CONTENIDO

1. INTRODUCCIÓN

Mutual SER EPS, con el fin de regular y mantener la seguridad de la información al interior y exterior de la Organización define las obligaciones de sus grupos de interés relacionando las normas, procedimientos y controles apropiados que estos deben cumplir, mediante políticas de seguridad de la información para proteger los recursos físicos y financieros, el buen nombre, la posición legal, los empleados y otros activos tangibles e intangibles preservando la confidencialidad, integridad y disponibilidad de los activos de información de la Organización.

Siempre teniendo en cuenta el marco general del funcionamiento de la organización, los objetivos organizacionales, los procesos misionales, adaptadas a las condiciones específicas y particulares de los grupos de interés de forma concisa, comprensibles y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción.

2. OBJETIVO

Establecer en la Organización directrices, lineamientos y/o intenciones enmarcados con el Modelo de seguridad de la información MSPI que conlleven a gestionar y minimizar los riesgos asociados con la pérdida, destrucción, modificación, acceso no autorizado, divulgación, duplicación, interrupción de sistemas, mal uso de los activos de información y tecnologías, entre otros.

3. ALCANCE

Todos los aspectos administrativos y de control que deben ser cumplidos (en relación con los activos de la información) por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con Mutual SER EPS para conseguir un adecuado nivel de protección de seguridad y calidad de la información en la Organización.

4. RESPONSABLE(S)

- Gerencia general.
- Comité de Seguridad de la Información.
- Director de Gestión Documental.
- Gerencia de Tecnología de la Información.
- Director de Control Interno y Calidad.
- Líderes de procesos.

5. NORMATIVIDAD

- Ley 1581 de 2012.

- Ley 1712 de 2014
- Ley 1078 de 2015
- Modelo de Seguridad y Privacidad de la Información (MSPI)
- Guía #2 – Elaboración de la Política General de seguridad y privacidad de la información MSPI v1
- Guía #3 – Procedimiento de seguridad de la información MSPI
- Guía #4 – Roles y responsabilidades MSPI
- Guía #5 – Gestión y clasificación de activos de la información MSPI
- NTC-ISO 27001 de 2013. *(De adherencia voluntaria).*

6. DEFINICIONES

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, por medio de la Estrategia de Gobierno en línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

- **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 la 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. POLÍTICAS DEFINIDAS.

7.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Mutual SER EPS, establece sus políticas de seguridad de la información para el Modelo de Seguridad y Privacidad de la Información (MSPI) herramienta estratégica para la planificación, implementación, evaluación y mejora del sistema de información, definiendo así el marco general para el diseño, adopción y promoción de lineamientos para la seguridad de la información.

A través de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), definido por el Ministerio de Tecnología de la Información y las Comunicaciones se busca preservar la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus medios a partir de la aplicación de los principios generales de gestión de la calidad y el pensamiento basado en riesgos, en aras de brindar soluciones y respaldo a las partes interesadas de la Organización.

Es así como, para el fin en mención se ha **conformado** el ***Comité de Seguridad de la Información*** para la Organización:

1. Presidente, quien será escogido dentro de los demás miembros del Comité
2. Secretario, quien será escogido dentro de los demás miembros del Comité
3. Representante de Seguridad Informática
4. Representante del Sistema de Gestión de la Calidad
5. Representante de Gestión Documental
6. Representante de Gestión de Tecnología de la Información
7. Representante de Ambiente Físico
8. Representante de Planeación y Control Interno
9. Representante de Gestión Jurídica
10. Representante de Gestión Humana
11. Representante de Comunicaciones

Nota: El Comité (*Conformado por 09 integrantes de la Organización)* puede invitar a las personas que considere necesarias, cuando así lo requiera, quienes tendrán voz, pero no voto.

El Comité de Seguridad de la Información de Mutual SER EPS, tendrá como **objetivos**:

- Asegurar el direccionamiento y apoyo gerencial para soportar la administración y desarrollo de proyectos e iniciativas enfocadas al mejoramiento continuo de la Seguridad de la Información a través de compromisos apropiados.
- Verificar el avance de los distintos proyectos e iniciativas en el contexto de la prestación del servicio por la organización que implican la aplicación de Seguridad de la Información.

- Asistir a los diferentes procesos de la Organización para determinar los recursos adecuados en el establecimiento, implementación, mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Promover políticas en materia de seguridad de la información y estrategias para la divulgación de éstas a todos los funcionarios y contratistas de la entidad.
- Revisar y mantener actualizada la Política de Seguridad de la Información de la Organización.
- Proponer estrategias para la divulgación de las políticas a todos los funcionarios y contratistas de la Organización.

La verificación del **cumplimiento** de las Políticas establecidas en Mutual SER EPS estará a cargo del ***Comité de Seguridad de la Información*** orientando a colaboradores, contratistas, proveedores y partes interesadas en el uso adecuado de la información y los recursos tecnológicos para mantener la confidencialidad, integridad y disponibilidad aplicando los controles de seguridad establecidos en las políticas que se encuentran documentas y establecidas en la declaración de ***Política de seguridad de seguridad y privacidad de la información*** de la Organización.

El incumplimiento de las Políticas de Seguridad de la Información podrá dar lugar a un proceso disciplinario para los funcionarios, y se podrá convertir en un incumplimiento del contrato respecto de los contratistas que podrá dar lugar a la imposición de sanciones e incluso su terminación del contrato. Estas son de carácter obligatorio para todo el personal de la organización, aplican también para los terceros y partes interesadas que tengan alguna relación con la organización.

7.2 GESTIÓN DE ACTIVOS

7.2.1 IDENTIFICACIÓN DE ACTIVOS.

Mutual SER EPS, mantiene un inventario de activos de información *(Matriz de Inventario y Valoración de Activos de Información)* teniendo en cuenta los niveles de clasificación como Confidencialidad, integridad y disponibilidad, para lo cual ha determinado que la **periodicidad** o frecuencia de realización de identificación, revisión y/o actualización del inventario de Activos de Información al interior de la organización se realizará anualmente sin embargo, esta podrá cambiar de acuerdo con las necesidades que surjan.

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.

De su parte, 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 o no de las especificaciones y medidas de seguridad de la información establecidas por estas Políticas, Normas, Procedimientos y prácticas que de ella surjan.

El inventario y clasificación de los Activos de Información es la base para identificar los Activos de Información y para gestionar los riesgos de seguridad de la información, así como para determinar los niveles de protección que se requieren. Un Activo de Información se encuentra presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos y bases de datos, de igual manera se contempla como Activo de Información al personal de colaboradores de la Organización, que cumplen unos criterios específicos como 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.

Los colaboradores designados de los procesos deberán identificar cuáles y cuantos activos de información tiene bajo responsabilidad en el proceso, éstos seleccionan y determinan la inclusión de los Activos de Información en el instrumento o herramienta de control establecida por la Organización, documento ***Matriz de Inventario y Valoración de Activos de Información***. En este instrumento se establecen: Los activos de mayor criticidad e impacto para la Organización en cada uno de los procesos, la clasificación del activo, la valoración del activo, el tipo de activo **identifica el propietario del activo de información**, la información básica del activo, la ubicación del activo, el etiquetado y manipulación de la información, entre otros…

7.2.2 CLASIFICACIÓN DE ACTIVOS.

Mutual SER EPS mantiene un inventario (*Matriz de Inventario y Valoración de Activos de Información)* de los Activos de Información, siempre teniendo en cuenta los niveles de **clasificación** (Confidencialidad, Integridad y Disponibilidad) con el objetivo de asegurar que la información recibe los niveles de protección adecuados ya que con base en su valor y de acuerdo con otras características particulares requiere un tipo de manejo especial.

El sistema de clasificación de la información definido en Mutual SER EPS, se basa las características particulares de la información, contempla la cultura y la dinámica de funcionamiento, está encaminada en dar cumplimiento a los requerimientos estipulados en leyes y normatividades actuales que afecten o puedan afectar a la Organización.

Clasificación.

Definición de los Criterios de Confidencialidad de la Información:

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, se adoptaron tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014:

- **Información Pública Reservada:**

Información disponible sólo para un proceso de la organización y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, reputacional o económica.

- **Información Pública Clasificada:**

Información disponible para todos los procesos de la organización y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta.

Esta información es propia de la organización o de terceros y puede ser utilizada por todos los funcionarios de la organización para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

- **Información pública:**

Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro o fuera de la organización, sin que esto implique daños a terceros, ni a las actividades o procesos de la organización.

- **No clasificada:**

Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información pública reservada.

Definición de los Criterios de Integridad de la Información:

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción, se adoptaron tres (3) niveles de clasificación:

- **A (ALTA):**

Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la organización.

- **M (MEDIA):**

Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la organización.

- **B (BAJA):**

Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la organización o entes externos.

- **NO CLASIFICADA:**

Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integralidad ALTA.

Definición de los Criterios de Disponibilidad de la Información:

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso, se adoptaron tres (3) niveles de clasificación.

1. **ALTA:**

La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

2. **MEDIA:**

La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la organización.

3. BAJA:

La no disponibilidad de la información puede afectar la operación normal de la organización o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

4. NO CLASIFICADA:

Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla1. Esquema General de clasificación.

Valoración del Activo de Información.

La valoración del Activo está fijada por la Criticidad de la Información; Definida como el cálculo automático que determina el valor general del Activo de acuerdo con la Clasificación de la Información, asociado a la Justificación que para cada valoración del activo de información describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad).

Definición de los Criterios de Criticidad de la Información:

Cálculo automático que determina el valor general del Activo de acuerdo con la Clasificación de la Información, se adoptaron tres (3) niveles de clasificación.

1. ALTA:

Activos de Información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencial, integridad y disponibilidad) es ALTA.

2. MEDIA:

Activos de Información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel MEDIO.

3. BAJA:

Activos de información en los cuales la clasificación de la información en todos sus niveles es BAJA.

