1. OBJETIVO DE LA POLÍTICA:

Definir los principios y las reglas básicas que garanticen la integridad, confidencialidad y disponibilidad de la información al interior de la EPS Familiar de Colombia, así como proteger los activos y la infraestructura tecnológica de la EPS contra amenazas y riesgos de seguridad.

2. ALCANCE DE LA POLÍTICA:

La presente política aplica a empleados, prestadores de servicio, terceros y demás partes interesadas que por sus funciones acceden, procesan, transportan y/o almacenan información de la EPS Familiar de Colombia y/o de terceros.

La Política deberá estar disponible en la página web corporativa de la EPS Familiar de Colombia www.epsfamiliardecolombia.com y en un repositorio común de la EPS Familiar de Colombia, de forma que sea accesible por todas las personas.

3. RESPONSABLES DE APLICACIÓN DE LA POLÍTICA

Los roles y responsabilidades en la implementación y mantenimiento de la política de seguridad de la EPS Familiar de Colombia son:

3.1. **Directivos:** Tienen la responsabilidad de establecer una cultura de seguridad y asignar recursos adecuados para la implementación y mantenimiento de la política de seguridad. También son responsables de supervisar el cumplimiento de las políticas y procedimientos de seguridad.

3.2. **Oficial de Seguridad de la Información:** Es responsable de liderar la estrategia de seguridad de la información de la EPS. Supervisa la implementación de controles de seguridad, coordina la respuesta a incidentes de seguridad y garantiza el cumplimiento de las regulaciones y normativas de seguridad.

3.3. **Vicepresidencia TIC:** Este equipo se encarga de implementar y mantener los controles de seguridad, monitorear los sistemas en busca de posibles amenazas, y responder a incidentes de seguridad.

3.4. **Empleados de la EPS Familiar de Colombia:** Deben seguir las políticas de seguridad al acceder a sistemas y datos de la EPS, y reportar cualquier incidente de seguridad o sospecha de actividad maliciosa.

3.5. **Terceros, proveedores, prestadores:** Tienen la responsabilidad de utilizar los sistemas de manera segura, seguir las políticas de seguridad establecidas y participar en la capacitación y concientización sobre seguridad.

Estos roles y responsabilidades colaboran en la protección de la información y los activos de la EPS, asegurando la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos para la atención médica.

4. TÉRMINOS Y DEFINICIONES

4.1. Información: es todo lo que reduce la incertidumbre entre varias alternativas posibles. Son los datos que necesitamos conocer para tomar decisiones de manera más efectiva (Olivarez, 2010).

4.2. Datos: Conjunto de símbolos que representan la información de manera que se permita su procesamiento (Olivarez, 2010)

4.3. Sistema Informático: Es el conjunto de elementos necesarios para la realización y utilización de aplicaciones informáticas. Está integrado por cuatro elementos principales: Equipos (hardware), Programas (software), Firmware y Personal informático (Olivarez, 2010)

4.4. Confiabilidad: Es la probabilidad de que un sistema se comporte tal y como se espera de él (Calderón Arateco, 2015)

4.5. Confidencialidad: En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos (Calderón Arateco, 2015)

4.6. Integridad: En términos de seguridad de la información, la 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 (Calderón Arateco, 2015)

4.7. Autenticación: Verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos (Calderón Arateco, 2015)

4.8. Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización (Calderón Arateco, 2015)

4.9. Vulnerabilidad: Se define como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

5. DESARROLLO DE LA POLÍTICA

5.1. Principios de la Política de Seguridad la Información

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar la EPS Familiar de Colombia.

Además, la EPS Familiar de Colombia establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- **Alcance estratégico:** La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de la EPS Familiar de Colombia de forma que

pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.

