# MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SALUD SOGAMOSO E.S.E.

## PROCESO RECURSOS INFORMÁTICOS

## CONTROL DE CAMBIOS

| FECHA | VERSIÓN. | DESCRIPCIÓN DEL CAMBIO |
|---|---|---|
| 01/10/2013 | 01 | Construcción del procedimiento |
| 12/06/2017 | 02 | Se actualiza el procedimiento en el objetivo, alcance y estructura, se incluye actividades MIPG y Seguridad de la Información, condiciones ambientales para conservación de activos de información, Manejo y uso de equipos de cómputo. Se suprime procedimiento de uso adecuado de equipos de computo |
| 23/03/2018 | 03 | Se incluye indicadores de Control |
| 15/06/2018 | 04 | Se cambia a Manual de Gerencia y Seguridad de la Información, se suprime autorización de acceso remoto para trabajo a colaboradores. |
| 28/02/2019 | 05 | Se recodifica con la nueva estructura |
| 13/09/2019 | 06 | Se realiza la adopción mediante Resolución 285 de 2019, se revisa los códigos de procedimientos y formatos que hacen parte de este manual, se incluye Plan de Seguridad Digital como parte de este. |
| 21/03/2020 | 07 | Incluye en el numeral 5.8.4 uso de conexiones remotas |
| 30/03/2020 | | Se crea el numera 6 con el procedimiento para diligenciar el Formato de Necesidades de información Código. GRI-F-009. |
| 10/06/2022 | 08 | se incluye detección de disfunciones en el sistema de información. |

| ELABORADO POR: | REVISADO POR: | APROBADO POR: |
|---|---|---|
| CARLOS PARADA | | JUNTA DIRECTIVA |
| **Cargo:** P.U GESTION DE RECURSOS INFORMATICOS | **Cargo:** P.E CALIDAD | **Cargo:** JUNTA DIRECTIVA |

## 1. OBJETIVO

Establecer el mecanismo de interacción colaborativo entre personas, recursos informáticos y procedimientos orientados a la identificación de las necesidades de información para garantizar la operación de la empresa atendiendo a su estructura organizacional, con el fin de seleccionar, recopilar, analizar, administrar y garantizar la seguridad de los datos e información clave para dirigir y mejorar el desempeño y competitividad de la entidad.

## 2. ALCANCE

**Desde**: el procesamiento de la información de forma sistémica, estandarizada, segura y confiable.
**Hasta:** el análisis y toma de decisiones para el mejoramiento continúo.

## 3. DEFINICIONES

### 3.1. Sistema de Información Gerencial

Colección de sistemas de información que interactúan entre sí y proporcionan información tanto para las necesidades operacionales como de la administración.

En teoría, una computadora no es necesariamente un ingrediente de un Sistema de Información Gerencial (SIG), pero en la práctica es poco probable que exista un SIG complejo sin las capacidades de procesamiento de las computadoras.

Es un conjunto de información extensa y coordinada de subsistemas racionalmente integrados que transforman los datos en información en una variedad de formas para mejorar la productividad de acuerdo con los estilos y características de los administradores y las empresas.

### 3.2 Seguridad de la información

Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

**3.3 Activo de información**: refiere al componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del instituto y, en consecuencia, debe ser protegido.

**3.4 Acuerdo de Confidencialidad:** Voluntad de mantener la confidencialidad de la información, 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 soportada en manual de funciones o contratos previamente establecidos.

**3.5 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.

**3.6 Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso informático.

**3.7 Centros de cableado:** Lugares físicos 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, paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

**3.8 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.

**3.9 Cifrado:** Es la 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.

**3.10 Confidencialidad:** Garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

### 3.11. Unidades de Conservación de la Información

#### 3.11.1. En medio físico

Para el almacenamiento y conservación de documentos en soporte de papel se deben utilizar cajas, y carpetas elaboradas en cartón neutro, los cuales garantizan de manera considerable la conservación de los mismos.

