo fuera de casa), reorganizando y fusionando numerales para simplificar contenido, como los lineamientos sobre medios removibles. Se actualizaron directrices sobre sesiones inactivas, dispositivos móviles, ingreso a áreas seguras, aseo de centros de datos y seguridad en la reutilización y eliminación de equipos. Se eliminaron elementos redundantes como gestión de autenticación, deberes de usuarios y criterios de talento humano, integrándolos en otras políticas. Se añadieron referencias a manuales y procedimientos específicos relacionados con cifrado, copias de respaldo, vulnerabilidades, transferencia de información, administración de datos personales y capacitación en seguridad. Las directrices sobre gestión de incidentes se consolidaron en una sección más amplia, optimizando la estructura del documento. Aprobado por Junta Directiva en Sesión No. 68 del 18 de diciembre de 2024.
04	04/08/2025	05	Se elabora una versión simplificada y generalizada del documento original, con el fin de facilitar el acceso, comprensión y divulgación de las políticas institucionales a todos los

OFICIAL

			interesados. Aprobado por Junta Directiva en sesión ordinaria realizada el 30 de julio de 2025, Acta No. 78.
05	27/03/2026	06	Se migra del proceso Gestión TIC a Direccionamiento Estratégico. Aprobado por Junta Directiva en Acta No. 78.
06	22/05/2026	07	Se actualiza documento en la nueva plantilla institucional. El contenido de esta política fue aprobado por Junta Directiva en Acta No. 78.

OFICIAL