INTRODUCCIÓN

Con el ánimo de mejorar la estrategia de Seguridad de la información de MEDICA COLOMBIA S.A.S., surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información. Para tal fin, es necesario establecer una Política general de Seguridad y protección de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

La Política general de seguridad y protección de la información es la declaración general que representa la posición de la Alta dirección de MEDICA COLOMBIA S.A.S con respecto a la protección de los activos de información. Este documento formaliza el compromiso de la dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales la entidad establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la Entidad, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad y sus convenios.

Con la implementación de políticas en seguridad de la información MEDICA COLOMBIA S.A.S busca dar cumplimiento a disposiciones legales y regulatorias emitidas por los diferentes organismos estatales, contar con una metodología de gestión de riesgos como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad de los procesos de la entidad.

Esta Política establece las responsabilidades generales aplicables a MEDICA COLOMBIA S.A.S. en lo que respecta al uso adecuado de la información y se

acompañará de otras políticas específicas enfocadas a grupos, servicios o actividades particulares.

1. NORMATIVIDAD

- Constitución Política de Colombia
- LEY 1581 DE 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- 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
- Ley 527-1999 Ley de comercio electrónico.

2. ALCANCE

El documento de Política de Seguridad de la Información reglamenta la protección y uso de los activos de información de MEDICA COLOMBIA S.A.S. y por tanto está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos (Colaboradores, contratistas, proveedores y otros)

3. DEFINICIONES

- **Confidencialidad**: los activos de información solo pueden ser accedidos y cust odiados por usuarios que tengan permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.
- **Autenticidad:** Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **Posibilidad de Auditoría:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

- **Protección a la duplicación:** Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- **No repudio:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- **Confiabilidad de la Información:** Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.
- **Activo de información:** recurso del sistema de información que tiene valor para la organización.
- **Activos de información:** bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura y las personas responsables de genera, transmitir y destruir información).
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
- **Evento de seguridad de la información:** Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
- **Incidente de seguridad de la información:** Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de MEDICA COLOMBIA S.A.S y amenazar la seguridad de la información.
- **Información confidencial (RESERVADA):** Información administrada por MEDICA COLOMBIA S.A.S en cumplimiento de sus deberes y funciones y que debido a aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.

- **Información confidencial (CONFIDENCIAL):** Información generada por MEDICA COLOMBIA S.A.S. en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de esta y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.
- **Información privada (USO INTERNO):** Información generada por la Cámara de Comercio en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.
- **Información pública:** Es la información administrada por MEDICA COLOMBIA S.A.S. en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo, la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social.

4. POLÍTICA GENERAL DE SEGURIDAD Y PROTECCION DE LA INFORMACIÓN

La gerencia de MEDICA COLOMBIA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de esta política que busca 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.

MEDICA COLOMBIA, con la protección de la información busca disminuir del impacto generado sobre sus activos, por los riesgos identificados 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 estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la institución.
- Cumplir con los principios de seguridad de la información.
- 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.
- Garantizar la continuidad del negocio frente a incidentes.

Por lo anterior mencionado MEDICA COLOMBIA declara que 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.

A continuación, se establecen los principios de seguridad que soportan la Política general de Seguridad y Protección de la Información de MEDICA COLOMBIA S.A.S:

- Proteger 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.

- Proteger 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.

- Proteger la información de las amenazas originadas por parte del personal.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizar 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.
- Garantizar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Utilizar la información solamente para fines de interés público de conformidad con la constitución y las leyes.
- La información confidencial de terceros que por cualquier circunstancia se conozca por parte de MEDICA COLOMBIA S.A.S., debe ser tratada bajo los mismos lineamientos establecidos para el tratamiento de la información confidencial de la Entidad.

- El acceso a los diferentes equipos informáticos y sistemas de información debe hacerse a través de los mecanismos de autenticación establecidos de acuerdo con los niveles de seguridad.

5. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

MEDICA COLOMBIA garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

1. Subgerencia
2. Dirección Médica.
3. Área de calidad.
4. Área de gestión Humana.
5. Área de Servicio al cliente.
6. Área financiera y contable.
7. Sistemas.

8. RESPONSABILIDADES

Área de Gestión de Calidad: es responsable de revisar y proponer a la gerencia para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la institución.

Los propietarios de activos de información: (Todos los colaboradores de la organización) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Coordinador de Talento Humano: será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

Asesor Jurídico: verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

El área de calidad: es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información.

9. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el

Comité de Seguridad de la Información, correspondiendo al área de Sistemas brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

10. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal de MEDICA COLOMBIA, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El área de Sistemas debe mantener un directorio completo y actualizado de tales perfiles.

11. SEGURIDAD FÍSICA Y DEL ENTORNO

Acceso: Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones.

Reporte e investigación de incidentes de seguridad: Todo el personal responsable de la información debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través del área de sistemas.

Protección contra software malicioso y hacking: Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

Copias de Seguridad: Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información.

Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Intercambio de Información con Organizaciones Externas: Las peticiones de información por parte de entes externos de control y clientes deben ser aprobadas por subgerencia.

Internet y Correo Electrónico: El correo electrónico institucional se debe usar con fines propios del cargo, no se debe manejar ni generar información personal, cualquier correo considerado como sospechoso se debe informar al área de sistemas.

Instalación de Software: Todas las instalaciones de software que se realicen sobre sistemas de la institución deben ser aprobadas por la subgerencia y el área de sistemas.

Nota: No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas.

12. CONTROL DE ACCESO

Categorías de Acceso: El acceso a los recursos de tecnologías de información institucionales debe estar restringidos según los perfiles de usuario definidos por el área de talento humano.

Control de Claves y Nombres de Usuario: El acceso a información restringida debe estar controlado en el caso de MEDICA COLOMBIA corresponde a información restringida la manejada en la historia clínica SEAD, y la información financiera y contable.

Corresponde al área de Sistemas en conjunto con la los proveedores de los softwares de historia clínica y contable elaborar, mantener y publicar los documentos de manuales de usuarios ofrece la institución a su personal.

El control de las contraseñas de red y uso de equipos es responsabilidad del área de sistemas.

Como requisito para la terminación de relación contractual - o laboral - del personal,

Se debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la institución.

13. POLÍTICAS ESPECÍFICAS

Forman parte integral de la Política de Seguridad de la Información, todas aquellas directrices que por su tema particular, requieren un mayor nivel de detalle y especialización para su definición, las cuales son elaboradas y mantenidas por las áreas de seguridad, según el dinamismo de la misión de MEDICA COLOMBIA S.A.S. las cuales a su vez pueden estar complementadas por estándares y guías.

14. CUMPLIMIENTO.

MEDICA COLOMBIA S.A.S reconoce abiertamente la importancia de la seguridad de la información, así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el uso inadecuado de los activos de información puede poner en peligro la continuidad de la prestación de los servicios o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos. Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización.

El desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado y lo estipulado en el Reglamento Interno de trabajo.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos de información de MEDICA COLOMBIA S.A.S con el objetivo de lograr un nivel de riesgo aceptable de

acuerdo con la visión, misión, planeación y estrategia de la compañía, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

Estas políticas a todo nivel, son mandatarias, por lo tanto deben ser cumplidas por todos los funcionarios, contratistas, proveedores y terceros que interactúen con los Sistemas de Información y demás recursos informáticos de MEDICA COLOMBIA S.A.S.

15. NOTIFICACIÓN DE INCIDENTES.

Toda violación de estas políticas se deberá notificar inmediatamente a servicioalcliente@medicacolombia.com

_____

SONIA LUCIA ARIAS HOYOS
Representante Legal