TABLA DE CONTENIDO

1. INTRODUCCIÓN

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

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

El objetivo de este documento es establecer las políticas en seguridad de la información de Mutual SER EPS, con el fin de regular la gestión de la seguridad de la información al interior y exterior de la Organización.

2. OBJETIVO

Gestionar y minimizar los riesgos asociados con la pérdida, destrucción, modificación, acceso no autorizado, divulgación, duplicación, interrupción de sistemas o mal uso de los activos de información y tecnologías para garantizar la seguridad de la información.

3. DESTINATARIOS DE LA POLÍTICA

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

4. RESPONSABLE(S)

- Comité de Seguridad de la Información.
- Gerencia de Tecnologías de la Información.

- Gerencia de Experiencia y Fidelización del Cliente (Director de Gestión Documental, Director de Comunicaciones, Director de Gestión Humana y Coordinador de Seguridad y Salud en el Trabajo).
- Coordinador de Control Interno y Calidad.

5. NORMATIVIDAD

- Ley 1712 de 2014.
- Ley 1581 de 2012.
- NTC ISO 27001 de 2013.

6. DEFINICIONES

- **Activo de información:** Es el elemento de información que la organización recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

- **Control:** Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

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

- **Integralidad:** Entendida como la preservación de la información de forma completa y exacta.

- **Disponibilidad:** Se denomina disponibilidad a la posibilidad de una cosa o persona de estar presente cuando se le necesita.

- **Criticidad:** Equilibrio entre la subjetividad con la objetividad.

- **Acuerdo de Confidencialidad:** Documento en los que los funcionarios del Mutual SER EPS o los provistos por terceras partes manifiestan su voluntad de mantener

la confidencialidad de la información de la organización, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

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

- **Autenticación:** Procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **Centros de cableado:** Habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

- **Centro de cómputo:** Zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

- **Cifrado:** Transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

- **Custodio del activo de información:** Unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

- **Derechos de Autor:** Conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la

creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

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

- **Equipo de cómputo**: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

- **Guías de clasificación de la información**: Directrices para catalogar la información de la Organización y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

- **Hacking ético:** Conjunto de actividades para ingresar a las redes de datos y voz de la Organización con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

- **Incidente de Seguridad:** Evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

- **Integridad**: Protección de la exactitud y estado completo de los activos.

- **Inventario de activos de información**: Lista ordenada y documentada de los activos de información pertenecientes a la organización.

- **Licencia de software**: Contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

- **Medio removible:** Cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CD, DVD y unidades de almacenamiento USB, entre otras.

- **Perfiles de usuario**: Grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

- **Propiedad intelectual:** Reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **Propietario de la información:** La organización Mutual SER EPS, es la propietaria de los activos de información que se genere o creen en las unidades organizacionales o procesos estratégicos, misionales y de soporte.

- **Recursos tecnológicos:** Componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la organización.

- **Registros de Auditoría:** Archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la organización. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

- **Responsable por el activo de información:** Persona o grupo de personas, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- **Sistema de información:** Conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por Mutual SER EPS o de origen externo ya sea adquirido por la Organización como un producto estándar de mercado o desarrollado para las necesidades de ésta.

- **Sistemas de control ambiental:** Sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características de este, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

- **Software malicioso:** Variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

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

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

7. ALCANCE DE LA POLÍTICA

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

8. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Junta Directiva de Mutual SER EPS aprueba esta Política de Seguridad de la Información, como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Organización.

La Junta Directiva y la Alta Dirección de la Organización demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad en la Organización.
- Facilitar la divulgación de este manual a todos los funcionarios de la Organización.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

En virtud de lo anterior, la Junta Directiva aprueba las siguientes políticas elaboradas por la Alta Gerencia, las cuales son de estricto cumplimiento para todos los miembros de la organización:

8.1 POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

En Mutual SER EPS la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Consciente de las necesidades actuales, Mutual SER EPS implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del Mutual SER EPS, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad de la Información de Mutual SER EPS se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la organización. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los objetivos de control de referencia y controles del Anexo A de la norma internacional ISO 27001:2013.

El Comité de Seguridad tendrá la potestad de proponer las modificaciones la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de éstas.

8.2 POLÍTICAS GENERALES DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Las Políticas Generales de Seguridad de la Información en Mutual SER EPS son:

- ✓ Las políticas para seguridad de la información se deben revisar anualmente o de manera inmediata si ocurren cambios significativos que sean catalogados como riesgosos.
- ✓ Un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información.
- ✓ Los activos de información identificados y clasificados para establecer los mecanismos de protección necesarios.
- ✓ Definición e implantación de controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen su disponibilidad.
- ✓ Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- ✓ Es responsabilidad de todos los funcionarios y contratistas reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- ✓ Contaremos con un Plan de Continuidad del Negocio que asegure el seguimiento de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.
- ✓ Garantizaremos el cumplimiento de las leyes y normativas legales y contractuales en nuestro ámbito de competencia.

8.3 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

8.3.1 Normas que rigen para la estructura organizacional de seguridad de la información:

Normas dirigidas a: ALTA DIRECCION:

- ✓ La Alta Dirección del Mutual SER EPS debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- ✓ La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- ✓ La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
- ✓ La Alta Dirección debe promover activamente una cultura de seguridad de la información en la organización.
- ✓ La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la Organización y al personal provisto por terceras partes.

Normas dirigidas a: ALTA DIRECCION Y UNIDAD DE PLANEACIÓN:

- ✓ La Alta Dirección y La Unidad de Planeación, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Organización.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:

- ✓ El Comité de Seguridad de la Información debe actualizar y presentar ante la Junta Directiva las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- ✓ El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- ✓ El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Normas dirigidas a: COORDINACIÓN DE CONTROL INTERNO Y CALIDAD:

- ✓ La Coordinación de Control Interno y Calidad debe liderar la generación de lineamientos para Gestionar la seguridad de la información de Mutual SER EPS y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- ✓ La Coordinación de Control Interno y Calidad debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
- ✓ La Coordinación de Control Interno y Calidad debe planear y ejecutar las auditorías internas a las políticas y procedimientos relacionadas con la Gestión de Seguridad de la Información de Mutual SER EPS a fin de determinar si los procesos y controles establecidos están conformes con los requerimientos institucionales, de seguridad y regulaciones aplicables.
- ✓ La Coordinación de Control Interno y Calidad debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte de los planes de acción derivados de las auditorías
- ✓ internas del Manual y procesos de Política de la Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

Normas dirigidas a: GERENCIA DE TECNOLOGIA DE LA INFORMACIÓN:

- ✓ La Gerencia de Tecnología de la Información debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica en la organización. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: TODOS LOS USUARIOS:

- ✓ Los funcionarios y personal provisto por terceras partes que realicen labores en o para Mutual SER EPS, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

8.3.2 Separación de deberes:

Toda actividad en la cual los funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

Todos los sistemas que manejen información crítica o media deben accederse a través de claves de acceso, implementando reglas de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, reducir la posibilidad de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

8.4 POLÍTICAS USO DE DISPOSITIVOS MÓVILES CORPORATIVOS

Mutual SER EPS proveerá las condiciones para el manejo de los dispositivos móviles corporativos (teléfonos inteligentes y tabletas, entre otros) que hagan uso de servicios de tecnología que ofrece la organización. Así mismo, velará las pautas para que los empleados hagan un uso responsable de los servicios y equipos proporcionados por la Organización, de igual manera se tendrá en cuenta lo siguiente:

- ✓ Es responsabilidad del empleado garantizar el adecuado uso del medio móvil asignado, conectándolo siempre a redes confiables, que no sean de acceso público para evitar que se contagien de cualquier amenaza pertinente a estos dispositivos (virus, troyanos, programa maligno).
- ✓ Los usuarios no deben usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- ✓ Los usuarios deben configurar métodos de seguridad en los dispositivos móviles
- ✓ institucionales para la protección de acceso no autorizados en los mismos, ni desinstalar el software provisto con ellos al momento de su entrega.
- ✓ Los usuarios no deben instalar programas desde fuentes desconocidas en los dispositivos móviles institucionales.
- ✓ Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- ✓ La Gerencia de Tecnología de la Información debe velar y corroborar las opciones de protección de los accesos de los dispositivos móviles que hagan uso de los servicios provistos por la organización de acuerdo con los lineamientos del MANUAL ADMINISTRACION DE LA SEGURIDAD A NIVEL DE LA RED
- ✓ No será permitido almacenar en dispositivos móviles personales información de Mutual SER EPS que no esté clasificada como pública.

