OBJETIVO:
Establecer las directrices, medidas y controles necesarios en los sistemas de información de Mediagnostica Tecmedi SAS, con el fin de garantizar la autenticidad, confidencialidad e integridad de los datos.

ALCANCE:
Esta política aplica a toda la información digital utilizada en los procesos de Mediagnostica Tecmedi SAS. Incluye a todos los trabajadores, contratistas, subcontratistas y proveedores que tengan acceso a información pública o privada, así como a todos los activos de información y equipos dedicados al tratamiento, almacenamiento y transmisión de datos.

OBLIGATORIEDAD:
La presente política es de carácter obligatorio y estricto cumplimiento por parte de todo el talento humano de Mediagnostica Tecmedi SAS, trabajadores, contratistas y subcontratistas.

El incumplimiento de esta política dará inicio a la aplicación de sanciones disciplinarias, contractuales o legales según corresponda al vinculo establecido, la gravedad del incumplimiento y las consecuencias de este.

MARCO NORMATIVO DE LA POLITICA:
- Constitución Política de Colombia, artículo 15.
- Código sustantivo del trabajo, artículo 58.
- Ley 1266 de 2008, sobre las disposiciones generales del Habeas Data
- Ley 1581 de 2012, sobre la protección de datos personales.
- Decreto 1377 de 2013, que reglamenta parcialmente la ley 1581 de 2012.
- Ley 2015 de 2020 por medio del cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones.
- Código Penal Colombiano, artículo 194.
- Código Penal Colombiano, Título VII BIS, de la protección de la información y los datos.
- Resolución 746 de 2022 del Ministerio TIC.
- Decreto 338 de 2022 (establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.)

ROLES Y RESPONSABILIDADES:
Para el cumplimiento de la Política de Seguridad de la Información Digital, se designará al proceso de Gestión de la Información, al comité de Seguridad de la Información y al proceso de Talento Humano para velar por su cumplimiento en cada una de sus áreas y la retroalimentación necesaria para la toma de decisiones.

DEFINICIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:
Se define el Comité Institucional de Gestión de la Información y Tecnología, como órgano operativo y de apoyo para coordinar la formulación y la implementación del Sistema de Gestión de Seguridad de la Información. Este comité está integrado por el Gerente General, la Directora de Gestión de la Información, el Director de Calidad y Mejora Continua, el Director de Ambiente Físico y el

Representante de Gestión de Riesgos.

ACUERDOS DE CONFIDENCIALIDAD:
Todo el talento humano de Mediagnostica Tecmedi SAS, terceros y contratistas, en el momento de la firma del contrato acepta los acuerdos de confidencialidad definidos por la compañía.

Cualquier violación a lo establecido en los acuerdos de confidencialidad se considerará como un "incidente de seguridad", que dará lugar a las sanciones y/o conducto regular pertinente.

Entre sus obligaciones para el adecuado manejo de los datos están:

- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
- No revelar información a terceras personas ni a usuarios no autorizados.
- No realizar acciones que supongan un peligro para la seguridad de la información.
- No sacar información de las instalaciones de la organización sin la debida autorización.
- Notificar los incidentes de los que tenga conocimiento a Gestión de la Información por escrito mediante los canales autorizados. Se entiende por incidentes, por ejemplo: la caída del sistema de seguridad informática, intento no autorizado de la salida de un documento o soporte, pérdida de datos o la destrucción total o parcial de soportes, cambio de ubicación física de bases de datos, divulgación de contraseñas a terceros, la modificación de datos por personal no autorizado, etc.

USO ADECUADO DE LOS ACTIVOS:
El acceso a la información estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos, a la competencia del proceso y a los permisos y niveles de acceso del talento humano.

Para la consulta de documentos cargados en el software utilizado en la compañía (CNT, PANACEA, MEDINET, MEDIHelp, MEDINDICADORES, plataformas de lectura de estudios, cuentas de correo institucionales) se establecerán privilegios de acceso al personal de la compañía de acuerdo con el desarrollo de sus funciones y competencias.

ACCESO A INTERNET:
El uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No se permite:

- El acceso a páginas que no tengan relación directa con la actividad laboral.
- Usar servicios interactivos, mensajería instantánea o redes sociales sin autorización.
- El intercambio no autorizado de información de propiedad de Mediagnostica Tecmedi SAS, de sus pacientes o de su talento humano, con terceros.