7.2.3 ETIQUETADO DE LA INFORMACIÓN.

Mutual SER EPS, ha adoptado y establecido el **mecanismo o método** recomendado en el Modelo de Seguridad y Privacidad de la Información (MSPI) para realizar el etiquetado de los Activos de Información consignados en el documento, *Matriz de Inventario y Valoración de Activos de Información* y se deben tener en cuenta las siguientes pautas generales:

- Se etiquetarán todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad.
- Se etiquetará el nivel de clasificación en relación a Confidencialidad, Integridad, y Disponibilidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como **NO CLASIFICADA**.
- Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente diligenciar la clasificación de la siguiente forma:
  - ✓ {Clasif: Confidencialidad} - {Clasif: Integridad} - {Clasif: Disponibilidad}
- Para los activos clasificados en Confidencialidad como:
  - ✓ INFORMACION PUBLICA RESERVADA se utiliza la etiqueta **IPR**.
  - ✓ INFORMACION PUBLICA CLASIFICADA, **IPC** y,
  - ✓ INFORMACION PUBLICA, **IPB**.
- Para los activos clasificados en Integridad como:
  - ✓ ALTA se utilizará la etiqueta **A**,
  - ✓ MEDIA, **M** y,
  - ✓ BAJA, **B**.
- Para los activos clasificados en disponibilidad como:
  - ✓ ALTA se utilizará la etiqueta **1**,
  - ✓ MEDIA, **2** y,
  - ✓ BAJA, **3**.

De esta manera, se realizarán las combinaciones de acuerdo con los criterios de clasificación de la información.

La actividad de **etiquetado** estará bajo la responsabilidad del líder de cada proceso quien(es) deberán etiquetar los Activos de Información identificados (en el documento; *Matriz de Inventario y Valoración de Activos de Información*) con mayor criticidad e impacto para la Organización.

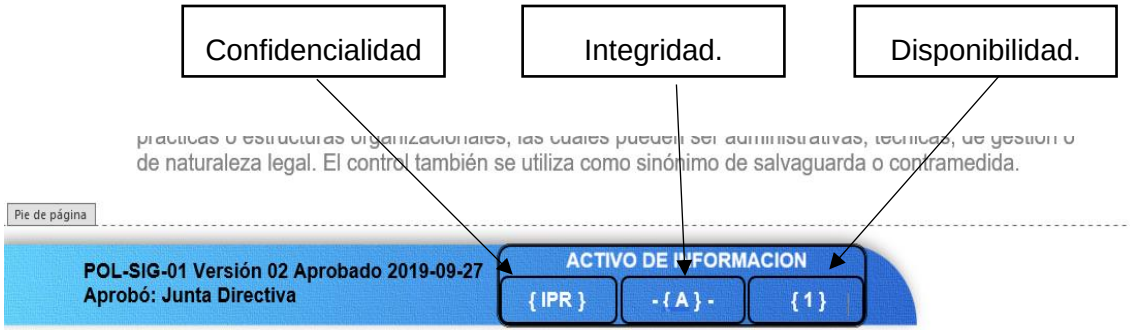

Figura 1 Etiquetado Activos de Información.

Mutual SER EPS, se asegura que los activos de información reciban un nivel apropiado de protección acuerdo al nivel de criticidad, derivado de la importancia de su clasificación por lo que se establece con carácter **obligatorio** la actividad del etiquetado de los Activos de Información identificados en la Organización y que se encuentran establecidos en la *Matriz de Inventario y Valoración de Activos de Información.*

7.2.4 DEVOLUCIÓN DE LOS ACTIVOS.

Mutual SER EPS, establece que para la entrega de los activos físicos y de la información (Equipos y Dispositivos Tecnológicos) cuando se presentan casos de; Cambio de propietario, donación, desechar o baja de un equipo de cómputo de usuario final y finalización del empleo acuerdo o contrato con la Organización, se debe seguir lo instaurado en el procedimiento **PRO-TIC-05** de igual manera establece que es responsable de su cumplimiento la Gerencia de Tecnología de la información garantizando la integridad del activo y la seguridad de la información.

7.2.5 GESTIÓN DE MEDIOS REMOVIBLES.

Mutual Ser EPS dispone de herramientas tecnológicas (aplicativos) que permiten realizar gestión y control de los medios removibles *(Memorias USB, Discos Duros Portátiles, Tarjetas de Memoria, Discos Ópticos "CD, DVD, Blu-Ray", cámaras digitales fotográficas, cámaras de video, celulares, etc.)* con el fin de brindar el acceso al personal de usuarios y/o funcionarios de la Organización de estos medios especiales.

Para los usuarios y/o funcionarios de la Organización se tiene establecido que el uso de medios removibles está direccionado con las actividades de almacenamiento provisional, transferencia rápida y directa de información, y eliminación de información almacenada.

De igual manera, para los usuarios y/o funcionarios de la Organización se tiene establecidos permisos frente a los medios removibles como son de; portabilidad, utilización, asignación, destrucción, almacenamiento, retención y/o confiscar, y monitorear.

En Mutual SER EPS **se autoriza** el **uso de medios removibles en casos como:**

- Configuración de equipos por el personal de técnicos.
- Copias de respaldo de los equipos por personal de técnicos.
- Actividades de recuperación de información por daños en equipos.
- Presentaciones para proyecciones.
- Activación de programas con llave de funcionamiento.
- Entre otros.

De igual manera, en Mutual SER EPS No se autoriza el uso de medios removibles en los siguientes casos:

- Cuando empleados o terceros que tengan vínculo contractual no cuente con la autorización requerida.
- Cuando empleados o terceros que tengan vínculo contractual o se encuentren desarrollando actividades para la Organización utilicen 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.
- Cuando se evidencie deterioro en el medio de almacenamiento.
- Cuando se evidencie daños en el medio de almacenamiento
- Cuando se encuentre infectado por virus.
- Entre otras…

La Gerencia de Tecnología de la Información es **responsable de las autorizaciones** emitidas a usuarios *(funcionarios, contratistas o terceros)* para el uso de medio de almacenamiento, previa solicitud con el cumplimiento de los requisitos establecidos.

La asignación de autorización para el uso de medios de almacenamiento incluyen **las responsabilidades específicas** que le corresponden al usuario para con el uso de dicho medio de almacenamiento "*por ejemplo: a funcionarios; Desinfección por antivirus del medio de almacenamiento antes de su uso, en caso de pérdida de algún medio removible se debe reportar a la gerencia de TI el evento sucedido, es responsable de salvaguardar el medio de almacenamiento, vigilar por el buen uso y del medio de almacenamiento y la información contenida en su poder, Etc."*

Mediante procedimiento se determinan las autorizaciones para el uso y no uso de medio de almacenamiento con sus respectivas responsabilidades para el usuario *(funcionarios, contratistas o terceros)* que lo solicite.

En Mutual SER EPS el **uso de medios removibles** se encuentra alineado con las **clasificaciones** de **activos de información** dispuestas en la política de "Clasificación de

Activos" reflejados en el documento ***Matriz de Inventario y Valoración de Activos de Información*** de la organización.

7.2.6 DISPOSICIÓN DE LOS ACTIVOS.

Mutual SER EPS ha determinado que para realizar de forma segura y correcta las actividades de eliminación, retiro, traslado o reúso de los activos cuando estos ya no se requieran, éstas se deben desarrollar conforme lo establecido en el procedimiento **POL-ADM-02** de manera obligatoria por los colaboradores de la Organización.

Así mismo, se establece que, con el fin de evitar el acceso o borrado no autorizado de la información contenida en estos activos, se debe realizar la toma de backup conforme a lo establecido en el procedimiento **PRO-TIC-11** así como en medios removibles y en activos de procesamiento y/o almacenamiento de información.

Las áreas responsables de la información con el apoyo de la Gerencia de Tecnología de la Información a su vez 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.

La Organización cuidará porque los medios magnéticos que contienen la información crítica (backup) sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta, el sitio externo donde se resguarden las copias de respaldo contará con los controles apropiados conforme a lo definido en el documento **INS-TIC-23.**

7.2.7 DISPOSITIVOS MÓVILES.

En mutual SER EPS la conexión inalámbrica es dinámica y es usada por cualquier funcionario contratistas o terceros de la Organización que la necesite en determinado momento cumpliendo las directrices de acceso a la red y asignación por área del negocio (VLAN). Pero, está determinado que: Los únicos **funcionarios** que pueden tener acceso a las redes inalámbricas para actividades como instalación son el personal del área de soporte del proceso de Gestión Tecnologías de Información.

De igual manera se ha determinado que los únicos contratistas o terceros que pueden llegar a tener acceso, previo cumplimiento de los requisitos establecidos de acceso, son del tipo de soporte de infraestructura de redes, configuraciones, proveedor de acceso relacionada directamente con las redes inalámbricas.

Además, cabe resaltar que; la mensajería electrónica en Mutual SER EPS se encuentra 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 la política de uso aceptable. Por tanto, la **instalación** de software o programas ***(chats corporativos y/o correos electrónicos de la Organización)*** deben ser realizada únicamente por el **personal** de la Gerencia de Tecnología de la Información.

Mutual SER EPS, provee las condiciones para el manejo de los dispositivos móviles institucionales que hacen uso de servicios de tecnología que ofrece la Organización, y establece que frente al uso correcto y ético de la **información almacenada** en los **Dispositivos móviles** está **en responsabilidad de** los funcionarios asignados a estos como;

- No almacenar en dispositivos móviles personales información de Mutual SER EPS que no esté clasificada como pública.
- 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).
- No hacer uso de los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- 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.
- No instalar programas desde fuentes desconocidas en los dispositivos móviles institucionales.
- Es deber que, 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 vigila y corrobora las opciones de protección (*los **controles de seguridad** que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información)* de los accesos de los dispositivos móviles que hacen uso de los servicios provistos por la organización de acuerdo con los lineamientos del **MAN-TIC-05.**

8. CONTROL DE ACCESO

Mutual SER EPS ha determinado los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad relacionados para los accesos a la información *(electrónicos, físicos.)* en la Organización así:

8.1 CONTROL DE ACCESO CON USUARIO Y CONTRASEÑA

Mutual SER EPS ejerce ***control de acceso a la red***, por tanto, los empleados no usarán conexiones distintas a las que provee Gerencia de TI, es así como, el uso de conexiones TOR como complemento de los navegadores no están autorizados, y las conexiones que se generen y se evidencien en los sistemas de control adoptados por el Direccionamiento Tecnológico tendrán las sanciones a que haya lugar.

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar, el camino de las comunicaciones es controlado se limitan las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales se encuentra autorizado a acceder mediante la implementación de controles en diferentes puntos de esta teniendo en cuenta:

- La navegación abierta en internet por la plataforma tecnológica es controlada (asignada según cargo del empleado).
- Las comunicaciones con origen y destino autorizados se controlan a través de firewalls de red.
- El acceso a las páginas web es controlado por las políticas de los Firewalls de red.
- 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.

