POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

EPS FAMILIAR DE COLOMBIA
Junto a ti

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Política de Seguridad de la Información (en adelante, Política) persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información,y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio de laEPS Familiar de Colombia.

Esta Política de Seguridad de la Información es la pieza angular por la que se rige el Cuerpo Normativo de Seguridad de la EPS Familiar de Colombia. El Cuerpo Normativo Seguridad (en adelante, CNS) es un conjunto de documentos a diferentes niveles que conforman de los requerimientos, directrices y protocolos que debe seguir la EPS Familiar de Colombia en materia de seguridad. El CNS deberá ser desarrollado por cada sociedad de la EPS Familiar de Colombia mediante un conjunto de documentos (normas de uso, estándares normativos, procedimientos, manuales, guías, buenas prácticas, etc.) de tal manera que cubran todos los aspectos que se presentan en la Política, llegando a nivel de proceso operativo.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

2. OBJETIVOS

2.1. Objetivos Generales

El objetivo principal de la presente Política de alto nivel es definir los principios y las reglas básicas para la gestión de la seguridad de la información. El fin último es Constituir los lineamientos y políticas de seguridad de la información de la EPS Familiar de Colombia garanticen la seguridad de la información, la integridad, confiabilidad y disponibilidad de la gestión de la información al interior de la compañía.

2.2. Objetivos Específicos

- Gestionar y mantener la seguridad de la información que se procesa dentro de la entidad y los servicios habilitados para los entes externos.
- Buscar que los clientes, contrapartes, terceros y trabajadores, conozcan sus responsabilidades y deberes, de la misma manera, estén informados de las amenazas respecto a la seguridad de la información con el fin de minimizar los riesgos de seguridad.
- Impedir el acceso sin autorización a los sistemas de información e infraestructura tecnológica de la entidad, así como el daño a la información de la entidad.
- Evitar daño, pérdida, robo o puesta en riesgo de los activos de información y la interrupción de las actividades de la entidad.
- Establecer los perfiles y roles dentro de la empresa, para la gestión y seguridad de la información.
- Definir directrices para contrarrestar las interrupciones en las actividades de la entidad y proteger los procesos más críticos en caso de fallas importantes de los sistemas de información o la infraestructura tecnológica y asegurar su restablecimiento adecuado.

3. ALCANCE

La Política es aplicable para todo la EPS Familiar de Colombia, que deberá cumplir este mínimo requisito sin perjuicio de tener políticas más restrictivas y mejorar la seguridad en la medida de lo posible. Adicionalmente, las filiales deberán adaptar y desarrollar esta Política en sus sociedades y deberán reportar a la matriz de la EPS Familiar de Colombia su adecuación a dicha Política, en ejecución de los procesos de monitorización del sistema de gestión de Compliancia de la EPS Familiar de Colombia. El alcance de la presente Política abarca toda la información de las sociedades de la EPS Familiar de Colombia con independencia de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente.

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 de la EPS Familiar de Colombia.

4. DEFINICIONES

- Tecnología: Es el proceso que le permite a los seres humanos diseñar herramientas y máquinas para controlar su ambiente material y aumentar la comprensión de este. (Olivarez, 2010) (Olivarez, 2010)
- 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) (Olivarez, 2010)
- Datos: Conjunto de símbolos que representan la información de manera que se permita su procesamiento. (Olivarez, 2010) (Olivarez, 2010)
- 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) (Olivarez, 2010)
- Hardware: Es el conjunto de piezas físicas que integran una computadora: unidad central de proceso, placa base, periféricos y redes. (Olivarez, 2010) (Olivarez, 2010)
- Redes: Hay dos tipos de redes. Uno de ellos son las redes locales, conocidas como LAN (local area network), que son un conjunto de computadoras personales conectadas entre si. El otro tipo de red son las redes de área amplia, conocidas como las computadoras están separadas por grandes dista 12 CPU guarda mucha información y se puede comunicar con el WAN (wide area network), en las que distancias. (Olivarez, 2010) (Olivarez, 2010)
- Software: Contiene las instrucciones que le permiten al equipo físico realizar una tarea específica. Están entregados por varios archivos que realizan diversas funciones. Hay tres tipos de software: los sistemas operativos, los lenguajes de programación y las aplicaciones informáticas. (Olivarez, 2010) (Olivarez, 2010)
- Personal Informático: Son los usuarios del sistema informático de los desarrolladores, quienes diseñan el sistema y el personal que se encarga de mantenerlo en funcionamiento. (Olivarez, 2010) (Olivarez, 2010)
- Confiabilidad: Es la probabilidad de que un sistema se comporte tal y como se espera de él. (Calderón Arateco, 2015) (Calderón Arateco, 2015)
- 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) (Calderón Arateco, 2015)
- 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) (Calderón Arateco, 2015)