- **Condiciones Ambientales**

El depósito de archivo debe tener una Temperatura de 15 a 20 °c con una fluctuación diaria que no exceda los 2°c. Una humedad relativa entre 45% y 60% con fluctuación diaria que no exceda del 5% entre valores máximos y mínimos.

#### 3.11.2. En medio Magnético

Para documentos en formato análogo como microfilm, cintas fonográficas, cintas de vídeo, rollos cinematográficos, fotografía entre otros, y digitales como disquetes, cintas DAT, CD, DVD, entre otros, se tendrá en cuenta lo siguiente:

Las fotografías y negativos deberán almacenarse en sobres individuales y en cajas de PH neutro.

Los rollos de microfilmación deberán mantenerse en su carrete y contenedor elaborados en material estable y químicamente inertes; cada rollo estará en una unidad

Las cintas magnéticas de audio, vídeo o de datos como DAT, entre otros, deberán almacenarse completamente rebobinadas en su respectivas cajas alejadas de campos magnéticos y fuentes de calor.

Los disquetes y los CD, entre otros, deben contar con una unidad de conservación plástica en polipropileno u otro polímero químicamente estable, que no desprenda vapores ácidos o contenga moléculas ácidas retenidas en su estructura. Cada unidad de conservación deberá contener solo un disquete o CD.

- **Condiciones Ambientales**

**Cintas de audio**
Temperatura de 10 a 18°C. Humedad relativa de 40% a 50%.

**Medios Magnéticos**
Temperatura 14 a 18°C. Humedad relativa de 40% a 50%.

**Discos ópticos**
Temperatura de 16 a 20°C. Humedad relativa de 35% a 45%.

**Microfilm**
Temperatura de 17 a 20°C. Humedad relativa de 30% a 40%.

### 3.11.3. Condiciones Ambientales para la Documentación en Medio Física y en Medio Magnético

El nivel de luz natural debe ser menor o igual a 100 lux. La radiación ultravioleta no debe superar los 70 micro vatios/lumen y su incidencia directa sobre la documentación y unidades de conservación. La iluminación artificial podrá hacerse con luz fluorescente de baja intensidad colocando filtros ultravioleta.

Se debe disponer de equipos para la atención de desastres como extintores de CO2, Solkaflan o multipropósito y extractores de agua de acuerdo con los riesgos de inundación o infiltración. Se aconseja evitar el empleo de extintores de polvo químico y de agua.

Se debe realizar limpieza permanente y adecuada de las instalaciones, de la estantería y de las unidades de conservación

**3.12 Scanner:** Es un periférico que se utiliza para convertir, mediante el uso de la luz, imágenes impresas o documentos a formato digital.

**3.13 Fotocopiadora:** Es aquella máquina que utilizamos para copiar o imprimir algún documento, es decir, para fabricar copias de papel a papel.
**3.14 Proyectores, Video Beam:** Es un equipo eléctrico, liviano y fácil de transportar, que permite proyectar imágenes, textos, videos y tiene sonido incorporado.

## 4. RESPONSABLES

Gerencia
Líder de Gestión de Recursos Informáticos
Líderes de Proceso

## 5. PROCEDIMIENTO

### 5.1 Identificación de Necesidades de Información

Las necesidades de información de las diferentes áreas de la Salud Sogamoso ESE, se establecen a partir de las solicitudes individuales y se consolidan en el formato **"Necesidades de información GRI-F-025 "**, donde se definen área que solicita la información, área que genera la información, información requerida, tipo de información, forma, comités que deben analizar la información, flujo de información (quien la genera, quien la recolecta, como la depura, como se presenta, a quien se presenta), Adicionalmente se establece si esta información tendrá manejo interno o externo, teniendo en cuenta si las herramientas informáticas existentes lo permiten o si no se crea la necesidad de adquisición, elaboración de una nueva.