8.5 POLÍTICAS PARA TRABAJO REMOTO

Mutual SER EPS aplicará una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el trabajo remoto, bajo las siguientes condiciones:

- ✓ El trabajo remoto es permitido para todos los empleados, siempre y cuando se utilice los equipos de cómputo asignado por la organización.
- ✓ Los empleados podrán acceder a la red de Mutual SER EPS únicamente por los medios de acceso remoto proporcionados por la Gerencia de Tecnología de la Información y utilizando los equipos de cómputo institucionales asignados para realizar sus funciones.
- ✓ Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado. Por lo tanto, todo funcionario o tercero que requiera tener acceso a los sistemas de información de Mutual SER EPS debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario y contraseña asignado por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

8.6 POLÍTICA DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

Mutual Ser EPS para dar cumplimiento al mantenimiento y mejora del modelo de seguridad de la información, tiene el compromiso de generar y mantener actualizada la identificación, clasificación y valoración de los activos de información, que son manejados en todos los procesos. Se deben considerar las siguientes condiciones:

- ✓ Los activos de información son reconocidos como valiosos para Mutual SER EPS.
- ✓ No son fácilmente reemplazables sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- ✓ Forman parte de la identidad y su vulneración puede poner en un nivel de riesgo las operaciones misionales y/o estratégicas de Mutual SER EPS.
- ✓ Mutual SER EPS cuenta con un sistema de información que permite registrar y clasificar los activos de información de acuerdo con el marco normativo nacional.
- ✓ Mutual SER EPS mantiene un inventario de los activos de información, teniendo en cuenta los niveles de clasificación como confidencialidad, integridad, disponibilidad y ubicación para lo cual debe realizar asignación de los responsables de los activos de información.
- ✓ Los líderes de proceso son responsables de mantener actualizado los activos de información a su cargo, además de dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

8.6.1 Inventario de activos

- ✓ Para realizar el inventario se deben aplicar el PROCEDIMIENTO PARA LA IDENTIFICACIÓN, GENERACIÓN Y MANTENIMIENTO DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN, en la cual se describe las actividades para identificar, clasificar, etiquetar y definir los responsables de los activos de información de la Organización.
- ✓ El inventario debe actualizarse como mínimo una vez al año y ser avalado por el Comité de Seguridad de la Información de la Organización.

8.6.2 Responsabilidad por los activos de información

Los líderes de proceso son responsables de mantener actualizado los activos de información a su cargo, además de dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

Control interno y Calidad es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por estas políticas y por las normas, procedimientos y prácticas que de ella surjan.

8.6.2.1 Propietario de la información

Debe identificar, actualizar y definir los controles de los activos de información que hacen parte de su área, dependencia o grupo de trabajo.

Responsabilidades

- ✓ Identificar los activos de Información.
- ✓ Definir controles y el uso adecuado de los activos de información identificados.
- ✓ Tomar decisiones sobre el buen uso de la información.
- ✓ monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- ✓ Hacer mantenimiento periódico y evaluar clasificación y valoración de los activos de información.
- ✓ Definir uso aceptable de los activos de información

8.6.2.2 Custodio de la información

Verificar y mantener la protección y privacidad de los activos de información que están bajo su custodia.

Responsabilidades

- ✓ Administrar y hacer efectivo los controles que el propietario del activo haya definido.
- ✓ Garantizar que los activos de información se encuentren disponible e íntegros y que solo personal autorizado acceda a ellos.
- ✓ Cumplir con los controles de seguridad establecidos para la protección de la información.
- ✓ Ejecutar las actividades propias de su cargo, de acuerdo con la custodia de la información.
- ✓ Los activos de información se encuentran sujetos a auditorías por parte de la Dirección de Control Interno de la Organización.
- ✓ La Gerencia de Tecnología de la Información es la responsable de los activos de información correspondientes a la plataforma tecnológica de MUTUAL SER y debe asegurar su operación y administración y establecer las configuraciones pertinentes con el objetivo de mantener la seguridad de la información.

- ✓ La Gerencia de Tecnología de la Información es responsable de configurar los equipos de cómputo de los empleados y de hacer entrega de estos, mediante acta de responsabilidad de equipo donde el usuario se compromete al cuidado del recurso asignado.

8.6.2.3 Usuario

Cumplir con las políticas establecidas para el buen uso del activo de información.

Responsabilidades

- ✓ Hacer buen uso de los activos de información asignados.
- ✓ Garantizar la confidencialidad, integridad y disponibilidad del activo de información.
- ✓ Reportar cualquier evento que atente contra la seguridad de la información.

8.6.2.4 Revisión periódica de los activos de información:

Para la realización del levantamiento, revisión y/o actualización del inventario de activos de Información se establecerá como periodicidad anual, sin embargo, esta podrá cambiar de acuerdo con las necesidades que surjan.

8.6.2.5 Recurso Humano como Activo de Información

La Gerencia de Experiencia y Fidelización del Cliente de Mutual SER EPS, considera como activos de la información a aquel recurso humano que, por cumplir una serie de criterios, son elementos claves para la organización. Los criterios para clasificar a un recurso humano como activo de la información son:

- ✓ Conocimiento de los procesos misionales y el Core de la organización.
- ✓ Experiencia superior a 10 años.
- ✓ Criticidad y transversalidad en los procesos misionales y el Core de la organización.
- ✓ Manejo de altos volúmenes de información de la organización.
- ✓ Restricción de su perfil técnico y competencias en el mercado.

8.7 POLÍTICAS PARA USO DE TOKENS DE SEGURIDAD

La Gerencia general de Mutual SER EPS determinará los funcionarios que se les entregará el dispositivo. Esta selección es realizada teniendo en cuenta la cantidad de transacciones que ellos realizan en un período de tiempo determinado.

- ✓ Los funcionarios con asignación de tokens son responsables del uso correcto del dispositivo, así como de su cuidado y custodia.
- ✓ No se permite transferencia del dispositivo a otra persona no autorizada.

8.8 POLÍTICAS GESTIÓN DE MEDIOS DE ALMACENAMIENTO DE DATOS

Los dueños de los activos de información son los únicos autorizados para el almacenamiento de datos en medios externos y son responsables del uso que se haga de estos.

No está permitido que los empleados o terceros que tengan vínculo contractual o se encuentren desarrollando actividades para la Organización usen medios de almacenamiento masivo de su propiedad para almacenar información sin que se cuente con la autorización requerida y las técnicas de cifrado para su protección.