- **Principio de disponibilidad:** Garantizar que la información y los sistemas de la EPS estén disponibles cuando se necesiten, minimizando el tiempo de inactividad y los tiempos de respuesta.
- **Gestión de riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando la probabilidad y el impacto de posibles amenazas.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
- Para el logro de los objetivos de esta Política, la EPS Familiar de Colombia deberá establecer una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación. La EPS Familiar de Colombia mantendrá la definición tanto del nivel de riesgo residual aceptado como de sus umbrales de tolerancia.

5.2. Formación y concienciación

La EPS Familiar de Colombia deberá asegurar que todo el personal recibe un nivel de formación y concienciación adecuado en materia de Seguridad de la Información, especialmente en materia de confidencialidad y prevención de fugas de información.

Así mismo, los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que pueda garantizarse el cumplimiento de esta Política.

Por otro lado, los empleados tienen la obligación de actuar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

5.3. Gestión de activos de información

La EPS Familiar de Colombia reconoce que la información es un activo valioso que debe ser protegido adecuadamente. Por lo tanto, se establece un procedimiento de gestión de activos de información para identificar, clasificar, proteger y mantener la integridad y la confidencialidad de los datos.

- **Identificar activos:** Se llevará a cabo un inventario completo de todos los activos de información de la EPS.
- **Clasificar activos:** Basado en su importancia y sensibilidad, cada activo de información será clasificado en diferentes niveles de seguridad. Esto permitirá aplicar medidas de protección adecuadas según el nivel de riesgo asociado a cada activo.
- **Proteger activos:** Se implementarán controles de seguridad física y lógica para proteger los activos de información contra accesos no autorizados, modificaciones no autorizadas y divulgación no deseada.
- **Mantener activos:** Se establecerán procedimientos para garantizar el mantenimiento continuo de los activos de información, incluyendo la aplicación de parches de seguridad, actualizaciones de software y copias de seguridad regulares. Esto asegurará la disponibilidad y la integridad de los datos en todo momento.
- **Supervisar y revisar:** La gestión de activos de información será supervisada y revisada regularmente para garantizar su eficacia y hacer ajustes según sea necesario. Se

realizarán auditorías periódicas para evaluar el cumplimiento de las políticas y procedimientos establecidos.

Además, la EPS Familiar de Colombia deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases: creación o recolección, distribución, uso o acceso, almacenamiento, destrucción.

5.4. Gestión de las copias de seguridad

La EPS Familiar de Colombia garantiza la conservación de la información mediante copias de seguridad y respaldo de aplicaciones, ficheros y bases de datos apoyado en un procedimiento para su adecuada implementación, donde su frecuencia se determinará en función de la sensibilidad e importancia de las aplicaciones o datos.

Se deberán realizar pruebas de restauración de las copias de seguridad disponibles y de los procesos de restauración definidos, a fin de garantizar el funcionamiento correcto de los procesos. Estas se realizarán de forma periódica y quedarán documentadas.
Se deberá establecer un período de retención de las copias de seguridad hasta su destrucción una vez terminado el periodo de existencia.

Las copias de seguridad, tanto de archivos maestros como de aplicaciones y archivos de información se deberán ubicar en lugares seguros con acceso restringido. Así mismo, las copias de respaldo se ubicarán preferentemente en un centro distinto al que las generó.

Todos los empleados de la EPS Familiar de Colombia tienen la obligación de respaldar la información almacenada en los equipos de cómputo asignados. La Vicepresidencia TIC brindará las herramientas tecnológicas requeridas para tal fin. El Oficial de Seguridad tendrá acceso sin restricciones, a la información almacenada en los equipos de cómputo de los empleados de la EPS Familiar de Colombia, para garantizar la completitud y oportunidad de estas copias.

5.5. Gestión de accesos

La EPS Familiar de Colombia se compromete a garantizar que el acceso a los sistemas y datos esté adecuadamente controlado y protegido para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Con este fin, se establece un procedimiento integral de gestión de accesos basado en los principios de necesidad de acceso mínimo, segregación de funciones y autenticación sólida.