- 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) (Calderón Arateco, 2015)
- Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. (Calderón Arateco, 2015) (Calderón Arateco, 2015)
- Administración: establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. (Calderón Arateco, 2015) (Calderón Arateco, 2015)
- Vulnerabilidad: Se define como debilidad de cualquier tipo que compromete la seguridad del sistema informático.
- Política de seguridad: se define como una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas. (Calderón Arateco, 2015) (Calderón Arateco, 2015) Contraseña: Es un código o una palabra que se utiliza para acceder a datos y sitios restringidos de una computadora. Las contraseñas generan cierta seguridad contra los usuarios no autorizados: el sistema de seguridad sólo puede confirmar que la contraseña es válida, y no si el usuario está autorizado a utilizar esa contraseña. (Grau, 2016) (Grau, 2016)

5. GENERALIDADES

5.1. Principios de la Política de 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 las sociedades 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.

- Seguridad integral: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información
- 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 los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- 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. La seguridad de la información será atendida, revisada y auditada por personal cualificado.
- Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

- La EPS Familiar de Colombia considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los niveles jerárquicos de su personal.

- Puesto que la Seguridad de la Información incumbe a todo el personal de la EPS Familiar de Colombia, esta Política deberá ser conocida, comprendida y asumida por todos sus empleados.

- Para la consecución 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. En el transcurso de este ciclo de mejora continua, la EPS Familiar de Colombia mantendrá la definición tanto del nivel de riesgo residual aceptado (apetito al riesgo) como de sus umbrales de tolerancia.

5.2. Compromiso de la Dirección

La Dirección de la EPS Familiar de Colombia, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados de la EPS Familiar de Colombia.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

5.3. Roles y responsabilidades

La EPS Familiar de Colombia se compromete a velar por la Seguridad de todos los activos bajo su responsabilidad mediante las medidas que sean necesarias, siempre garantizando el cumplimiento de las distintas normativas y leyes aplicables.

Tanto la EPS Familiar de Colombia como cada filial deberán nombrar una figura responsable de definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura deberá establecerse desde un entorno de gobierno y gestión, será independiente de cualquier área organizativa reportando al órgano de gobierno o en su defecto a su comisión de auditoría y tendrá entre sus funciones y responsabilidades el aplicar principios de segregación de funciones y el contacto con las autoridades y grupos de interés especiales en materia de seguridad de la información.

La figura asumirá las funciones que, con carácter general, sean atribuidas por la presente Política de Seguridad de la Información a dicha figura.

Será su responsabilidad desarrollar y mantener la Política, asegurándose que ésta sea adecuada y oportuna según evolucione tanto la sociedad de la EPS Familiar de Colombia de la que sea responsable como la regulación vigente.

Todos los funcionarios, contratistas y terceras partes de la EPS Familiar de Colombia: Cumplir con las políticas de seguridad de la EPS.

5.4. Gestión de la Seguridad de los Recursos Humanos

El departamento de Recursos Humanos deberá realizar su gestión teniendo en cuenta los criterios de seguridad establecidos en la Política de Seguridad de la Información, siendo este un punto clave para asegurar su cumplimiento.

Se deberán salvaguardar los requisitos establecidos en la presente Política en todo momento, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desistimiento de contratos de los empleados.

5.5. 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 en los plazos que exija la normativa vigente, especialmente en materia de confidencialidad y prevención de fugas de información.

Asimismo, 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 obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

6. DESCRIPCION DE LA POLITICA

6.1. Política de mesas limpias

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos (véase el Anexo: Niveles de clasificación).
- Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

6.2. Gestión de activos

Se deberán tener identificados e inventariados los activos de información necesarios para la prestación de los procesos de negocio de la EPS Familiar de Colombia. Adicionalmente, se deberá mantener actualizado el inventario de activos.

Se deberá realizar la clasificación de los activos en función del tipo de información que se vaya a tratar, de acuerdo con lo dispuesto en el apartado 7. Clasificación de la información.

Se deberá asignar un responsable encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida. El responsable deberá mantener un registro formal de los usuarios con acceso autorizado a dicho activo.

Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido.