8.8.1 Transferencia de medios de soporte físico

- ✓ Se utilizan servicios de mensajería, a través de empresas transportadoras y/o personas naturales con experiencia en el sector. Para la protección de la información, durante el transporte de medios de soporte físico se deben tener en cuenta las instrucciones dadas a través de las herramientas multimedia y correo electrónico.
- ✓ La entrega física de información reservada se realiza por mensajeros de la Organización, cumplen con las mismas características, estipulados en el ítem anterior.

8.8.2 Acceso a redes y recursos de red

Con el fin de garantizar que los usuarios accedan a los servicios de redes de manera segura, se realizan los siguientes lineamientos:

1. La Gerencia de Tecnología de la Información como responsables de las redes de datos y los recursos de red debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

2. La navegación en internet es asignada según cargo del empleado.
3. El acceso a las páginas web es controlado por las políticas de los Firewalls de red.
4. Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

8.9 POLÍTICA DE GESTIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN

El proceso de gestión de usuarios se realiza conforme al procedimiento creación, modificación y eliminación de usuarios del sistema de información, cuyo alcance es creación, modificación, bloqueo y retiro de las cuentas de los usuarios, con el fin de que puedan tener el acceso necesario según sus funciones en la Organización.

La contraseña es confidencial e intransferible, por lo tanto, la fuga, modificación, borrado de la información o actividad que sea realizada a través de su usuario sea de manera intencional o negligente, será responsabilidad del usuario. Las sanciones se establecen en el Reglamento Interno del trabajo.

La Gerencia de Tecnología de la Información velará porque los empleados y terceros solo tengan acceso a la información necesaria para las labores propias.

8.9.1 Responsabilidades de acceso de los usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información de la Organización realizarán un uso adecuado y responsable salvaguardando la información a la cual les es permitido el acceso.

Los usuarios deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otras personas.

Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica deben acogerse a lineamientos de contraseñas de la Organización.

8.9.2 Derechos de acceso privilegiado

La gestión de usuarios con acceso privilegiado se realiza conforme al PROCEDIMIENTO PARA LA CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN, con el fin de que puedan tener el acceso necesario según sus funciones en la Organización.

La Gerencia de Tecnología de la Información establecerá los mecanismos que permitan un monitoreo posterior de la actividad de los usuarios administradores de las plataformas o servicios de Tecnología.

La Gerencia de Tecnología de la Información debe establecer los controles para que los usuarios finales del sistema de información no tengan instalados en sus equipos de cómputo programas o software que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

8.9.3 Gestión de autenticación usuarios y contraseñas.

Los usuarios deben cumplir las siguientes prácticas relacionadas con su usuario y contraseñas secretas:

- ✓ Cambiar periódicamente su contraseña a través del aplicativo de Autoservicio de contraseñas
- ✓ Aplicación de política de contraseñas: longitud de contraseña mínima; no contenga nombres, números de teléfono y fechas de nacimiento; cambiar contraseñas temporales; no reusar claves o contraseñas para propósitos personales o diferentes al corporativo.
- ✓ No visualizar contraseñas en la pantalla cuando se ingresan a las aplicaciones
- ✓ No divulgar claves o contraseñas de acceso.
- ✓ Evitar copiar las contraseñas en papel o archivo de software
- ✓ Cambiar las claves o contraseñas de autenticación secreta cuando considere que se pueda comprometer la información.
- ✓ Exigir cambio de las contraseñas en forma regular.

8.9.4 Control de acceso a sistemas y aplicaciones

Las Gerencias de área de la Organización como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por

la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La Gerencia de Tecnología de la Información como responsable de la administración de dichos sistemas de información y aplicativos, propenderá por la seguridad de estos a través de mecanismos de control de acceso lógico. También establecerá buenas prácticas de desarrollo para el control de acceso a las aplicaciones.

La Gerencia de Tecnología de la Información debe establecer que usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción y debe asegurar que los desarrolladores internos o externos, posean acceso limitado a los datos de los ambientes productivos.

8.9.5 Programas utilitarios privilegiados.

La organización a través de las políticas del dominio no permite la instalación de software y cambios de configuración del sistema, por lo tanto, los usuarios finales no deben tener privilegios de usuario administrador excepto los técnicos del área de Soporte de la Gerencia de Tecnología de la Información. Estos últimos son los responsables de las configuraciones de los equipos de cómputo de usuario final.

Es responsabilidad de los usuarios informar a la Gerencia de Tecnología de la Información de manera inmediata se le permita instalar programas o hacer cambios de configuración en su equipo de cómputo asignado.

8.9.6 Ingreso seguro aplicaciones y equipos de computo

Las aplicaciones corporativas deberán cumplir con los siguientes lineamientos de seguridad en cuanto al acceso:

- ✓ No mostrar información del sistema, hasta tanto el proceso de inicio de sesión se haya completado.
- ✓ En intentos fallidos de autenticación evitar visualizar mensajes que puedan ser usados para descifrar los datos del usuario y contraseña, o indicar que parte de los datos que se digitaron son correctos.
- ✓ Solicitar todos los datos de entrada antes de realizar el proceso de validación de acceso a las aplicaciones.
- ✓ No debe mostrarse las contraseñas que se están digitando en las aplicaciones.
- ✓ No trasmitir en texto claro las contraseñas de los usuarios a través de la red.

- ✓ Determinar un evento de seguridad en los casos de violación de controles de acceso a las aplicaciones.
- ✓ Cierre de sesiones inactivas después de un tiempo de inactividad.
- ✓ Todo el equipo de cómputo de usuario final debe tener configurado acceso seguro mediante usuario y contraseña.
- ✓ Los usuarios deben bloquear sus sesiones en los equipos de cómputo, cuando deban abandonar temporalmente su puesto de trabajo.
- ✓ Los usuarios deben apagar los equipos de cómputo al finalizar la jornada laboral.
- ✓ Por el tipo de negocio de la organización, no se limita el tiempo de conexión, ni se establecen restricciones en las sesiones en la jornada laboral.

8.10 POLITICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

El cumplimento de esta política es de carácter obligatorio para todos los funcionarios y terceros vinculados a Mutual Ser EPS independientemente del nivel de las tareas que desempeñe.

8.10.1 ÁREAS SEGURAS.

Las áreas seguras hacen referencias a espacios que custodian los servicios de procesamiento de información sensible, estas áreas son protegidas físicamente contra accesos no autorizados, daño e interferencia a las instalaciones y a la información de la organización.

Estas áreas contaran con barreras, controles de acceso y perímetros definidos para garantizar la protección de la información que resguardan.

8.10.1.1 Perímetro de seguridad física.

Los perímetros de seguridad en Mutual Ser EPS estarán delimitados por una o más barreras tales como: paredes, puertas de acceso, lector biométrico de control de asistencia y tiempos, dispositivo de autenticación.

- ✓ Las instalaciones de procesamiento de información estarán ubicadas dentro del perímetro de un edificio o área de construcción físicamente sólida. Las paredes externas del área deberán ser sólidas y todas las puertas que comunican con el exterior deberán estar adecuadamente protegidas contra accesos no autorizados.