Se asignarán identificaciones de usuario únicas a cada empleado, acompañadas de medidas de autenticación robustas, como contraseñas seguras, para verificar la identidad de los usuarios antes de permitirles acceder a los sistemas y datos de la EPS.

Los privilegios de acceso se asignarán de manera específica y limitada, basados en las responsabilidades laborales de cada empleado y en el principio de necesidad de acceso mínimo. Esto se realizará mediante roles y perfiles de usuario que definan los niveles de acceso necesarios para cada función dentro de la organización.

Además, se establecerán procedimientos para la creación, modificación y eliminación de cuentas de usuario de manera segura y oportuna.

La EPS Familiar de Colombia deberá definir la Norma de buen uso y responsabilidad sobre la información alineada con las buenas prácticas en seguridad. La Norma de buen uso y responsabilidad sobre la información definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña y deberá ser conocida por todos los empleados de la EPS Familiar de Colombia.

El Oficial de Seguridad debe velar por la confidencialidad y administración de los usuarios y contraseñas de carácter institucional, utilizados para acceder a los portales transaccionales de terceros.

5.6. Privacidad de la información

La EPS Familiar de Colombia deberá asegurar la privacidad de los datos de carácter personal con el objetivo de proteger los derechos fundamentales de las personas físicas, especialmente su derecho al honor, intimidad personal y familiar y a la propia imagen, mediante el establecimiento de medidas para regular el tratamiento de los datos.

La EPS Familiar de Colombia deberá cumplir con la legislación vigente en materia de protección de datos personales en función de la jurisdicción en la que esté establecida y opere (a modo ilustrativo, la Ley 1581 de 2012, de Protección de Datos y el Proyecto deLey 300 de 2020 Garantías de los Derechos Digitales en Colombia) y deberá incluir las medidas necesarias para cumplir con la normativa.

5.7. Prevención de fugas de información y gestión de incidentes

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros. Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información.

La EPS Familiar de Colombia deberá definir procedimientos para evitar la ocurrencia delas situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Todos los empleados de la EPS Familiar de Colombia tienen la obligación y responsabilidad de la identificación y notificación de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información.

Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina

un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

5.8. Continuidad de Negocio

Respondiendo a requerimientos de calidad y buenas prácticas, la EPS Familiar de Colombia deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la sociedad actúe en caso de ser necesario. Este Plan de Continuidad deberá ser actualizado y probado periódicamente. Además, se deberá definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio, este plan abarcará la continuidad del funcionamiento de las tecnologías de información y comunicación.

5.9. Seguridad en los Proveedores

Sobre los proveedores de servicios que gestionen información de la EPS familiar de Colombia, deberán definirse y velar por su cumplimiento, los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en la presente Política.

5.10. Sanciones disciplinarias

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de

la EPS Familiar de Colombia. Es responsabilidad de todos los empleados de la EPS Familiar de Colombia notificar al responsable de Seguridad de la Información de la sociedad afectada cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

5.11. Revisión de la Política

La presente Política de Seguridad de la Información, será revisada y aprobada por la Junta Directiva de la EPS Familiar de Colombia. Si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de la EPS Familiar de Colombia.

6. NORMATIVIDAD:

- Ley 1581 de 2012, de Protección de Datos
- Proyecto de Ley 300 de 2020 Garantías de los Derechos Digitales en Colombia
- Ley 1273 de 2009 – De La Protección de la Información y de los datos.
- ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27002:2005 – Código para la Práctica de la Gestión de la Seguridad de la Información.
- ISO 22301:2012 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO: 9001.
- Resolución 497 del 2021

7. CONTROL DE CAMBIOS

VERSIÓN	ÍTEM	CAMBIO REALIZADO	JUSTIFICACIÓN	FECHA
1	Todos	Elaboración del documento	Elaboración del documento	01/04/2023
2	Todos	Se reestructura y actualiza documento.	Modificación del documento	30/04/2024