- Realizar descargas que comprometan la integridad tecnológica.

b) Monitoreo: Gestión de la Información realiza monitoreo permanente de historiales de navegación y páginas web visitadas por parte del talento humano.

c) Responsabilidad individual: Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información.

d) Uso permitido: El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de Mediagnostica Tecmedi S.A.S

CORREO ELECTRONICO:
El talento humano de Mediagnostica Tecmedi SAS que haga uso de una cuenta de correo institucional deberá seguir las siguientes normas:

a) La coordinadora de sede o el líder de proceso es responsable de la entrega de las cuentas de correo a su grupo de trabajo, así mismo de su recepción al momento de traslado o retiro del funcionario, comprometiéndose con el cambio obligatorio de la contraseña ante cualquier novedad.

b) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la compañía.

c) Los mensajes y la información contenida en los buzones de correo son propiedad de Mediagnostica Tecmedi S.A.S y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

d) Se recomiendo que los archivos adjuntos a terceros o externos de la empresa deben ser enviados en formatos no editables. En caso de enviar un formato original, la responsabilidad es exclusiva del usuario del correo.

e) No está permitido utilizar el correo institucional en equipos que no pertenezcan a la infraestructura tecnológica de Mediagnostica Tecmedi S.A.S sin autorización por escrito de la coordinadora de sede o líder de proceso.

f) No se permitirá el acceso a cuentas de correo personales en los equipos de cómputo de Mediagnostica, dentro o fuera de la red de la compañía.

g) Toda cuenta de correo electrónico institucional debe contar con doble factor de autenticación.

RECURSOS TECNOLOGICOS:
El uso adecuado de los recursos tecnológicos asignados por Mediagnostica Tecmedi SAS a su talento humano quedará reglamentado bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de Mediagnostica Tecmedi S.A.S, que no sean considerados como biomédicos es responsabilidad del proceso de Gestión de la Información. En los equipos biomédicos la responsabilidad será del proceso de Ambiente Físico.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, ni realizar actividades de administración remota.

c) No se permite la conexión de dispositivos personales (Celulares, tablets. Etc) a la infraestructura de red de la compañía.

d) Whatsapp: Para el uso y soporte de esta aplicación están autorizados únicamente para el personal de la Central de Citas de Mediagnostica y aquellos con autorización escrita. El proceso o personal que haga uso de este software será responsable del modo de uso, la información procesada y de las copias de seguridad.

CONTROL DE ACCESO FISICO:
Se consideran áreas de acceso restringido aquellas que están definidas para el almacenamiento de información o manejo de comunicaciones. Por lo tanto, estas áreas deben ser protegidas de accesos no autorizados con medidas de control de acceso y procedimientos de seguridad para proteger la información de daños intencionales o accidentales.

PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS:
Los equipos que hacen parte de la infraestructura tecnológica de Mediagnostica Tecmedi SAS deben ser ubicados y protegidos adecuadamente para prevenir pérdidas de información o daños físicos. Se deben adoptar controles para evitar amenazas como fuego, interferencias electromagnéticas. Etc. El proceso de Gestión de Ambiente Físico de Mediagnostica Tecmedi S.A.S monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos.

PROTECCION CONTRA SOFTWARE MALICIOSO: Mediagnostica Tecmedi S.A.S provee de herramientas de protección ante software malicioso, las cuales se encuentran en constante monitoreo y actualización. Adicionalmente se informa al talento humano de las amenazas que pueden afectar la seguridad de la información.

Para garantizar la integridad y confidencialidad de la información, no se permite:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por Gestión de la Información.
- Intentar introducir cualquier código de programación que afecte el desempeño de cualquier dispositivo de la compañía.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- La instalación de cualquier software sin la autorización previa del área de Gestión de la Información está prohibida. Esta medida previene riesgos de seguridad y asegura el cumplimiento de las políticas organizacionales.

ACCESO REMOTO:
El acceso remoto a los equipos dentro de la red de Mediagnostica Tecmedi S.A.S será de uso exclusivo por parte de Gestión de la Información para tareas de monitoreo, soporte o auditoría, teniendo en cuenta los cuidados necesarios con la privacidad de la información alojada en los

equipos.

No se permite el uso de herramientas de acceso remoto que no se encuentren avaladas por Gestión de la Información, ya que será esté proceso el que definirá la forma más segura de brindar acceso, de acuerdo a la necesidad de cada usuario o proceso.

En caso de que se opte por realizar la conexión mediante el uso de una VPN, se debe implementar que el acceso a esta sea con doble factor de autenticación.

TRABAJO A DISTANCIA:
Los equipos que se asignen para realizar trabajo a distancia con y sin acceso virtual deben cumplir con los requisitos de seguridad de la información previamente definidos por Gestión de la Información, adicionalmente el acceso a la red de Mediagnostica Tecmedi S.A.S se hará únicamente mediante conexión por VPN, la cual será asignada y configurada por Gestión de la Información.