8.10.1.2 Controles de acceso físico.

Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial y sensible, así como aquellas en las que se encuentren los equipos que soporten a los sistemas de información y comunicaciones deben ser protegida con las siguientes medidas de control de acceso físico:

- ✓ Los Centros de datos en Mutual Ser EPS contarán con uno de los siguientes mecanismos de control de acceso: cerraduras, control biométrico, tarjetas de control de acceso, puertas o gabinetes para rack.
- ✓ El ingreso de terceros a los Centros de Cómputo, Centros de Cableado y Archivo debe estar debidamente autorizado.
- ✓ Todos los funcionarios, contratistas o terceros deben portar la identificación o distintivo que los acredite que prestan servicios, son funcionarios o realizan una visita en las instalaciones de Mutual SER EPS y no deberán ingresar a las áreas donde no tengan la debida autorización.
- ✓ Los miembros de Unidad de planeación y Junta directiva tendrán acceso libre a las instalaciones.
- ✓ Para las sedes que aplique software de control de acceso o áreas de recepción (Oficinas Regionales y de Nivel Central), las recepcionistas recibirán al visitante o contratista y solicitarán la autorización de acceso al trabajador a visitar. En estas sedes, se solicitará documento de identificación para realizar registro y se tomará foto o huella para entregar “Pase”, el cual el visitante o contratista debe portar en sitio visible durante su estancia en las instalaciones, al finalizar su estancia este debe entregar el “Pase de Visitante” a la recepcionista quien registrará la salida. Para las sedes que no aplique el software, el Vigilante o recepcionista realizará el registro de visitantes.
- ✓ La limpieza y aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de Auxiliares de TI, el personal de Servicios Generales debe ser instruido con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

8.10.1.3 Seguridad de oficinas e instalaciones.

La empresa dispone de los siguientes lineamientos para garantizar la seguridad de oficinas e instalaciones en las que se procese información:

- ✓ Todos los colaboradores deberán dar estricto cumplimiento a lineamientos y normas de Seguridad y Salud en el trabajo.
- ✓ Las instalaciones de sedes principales contaran con vigilantes y / o Sistemas de intrusión o anti-intrusión de alarmas conectado con central de monitoreo 24 horas y Sistema de Circuito Cerrado de TV (CCTV).
- ✓ Las áreas seguras (Datacenter y áreas de archivo) se ubicarán de tal forma que se evite el acceso al público.
- ✓ Aquellas áreas en las cuales se realice procesamiento de información serán acondicionadas en instalaciones discretas, en las cuales no se dé indicaciones sobre su propósito.
- ✓ Se determina que los listados telefónicos internos y direcciones de oficinas en donde se procese información sensible no serán de fácil acceso al público.

8.10.1.4 **Protección contra amenazas externas y del entorno**.

Mutual SER EPS define la protección de los perímetros mediante los siguientes controles establecidos en sus sedes según aplique:

- ✓ El almacenamiento de productos peligrosos o combustibles para el funcionamiento de plantas eléctricas se ubicarán a una distancia prudente de los centros de cableado, en los cuales se prohíbe de manera estricta el almacenamiento de productos yo materiales de oficina.
- ✓ Todas las instalaciones dispondrán de equipos contraincendios, vías o planos de evacuación. ubicados estratégicamente dentro de las instalaciones.

8.10.1.5 **El trabajo en áreas seguras**.

- ✓ El ingreso de terceros a los Centros de Cómputo, Centros de Cableado y Archivo debe estar debidamente autorizado y supervisado independiente de la actividad que realice.
- ✓ Salvo autorización no se permite el ingreso de equipos de video o de grabación, audio o dispositivos móviles a las áreas seguras.

8.10.1.6 **Áreas aisladas de carga y despacho y acceso público.**

El acceso al área de despacho carga y recibo de encomiendas está permitido únicamente al personal autorizado.

Los suministros y encomiendas solo pueden ser cargadas y descargadas en el área de recepción y bodega según aplique, el personal de empresas transportadoras o proveedores no deben tener acceso a otras partes de la edificación.

Todo el material que ingresa a las instalaciones debe ser registrado de acuerdo con los procedimientos establecidos.

8.10.2 SEGURIDAD DE LOS EQUIPOS DE COMPUTO

8.10.2.1 Instalación y protección de equipos de cómputo

- ✓ La instalación de equipos de cómputo, periféricos y software estará a cargo de la Gerencia de Tecnología de la Información.
- ✓ Los equipos nuevos son asignados desde nivel central a usuarios específicos, los cuales deberán firmar el Acta de responsabilidad de equipo de cómputo. En ninguna circunstancia puede ser reasignado a otro usuario sin previa aprobación de la Gerencia de Tecnología de la información y la Gerencia de Experiencia y Fidelización del Cliente.
- ✓ En referencia a la asignación, cambio y re-potenciamiento de los equipos de cómputo, la Organización cuenta con la tabla de homogenización de equipos de cómputo que establece los requisitos mínimos en términos de hardware y software de usuario final.
- ✓ No está permitido manipular el hardware y software de los equipos de cómputo sin la autorización previa de la Gerencia de Tecnología de la Información.

8.10.2.2 Suministro eléctrico de equipos de cómputo

Para el cableado de energía eléctrica se debe cumplir con los estándares establecidos por el área de Ambiente Físico de la Organización.

Los equipos de cómputo deben conectarse al cableado eléctrico regulado.

8.10.2.3 Seguridad del cableado de datos

Se debe cumplir con los estándares establecidos en la Organización para cableados estructurado que transporta datos o brinda apoyo a los servicios de información con el fin de protegerlos contra intercepción o daño.

8.10.2.4 Mantenimiento de equipos de cómputo y dispositivos.

- ✓ El mantenimiento preventivo y correctivo de equipos de cómputo estará a cargo de la Gerencia de Tecnología de la Información y su programación será enmarcada por el PROCEDIMIENTO PARA EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE CÓMPUTO.
- ✓ Será responsabilidad directa del usuario si el equipo es intervenido por un tercero no autorizado por la Gerencia de Tecnología de la Información.
- ✓ Cualquier cambio de equipo debe estar avalado por diagnóstico de fallo definitivo por parte de la Gerencia de Tecnología de la Información y/o justificación de Salud Ocupacional.
- ✓ La asistencia técnica que presta la Gerencia de Tecnología de la Información e instalación de software está exclusivamente dirigida a aquellos equipos que sean propiedad de la Organización.
- ✓ En caso de que un equipo de cómputo sufra daños o averías por factores como golpes, derrame de líquidos u otros aspectos relacionados con el mal uso y se evidencie negligencia, el usuario tendrá que responder por los gastos de reparación o adquisición, conforme a lo descrito en el Acta de responsabilidad de equipos de cómputo.

8.10.2.5 Escritorio y pantalla limpios

La Organización promueve política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información. Los empleados deben seguir los siguientes lineamientos:

- ✓ Almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivos seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.
- ✓ Proteger los puntos de recepción y envío de correo y las máquinas de fax no atendidas.
- ✓ No ubicar archivos o accesos directos a información confidencial en el escritorio de su equipo de cómputo.

8.10.2.6 Seguridad de equipos fuera de los locales de la Organización.

- ✓ Los equipos de cómputo no deben ser dejados desatendidos en lugares públicos, vehículos o cuando sean transportados.
- ✓ En caso de pérdida o robo de un equipo de cómputo de la Organización, se debe informar a la Gerencia de Tecnología de la Información, Gerencia de Experiencia y Fidelización del Cliente y se debe poner la denuncia ante la autoridad competente.

8.10.2.7 Seguridad en la reutilización o eliminación de equipos de cómputo.

Los equipos de cómputo y los medios de almacenamiento de datos reusable tales como discos duros que se vaya a asignar a otro usuario, retirar o dar de baja de la Organización se debe borrar de forma que no sea recuperable, de acuerdo con el PROCEDIMIENTO PARA RETIRO DE EQUIPOS Y DISPOSITIVOS TECNOLOGICOS.