El **control de acceso** a los **servicios de red** tanto internos como externos es realizado para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos. Por lo tanto, se desarrollan actividades con el fin de activar y desactivar derechos de acceso a las redes las cuales se encuentran descritas en el **MAN-TIC-05.**

Mutual SER EPS a través de la Gerencia de Tecnología de la Información ejerce control de acceso en **Aplicaciones** de la siguiente forma:

- Para acceder a las aplicaciones corporativas se requiere de un usuario autorizado para acceder a cada aplicación en particular.
- Se debe asignar un usuario único para cada funcionario.
- Cada usuario tiene asignado un rol, el cual a su vez tiene una serie de permisos de acceso concedidos al usuario que lo posea.
- Las aplicaciones están protegidas por el contexto de la sesión que se genera cuando se ingresa correctamente una combinación de usuario contraseña, de esta manera no se puede acceder a una URL o modulo en particular sin antes establecerse una sesión.
- Para acceder a las aplicaciones internas de manera remota, se requiere conexión mediante una VPN.
- El tiempo de actividad del usuario en el sistema está limitado al periodo laboral en la empresa o a al periodo especifico que se solicite.
- Los usuarios (funcionarios, contratistas o terceros) utilizan diferentes perfiles para los ambientes de desarrollo, pruebas y producción
- Asegurando que los desarrolladores internos o externos posean acceso limitado a los datos de los ambientes productivos.
- Las Gerencias de área de la Organización como propietarias de los aplicativos que apoyan los procesos y áreas que lideran, cuidarán por la asignación, modificación y revocación de privilegios de accesos a sus aplicativos de manera controlada.

- No se muestra información del sistema, hasta tanto el proceso de inicio de sesión se haya completado.
- 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 se transmite en texto claro las contraseñas de los usuarios a través de la red.
- Cierre de sesiones inactivas después de un tiempo de inactividad.
- Todo el equipo de cómputo de usuario final *(funcionarios, contratistas o terceros)* debe tener configurado acceso seguro mediante usuario y contraseña.
- Bloquear las sesiones en los equipos de cómputo, automáticamente cuando los usuarios *(funcionarios, contratistas o terceros)* deben deban abandonar temporalmente su puesto de trabajo.
- Los usuarios *(funcionarios, contratistas o terceros)* 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.
- Evitando visualizar mensajes que puedan ser usados para descifrar los datos del usuario y contraseña en intentos fallidos de autenticación y/o indicando que parte de los datos que se digitaron son correctos.

De igual manera, Mutual SER EPS a través de la Gerencia de Tecnología de la Información ejerce control de acceso en **Sistemas de Información** de la siguiente forma:

- Para acceder a los sistemas de información se requiere de un usuario autorizado para acceder a cada sistema en particular.
- Se debe asignar un usuario único para cada funcionario.
- Cada usuario tiene asignado un rol, el cual a su vez tiene una serie de permisos de acceso concedidos al usuario que lo posea.
- Las aplicaciones están protegidas por el contexto de la sesión que se genera cuando se ingresa correctamente una combinación de usuario contraseña, de esta manera no se puede acceder a una URL o modulo en particular sin antes establecerse una sesión.
- Para acceder a los sistemas internos de manera remota, se requiere conexión mediante una VPN.
- El tiempo de actividad del usuario en el sistema está limitado al periodo laboral en la empresa o a al periodo especifico que se solicite.
- Las Gerencias de área de la Organización como propietarias de los sistemas de información que apoyan los procesos y áreas que lideran cuidarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas de manera controlada.

En Mutual SER EPS Se encuentran claramente **determinados** e identificados los **responsables** *(Procesos, Roles)* para autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas establecidos así:

La Gerencia de Tecnología de la Información, es responsable de las redes de datos y los recursos de red.*(ésta propende porque dichas redes sean protegidas debidamente contra accesos no autorizados a través de mecanismos de control de acceso lógico),* el Proceso de Gestión Humana es responsable de autorizar la creación, suspensión o eliminación de usuario (ID) y contraseñas, en el caso de las modificaciones de usuarios y contraseñas son de responsabilidad conjunta entre el Proceso de Gestión Humana y La Gerencia de TI.

Todo lo concerniente a creación, modificación suspensión o eliminación de usuarios (ID) y contraseñas es decir los **procedimientos** formales de autorización, se encuentran establecidos en el procedimiento **PRO-TIC-04**.

Los **funcionarios** de Mutual SER EPS al contar con un **usuario** o **contraseña** de la Organización tienen la **responsabilidad** en:

- Realizar un adecuado uso de los recursos tecnológicos y los sistemas de información de la Organización salvaguardando la información a la cual les es permitido el acceso.
- Las acciones realizadas en los recursos tecnológicos y los sistemas de información de la Organización, así como del usuario y contraseña asignados para el acceso a estos.
- Acogerse a lineamientos de contraseñas de la Organización. PRO-TIC-04.
- Cambiar periódicamente su contraseña a través del aplicativo de Autoservicio de contraseñas, teniendo en cuenta *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 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 de forma regular.
- Proteger sus contraseñas las cuales son de uso personal e intransferible,
- Evitar que las contraseñas sean fáciles de recordar;
- Que no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.).

Los **contratista o terceros** de Mutual SER EPS al contar con un **usuario** o **contraseña** de la Organización tienen la **responsabilidad** en:

- El manejo, administración y su custodia.
- El uso de éstas es personal e intransferible.
- Protegerlas contra robo, hurto.
- Acogerse a lineamientos de contraseñas de la Organización. **PRO-TIC-04.**

- Dar aviso inmediato a la Organización cuando considere que el usuario y contraseña han sido conocidos por otros y se corre peligro de ser utilizados indebidamente.
- Dar aviso cuando ha perdido su control o custodia.

La Organización ha establecido que los **usuarios (ID),** de los recursos tecnológicos **y las contraseñas** de acceso a los distintos sistemas de información son **personales** e **intransferibles**, los usuarios no deben compartir sus cuentas de **usuario** y **contraseñas** con otras personas, su buen resguardo es obligación de quien las custodie su definición y protección están contempladas en PRO-TIC-04.

De igual manera, la Organización ha establecido en el documento **PRO-TIC-04** que por cada **funcionario**, **contratista** o **tercero** se asigna un usuario y una contraseña a éste para el acceso.

8.2 SUMINISTRO DEL CONTROL DE ACCESO

Mutual SER EPS ha establecido **procedimientos** específicos para la gestión de derechos y/o privilegios a cada uno de los usuarios (ID) en materia de asignación, modificación, revisión o renovación.

Para la ***gestión de asignación*** de derechos y/o privilegios a cada uno de los **usuarios** (ID) creados en Mutual SER EPS se ha establecido **directrices** como son:

- Las Gerencias de área de la Organización como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, vigilarán 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 debe establecer que los 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.
- 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.
- La Gerencia de Tecnología de la Información establece 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.
- Para permisos especiales de personal externo a la Organización, proveedores o dispositivos que requieran cuenta de usuario, se debe solicitar por medio de un caso en ZONA TIC,
- Otros...

De igual manera, en el *procedimiento de creación, modificación y eliminación de usuarios del sistema de información* **PRO-TIC-04**, se encuentran determinadas éstas directrices para mayor claridad.

Para la ***gestión de modificación*** de derechos y/o privilegios a cada uno de los **usuarios** (ID) creados en Mutual SER EPS se ha establecido **directrices** como son:

- Se debe diligenciar el formato establecido por la Organización.
- Se debe de validar la información contenida en el formato de solicitud.
- Se deben establecer privilegios en los aplicativos que correspondan.
- Se debe notificar a las instancias que correspondan.
- Se deben utilizar las tablas de perfiles de usuarios del sistema de información.
- Se deben utilizar las tablas de roles/ tipo de usuario por aplicación.
- Para permisos especiales de personal Interno de la Organización que requieran configuración adicional de los roles preestablecidos se debe solicitar por medio de un caso en ZONA TIC.
- Otras…

De igual manera, en el *procedimiento de creación, modificación y eliminación de usuarios del sistema de información* **PRO-TIC-04**, se encuentran determinadas éstas directrices para mayor claridad.

Para la ***gestión de revisión*** de derechos y/o privilegios a cada uno de los **usuarios** (ID) creados en Mutual SER EPS se ha establecido **directrices** como son:

- Se debe diligenciar el formato establecido por la Organización.
- Se debe de validar la información contenida en el formato de solicitud.
- Se deben actualizar y/o modificar privilegios en los aplicativos que correspondan.
- Se debe notificar a las instancias que correspondan.
- Se deben utilizar las tablas de perfiles de usuarios del sistema de información.
- Se deben utilizar las tablas de roles/ tipo de usuario por aplicación.
- Las tablas de roles y accesos se deberán actualizar anualmente.
- Otras…

De igual manera, en el *procedimiento de creación, modificación y eliminación de usuarios del sistema de información* **PRO-TIC-04**, se encuentran determinadas éstas directrices para mayor claridad.

Para la ***gestión de revocación*** de *derechos* y/o privilegios a cada uno de los **usuarios** (ID) creados en Mutual SER EPS se ha establecido **directrices** como son:

- Se debe deshabilitar el usuario el mismo día del retiro/revocación.
- Se debe notificar a las instancias que correspondan.
- Se debe diligenciar el formato establecido por la Organización.
- Se debe de validar la información contenida en el formato de solicitud.

- Se deben deshabilitar privilegios en los aplicativos que correspondan.
- La cuenta de correo electrónico no estará disponible por ningún medio.
- Otras…

De igual manera, en el *procedimiento de creación, modificación y eliminación de usuarios del sistema de información* **PRO-TIC-04**, se encuentran determinadas éstas directrices para mayor claridad.

Para **los casos especiales** como lo son **los usuarios (ID)** con **privilegios superiores**, utilizados para la **administración de infraestructura** en Mutual SER EPS se ha establecido **directrices** como son:

- Solamente está autorizado el personal de técnicos del área de soporte instalación de software y cambios de configuración del sistema.
- Las configuraciones de los equipos de cómputo de usuario final son del personal de técnicos del área de soporte.
- La gestión de usuarios con acceso ***especial y/o privilegiado*** se realiza conforme al PROCEDIMIENTO DE CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN **PRO-TIC-04**, con el fin de que puedan tener el acceso necesario según sus funciones en la Organización.