Se deberán actualizar de manera periódica las configuraciones de los activos para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

6.3. Gestión del ciclo de vida de la información

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. El ciclo de vida de un activo de información consta de las siguientes fases:

1. Creación o recolección: esta fase se ocupa de los registros en su punto de origen. Esto podría incluir su creación por un miembro de la EPS Familiar de Colombia o la recepción de información desde una fuente externa. Incluye correspondencia, formularios, informes, dibujos, entrada/salida del ordenador u otras fuentes.
2. Distribución: es el proceso de gestión de la información una vez que se ha creado o recibido. Esto incluye tanto la distribución interna como externa, ya que la información que sale de la EPS Familiar de Colombia se convierte en un registro de una transacción con terceros.
3. Uso o acceso: se lleva a cabo después de que la información se distribuya internamente, y puede generar decisiones de negocio, generar nueva información, o servir para otros fines. Detalla el conjunto de usuarios autorizados por la EPS Familiar de Colombia a acceder a la información.
4. Almacenamiento: es el proceso de organizar la información en una secuencia predeterminada y la creación de un sistema de gestión para garantizar su utilidad dentro de la EPS Familiar de Colombia. Si no se establece un método de almacenamiento para la presentación de información, su recuperación y uso resultaría casi imposible.
5. Destrucción: establece las prácticas para la eliminación de la información que ha cumplido los periodos de retención definidos y la información que ha dejado de ser útil para la EPS Familiar de Colombia. Los periodos de conservación de la información deberán estar basados en los requisitos normativos, legales y jurídicos que afectan la EPS Familiar de Colombia. También deberán tenerse en cuenta las necesidades de negocio. Si ninguno de estos requisitos exige que la información sea conservada, deberá ser desechada mediante medios que garanticen su confidencialidad durante el proceso de destrucción.

La EPS Familiar de Colombia deberá identificar medidas de seguridad de acuerdo con la presente Política para asegurar la correcta gestión del ciclo de vida de los activos.

6.4. Gestión de las copias de seguridad

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, semanal, salvo que en dicho período no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de impacto alto para la EPS Familiar de Colombia y/o de elevado nivel de transaccionalidad.

Como normal general, la frecuencia con la que se realizarán las copias de seguridad se determinará en función de la sensibilidad de las aplicaciones o datos, de acuerdo con los criterios de clasificación de información declarados en el anexo "Niveles de clasificación".

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados.

Como norma general y siempre que sea posible, se deberá requerir que la información en las copias de seguridad esté cifrada. Este requerimiento será obligatorio para determinados tipos de información confidencial.

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. Asimismo, las copias de respaldo se ubicarán preferentemente en un centro distinto al que las generó.

Se deberá garantizar que existe una copia de seguridad adicional de la información sensible protegida ante escritura, de forma que se garantice su integridad ante la necesidad de recuperación frente a posibles incidencias de seguridad asociadas, por ejemplo, a Ransomware.

6.5. Clasificación de la información

Se deberá definir un modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad. El modelo de clasificación deberá integrar los requisitos y condiciones establecidos en el presente apartado de la Política.

El modelo de clasificación deberá tener un responsable encargado de su actualización cuando se crea conveniente, así como de dar a conocer el modelo de clasificación a todos los empleados de la EPS Familiar de Colombia.

6.6. Tipos de información

La EPS Familiar de Colombia deberá clasificar la información en función del soporte en el que está siendo utilizado:

a) Soportes lógicos: información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.
b) Soportes físicos: información que esté en papel, soportes magnéticos como USBs, DVDs, etcétera.

6.7. Niveles de clasificación

En función de la sensibilidad de la información, la EPS Familiar de Colombia deberá catalogar la información en cinco niveles, véase la definición precisa en el Anexo "Niveles de clasificación":

- Uso público
- Difusión limitada
- Información confidencial
- Información reservada
- Información secreta

6.8. Gestión de información privilegiada

La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada. Este tipo de información se deberá enviar cifrada y mediante protocolos seguros.

6.9. Manipulación de la información

La EPS Familiar de Colombia se encargará de desarrollar e implementar un conjunto adecuado de procedimientos para la correcta manipulación de la información. Se deberán

adoptar las medidas necesarias para proteger la información de acuerdo con su clasificación.

La información privilegiada estará en todo momento custodiada durante todo el ciclo de vida de esta.