8.10.2.8 Traslado de activos.

- ✓ Cuando sean transportados, los equipos de cómputo deben tratarse bajo medidas de seguridad que garanticen su integridad física y lógica. Entre estas medidas tenemos:

    - Apagar correctamente el equipo que se va a trasladar.
    - Empacar con icopor u otro material que garantice la protección del equipo.
    - Rotular y transportar los equipos de acuerdo con los lineamientos del área de Gestión Documental de la Organización.

- ✓ Los equipos portátiles siempre deben ser llevados como equipaje de mano y en un bolso o morral adecuado para este fin.

8.10.2.9 Ubicación y protección de los equipos de cómputo

- ✓ La ubicación de equipos de cómputo y periféricos estará a cargo de la Gerencia de Tecnología de la Información.

- ✓ Es responsabilidad del usuario mantener el equipo de cómputo que se le asigne en condiciones adecuadas de higiene, conforme a las recomendaciones de buen uso de la Gerencia de Tecnología de la Información.
- ✓ Los usuarios responsables de los equipos de cómputo deben bloquear la sesión en el momento de abandonar su puesto de trabajo.
- ✓ Los usuarios deben apagar el equipo de cómputo y otros recursos tecnológicos asignados al finalizar su jornada laboral.
- ✓ Los usuarios responsables de los recursos tecnológicos deben notificar inmediatamente a la Gerencia de Tecnología de la Información cuando se presente una falla o problema de hardware o software mediante la herramienta Centro de servicios MUTUAL SER.

8.11 POLÍTICA DE ACCESO A DATACENTER Y CUARTOS DE TELECOMUNICACIONES

Para la protección de los equipos en los centros de procesamientos como los Datacenter (DC) y los Cuartos de Telecomunicaciones ubicados en las oficinas principales de cada regional, se presenta las siguientes normas básicas para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. Los lineamientos específicos se encuentran contemplados en el documento POLÍTICA DE DATA CENTER Y CUARTO DE TELECOMUNICACIONES.

8.12 POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Gerencia de Tecnología de la Información asignará las funciones específicas y responsables de garantizar la operación y administración de los recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Las funciones específicas se contemplan en los perfiles de cargo de la Gerencia de Tecnología de la Información.

8.13 POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Con el fin de prevenir y detectar códigos maliciosos, se definen aspectos basados en software, concientización de usuarios y gestión del cambio. Dichos controles contemplan las siguientes directrices:

- ✓ Instalar y actualizar el software de detección y reparación de virus, Sistema de Prevención de Intrusos, antispyware, y otras herramientas de seguridad informática con el fin de examinar computadores y medios informáticos, como medida preventiva y rutinaria en todos los equipos de cómputo de la Organización.
- ✓ No se permite el uso de software no autorizado por la Gerencia de Tecnología de la Información.
- ✓ Mantener los sistemas operativos con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
- ✓ Revisar periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- ✓ Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- ✓ Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.
- ✓ La herramienta de antivirus que se implemente en la organización tendrá carácter de corporativo y por lo tanto será obligatoria su instalación en servidores y equipos de cómputo. Cualquier equipo que no cuente con los controles establecidos, no podrá ser conectado a la red de datos de la Organización.
- ✓ No se permite la conexión de equipos de contratistas o terceros a la plataforma tecnológica, con equipos que no cuenten con los controles establecidos para su funcionamiento dentro de la red institucional.

8.14 POLÍTICAS DE CIFRADO DE DATOS

Mutual SER EPS vela por proteger la información pública clasificada y pública reservada mediante mecanismos de cifrado al momento de ser transferida o transmitidas. Las claves de acceso a sistemas de información y sistemas operacionales se almacenan en forma cifrada para preservar su confidencialidad. Los lineamientos de cifrado se encuentran descritos en el documento POLITICA DE CIFRADO DE DATOS.

8.15 POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

MUTUAL SER EPS certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas responsables de la información, con el apoyo de la Gerencia de Tecnología, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la organización velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

8.15.1 Normas de copias de respaldo de la información

- ✓ La Gerencia de Tecnología, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- ✓ La Gerencia de Tecnología, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- ✓ La Gerencia de Tecnología debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos información de la organización.
- ✓ Es responsabilidad de los usuarios de la plataforma tecnológica de MUTUAL SER EPS identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.
- ✓ El usuario final debe realizar la copia de sus datos en la plataforma de respaldo corporativa.

8.16 POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

- ✓ MUTUALSER EPS realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la

plataforma tecnológica y los sistemas de información de la organización. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

- ✓ La Gerencia de Tecnología definirá la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la organización. El equipo de Arquitectura de TI frecuentemente realizará revisiones de logs y se reunirá a analizar los resultados del monitoreo efectuado.

8.16.1 Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

- ✓ La Gerencia de TI, a través de sus funcionarios, debe determinar los eventos y habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica
- ✓ administrada, acorde con los eventos a auditar establecidos.
- ✓ La Gerencia de Tecnología y el equipo de arquitectura de TI, deben definir cuáles monitoreos se realizarán de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la organización. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.
- ✓ La coordinación de desarrollo y evolución de software debe garantizar, que el equipo de desarrollo registre en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Gerencia de Tecnología.
- ✓ La coordinación de desarrollo y evolución de software debe garantizar, que el equipo de desarrollo no almacene datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.
- ✓ Para garantizar la exactitud de los registros de auditoría, los servidores se configuran con la hora legal colombiana.

8.17 POLÍTICAS DE CONTROL AL SOFTWARE OPERATIVO

1. La Gerencia de Tecnología de la Información de MUTUAL SER establecerá controles en la instalación de software en los Sistemas Operativos y se cerciorará

de contar con el soporte de los proveedores de dicho software y garantizará que los servicios se mantengan operando con normalidad.

2. El acceso a proveedores que soportan el software instalado en los sistemas operativos debe ser temporal, evaluado, aprobado y monitoreado por la Gerencia de Tecnología de la Información.
3. Antes de realizar una actualización del Sistema Operativo se debe revisar los riesgos y evaluar el impacto en los servicios de TI asociados a éste.

8.18 POLÍTICA DE GESTIÓN DE VULNERABILIDADES TECNICAS

MUTUAL SER EPS, a través de la Gerencia de Tecnología y el equipo de Arquitectura de TI, debe establecer los mecanismos de revisión de las vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica, estableciendo las siguientes normas:

- ✓ La Gerencia de Tecnología de la Información y el equipo Arquitectura de TI es responsable de realizar las pruebas de vulnerabilidades y hacking ético con una periodicidad establecida.
- ✓ La Gerencia de Tecnología y el equipo de Arquitectura de TI, deben generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
- ✓ El equipo de Arquitectura de TI debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos
- ✓ La Gerencia de Tecnología, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

8.19 POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

1. Mutual SER EPS establecerá, a través de la Gerencia de Tecnología de la Información, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.
2. De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la organización. Todas las normas de gestión y aseguramiento de

las redes de datos se soportan bajo el MANUAL ADMINISTRACIÓN DE LA SEGURIDAD A NIVEL DE LA RED.

8.20 POLÍTICA DE MENSAJERÍA ELECTRÓNICA

La mensajería electrónica en la Mutual SER EPS, está asociada a los servicios de correo electrónico de los dominios adquiridos formalmente por la organización y a la plataforma de comunicaciones unificada aprobada y establecida por la Gerencia de TI, la cual se encuentra regulada por los términos de uso adecuado. Por tanto, no está permitido intercambiar información institucional a través de otras plataformas de correo o mensajería instantánea, no obstante, en caso de requerirse otro medio debe solicitarse concepto a la Gerencia de Tecnología de la Información.

8.21 POLÍTICA PARA LA TRANSFERENCIA DE INFORMACIÓN

La organización establecerá políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación al interior y exterior Mutual SER EPS.