Para **los casos especiales** como lo son **los usuarios (ID)** con **privilegios superiores** utilizados para la **administración de aplicaciones** en Mutual SER EPS se ha establecido **directrices** como son:

- La asignación de permisos especiales el caso de ZONA TIC debe estar aprobado por la gerencia de TI.
- La gestión de usuarios con acceso ***especial y/o privilegiado*** se realiza conforme al PROCEDIMIENTO DE CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN **PRO-TIC-04**, con el fin de que puedan tener el acceso necesario según sus funciones en la Organización.

Para **los casos especiales** como lo son **los usuarios (ID)** con **privilegios superiores** utilizados para la **administración de sistemas de información** en Mutual SER EPS se ha establecido **directrices** como son:

- La gestión de usuarios con acceso ***especial y/o privilegiado*** se realiza conforme al PROCEDIMIENTO DE CREACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE USUARIOS DEL SISTEMA DE INFORMACIÓN **PRO-TIC-04**, con el fin de que puedan tener el acceso necesario según sus funciones en la Organización.

8.3 GESTIÓN DE CONTRASEÑAS

En Mutual SER EPS, la Gerencia de Tecnología de la Información como responsable de la administración de la red, aplicaciones y/o sistemas de información, propenderá por la

seguridad de estos a través de mecanismos de control de acceso lógico, y el establecimiento de buenas prácticas de desarrollo para el control de acceso a las aplicaciones.

Entre los lineamientos mínimos en cuanto a *calidad* que tienen las contraseñas para ser usadas en los *accesos a la red* de Mutual SER EPS se tienen.

- ✓ Contraseñas de amplia longitud.
- ✓ Imposibilidad de predecir.
- ✓ Diversidad de caracteres a utilizar.
- ✓ Vigencia controlada.
- ✓ No se reutilizan contraseñas previas.
- ✓ No se utilizan datos personales.
- ✓ No se utilizan palabras contenidas en un diccionario.
- ✓ Entre otros...

Además, los lineamientos mínimos en cuanto a *calidad* que tienen las contraseñas para ser usadas en los *accesos a aplicaciones* y/o *sistemas de información* de Mutual SER EPS se tienen

- ✓ Contraseñas de amplia longitud.
- ✓ Imposibilidad de predecir.
- ✓ Diversidad de caracteres a utilizar.
- ✓ Vigencia controlada.
- ✓ No se reutilizan contraseñas previas.
- ✓ No se utilizan datos personales.
- ✓ No se utilizan palabras contenidas en un diccionario.
- ✓ Entre otros...

De igual manera se establecen parámetros mínimos, indicados a los funcionarios, contratistas y/o terceros para que una contraseña sea considerada como fuerte en Mutual SER EPS

- ✓ Deben contener caracteres alfanuméricos
- ✓ Deben contener letras en Mayúsculas y minúsculas.
- ✓ Deben cumplir con la longitud de contraseña mínima;
- ✓ No pueden contener nombres, números de teléfono y fechas de nacimiento.
- ✓ No se permite reusar claves o contraseñas para propósitos personales o diferentes al corporativo.
- ✓ Entre otros...

Para garantizar el acceso a la información en la red, en las aplicaciones y sistemas de información) en la Organización, el proceso de Gerencia de TI establece acceso por usuario (ID) con contraseña fuerte *(criterios establecidos por la organización en* **PRO-TIC-**

04 esto permite realizar de manera confiable la correspondiente autenticación para dar acceso a la información de forma segura.

8.4 PERÍMETROS DE SEGURIDAD

La seguridad perimetral informática en Mutual Ser EPS tiene igual importancia que la seguridad física de las instalaciones, claramente ambos encaminados a proteger de intrusos el perímetro definido, esta actividad es la primera línea de defensa establecida por la Organización con el fin de reducir el riesgo de pérdida de información crítica, sensible.

En Mutual Ser EPS se han determinado;

- **Perímetros físicos de seguridad** en la Organización en los que se encuentra **información crítica, sensible** y que **tienen acceso** los funcionarios, contratistas o terceros, según aplique:
  - ✓ **Datacenters***: A los Datacenter UNICAMENTE tienen acceso permanente el o los Auxiliares de TI de la Oficina (mantienen registros de ingresos a DC y las llaves).*
  - ✓ **Archivo Central** *Solo tienen acceso PERMANENTE el personal adscrito a la DIRECCION DE GESTIÓN DOCUMENTAL.*
  - ✓ **Archivos Satélites***: Solo tienen acceso PERMANENTE el personal adscrito a la DIRECCION DE GESTIÓN DOCUMENTAL.*
  - ✓ **Sedes Administrativas Regionales Principales**: *(CARTAGENA: SEDE CONCEPCION, SEDE RONDA REAL 7PISO y 2 PISO, SEDE AMPARO; CARMEN DE BOLIVAR; MAGANGUE; BARRANQUILLA; SANTAMARTA; Y MONTERIA). A estas oficinas ubicadas en las sedes administrativas pueden ingresar todos los funcionarios internos de Mutual SER EPS previa* ***identificación.***

- **Perímetros físicos de seguridad** en la Organización donde se encuentra **información crítica, sensible** y que **NO tienen acceso** los funcionarios, contratistas o terceros, según aplique:

  - ✓ **Datacenters.**
  - ✓ **Archivo Central.**
  - ✓ **Archivos Satélites.**
  - ✓ **Sedes Administrativas Regionales Principales.**

"Salvo previa autorización por el responsable de autorizar o no el ingreso en cada una de las áreas delimitadas como de acceso restringido".

- **Perímetros físicos de seguridad** en la Organización donde se **realiza almacenamiento y/o procesamiento de información** y que **tienen acceso** los funcionarios, contratistas o terceros, según aplique:

- ✓ **Datacenters***: A los Datacenter UNICAMENTE tienen acceso permanente el o los Auxiliares de TI de la Oficina (mantienen registros de ingresos a DC y las llaves).*
- ✓ **Archivo Central** *Solo tienen acceso PERMANENTE el personal adscrito a la DIRECCION DE GESTIÓN DOCUMENTAL.*
- ✓ **Archivos Satélites***: Solo tienen acceso PERMANENTE el personal adscrito a la DIRECCION DE GESTIÓN DOCUMENTAL.*
- ✓ **Sedes Administrativas Regionales Principales**: *(CARTAGENA: SEDE CONCEPCION, SEDE RONDA REAL 7PISO y 2 PISO, SEDE AMPARO; CARMEN DE BOLIVAR; MAGANGUE; BARRANQUILLA; SANTAMARTA; Y MONTERIA). A estas oficinas ubicadas en las sedes administrativas pueden ingresar todos los funcionarios internos de Mutual SER EPS previa* ***identificación.***

- **Perímetros físicos de seguridad** en la Organización donde se **realiza almacenamiento y/o procesamiento de información** y que **NO tienen acceso** los funcionarios, contratistas o terceros, según aplique:

  - ✓ **Archivo Central.**
  - ✓ **Archivos Satélites.**
  - ✓ **Sedes Administrativas Regionales Principales.**

"Salvo previa autorización por el responsable de autorizar o no el ingreso en cada una de las áreas delimitadas como de acceso restringido".

La Gerencia de Tecnología de la Información, la Directora de Gestión Documental, la Gerencia Regional cada uno de los anteriores en sus correspondientes áreas **son los responsables** de **autorizar** o **no ingresos** y a su vez acompañar el ingreso en dado caso de los terceros a las áreas delimitadas como de acceso restringido en la Organización.

8.5 ÁREAS DE CARGA

Mutual SER EPS define que los suministros y encomiendas (paquetes físicos) solo pueden ser despachados y cargados en el área de *Recepción* y *Bodega* según aplique. El personal de empresas transportadoras o proveedores no deben tener acceso a otras áreas de la edificación.

El acceso al área de despacho carga y recibo de encomiendas está restringido al personal no identificado y autorizado.

Todo el material que ingresa a las instalaciones debe ser registrado de acuerdo con el procedimiento establecido **POL-SIG-06** se inspecciona y examina para determinar posibles amenazas.

Para efectos de garantizar el cumplimiento de esta política la Organización ha determinado la realización de inspecciones aleatorias por el proceso de CONTROL DE LA GESTIÓN.

9. NO REPUDIO

Mutual Ser EPS implementa mecanismos que permiten hacer seguimiento, recolectar y disponer, mantener y validar evidencia irrefutable sobre la identidad de los destinatarios y remitentes de transferencia de información desde y hacia la organización. Estas acciones tratan los siguientes aspectos:

- Realizar seguimiento a las acciones de creación, origen, recepción, entrega de información y otros que realice cualquier usuario *(funcionarios, contratistas y/o terceros)* de Mutual Ser EPS para obtener la evidencia objetiva necesaria para el manejo de cualquier incidente que pudiese tener lugar.

    - Todas las aplicaciones de la compañía requieren de usuario y contraseña para su acceso y cualquier tipo de actividad que se realice quedará registrada con los datos del usuario en sesión.
    - La compañía cuenta con certificados SSL, Firmas digitales y Tokens de Acceso para garantizar la autenticidad de las transacciones que se realizan en los portales.

- Definir el *periodo de retención* o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros.

- Ejecuta auditorías por parte de la Gerencia de TI, como procedimiento para asegurarse que los funcionarios, contratistas y/ o terceros no nieguen haber realizado una acción.

    - La Organización cuenta con una herramienta de auditoria de bases de datos para analizar los registros de las transacciones de una manera más ágil y confiable.
    - La consola de gestión antimalware provee registro de las actividades de los usuarios que permiten auditar algún evento de seguridad que pueda ocurrir.

- Establecer herramientas de certificación del correo electrónico de manera que los servicios de intercambio electrónico de información son garantía de no repudio, como en los procesos jurídicos y mensajería.

    - El correo corporativo permite a los funcionarios configurar confirmaciones de entrega y lectura de los correos enviados.