6.10. 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 de Ley 300 de 2020 Garantías de los Derechos Digitales en Colombia) y deberá incluir las medidas necesarias para cumplir con la normativa.
Se deberán implementar medidas adecuadas para asegurar la privacidad de la información en todas las fases de su ciclo de vida (de acuerdo con el apartado 6.2. Gestión del ciclo de vida de la información).

6.11. Prevención de fugas de información

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 deberán analizar los vectores de fuga de información, en función de las condiciones y operativa de trabajo de cada sociedad de la EPS Familiar de Colombia. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo para cada sociedad, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos en sus diferentes estados del ciclo de vida.

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

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad conocidos

- Uso adecuado de dispositivos extraíbles como USBs, Discos Extraibles o similares
- Uso del correo electrónico
- Transmisión de información de forma oral
- Impresión de documentación
- Salida de documentación
- Uso de dispositivos móviles
- Uso de Internet
- Escritorios limpios y ordenados (véase el apartado 5.2. Política de mesas limpias)
- Equipos desatendidos

6.12. Control de acceso

Todos los sistemas de información de la EPS Familiar de Colombia deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.

El control de acceso se entenderá desde la perspectiva tanto lógica (enfocado a sistemas de la información) como física (véase el apartado 11. Seguridad Física y del Entorno).

6.12.1. Requisitos de negocio para el control de acceso

La EPS Familiar de Colombia deberá asumir una serie de requisitos de negocio para el control de acceso, que serán, al menos, los siguientes:

- Los usuarios deberán ser únicos y no podrán ser compartidos. Asimismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio.
- Se prohibirá el uso de usuarios genéricos. En su defecto, se utilizarán cuentas de usuario asociadas a la identidad nominal de la persona asociada.
- Siempre que sea posible, se deberá de disponer de un doble factor de autenticación (MFA) para el acceso a los sistemas de información, siendo obligatorio para aquellos que puedan ser accesibles desde redes públicas.

6.12.2. Derechos de acceso

La EPS Familiar de Colombia deberá implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.
Los derechos de acceso deberán ser establecidos en función de:

- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: Solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.
- Asimismo, ningún usuario deberá poder acceder por sí mismo a un sistema de información controlado sin la aprobación del responsable del propio usuario (o de la persona designada).

6.12.3. Control de acceso lógico

La EPS Familiar de Colombia deberá establecer una Política de contraseñas adecuada y alineada con las buenas prácticas en seguridad. La política de contraseñas definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña.

La Política de contraseñas deberá ser conocida por todos los empleados de la EPS Familiar de Colombia.

6.13. Teletrabajo

Se deberá controlar el acceso remoto a la red de las sociedades de la EPS Familiar de Colombia en la modalidad de trabajo a distancia, esto es, desde fuera de las instalaciones propias.

Los servicios de conexión al trabajo en remoto estarán destinados exclusivamente a personal de la EPS Familiar de Colombia. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del responsable de seguridad.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto podrá ser propiedad del empleado o proporcionado por la EPS Familiar de Colombia. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

a) Capacidad de realizar una conexión a través de una VPN.
b) Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.
c) Software antivirus instalado.
d) Software de firewall/cortafuegos personal instalado.

El teletrabajo desde un equipo propio del trabajador requerirá de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo en remoto no suponga una amenaza

para la seguridad de la información de la EPS Familiar de Colombia. Además, se podrán establecer medidas de seguridad adicionales a las existentes para asegurar de una manera más fiable la conexión segura en remoto.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad.

6.14. Gestión del ciclo de vida de la identidad

Las sociedades de la EPS Familiar de Colombia deberán definir e implementar un adecuado sistema de gestión del ciclo de vida de la identidad. La identidad es el conjunto de características que identifican de forma unívoca a toda persona con acceso físico o lógico a los sistemas de información de la EPS Familiar de Colombia. El ciclo de vida de la identidad es el proceso que sigue la identidad de un usuario desde su creación hasta su eliminación.

El ciclo de vida de la identidad se compone de las siguientes actividades:

a) Creación y asignación de la identidad
b) Revisión periódica
c) Modificación o eliminación

La gestión de este ciclo requiere definir los requisitos de seguridad y responsabilidades de cada una de las etapas, con el objetivo de centralizar y facilitar los procesos de gestión asociados a las mismas.

La gestión del ciclo de vida de la identidad deberá estar alineado con el Departamento de RRHH con el objetivo de verificar las identidades en función de las altas y las bajas de empleados y su correspondencia en los sistemas de información.