La política aplica a los Gerentes de área, directores, Coordinadores, empleados, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de Mutual SER EPS.

La Gerencia de Tecnología de la Información debe implementar las herramientas necesarias para asegurar la transferencia de información digital al interior y exterior de Mutual SER EPS, contra interceptación, copiado, modificación, enrutado y destrucción. En caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros.

Los empleados de Mutual SER EPS que traten temas o información clasificada como información pública reservada o información pública clasificada (privada o semiprivada), lo deberán hacer en lugares seguros y/o por medios de comunicación seguros.

8.22 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Mutual Ser EPS, a través de la Gerencia de Tecnología de la Información y la Coordinación de Nuevos Desarrollos y Evolución, establecen las siguientes directrices para la adquisición, desarrollo y mantenimiento de software, con el fin de garantizar la integridad del sistema de información:

- ✓ Todos los desarrollos de nuevos aplicativos y/o mejoras, deberán cumplir con los requisitos establecidos en los Procedimientos de Desarrollo de software relacionados en el Sistema de Calidad de la Organización.
- ✓ Para los nuevos aplicativos desarrollados por personal externo, la Gerencia de Tecnología de Información se debe asegurar de que las cláusulas de confidencialidad, integridad y seguridad de la información queden especificadas en el contrato, así como el cumplimiento de la ley 23 de 1982.
- ✓ Los derechos patrimoniales de cualquier software desarrollado para la organización deben quedar a disposición de Mutual Ser EPS.
- ✓ La copia no autorizada del código fuente de cualquier software desarrollado o adquirido y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- ✓ La Gerencia de Tecnología de la Información es responsable de investigar e implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo de software seguro, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
- ✓ El MANUAL PARA CONTROL DE CAMBIOS DE SOFTWARE especifica el proceso de control de cambio de software, incluyendo la publicación en ambiente productivo
- ✓ La Gerencia de Tecnología de la Información es responsable de garantizar que los ambientes de desarrollo y producción para el desarrollo de software estén separados físicamente o virtualizados.
- ✓ La Gerencia de Tecnología de la Información es responsable de desarrollar estrategias para analizar la seguridad en los sistemas de información, como no usar datos sensibles en ambientes de prueba y usar diferentes perfiles para pruebas y producción
- ✓ La Gerencia de Tecnología de la Información es responsable de evaluar y notificar a la Gerencia encargada si un software se debe dar de baja.

- ✓ La Gerencia de Tecnología de la Información debe evaluar todo software adquirido con la herramienta antivirus antes de ser instalada en los equipos de cómputo o servidores de la Organización.
- ✓ Cuando un proveedor suministre modificaciones de paquetes de software adquiridos, se deben analizar: los términos y condiciones de la licencia, para determinar si los cambios a realizar están permitidos; la conveniencia de realizar las modificaciones por personal de la Organización o contratarlas con el proveedor o un tercero y el impacto del cambio en la Organización.
- ✓ El contenido publicado en la página WEB de la Organización es solicitado por la Dirección de Comunicaciones o quien la Gerencia de Experiencia y Fidelización del Cliente encargue para esta labor.
- ✓ Cualquier cambio en la plataforma tecnológica de la organización, está sujeta en el PROCEDIMIENTO PARA GESTIÓN DE CAMBIOS SOBRE LA INFRAESCTRUCTURA DE SERVICIOS DE TI. Se debe garantizar que después del cambio, los sistemas de información involucrados funcionen correctamente en ambiente productivo para evitar fallas o indisponibilidad de estos.

8.23 POLÍTICA DE RELACIONES CON LOS PROVEEDORES

Los proveedores de la Organización que tengan acceso a los activos de información se rigen por los siguientes lineamientos:

1. Todo tercero con acceso a la información de la Organización debe firmar Acuerdo de confidencialidad y compromiso de cumplimiento de política de seguridad de la Información.
2. Los contratos realizados con los terceros con acceso a la información deben tener claramente definidos los acuerdos de niveles de servicios.
3. La Gerencia de Tecnología de la Información debe establecer las condiciones de conexión para los equipos de cómputo y dispositivos móviles de los terceros a la red de la Organización.
4. Los empleados responsables de la realización y/o firma de contratos o convenios con terceros se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

8.24 POLÍTICA DE GESTIÓN DE LA PRESTACION DE SERVICIOS DE TERCERAS PARTES

La Organización y cada Gerencia de área propenderán por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos de servicios establecidos con estos.

8.25 POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

La política de gestión de incidentes de seguridad de la información se encuentra dirigida a todo los terceros internos y externos que tienen acceso a los activos de información de la organización y busca asegurar que los incidentes o eventos relacionados con la seguridad de la información sean identificados y tratados de forma oportuna, disminuyendo los daños que puedan ser ocasionados y evitando en lo posible la propagación de la falla. El detalle de las actividades que deben ser realizadas se encuentran definidas en el Procedimiento GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

8.26 POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES DEL SOFTWARE

- ✓ La Gerencia de Tecnología de la Información debe certificar que todo el software que se ejecuta en la organización esté protegido por derechos de autor y requiera licencia de uso, o en su lugar sea software de libre distribución y uso.
- ✓ La Gerencia de Tecnología de la Información debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en los equipos de cómputo de la organización para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado corresponda únicamente al permitido.
- ✓ Los usuarios no deben instalar software o sistemas de información en sus equipos de cómputo suministrados para el desarrollo de sus actividades, la Gerencia de Tecnología de la Información aplicará los controles requeridos para este fin.
- ✓ Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

8.27 POLÍTICA DE SEGURIDAD PARA LA ADMINISTRACIÓN DE DATOS PERSONALES

Para la correcta administración de datos personales, Mutual SER EPS definió la Política de Tratamiento de Datos Personales, en cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013, dentro de la cual se definen los aspectos esenciales aplicables a la administración de los datos personales los cuales se dará un tratamiento de carácter transparente, lícito, seguro, confiable, y únicamente se emplearán para los fines concernientes el objeto social de Mutual SER EPS.

Mutual SER EPS se compromete en el marco normativo a proteger y Gestionar la seguridad de los datos personales y mantener la reserva y/o confidencialidad de la información almacenada en las bases de datos. Para tal efecto se establecen las políticas, lineamientos y procedimientos y estándares de seguridad de la información para la organización.

Los responsables del tratamiento de las bases de datos personales en conjunto con el comité de seguridad de la información deben definir los niveles de seguridad para cada base de datos que se maneje por Mutual SER EPS de acuerdo con la naturaleza de la información que contenga la misma y debe ser categorizada según la clasificación contenida en la Política de Tratamiento de Datos Personales a fin de establecer controles en el acceso de la información.

Asimismo, los responsables del tratamiento deben velar por el correcto almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, mediante el uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

En caso de ser necesario suministrar información a un tercero por la existencia de un vínculo contractual es de obligatorio cumplimiento la suscripción de un acuerdo de confidencialidad con anterioridad a la transmisión de las bases de datos.

Los funcionarios encargados del tratamiento y contratistas con acceso a las bases de datos personales de las cuales Mutual SER EPS es responsable, deberán cumplir los lineamientos generales y específicos a fin de evitar tratamiento indebido, accesos no autorizados, exposición y perdida de la información contenida en las bases de datos y no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

En el evento de finalizar alguna de las labores de tratamiento de Datos Personales por los funcionarios, contratistas o encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con Mutual SER EPS, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.