10. PRIVACIDAD Y CONFIDENCIALIDAD

Mutual SER EPS se compromete a proteger y gestionar la seguridad de los datos personales, mantener la ***privacidad y confidencialidad*** de la información ***almacenada*** en las bases de datos de la Organización garantizando los derechos a la intimidad personal y familiar, al buen nombre de los funcionarios, asociados, afiliados, prestadores, proveedores y/o titulares de dicha información durante el tratamiento de los ***datos personales***, y en consecuencia todas las actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Así mismo, permitirá al titular de la información de los datos personales ejercer el derecho de conocer, actualizar y rectificar sus datos personales frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento este expresamente prohibido o no haya sido autorizado.

Para tal efecto se establecen y aplican ***Políticas de Tratamiento y Protección de Datos Personales*** alineadas con el marco regulatorio ***vigente***, del estado Colombiano.

10.1 ÁMBITO DE APLICACIÓN

La presente política es aplicada de ***manera inmediata*** en la ***recolección***, ***manejo, tratamiento, atención de consultas, reclamos***, todos estos relacionados con ***los datos personales*** registrados de; funcionarios, asociados, afiliados, prestadores, proveedores y/o titulares de dicha información en cualquiera de las bases de datos de la Organización, los cuales se emplearán exclusivamente para los fines que fueron autorizados concernientes con nuestro objeto social.

10.2 EXCEPCIÓN AL ÁMBITO DE APLICACIÓN DE LAS POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

La política será aplicable a los datos personales registrados en cualquier base de datos de la Organización cuyo titular sea una persona natural, salvo por las **excepciones** previstas en la ley *(como, por ejemplo: Procesos judiciales, derecho de infancia y adolescencia, salud pública, seguridad nacional, administración de justicia (delitos y faltas carcelarias)*, información solicitada por entes institucionales y de control. El tratamiento de la información y datos personales sensibles sólo podrá realizarse con el consentimiento previo, expreso e informado de sus titulares, manifestado por escrito, electrónica, oral o mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

10.3 PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

Mutual SER EPS en procura de garantizar ***la protección de datos personales*** aplicará los siguientes ***principios*** de manera armónica e integral, éstos constituyen las reglas a seguir en la recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario:

- **Principio de legalidad:** El tratamiento que dará a los *datos personales* en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario, *se regirá por la legislación vigente* referente a este tema.

- **Principio de finalidad:** El tratamiento que dará a los *datos personales* en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario que realice la Organización, obedecerán a una finalidad legítima en consonancia con la Constitución Política de Colombia la cual será *informada* al respectivo titular de los datos personales.

- **Principio de libertad:** El tratamiento que dará a los *datos personales* en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario que realice la organización sólo puede ejercerse con *el consentimiento previo expreso e informado* del *Titular*, los *datos personales* no podrán ser obtenidos o divulgados sin *previa autorización* en ausencia de mandato legal o judicial que releve el consentimiento.

- **Principio de veracidad o calidad:** La información sujeta a tratamiento *(datos personales en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario)* en la Organización, debe ser; veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Principio de transparencia:** En el tratamiento de *datos personales*, la Organización *garantizará* al titular su derecho de *obtener* en cualquier momento y sin restricciones, *información* acerca de la existencia de cualquier tipo de *información o dato* personal que sea de su interés o titularidad.

- **Principio de acceso y circulación restringida:** El tratamiento de *datos personales en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación y supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario* que realice la organización,

sólo podrá hacerse por *personas autorizadas* por el *titular* y/o por las *personas* previstas en la Ley, en la normatividad vigente y/o la Constitución. Los *datos personales*, salvo la información pública, *no podrán* estar disponibles en internet u otros medios de divulgación o comunicación masiva, *salvo* que el acceso sea técnicamente controlable *para brindar* un conocimiento restringido *sólo a los titulares* o *terceros autorizados* conforme a la Ley.

- **Principio de seguridad**: La *información* sujeta a tratamiento *(datos personales en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario)* por la Organización, se *manejará* con las medidas técnicas, humanas y administrativas que sean necesarias para *garantizar* la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **Principio de confidencialidad:** Todos *las personas* que en la Organización que participen en el *tratamiento de datos* personales en cuanto a su recolección, almacenamiento, manipulación, uso, análisis, circulación, supresión de información, intercambio, transferencia y transmisión o cualquier otro tratamiento que llegue a ser necesario están obligados a *garantizar* la *reserva* de la *información* por lo que se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros la información que llegaren a conocer en la ejecución y ejercicio de sus funciones. Esta obligación persiste y se mantendrá inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento de los datos, *pudiendo sólo* realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas expresamente por la Ley de Protección de Datos.

10.4 DERECHOS DE LOS TITULARES

Conforme a lo contemplado por la normatividad vigente aplicable en materia de protección de datos, Mutual SER EPS informa todas las partes interesadas que los siguientes son los *derechos* de los *titulares* de los *datos personales*:

- *Conocer, actualizar y rectificar* sus datos personales frente a la Organización en su condición de responsable o encargado del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- *Solicitar* prueba de la autorización otorgada a la Organización para el tratamiento de datos personales, mediante cualquier medio válido, salvo en los casos en que no es necesaria la autorización.

- *Ser informado* por la Organización, previa solicitud, respecto del uso que les dará a sus datos personales.

- *Revocar* la autorización y/o solicitar la *supresión de dato(s)* personales de las bases de datos o archivos cuando en el tratamiento *el titular* lo considere y/o indique la existencia de un tratamiento indebido o que vulnere su privacidad y no se respeten los principios, derechos y garantías constitucionales y legales.

- *Presentar* quejas por infracciones a lo dispuesto en la Ley de Protección de Datos Personales y las demás normas que la modifiquen, adicionen o complementen, ante la *Superintendencia de Industria y Comercio* entidad de vigilancia encargada de la protección de los datos personales.

10.5 AUTORIZACIÓN DEL TITULAR

Mutual SER EPS a través del uso de diferentes medios *(documento físico, electrónico, sitios web, internet, oral y expresa*, *mensaje de datos, mecanismo técnicos o tecnológicos idóneo y/o en cualquier otro formato)* que pueden ser objeto de consulta y verificación posterior le permiten obtener **autorización del titular** "*consentimiento mediante conductas inequívocas a través de las cuales le permite concluir que de no haberse surtido la misma por parte del titular o la persona legitimada para ello los datos no se hubieran almacenado o capturado en las bases de datos",* para el tratamiento de sus datos personales. Esta autorización es solicitada por la Organización de manera expresa e informada previa al tratamiento de los datos personales.

No es *requerida* autorización por parte del titular en los *casos* de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

- Datos de naturaleza pública.

- Casos de urgencia médica o sanitaria.

- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

- Datos relacionados con el registro civil de las personas.

10.6 DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO

Mutual SER EPS como responsable del tratamiento de los *datos personales*, tiene los siguientes *deberes* sin perjuicio de otros previstos en las disposiciones que regulen o lleguen a regular esta materia:

- *Garantizar* al titular, en todo tiempo el pleno y efectivo ejercicio del derecho fundamental hábeas data.

- *Solicitar y conservar,* según las disposiciones de ley, *copia* de la respectiva *autorización* otorgada por el *titular* para el tratamiento de los datos personales.
- *Informar* debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
- *Mantener* segura la información para impedir adulteración, pérdida, consulta, acceso no autorizado o fraudulento, garantizando su integralidad.
- *Garantizar* que la información suministrada sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- *Mantener* actualizada la información.
- *Rectificar* la información cuando sea incorrecta y comunicar lo pertinente.
- *Respetar* las condiciones de seguridad y privacidad de la información del titular.
- *Tramitar* oportunamente las consultas o reclamos formulados por los titulares.
- *Adoptar* un manual de políticas y procedimientos para garantizar la adecuada protección de datos personales.
- *Identificar* cuando determinada información se encuentra en discusión por parte del titular.
- *Informar* a solicitud del titular sobre el uso dado a sus datos.
- *Informar* a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- *Cumplir* las instrucciones que imparta la superintendencia de industria y comercio y demás Entes de control.

10.7 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Mutual SER EPS protege la información clasificada mediante mecanismos de cifrado al momento de ser transferida o transmitidas descritos en el documento **POL-TIC-01**. Las claves de acceso a sistemas de información y sistemas operacionales se almacenan en forma cifrada para preservar su confidencialidad.

La confidencialidad de la información que circula o se genera a través de los diferentes sistemas de información en Mutual SER EPS es asegurada implementado distintos mecanismos relacionados a continuación, que ayudan a que su información este cifrada para evitar que personas no autorizadas pueda acceder a esta. en la actualidad los siguientes son los controles (mecanismos) implementados en la Organización:

- Cifrado de discos duros en portátiles.
- Aplicaciones configuradas con certificados SSL que cifran la comunicación para evitar que la información viaje en texto claro.
- Conexión remota cifrada a través de VPN.
- Información almacenada en repositorios de la nube cifrada.
- Comunicaciones hacia Datacenter en la nube de manera cifrada.
- El correo electrónico con característica de cifrado en el mensaje que se desee.

De igual manera, para la **autenticidad** de la información que **circula** o se **genera** a través de los **diferentes** sistemas de información en Mutual SER EPS se han establecido distintos métodos de acuerdo el caso:

- **Autenticidad de sitios WEB:** Nuestros sitios web cuentan con **certificados de seguridad SSL** emitidos específicamente para Mutual SER EPS lo cual garantiza a nuestros usuarios que no están en un sitio falso.
- **Tokens:** para las transacciones financieras y accesos que requieren altos niveles de seguridad se usan tokens de seguridad los cuales son dispositivos físicos que permiten autenticar en un sistema solo a la persona que lo posee (además del usuario y contraseña).
- **Autenticación Multifactor:** Algunas de nuestras aplicaciones cuentan con un requisito adicional de autenticación como puede ser un pin aleatorio y de rotación constante que solo puede tener el usuario asignado a esa cuenta, y este puede llegar por SMS o desde una APP móvil.
- **Biometría:** Sistema biométrico implementado de huella dactilar para el registro de asistencia, acceso a Datacenters y archivos de la Organización, éste garantiza que la persona (funcionario, contratista o tercero) que se registra es la autorizada para ingresar.

Todo funcionario, contratista y/o tercero vinculado a la Organización, deberá firmar el documento **ACUERDO DE CONFIDENCIALIDAD MUTUAL SER EPSS,** compromiso que trata de no divulgar de ninguna manera la información interna y externa que conozca de la Organización, así como la relacionada con las funciones que desempeña en mutual SER EPS, garantizando que la información conocida por éstos bajo ninguna circunstancia será revelada ni total ni parcialmente por ningún medio electrónico, verbal, escrito u otro, sin contar con previa autorización de Mutual SER EPS.