6.15. Seguridad

6.15.1. Seguridad Física y del Entorno

Los espacios físicos donde se ubiquen los sistemas de información de la EPS Familiar de Colombia deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados a sistemas de información, robo o sabotaje) y accidentes ambientales (incendios, inundaciones, cortes de suministro eléctrico, etc.).

Además, deberá haber un control de acceso físico a la información que se encuentre en formato físico mediante un registro en papel sobre quién accede a la información. Por otra

parte, la información confidencial se deberá almacenar con medidas específicas como armarios ignífugos.

6.15.2. Seguridad en trabajo en la nube o cloud

La EPS Familiar de Colombia deberá mantener una política de trabajo en la nube o cloud computing que establezca las medidas de seguridad adecuadas para la confidencialidad, integridad y disponibilidad de la información. Dependiendo de tipo de modelo de servicio en la nube, se deberán aplicar diferentes medidas de seguridad:

a) Infraestructura: en primer lugar, se deberá asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deberán establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes deberán estar registrados y conectados con el objetivo de obtener la trazabilidad adecuada.
b) Plataforma: de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio deberá proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro, de acuerdo con el apartado 15. Seguridad en el ciclo de vida del desarrollo de sistemas.
c) Software: de forma adicional a las medidas indicadas en el modelo de servicio de Plataforma, la EPS Familiar de Colombia y el Proveedor deberán seguir OWASP (Open Web Application Security) como guía para la seguridad de las aplicaciones.

6.15.3. Seguridad en la operativa

Todos los sistemas de información de la EPS Familiar de Colombia que procesan o almacenan información de su propiedad deberán contar con las medidas de seguridad oportunas que optimicen su nivel de madurez adecuado (monitorización, control de cambios, revisiones, etc). Asimismo, se deberán gestionar, controlar y monitorizar las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluidos los controles de acceso a la red, protegiendo así toda la información que se transfiera a través de estos elementos y/o entornos.

6.15.4. Seguridad en las telecomunicaciones

La arquitectura de red de la EPS Familiar de Colombia deberá contar con medidas de prevención, detección y respuesta para evitar brechas en los dominios internos y externos. Se entiende por “dominio interno” la red local compuesta por los elementos tecnológicos de la EPS Familiar de Colombia accesibles exclusivamente desde la red interna. Por otra parte, se entiende por “dominio externo” la red accesible desde el exterior de la red de la EPS Familiar de Colombia.

Es de suma importancia la administración de seguridad de las redes que atraviesan el perímetro de la EPS Familiar de Colombia, implantando controles adicionales para los datos sensibles que circulen por las redes de comunicación públicas.

Por ello, la EPS Familiar de Colombia definirá las pautas de seguridad a seguir con relación a la transferencia de información, así como las medidas de seguridad en la utilización de equipos portátiles, servicios de Internet y correo electrónico, y de controles específicos que permitan una conexión segura a los sistemas de información de la EPS Familiar de Colombia desde fuera de sus instalaciones.

16.15.5. Seguridad en el ciclo de vida del desarrollo de sistemas

Toda la adquisición, desarrollo y mantenimiento de los sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, deberá realizarse una gestión de las pruebas, el seguimiento de los cambios, y el inventario del software.

Cada departamento de la EPS Familiar de Colombia deberá tener en cuenta la seguridad de la información en sus procesos de sistemas y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

16.15.6. Seguridad en los Proveedores

Se deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad de negocio.

Sobre los proveedores de estos servicios se deberán cuidar 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.

16.16. Gestión de Incidentes

Todos los empleados de la EPS Familiar de Colombia tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad de la sociedad de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, la EPS Familiar de Colombia deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

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.

16.17. 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.

La EPS Familiar de Colombia deberá encargarse de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio. La formación en materia de Continuidad del Negocio deberá ser revisada periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

6.18. Cumplimiento regulatorio

La EPS Familiar de Colombia deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

6.19. Auditorías de Seguridad y gestión de vulnerabilidades

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo con su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

6.20. Gestión de Excepciones

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada a la Vicepresidencia TIC de la EPS familiar de Colombia. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

6.21. 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.

6.22. Políticas

Para la EPS Familiar de Colombia los activos de información que se generan almacenan y procesan son un recurso de suma importancia y por ende propenderá por preservar su confidencialidad, integridad y protección. Es política de la EPS trabajar constantemente en proteger los archivos de información contra todo tipo de amenazas ya sean internas o externas, cumpliendo para ello las siguientes condiciones:

Todas las cuentas de usuarios de acceso a los sistemas de información de la EPS Familiar de Colombia estarán vigentes únicamente mientras se encuentre activa la relación laboral o contractual que les dio origen.