Esta política es de estricto cumplimiento y su desacato se considerará un incidente de seguridad que, dependiendo de gravedad da lugar a un proceso disciplinario acorde a los lineamientos establecidos dentro del REGLAMENTO INTERNO DEL TRABAJO MUTUAL SER EPS. Las políticas establecidas por Mutual SER EPS respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente.

En MUTUAL SER EPS se realizarán jornadas de capacitación para que las áreas con mayor nivel de interacción con la administración de datos personales y las disposiciones adoptadas para que en desarrollo de su labor tengan acceso a datos personales de titulares, bien sea porque los hayan suministrado a MUTUAL SER EPS o los hayan recibido de ellas, se les exige el cumplimiento de la política interna.

8.27.1 Transferencia de datos personales a países terceros

De acuerdo con el Título VIII de la Ley 1581 de 2012 de Protección de Datos Personales (LEPD) Mutual SER EPS prohíbe la transferencia de datos personales a países que no suministren niveles mínimos de protección de datos de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio y la normativa vigente.

Esta prohibición no regirá cuando se trate de:

- ✓ Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- ✓ Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- ✓ Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

- ✓ Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- ✓ Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. Se debe tener en cuenta que, en los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

Las transmisiones internacionales de datos personales que se efectúen entre Mutual SER EPS y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

8.27.2 Registro nacional de bases de datos

Mutual SER EPS se reserva, en los eventos contemplados en la ley y en sus manuales y reglamentos internos, la facultad de mantener y catalogar determinada información que repose en sus bases o bancos de datos, como confidencial de acuerdo con las normas vigentes, sus estatutos y reglamentos, todo lo anterior y en consonancia con el derecho fundamental y constitucional a la salud. Mutual SER EPS debe, de acuerdo con la normatividad vigente y la reglamentación que expida el gobierno nacional, realizar el registro de sus bases de datos, ante El Registro Nacional de Bases de Datos (RNBD).

8.28 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS PERSONALES

Los funcionarios encargados del tratamiento deben identificar riesgos relacionados con el tratamiento de los datos personales y establecer controles con el fin de mitigar sus causas, mediante la implementación de las políticas internas de seguridad y de acuerdo con la política de riesgos y el sistema de administración de riesgos y se implementarán las medidas de protección necesarias para evitar o minimizar los daños en el evento que una amenaza sea concretada.

El área de control interno y calidad será el encargado de realizar auditorías periódicas anual a las políticas de tratamiento de datos personales, de seguridad para la

administración de datos personales, y de administración de riesgos asociados al tratamiento de los datos personales.

8.29 LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN APLICABLE A GESTIÓN HUMANA

8.29.1 SELECCIÓN DEL RECURSO HUMANO

La Organización reconoce que el recurso humano es uno de los más importantes para alcanzar los objetivos estratégicos, por esto se cuenta con procedimientos de calidad para seleccionar y vincular personal idóneo y calificado. Esto último se garantiza con el cumplimiento del PROCEDIMIENTO DE SELECCIÓN DE PERSONAL, que incluye la verificación de la información proporcionada por los candidatos a empleos en la organización: referencias, experiencia, estudios y que los aspirantes cumplan con los perfiles de cargo, estos están debidamente documentados y contiene funciones, áreas de responsabilidad, competencias, activos e información a cargo, experiencia, entre otras.

8.29.2 ACUERDOS CONFIDENCIALIDAD Y SEGURIDAD DE INFORMACIÓN.

Todos los funcionarios deben aceptar los acuerdos de confidencialidad establecidos en las cláusulas contractuales. Estos compromisos enmarcan la protección y buen uso de la información.
Para el caso de contratistas, los respectivos contratos y ordenes de compras, incluyen una cláusula de confidencialidad de igual manera cuando se permita el acceso y/o transferencia de la información.

8.29.3 EDUCACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN.

Las estrategias para mejorar la cultura organizacional sobre la Seguridad de la Información se realizan a través de capacitaciones en los procesos de inducción de usuarios nuevos, emisión de boletines por Intranet, el uso de herramientas colaborativas en línea y conocimiento transferido por los Auxiliares de Servicios TI en sus labores de soporte técnico.

8.29.4 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

Las estrategias para mejorar la cultura organizacional sobre la Seguridad de la Información, las cuales se diseñan para impactar sobre el recurso humano, están soportadas con el plan de comunicación y un conjunto de actividades de capacitación y sensibilización, como son: inducción de usuarios nuevos, conferencias de seguridad, seminarios online (Que generan memorias o presentaciones que pueden ser útiles), consultoría con proveedores de seguridad de la información, envío de correos electrónicos, Newsfeed o boletines sobre seguridad en sitios web y conocimiento transferido por los Auxiliares de Servicios TI en sus labores de soporte técnico.

Para identificar las necesidades del proceso fortalecimiento y apropiación de la Seguridad de la Información en Mutual SER, se establece un conjunto de roles, en los cuales se concentrará el apoyo necesario para diseñar el plan de capacitación y sensibilización adecuada, conformado por:

1. Gerentes, directores y coordinadores
2. Personal de seguridad (oficiales de seguridad)
3. Responsables de sistemas de información
4. Administradores de sistemas de información y personal de soporte
5. Usuarios finales

Los métodos para identificación de necesidades son los siguientes:

1. Entrevistas con grupos clave o usuarios que hagan parte de los roles definidos previamente.
2. Encuestas organizacionales.
3. Verificar comportamientos generales del personal (sesiones abiertas, escritorios limpios etc.)
4. Verificación de los incidentes de seguridad de la información, son una fuente muy importante para identificar vulnerabilidades y amenazas en el sistema. Dependiendo de la causa raíz que se identifique, se puede obtener información para determinar si es necesario capacitar o para sensibilizar a la población con base a la información obtenida.
5. Análisis de eventos en los dispositivos de seguridad.
6. Tendencias en el sector donde se desempeña la Organización.

7. El plan de comunicación contiene el cronograma de sensibilización y capacitación anual, sobre la política de la seguridad de la información y los temas de interés que se estarán desarrollando a lo largo del periodo establecido, determinando la frecuencia de la actividad, a quien va dirigido, responsable y las fechas específicas.

8.29.5 GESTIÓN DE INCIDENTES

Si se identifican posibles riesgos que se puedan generar durante el acceso, procesamiento, comunicación o gestión de la información por parte de funcionarios, se debe cumplir el GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION y cumplimiento de las acciones dispuestas en el REGLAMENTO INTERNO DEL TRABAJO MUTUAL SER EPS.

En el caso de terceros se les deben comunicar los mecanismos de control necesarios para que la seguridad de Mutual SER EPS y estos deben ser aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

8.29.6 SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de Mutual SER EPS. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones disciplinarias, jurídicas o judiciales ante las autoridades competentes, de acuerdo con las circunstancias, si así lo ameritan.

8.29.7 RETIRO DE EMPLEADOS

En los casos de retiro de empleados se siguen los procedimientos de RETIRO DEL RECURSO HUMANO, donde se describen los pasos como el personal hace entrega formal de los activos y recursos tecnológicos asignados.

Para la entrega de cargo, se debe verificar el cumplimiento de unas condiciones de retiro, soportadas en el Acta de Entrega de Cargo. Entre las condiciones mencionadas se contempla:

1. Reporte veraz de los compromisos y obligaciones con el área, verificadas por el Jefe Inmediato.
2. Entrega del puesto de trabajo y aquellos elementos de soporte a sus labores, verificado por la Gerencia de Gestión de Experiencia y Fidelización del Cliente.
3. Entrega de equipos tecnológicos asignados (PC, portátil, Pantallas, dispositivos tecnológicos, memoria USB, entre otros), verificado por la Gerencia de TI.
4. Respaldo de la información, verificado por la Gerencia de TI.
5. Paz y salvo, verificado por la Gerencia de Gestión de Experiencia y Fidelización del Cliente.
6. Paralelamente, se realiza el de PROCEDIMIENTO CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN, donde se describe como deben ser bloqueados todos sus privilegios de acceso al Sistema de información de la Organización.