El acuerdo rige a partir de la vinculación del funcionario a la organización y/o contratación del servicio y su vigencia se encuentra establecida durante el término que dure la relación laboral o contractual y hasta por un término adicional de no menos de 5 años después de la terminación de la misma.

11. INTEGRIDAD

Todos los usuarios *(funcionarios, contratistas y/o terceros)* que hacen parte o prestan sus servicios a Mutual SER EPS se deben comprometer en proporcionar un manejo integro e integral de la información conocida o administrada por los mismos tanto interna como externa.

Es así como la Organización propenderá porque toda la información verbal, física o electrónica, sea entregada o transmitida integralmente, sin modificaciones ni alteraciones, al destinatario correspondiente únicamente por los medios correspondientes autorizados, exceptuando los casos en que lo determinen las personas autorizadas y/o responsables de dicha información.

Mutual SER EPS tiene establecido que, en el caso de la **vinculación contractual** con los usuarios *(funcionarios, contratista y/o terceros)* el compromiso de administración y manejo integro e integral de la información interna y externa *(ej.: uso de información que se suministra o genera por la ejecución de convenios, acuerdos, contratos o similares entre otros.)* hará parte de las cláusulas de los respectivos contratos, bajo la denominación de **Cláusula de integridad de la información.**

El tiempo de vigencia de la **Cláusula de integridad de la información**¸ estará acorde al tipo de vinculación del personal *(funcionarios, contratistas y/o terceros)* al cual aplica el cumplimiento.

12. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

Mutual SER EPS con el fin de *asegurar*, *recuperar* o *restablecer* la disponibilidad de los procesos que soportan el *Sistema de Gestión de Seguridad de la Información* como de *procesos Misionales* de la Organización en caso de la ocurrencia de un *incidente de seguridad de la información* que pueda alterar el normal funcionamiento de estos, cuenta con un **plan de continuidad del negocio** que le permite *minimizar el impacto y recuperación* por perdida de activos de información hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación, es así que, puede seguir brindando los servicios al cliente interno como externo y demás partes interesadas.

Los siguientes aspectos han sido definidos por la Organización con la participación de los líderes de cada proceso cliente.

- Niveles de disponibilidad:

Mutual SER EPS se asegura por el *cumplimiento* de los niveles de *Disponibilidad de Servicios e Información* acordados con *clientes, proveedores y/o terceros* en función de las *necesidades y /o requisitos* establecidos por la Organización, así como los *acuerdos* de nivel de *servicios ofrecidos* y *evaluaciones de riesgos*.

- Planes de recuperación:

Mutual SER EPS cuenta con *planes de recuperación* que incluyen las necesidades de disponibilidad de la Organización, asegurando la continuidad de las operaciones tecnológicas de sus procesos críticos, siempre teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en cada una de las políticas de seguridad de la información.

- Interrupciones:

Mutual SER EPS esta alerta de la *gestión de interrupciones de mantenimiento* de los servicios que puedan afectar la disponibilidad del mismo.

- Acuerdos de nivel de servicio:

Mutual SER EPS tiene en cuenta los *acuerdos de niveles de servicios (ANS)* en las *interrupciones del servicio.*

- Segregación de ambientes:

Mutual SER EPS con el fin de minimizar el impacto de la *indisponibilidad del servicio* durante las fases de desarrollo, pruebas y producción, establece la *segregación de ambientes* para minimizar los *riesgos* de puesta en funcionamiento de cambios y nuevos desarrollos.

- Gestión de cambios:

Mutual SER EPS incluye la *gestión de cambios* en los pasos de producción con el fin de que éstos afecten **mínimamente** la *disponibilidad de servicios e información* en la organización, realizándolos bajo condiciones controladas.

13. REGISTRO Y AUDITORÍA

Mutual SER EPS en pro de asegurar el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información establece que:

Es de ***responsabilidad*** de la *Dirección de Control Interno y Calidad* asegurarse de la planificación y realización de las ***auditorías periódicas*** de acuerdo con el programa de auditoría de la Organización a ***los sistemas*** de información y a las ***actividades relacionadas*** a la ***gestión de activos de información***, como además de, la revisión, aprobación, distribución e ***informe*** de los ***resultados*** de la auditoría a las partes interesadas.

El procedimiento de auditoría en *Mutual SER EPS* además de aplicarse a *los procesos, procedimientos e información documentada en general, así como al cumplimiento de*

requisitos legales, normativos, reglamentarios internos y externos aplicables del sistema de gestión de la Organización éste también incluye los ***registros de las copias de seguridad almacenados*** en las bases de datos correspondientes y el ***correcto funcionamiento de estas***, de igual manera, se tiene en cuenta toda la ***información*** referente a ***registros y monitoreos*** de eventos de seguridad ocurridos en la Organización.

La Organización asegura a través de la Dirección de Control Interno y Calidad la realización de auditorías planificadas con frecuencias, objetivos y alcances definidos, criterios *(normatividad y requerimientos legales.)* de auditoria específicos con la naturaleza de Mutual SER EPS establecidos en el programa de auditorías.

El proceso sistémico de auditoria en Mutual SER EPS con objetivos pertinentes y suficientes proporcionará resultados confiables ***garantizando***, la ***evaluación*** de los controles establecidos en los procesos para el cumplimiento de los requisitos exigidos por el Modelo de Seguridad y Privacidad de la Información (MSPI), la ***eficiencia de los sistemas*** adquiridos y/o desarrollados, el ***cumplimiento*** de las ***políticas de seguridad*** de la información como de los ***procedimientos*** implementados y establecidos en la Organización. Además de ***recomendar*** las deficiencias detectadas.

Mutual SER EPS con el fin de realizar ***revisión periódica*** de los niveles de riesgos a los cuales está expuesta ha establecido la realización de auditorías al menos una vez en el año, éstas se encuentran alineadas con los objetivos estratégicos y los de gestión de procesos en la Organización.

Toda la información referente a las actividades y acciones desarrolladas en el procedimiento de auditorías en Mutual SER EPS, se encuentran establecidas en el PROCEDIMIENTO PARA AUDITORIAS INTERNAS. **PRO-SIG-02.**

14. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

En Mutual SER EPS la política de gestión de incidentes de seguridad de la información se encuentra ***dirigida*** a todos los ***usuarios*** *(funcionarios, contratistas o terceros)* que tienen acceso autorizado a cualquiera de los diferentes sistemas de información de la Organización.

Ésta procura 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 evitando en lo posible la propagación de la falla.

Al igual que con las demás políticas de seguridad de la información, la alta dirección de la Organización con su ***aprobación*** demuestra su compromiso para con la gestión de incidentes de seguridad de la información.

La política de la organización contempla: Que se debe ***reportar*** todos aquellos presuntos incidentes de seguridad identificados por los usuarios apoyándose en la información que

coadyuva a determinar el suceso como posible incidente, de igual manera, se debe ***reportar*** al ***centro de servicios*** MUTUAL SER indicando la categoría de clasificación de los incidentes conforme lo establecidas en el procedimiento. Finalmente, como medios a utilizar para hacer el reporte establece las PQR y correo electrónico.

Para gestionar los eventos *(presuntos incidentes de seguridad)* la Organización tiene establecido tres niveles de selección de ***responsable*** como son; el nivel central, nivel regional y nivel local. Esto con el fin de designar de manera adecuada a los profesionales que atenderán (*acorde con sus competencias)* cada una de las diferentes categorías determinadas.

Todas estas ***actividades*** del proceso de gestión de incidentes en Mutual SER EPS, son explicadas de manera general desde el reporte hasta su resolución y se encuentran establecidas en el procedimiento GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN **PRO-TIC-19,** en el cual se establece el esquema de gestión a seguir *(Ejecución)* y procedimientos para el reporte de incidentes de seguridad. De igual manera, el procedimiento describe en la etapa de ejecución el ***equipo de funcionarios de la organización que manejará los incidentes*** en la organización quienes tienen definida una estructura general para la gestión de incidentes y vulnerabilidades de seguridad.

Esta política de la Organización contempla **aspectos legales** a tener en cuenta para así dar cumplimiento a la gestión de incidentes de seguridad de la información tales como; ley 1273 de 5 enero del 2009 por medio de la cual se modifica el Código Penal. Título VII Bis "De la protección de la información y de los datos". Artículos 269A a 269J, Ley 1581 17-oct-2012 Por la cual se dictan disposiciones generales para la protección de datos personales, Ley 1712 06-mar-2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, Decreto 1377 27-jun-2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Decreto 886 13-may-2014 Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos, Decreto 2573 12-dic-2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones, Decreto 103 20-ene-2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones, Decreto 1078 26-may-2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018, Decreto 1008 14-jun-2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital, estos requisitos legales se han determinado y establecido en el documento **Normograma** de Mutual SER EPS.

15. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Las estrategias para mejorar la cultura organizacional sobre la Seguridad de la Información en Mutual SER EPS se desarrollan a través de; Capacitaciones, en los procesos de inducción de usuarios nuevos, mediante emisión de boletines por Intranet, de igual manera con el uso de herramientas colaborativas en línea y conocimiento transferido por los Auxiliares de Servicios TI en sus labores de soporte técnico en la Organización, todo esto con la finalidad de disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

La alta dirección de Mutual SER EPS representada en la figura del Gerente General se ***compromete*** con la asignación y destinación de los recursos suficientes que permitan desarrollar los programas de formación y/o capacitación de manera eficaz.

En temas relacionados con la ***seguridad de la información*** en Mutual SER EPS se tiene establecido que **todo** el **personal de TI** debe ser ***entrenado*** en esta actividad.

- Analista de TI.
- Analista de Mesa de Ayuda.
- Auxiliar de Mesa de Ayuda.
- Analista de TI Nivel 1(Base de Datos, Servidores, Telecomunicaciones, Aplicaciones, Negocios, Datos, Soporte, QA, Desarrollo. Devops).
- Analista de TI Nivel 2 (Soporte Técnico, Aplicaciones, Seguridad Informática, DBA, Negocios, Servidores, Telecomunicaciones, Datos, Soporte, Agile Coach, Desarrollo).
- Auxiliar de Servicios TI.
- Coordinación de Desarrollo y Evolución.
- Coordinación de Análisis de Negocio
- Coordinación de infraestructura y operaciones.
- Dirección de Datos e Información.
- Dirección de Arquitectura Empresarial.
- Project Manager.
- Gerencia de Tecnología de la Información.
- Comité de seguridad de la información.
  - Gerencia General, quien lo presidirá.
  - Coordinación de Proyectos Gerenciales.
  - Gerencia de Tecnología de la Información.
  - Dirección Dpto. de Gestión Documental.
  - Dirección Dpto. de Gestión Humana.
  - Dirección Jurídica.
  - Gestión Calidad – Contratación.