COPIAS DE SEGURIDAD:
Gestión de la Información será responsable únicamente de la información almacenada en los servidores instalados en la sede Administrativa, de los servidores de Panacea AWS, y en los cuartos de Sistemas en cada una de las sedes asistenciales.
La información que se encuentre en los computadores asignados a cada funcionario es responsabilidad del usuario final según lo estipulado en las actas de entrega de equipos de cómputo, por lo tanto, es responsabilidad de cada proceso definir la información a la cual debe realizar sus copias de seguridad y los dispositivos autorizados para este fin. Se establece la frecuencia de copias de seguridad como mínimo una vez por semana.

GESTIÓN DE MEDIOS REMOVIBLES:
El uso de medios de almacenamiento removibles (ejemplo: CD’s, DVD’s, memorias USB, discos duros externos etc) estará permitido siempre y cuando el proceso de Gestión de la Información tenga conocimiento de este, y en el caso que aplique, haya pasado por un proceso de verificación de seguridad antes de su uso. Cualquier uso no informado será considerado como “incidente de seguridad” y será reportado.

INTERCAMBIO DE INFORMACION:
Todo el talento humano de Mediagnostica Tecmedi S.A.S es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

CONTROL DE ACCESO LÓGICO:
Todo acceso a las diferentes bases de datos de la compañía debe cumplir un conducto regular de solicitud de creación y/o modificación por parte del líder de cada usuario mediante ticket en la plataforma de MediHelp dirigido a Gestión de la Información.

Previo a la entrega de cualquier usuario o clave, debe realizarse una capacitación en seguridad de la información, de tal forma que todo el talento humano comprenda su responsabilidad del buen uso que haga de las credenciales de acceso asignadas, ya que son de uso personal e intransferible. Así mismo y como protocolo de seguridad, cada usuario deberá realizar modificación a sus contraseñas de acceso como mínimo una vez cada tres meses.

Dependiendo de las políticas de seguridad de cada sistema de información se establece como recomendación de contraseñas seguras: mínimo 8 caracteres, combinando letras mayúsculas, minúsculas y números.

Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de información de Mediagnostica Tecmedi S.A.S, debe estar autorizado exclusivamente por Gestión de la Información.

SEGURIDAD BÁSICA EN PUESTOS DE TRABAJO:
Para evitar filtraciones de información, todo el talento humano en Mediagnostica Tecmedi S.A.S debe garantizar la confidencialidad cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales.

Esto incluye: documentos impresos, CD's, dispositivos de almacenamiento USB y medios removibles autorizados en general. Todos los equipos deben ser apagados al finalizar la jornada laboral para prevenir daños físicos.

MODIFICACIÓN:
Mediagnostica Tecmedi SAS se reserva el derecho de modificar esta Política en cualquier momento y notificará a los Titulares sobre cualquier cambio, con la actualización del contenido en la página web y en los documentos que la incluyan.

TABLA DE CONTROL DE CAMBIOS

VERSIÓN	CAMBIO	JUSTIFICACIÓN
1	Versión Inicial	Cumplimiento a requisito legal. Ley 1581 de 2012 y su Decreto 1377 de 2013.
2	1. Unificación de criterios, buscando reducir el tamaño del documento y evitar la redundancia. 2. Ingresar políticas para el manejo de archivo físico. 3. Ingresar políticas de manejo de Whatsapp.	Ciclo de revisión de documentación del proceso.
3	1. Adición de roles y responsables, junto con los lineamientos del comité de seguridad de la información. 2. Adición de norma de acceso remoto y teletrabajo 3. Se agregan controles de acceso relacionados con correo electrónico. 4. Unificación de criterios.	Ciclo de revisión de documentación del proceso.
4	Se adiciona al marco legal: Resolución 746 de 2022 del Ministerio TIC. Decreto 338 de 2022. Se modifican los item de referentes a: Correo electrónico, WhatsApp, Protección contra Software malicioso, Acceso remoto, Copias de seguridad, Gestión de medios removibles, Control de acceso lógico.	Ciclo de revisión de documentación del proceso.

TABLA DE AUTORIZACIONES

ELABORÓ	REVISÓ	APROBÓ
Nombre: Leidy Milena Díaz A.	Nombre: Leidy Milena Díaz A.	Nombre: Arleys San Martín Bolívar
Cargo: Directora de Gestión de la Información	Cargo: Directora de Gestión de la Información	Cargo: Director de Calidad y Mejora Continua
Fecha: 09/07/2025	Fecha: 09/07/2025	Fecha: 10/07/2025