8.29.8 RESPONSABILIDADES DE LOS USUARIOS DEL SISTEMA DE INFORMACIÓN

1. Los usuarios del sistema de información tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información de la Organización, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.
2. Todo usuario que utilice los recursos del Sistema de Información debe velar por la integridad, confidencialidad y disponibilidad de la información organizacional bajo su responsabilidad.
3. El usuario del Sistema de Información evitará hacer uso de los recursos de tecnologías de la información para actividades diferentes a aquellas afines con su actividad laboral.
4. Las contraseñas de acceso de los distintos sistemas de información son personales e intransferibles. Su buen resguardo es obligación de quien las custodie y su definición y protección están definidas en: PROCEDIMIENTO CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN.

5. Las instalaciones de software o programas deben ser realizada únicamente por el personal de la Gerencia de Tecnología de la Información.
6. Todo software utilizado en la Organización debe contar con licencia, y dar cumplimiento a las condiciones de uso. El uso de programas sin su respectiva licencia e instalación sin autorización por parte de la Gerencia de Tecnología de la Información u obtenidos por otras fuentes (internet, ejecutables portables, dispositivos USB) puede implicar materialización del riesgo de seguridad de la información (código malicioso, afectación en servicios, etc.).
7. El usuario del sistema de información es responsable por la información almacenada en los equipos de cómputo asignados. Se prohíbe archivar en los equipos de la organización documentos u otro tipo de datos externos no pertinentes a la actividad productiva o que pueda presentar violación de los derechos de autor y de propiedad intelectual en las carpetas destinadas solo para almacenar información corporativa (equipo local o servidores).
8. Al hacer consultas y/o búsquedas en cualquier aplicativo del Sistema de Información, se debe diligenciar el mayor número de detalles con el objeto de evitar saturación en los canales de telecomunicaciones o la generación de un alto número de transacciones en los motores de bases de datos que conllevarían un alto consumo de recursos del sistema y el consecuente detrimento de su rendimiento.
9. Al usar el servicio de navegación en Internet, se prohíbe el acceso a sitios web que puedan atentar contra la integridad de la información, tales como: sitios pornográficos, descargas de software no autorizados, entre otros. La Gerencia de Tecnología de la Información garantiza que los equipos de cómputo cuenten con antivirus, actualizaciones del Sistema operativo con el fin de tener controles de seguridad en la navegación.
10. Toda la información usada, trasmitida o almacenada dentro de los procesos de la Organización es propiedad de esta por lo cual debe seguir los lineamientos para su tratamiento. Como postura general, está completamente prohibida la destrucción, copia o distribución de los archivos de la Organización sin la autorización de la unidad funcional.
11. Los buzones de correo electrónico y los sistemas de mensajería instantánea de la Organización son herramientas que facilitan

comunicaciones a nivel organizacional, por ello su uso debe limitarse a temáticas referentes a las actividades productivas.

12. Los usuarios son responsables de todas las actividades que realicen con sus cuentas de correo electrónico. Se recomienda cambiar la contraseña periódicamente. El uso indebido del correo electrónico puede acarrear responsabilidades civiles y penales.
13. No está permitido facilitar u ofrecer las cuentas de correo a terceras personas.
14. No está permitido enviar mensajes desde direcciones no asignadas por los responsables del correo electrónico. Es ilegal manipular las cabeceras de los mensajes de correo electrónico salientes (falsificación de identidad).
15. La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún empleado debe utilizar una cuenta diferente a la asignada.
16. Los mensajes y la información contenida en los correos electrónicos corporativos no deben ser utilizado para actividades personales.
17. Se prohíbe él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas.
18. Se restringe el envío de archivos que contengan extensiones ejecutables.
19. El usuario es el responsable de realizar la copia de sus datos en la plataforma de almacenamiento disponible.
20. Cumplir con las normas de buen uso de equipos y recursos tecnológicos.
21. Todo dispositivo de almacenamiento externo tales como: Memorias USB, CD-ROM, DVD, entre otros, deben ser escaneadas por el software Antivirus para la detección de software nocivo y/o virus, antes de hacer uso de estos.
22. Los usuarios del sistema de información solo tendrán acceso a datos y recursos tecnológicos asignados, y serán responsables administrativa y legalmente de la divulgación de información no autorizada en medios electrónicos, lugares públicos, en conversaciones o situaciones que en general que pongan en riesgos la seguridad y el buen nombre de la Organización.

23. Los usuarios del sistema de información son responsables de salvaguardar la información contenida en documentos, formatos, y toda la producida como resultado de los procesos de la Organización.
24. Cualquier incidente de seguridad informática debe ser registrado a través de la Centro de servicios de la Gerencia de Tecnología de la Información para el respectivo proceso de verificación, investigación de acuerdo con los procedimientos de la Organización.
25. Las herramientas de acceso remoto estarán controladas por la Gerencia de Tecnología de la Información. El uso de conexiones diferentes o uso de software o complementos de los navegadores diferentes a los autorizados por la Gerencia de Tecnología de la Información tendrá las sanciones que haya lugar de acuerdo con el Reglamento Interno del trabajador.
26. La Organización cuenta con herramienta de chat e Intranet corporativos. La organización cuenta con restricciones para el acceso a redes sociales, paginas interactivas de mensajería instantánea. En caso tal se requiera acceso a redes sociales para el
27. cumplimiento de funciones de un proceso, debe ser autorizado por la Gerencia de Tecnología de la Información.
28. El uso de canales de streaming o reproducciones de videos solo se permite a los usuarios que de acuerdo con las funciones del cargo lo requieren. Esto con el fin de evitar saturación de los canales de internet.
29. La descarga P2P o de archivos de páginas en donde se almacena contenido multimedia se encuentra restringida con el fin de evitar que sean descargados archivos maliciosos o que atenten contra la propiedad intelectual y derechos de autor.

9. CICLO DE VIDA DE LOS DATOS

9.1 Fases de la gestión de los datos

La información que se Gestiona en la organización y que sirve de insumo para tomar decisiones, pasa por diferentes fases que permiten depurarla y hacerla consistente y válida al momento de utilizarla, estas fases son:

1. Captura: Fase que consiste en ingresar al sistema de información los producidos en los procesos básicos o de línea, desde la afiliación, contratación de red, contacto con prestadores, autorización de servicios, monitorización del contacto con prestadores, auditoria y evaluación de la satisfacción del usuario con los

servicios recibidos y los datos de los procesos de apoyo administrativos y financieros.

2. Para los diferentes datos y por cada proceso el sistema tiene diseñado un formulario de captura que permite el registro del dato, orientado siempre a permitir al usuario el manejo amable del software.
3. Validación: Fase automática del sistema diseñada por clientes y proveedores del proceso, que permite la captura inteligente del dato. Su función básica es dejar que se almacene solo aquella información que previamente ha pasado por una malla de validación y alertar sobre datos errados ingresados al sistema. La validación incluye.

10. VIGENCIA

El presente Manual de Políticas de Seguridad de la Información rige a partir del 27 de septiembre de 2019, fecha en que fue aprobada por la Junta Directiva de la Mutual SER EPS, hasta la modificación o sustitución de los lineamientos a que sea sujeto el presente documento.

11. CONTROL DE CAMBIOS

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