De igual manera, se tiene establecido que ***todos*** *los* ***colaboradores/funcionarios*** *de la Organización sin excepción alguna deben* ser **sensibilizados** en temas relacionados con la ***seguridad de la información***.

Para identificar las necesidades en fortalecimiento y apropiación de la Seguridad de la Información en el personal de Mutual SER, se establece un conjunto de roles, en los cuales se concentrará el apoyo necesario para desarrollar 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 las causas raíz que se identifiquen, 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 (firewall, IDS/IPS, sistemas SIEM) o intrusiones en páginas web.
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.

Todos los Usuarios en Mutual SER EPS *(que deban ser entrenados y/o que deban ser sensibilizados)*, tienen la **obligación** de asistir a los **eventos** o **cursos** de capacitación en temas relacionados con la seguridad de la información.

Mutual SER EPS tiene establecido como de responsabilidad a la **Gerencia Tecnología de Información** realizar **revisiones** con periodicidad semestral (cada seis meses) a los **resultados** de las capacitaciones ***(relacionadas con la seguridad de la información)*** para el mejoramiento de los procesos en Organización.

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** los programas de (Capacitación y Sensibilización en temas relacionados con la ***Seguridad de la Información***) conformado por:

- **Gerente Tecnología de Información**: Responsable de Identificar y hacer seguimiento de la eficacia de las Capacitaciones y Sensibilizaciones en temas relacionados con la **Seguridad de la Información** para el mejoramiento de los procesos en la Organización.

- **Coordinación de Gestión del Conocimiento**: Responsable de planificar, implementar y verificar la realización de las Capacitaciones y Sensibilizaciones en temas relacionados con la **Seguridad de la Información** en la Organización.

- **Gerencia General**: Responsable de gestionar los recursos (económicos, infraestructura, personas tecnología, etc.) necesarios para la realización de las Capacitaciones y Sensibilizaciones en temas relacionados con la **Seguridad de la Información** para la Organización.

En Mutual SER EPS los **programas** de ***capacitación y sensibilización*** *en temas relacionados con la* ***seguridad de la información*** son **comunicados** por:

- **Coordinación de Gestión del Conocimiento**: A todos los procesos de la organización mediante el documento denominado **Plan de Formación**.

La documentación sobre **planes de estudio** y **desarrollo** de los programas en temas relacionados con la ***seguridad de la información*** en Mutual SER EPS son gestionados y administrados por la **Coordinación de Gestión del Conocimiento**, enmarcados en la Política de Gestión del Conocimiento **POL-SIG-07**, descritos e implementados conforme al procedimiento de identificación, diseño y construcción de soluciones de gestión del conocimiento **PRO-SIG-12**...

El personal capacitado en temas relacionados con l**a seguridad de la información** tiene el **Compromiso** para con Mutual SER EPS de:

- Mejorar el conocimiento sobre seguridad de la información.
- Aplicar el conocimiento sobre seguridad de la información adquirido.
- Incrementar la eficiencia de las tareas a realizar relacionadas con seguridad de la información.
- Aprovechar de manera eficiente las herramientas de seguridad.
- Aprovechar de manera eficiente los controles de seguridad.
- Ayudar a crear y mantener una cultura sólida de seguridad de la información.
- Mejorar la eficiencia del sistema de gestión de seguridad de la información
- Prevención de sanciones, infracciones, o faltas graves de seguridad de la información.

- Reducir los riesgos de error humano relacionados con la seguridad de la información.
- Otras...

Demás **compromiso**s se encuentran consignadas el procedimiento de identificación, diseño y construcción de soluciones de gestión del conocimiento **PRO-SIG-12**.

El personal capacitado en temas relacionados con l**a seguridad de la información** tiene la **Obligación** para con Mutual SER EPS de:

- Utilizar apropiadamente las herramientas de seguridad de la información de la Organización.
- Utilizar los conocimientos adquiridos en seguridad de la información para el beneficio de la Organización.
- Cumplir con las expectativas depositadas en él por la Organización en materia de seguridad de la información.
- Respaldar la política de seguridad de la organización en el desarrollo de sus actividades.
- Actuar coherentemente en el desarrollo de sus actividades en procura de la seguridad de la información.
- Proceder conforme lo establecido por el sistema de seguridad de la información de la Organización.
- Otras...

Demás obligaciones se encuentran consignadas el procedimiento de identificación, diseño y construcción de soluciones de gestión del conocimiento **PRO-SIG-12**.

15.1 POLÍTICA DE ESCRITORIO LIMPIO

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.
- 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.
- Los equipos de cómputo no deben ser dejados desatendidos en lugares con acceso al público.

15.2 POLÍTICA DE USO ACEPTABLE.

Mutual SER EPS, ha establecido **directrices comportamentales** enfocadas al **uso aceptable** *(relacionadas directamente con el debido comportamiento de los **usuarios (funcionarios, Contratistas y/o terceros)**)* para con los activos de información equipos, software instalado, hardware, periféricos, aplicaciones y sistemas de información, todas adecuadas para proteger los recursos corporativos y la información confidencial de la organización.

En relación con el manejo de la información:

- El usuario que realice actividades para la Organización tiene acceso únicamente a la información necesaria para el desempeño de las actividades haciendo un uso profesional y ético de ésta.
- Los usuarios que requieran acceso a información deben cumplir con los requisitos legales, normativos reglamentarios procedimentales o de cualquier otra índole definida por la Organización.
- Los usuarios de 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 que requieran acceso a información no contemplada como necesaria para el desempeño de sus actividades en la organización, debe ser autorizada formalmente.
- Los usuarios deben considerar el nivel de clasificación de la información, a la cual tienen acceso para el desempeño de las actividades del cargo, y el uso responsable que deben hacer de ésta.
- Todos los usuarios que prestan sus servicios a la Organización se deben comprometer a realizar sus mejores esfuerzos para aplicar todos los controles de seguridad de la información definidos en el sistema de gestión de seguridad de la información de Mutual SER EPS para garantizar la preservación de la Confidencialidad, Integridad y Disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades.
- Los usuarios que prestan sus servicios a la Organización deben coadyuvar en identificar y tratar los riesgos que puedan afectar los activos de información.

- Los usuarios que prestan sus servicios a la Organización se comprometen a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está comprometida la Mutual SER EPS para la protección de la información a su cargo.
- Los usuarios que prestan sus servicios a Mutual SER EPS en aras de la protección de la información a su cargo, se comprometen a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está comprometida la Organización.
- Los usuarios deben hacerse responsables del usuario y contraseña asignados para el acceso a la información.
- Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica deben acogerse a lineamientos de contraseñas de la Organización

De igual manera, se establecen las siguientes restricciones.

- Utilizar la información de la Organización para fines personales.
- No se permite el acceso a información de la Organización sin justificación objetiva.
- Modificación de los controles de seguridad que protejan la información de la Organización.
- Cualquier acción sobre la información de la Organización que se considere como ilegal.
- Modificación de la información de la Organización sin contar con la autorización formal para dichas modificaciones
- Divulgación no autorizada de información de la Organización.
- Utilizar la información de la Organización para fines diferentes a los requeridos para el cumplimiento de las funciones asignadas.
- Eliminación de los controles de seguridad que protejan la información de la Organización.
- Cualquier acción sobre la información de la Organización, no autorizada por las leyes, regulaciones, normas o procedimientos a los que está comprometida la Organización.

En relación con el empleo de los activos asociados con información

- El acceso al mismo implica la aceptación al monitoreo de los recursos e información contenida en el mismo.
- El uso del equipo está reservado únicamente para uso institucional.
- El usuario responsable del equipo tiene como deber el cumplimiento de las políticas de Seguridad de la Información.
- El usuario es responsable del equipo asignado y tiene como deber, el cumplimiento de directrices de buen uso de los recursos tecnológicos de la Organización.
- Los usuarios de los recursos tecnológicos la Organización realizarán un uso adecuado y responsable salvaguardando la información a la cual les es permitido el acceso.
- 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.

En relación con el empleo del servicio de Internet:

- Los usuarios deben utilizar únicamente el servicio de internet para las funciones propias del cargo asignado en la Organización.
- Los usuarios se deben comprometerse con el buen uso de los servicios de internet, el acceso a este dependerá del rol que desempeñan en la Organización.
- Los usuarios son responsables del contenido de las comunicaciones que emita desde la red de la Organización.
- Los usuarios son responsables del contenido de cualquier información que emita desde la red de la Organización.
- Los usuarios son responsables de cualquier información que descargue desde internet empleando la red de la Organización.

De igual manera, se establecen las siguientes restricciones.

- No está autorizado a ningún usuario el acceso a sitios de “hacking” o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de la Organización.
- No está autorizado el acceso a sitios Web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.
- No está autorizado el acceso a sitios de música, juegos, vídeos, u otros sitios de entretenimientos on-line.
- No está autorizado el acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía, salvo, en los casos que estén expresa y formalmente autorizados con apego a funciones explícitamente definidas para el funcionario.
- Está prohibido el uso del servicio de acceso a Internet de la Organización para realizar o propiciar propaganda política.
- No está autorizado el acceso a sitios Web relacionados con actividades de juego, apuestas, o actividades ilegales en general.
- Esta estrictamente prohibido el uso, no autorizado de una cuenta de acceso a Internet diferente a la formalmente asignada al usuario.
- Está prohibido el uso del servicio de acceso a Internet de la Organización para realizar o propiciar propaganda comercial de productos o servicios de propiedad de los usuarios.
- Todas las conductas definidas como delito informático en la ley 1273 de 2009 están prohibidas y no se debe hacer uso del servicio de acceso a Internet de la Organización para fines no lícitos.
- No es aceptable el uso del servicio de acceso a Internet para actividades comerciales.