Cuando un funcionario de la EPS se encuentre en el disfrute de sus vacaciones, por seguridad de la información institucional la clave de acceso será bloqueada por dicho periodo y esta se reactivará cuando este haya regresada del disfrute de su tiempo de descanso.

Los funcionarios deberán abstenerse de navegar en sitios de juegos en línea, pornografía, terrorismo y cualquier categoría que esté fuera del contexto laboral.

Los funcionarios tienen totalmente prohibido almacenar archivos externos no pertinentes al objetivo misional de la actividad productiva de la EPS Familiar de Colombia, estos son de uso exclusivo para almacenar información corporativa.

Cuando el funcionario de la EPS se retire de su sitio de trabajo deberá bloquear su sesión personal evitando comprometer información.

Los funcionarios de la EPS no deben instalar ningún programa o software sin la autorización de la Dirección de Gestión TIC, se debe realizar la solicitud por medio de la mesa de ayuda.
Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 20 minutos para evitar accesos no autorizados.

Está prohibida la suplantación de usuarios por lo tanto las claves y controles de acceso a las aplicaciones del sistema de información son personales e intransferibles.

Los recursos de los bienes o servicios informáticos tecnológicos provistos por la EPS a sus funcionarios son para uso exclusivo del ejercicio de sus funciones.

El acceso a Internet debe ser por el canal contratado y aprobado por la EPS Familiar de Colombia. No se autoriza hacer conexiones no controladas ni limitadas hacia Internet por otro medio.

La conexión a las redes de la compañía se debe hacer de manera segura. No podrán tener acceso a la red inalámbrica de la EPS, usuarios y equipos no autorizados.

Todas las conexiones por medio de redes públicas (celular, Internet) o por acceso remoto deberán ser autenticadas para evitar que la información sea develada o alterada sin autorización.

La propiedad intelectual de los desarrollos de software, productos y servicios de la entidad deberán protegerse.

Todas los archivos de datos y las bases de datos criticas utilizadas por las diferentes divisiones de la compañía para su objeto misional, deberán contar con el respaldo necesario para recuperase en caso de imprevistos o ataques a la seguridad de la información.

La información contenida en los servidores y equipos de cómputo se respalda de forma periódica siguiendo el manual de procedimientos para copias de seguridad de la información.

La Dirección de Gestión de TICS podrá monitorear el correcto uso de los recursos de acceso a internet y podrá deshabilitar los permisos de acceso a Internet en el momento en que lo considere necesario.

6.23. Revisión de la Política

La aprobación de esta Política implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por el Consejo de Administración. No obstante, 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.

6.24. Anexo: Niveles de clasificación

Nivel	Detalle Nivel	Ejemplos
Uso público	Se trata de la información que puede ser conocida por cualquier tipo de persona y su utilización fraudulenta no supone un riesgo para los intereses de la EPS Familiar de Colombia.	Son ejemplos de este tipo de información los catálogos de productos y la información disponible en la página Web.
Difusión limitada	Es la información utilizada por las áreas de la EPS Familiar de Colombia y cuya utilización fraudulenta supone un riesgo para los intereses del Grupo poco significativo.	Son ejemplo de este tipo de información los correos electrónicos y los documentos de trabajo de las áreas del Grupo.
Información Confidencial	Es aquella información que solo puede ser conocida por un número reducido de personas y para la que un uso fraudulento puede suponer un impacto para los intereses de la EPS Familiar de Colombia significativo.	Son ejemplos de este tipo de información los informes de auditoría y de estrategia del Grupo.
Información Reservada	Es la información que únicamente debe conocer el propietario de la misma y cuya divulgación puede suponer graves perjuicios para los intereses del Grupo.	Son ejemplos comunicaciones entre los altos directivos o accionistas con decisiones relevantes para la operativa de negocio.
Información Secreta	Es aquella cuya revelación no autorizada puede causar un perjuicio excepcionalmente grave a los intereses esenciales del Grupo.	Son ejemplos las claves criptográficas, información sobre fusiones o adquisiciones o cualquier otra información que pueda poner en riesgo el valor de la acción.

7. 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

8. CONTROL DE CAMBIOS

VERSIÓN	ITEM	CAMBIO REALIZADO	JUSTIFICACIÓN	FECHA
1	N/A	Elaboración del documento	Elaboración del documento	01/04/2022

	REALIZÓ	REVISÓ	APROBÓ
NOMBRE			
CARGO			