En relación con el empleo del servicio de correo electrónico:

- Los usuarios harán buen uso del correo electrónico asignado que primordialmente está destinado para desarrollar sus funciones en la organización.
- Son de su entera responsabilidad (del usuario) los usos diferentes que dé al correo electrónico a los necesarios para el cumplir de las funciones encargadas.
- El uso con fines personales del correo institucional es responsabilidad del usuario.
- Serán de su entera responsabilidad (del usuario) los incidentes de seguridad de la información en la Organización generados por el uso de servicios de correo electrónico no autorizados.
- La contraseña como el usuario de acceso al servicio de correo electrónico de la Organización no debe exhibirse en público ni ser divulgada a ninguna persona.
- Los correos electrónicos deben contener una nota de confidencialidad ubicada al final del texto, después de la firma de este, este mecanismo es una medida preventiva de divulgación no autorizada de contenidos de correo electrónico así:

NOTA DE CONFIDENCIALIDAD: *El contenido de este mensaje (incluidos sus anexos) puede contener información privilegiada y/o confidencial. En cumplimiento a la ley estatutaria 1581 de 2012, si usted no es el destinatario real del mismo, por favor informe de ello a quien lo envía y destruya esta comunicación de todos los medios de almacenamiento donde se encuentre el mismo, y destruya todas las copias físicas de manera inmediata.*
Está prohibida la retención, grabación, utilización o divulgación de este mensaje o sus anexos, por cualquiera que no sea su destinatario original con cualquier propósito. Este mensaje ha sido verificado con software antivirus; sin embargo, eso no garantiza que el mismo se encuentre libre de todo virus o código malicioso; en consecuencia, de esto, el remitente de este no se hace responsable por la presencia en él o en sus anexos de algún virus que pueda generar daños en los equipos o programas del destinatario.

- La responsabilidad del contenido de los mensajes de correo electrónico será del usuario remitente, el receptor no deberá alterar los mensajes sin la autorización del emisor.
- Antes de enviar un correo el usuario deberá verificar que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el asunto.
- El mantenimiento del buzón de correo es de responsabilidad del usuario.
- Cuando un funcionario requiere ausentarse de la Organización por períodos de varios días se recomienda programar el correo electrónico para que automáticamente responda a los remitentes, *indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia*.

De igual manera, se establecen las siguientes restricciones.

- 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.

- Uso del correo electrónico para comunicaciones personales o institucionales como; difusión avisos clasificados o publicidad comercial no deseada o beneficio personal.
- Está prohibida la Interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, por lo que está prohibida la interceptación de los mensajes de correo electrónico sin autorización legal, como lo *establece la ley 1273 de 2009 sobre delitos informáticos*.
- Está prohibido el acceso abusivo a un sistema informático, por lo tanto, está prohibido acceder al buzón de correo electrónico de otros funcionarios sin la debida autorización, como lo *establece la ley 1273 de 2009 sobre delitos informáticos*.
- Crear mensajes suplantando la identidad de un usuario.
- Enviar mensajes suplantando la identidad de un usuario.
- Alterar mensajes suplantando la identidad de un usuario.
- Borrar mensajes suplantando la identidad de un usuario.

15.3 ÉTICA EMPRESARIAL.

En Mutual SER EPS la filosofía de trabajo tiene como propósito impulsar, crear y mantener una cultura ***ética*** y de principios, con ***buenas prácticas de gobierno***. Es así como se insta a cada uno de los colaboradores *(funcionarios, contratistas o terceros)* y demás partes interesadas a apropiarse de estas conductas y estar vigilantes para que cada uno asuma el compromiso que corresponde, así:

Política para la Gestión Ética y de Conducta frente a los Usuarios.

La atención centrada en el usuario es una estrategia para la gestión de calidad de la empresa por lo cual los trabajadores adoptan y aceptan los siguientes postulados:

- Los usuarios se atienden en forma cordial, amigable y con respeto, sin distingo por su condición social, raza, religión, género o filiación política.
- Se garantiza la atención en la red de prestadores con criterios de calidad tales como oportunidad, accesibilidad, seguridad, pertinencia, continuidad e integralidad.
- Se cuenta con recurso humano competente y capacitado para informar, indicar y acompañar al usuario con el fin de asegurar la atención efectiva.
- Se facilita el proceso de recepción, trámite y respuestas a las inquietudes, quejas, reclamos, peticiones y sugerencias de los usuarios.
- Se propicia entre los afiliados – asociados y la organización, la participación y libre expresión de sus ideas y conceptos, enmarcados en el respeto y las buenas costumbres.
- Se propende por solucionar los problemas de los afiliados en el momento que lo necesite y en la justa proporción a sus necesidades.
- Se realiza atención personalizada a los usuarios, garantizando espacios para la privacidad.
- Se actúa en representación de los usuarios siendo compradores inteligentes de servicios.

- La organización ejecuta los recursos del régimen subsidiado y contributivo de manera responsable y eficiente, cuidando que siempre sea el usuario y su familia los beneficiarios directos.

Política para la Gestión Ética y de Conducta frente a los funcionarios de la Organización.

- Los regalos u obsequios que espontáneamente las empresas envíen a funcionarios se entienden como institucionales y se rifan al final del año entre todos los colaboradores.
- Se propician espacios para aportar, debatir o discutir ideas, en forma libre y espontánea, sin distingo de condición social, raza, religión, género o filiación política.
- Los funcionarios informan con oportunidad cuando hay conflicto de interés que pueda generar un beneficio personal o familiar y pueda verse afectada la organización.
- Los funcionarios no pueden hacer parte de grupos al margen de la Ley, ni cometer actos fraudulentos en contra de la organización y las normas colombianas.
- No está permitido el acceso a páginas de Internet relacionadas con contendidos terroristas, grupos al margen de la Ley o pornográficos.
- Se aplican procesos de selección, vinculación, reclutamiento y entrenamiento del recurso humano en armonía con las políticas de la organización.
- Se considera práctica contra las buenas costumbres, el respeto y las normas vigentes aprovecharse de la jerarquía del cargo para realizar acoso sexual o laboral.
- Se propende por la ubicación de los funcionarios en los cargos de acuerdo con el perfil de competencias, realizando promoción interna cuando se necesita proveer vacantes.
- Se promueve y facilita el desarrollo de las competencias de los funcionarios y el mejoramiento de sus condiciones personales y familiares.
- Se promueve un clima organizacional, acorde con la cultura empresarial, en donde el funcionario se sienta a gusto con su equipo de trabajo y con la organización.

Política para la Gestión Ética y de Conducta frente al Manejo de la Información y el Uso de los Bienes de la Organización.

- La organización está dispuesta para suministrar la información pertinente que requieran las entidades de dirección, inspección, control y vigilancia, directivos, proveedores, afiliados, asociados y comunidad en general.
- La información o bienes que se genera como producto del ejercicio de las funciones de los colaboradores son de propiedad intelectual de la organización.
- Se respetan los acuerdos de confidencialidad suscritos con clientes externos para el uso de la información que se suministra o genera por la ejecución de convenios, acuerdos, contratos o similares, no aprovechándola en beneficio propio, ni utilizándola con terceros para fines diferentes a los inicialmente convenidos.

- Cada funcionario de la organización responderá por la custodia y buen uso de los bienes suministrados por la organización para el ejercicio de sus responsabilidades, salvo el deterioro por el uso.
- La información, bienes y servicios que suministra la organización no deben utilizarse para beneficio personal o familiar.
- La organización utilizará la información consignada en las Historias Clínicas única y exclusivamente para los fines relacionados con la atención al usuario, manteniendo en todo momento la reserva legal y de confidencialidad.
- Solo se suministrará información sobre la condición de salud de un afiliado cuando así lo requieran las autoridades judiciales y de Salud en los casos previstos en la normatividad vigente, así como las demás personas determinadas en la Ley.
- No está permitido utilizar los equipos de cómputo para realizar trabajos personales o familiares, así como grabar información relacionada con grupos al margen de la Ley, pornografía, pedofilia, etc.

Política para la Gestión Ética y de Conducta frente a Actores Externos, la Sociedad, el Estado, la Competencia y el Medio Ambiente.

- Se actúa con honestidad y transparencia tanto al interior como al exterior de la organización, velando por el buen nombre de la organización.
- La organización hace valer la palabra empeñada en el cumplimiento de los compromisos que se adquieren con clientes externos.
- No se exige, ni se acepta, ni se suministra dadivas u obsequios a proveedores en contraprestación de las funciones propias de la organización.
- En las relaciones contractuales y comerciales se propende por la aplicación de la estrategia del GANA-GANA.
- Se promueve y respeta la sana competencia entre las EPS, evitando prácticas fraudulentas para permanecer o posicionarse en el mercado del aseguramiento.
- La organización se abstiene de participar en los procesos políticos de elección popular, salvo la promoción del ejercicio individual de elector que es deber de todos los funcionarios de Mutual SER EPS.
- Se promueve la protección del medio ambiente y el desarrollo sostenible

Política de cumplimiento anticorrupción, antisoborno y antifraude.

La Política de cumplimiento Anticorrupción, Antisoborno y Antifraude de Mutual SER EPS tiene como propósito declarar públicamente su compromiso con un actuar ético y transparente ante sus grupos de interés mediante la implementación de una filosofía de Cero Tolerancia ante actos que contraríen sus principios organizacionales.

Con esta política Mutual SER EPS pretende establecer las pautas para la incorporación de prácticas contra la corrupción, el soborno y el fraude a fin de conducir sus negocios con honestidad e integridad, y en estricto cumplimiento con las leyes antisoborno, anticorrupción y antifraude aplicables.

Los lineamientos y mecanismos de ejecución de la presente política se pueden consultar en la política de cumplimiento Anticorrupción, Antisoborno y Antifraude. **POL-CDG-04** Todas estas expresadas en el documento denominado **CÓDIGO DE CONDUCTA Y BUEN GOBIERNO** de Mutual SER EPS.

16. CICLO DE VIDA DE LOS DATOS

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.

17. VIGENCIA

El presente documento, ***Políticas de Seguridad de la Información*** rige a partir del ***27 de septiembre de 2020***, 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.

18. 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	30/11/2020	03	Reestructuración políticas de seguridad de la información, conforme a la Guía 2 - Elaboración de la política general de seguridad y privacidad de la información del Modelo de Seguridad y Privacidad de la Información (MSPI)