Para las nuevas necesidades de información, los clientes internos deben solicitar en el formato preestablecido al proceso de Recursos Informáticos para que se establezca: Fuente de la Información, método de recolección. Información específica requerida, forma de presentación de la información (Cualitativa, cuantitativa, mixta), periodicidad, estandarización de variables, responsable de generar la información, y el objetivo de generar la información.

### 5.2 Diseño de Herramienta Informáticas con Base en las Necesidades de Cada Área y/o Servicio Administrativo, Asistencial o de la Dirección.

Tomando en cuenta las necesidades de información identificadas, se busca que Salud Sogamoso E.S.E. cuente con herramientas informáticas que permita emitir respuesta eficaz y oportuna a los procesos y facilitar así la toma de decisiones acorde con las herramientas existentes (Sistema de Información CNT, Interfaz de Laboratorio Enterprise, Ventanilla Única

de correspondencia, Página Web e Intranet, tablero de Indicadores estratégicos, control de UVR producidas, medición de adherencia a Guías entre Otros). Para reportes del sistema de información se realizara a través de Report Server las cuales se diseñaran acorde a las necesidades.
De no existir la herramienta es evaluado por el proceso de Recursos Informáticos el medio para el diseño y posterior desarrollo ya sea a través del recurso humano existente o si se requiere de adquisición a proveedor externo.

### 5.3 Efectividad de las Herramientas Informáticas

Salud Sogamoso ESE cuenta con Herramienta Informática que responden de forma efectiva a las necesidades de los usuarios, es amigable y sensible para detectar oportunamente los cambios y ajustes según necesidades, (Sistema de Información CNT, Interfaz de Laboratorio Enterprise, Ventanilla Única de correspondencia, Página Web e Intranet, Tablero de Indicadores estratégicos, Control de UVR producidas, Medición de Adherencia a Guías, comprobador de derechos de los usuarios, reporte de eventos adversos entre Otros)que permite la centralización y almacenamiento dela información producida en área asistencial y administrativa, lo que conlleva a generar información específica de la atención de los usuarios y financiera de un periodo específico de acuerdo a las necesidades identificadas.
Con la Herramienta Informática de ventanilla única de correspondencia se permite llevar el control en la entrada y salida de correspondencia interna y externa.
De acuerdo al formato de necesidades de información el proceso de Recursos Informáticos de Salud Sogamoso E.S.E. procede a diseñar las consultas de las Bases de Datos, teniendo en cuenta las variables que almacenan los datos requeridos, se realiza la consolidación y se adecua al formato solicitado.

### 5.4 Recopilación de Información y Manejo Eficiente

La recopilación de registros al sistema de información de Salud Sogamoso E.S.E.se realiza por los clientes internos tanto del área asistencial como administrativa, posteriormente es almacenada y procesada por el sistema de información (CNT) y demás herramientas informáticas disponibles en la entidad, para el análisis de la información es bajo la responsabilidad de líder del proceso involucrado, cumpliendo con la normatividad de Protección de datos la cual se establece mediante la política y procedimiento TRATAMIENTO Y PROTECCION DE DATOS PERSONALES.

### 5.5 Integralidad, Confiabilidad, Disponibilidad, Oportunidad, Consistencia de la Información

Una vez generada la información solicitada por clientes internos y/o externos de la entidad, el líder de recursos informáticos hace verificación de datos acorde a la solicitud realizada de tal forma que se pueda garantizar confiabilidad e integralidad de los datos registrados en el formato del informe, posteriormente será enviada a procesos y/o oficina que realizo la solicitud para ser evaluada y analizada por el responsable del proceso.

Los datos registrados en el Sistema de Información se encuentran a disposición de los usuarios que han sido previamente autorizados para tener acceso a información, ya sea al sistema CNT, intranet de Salud Sogamoso ESE y equipo en la Red dispuesto por el área de recursos informáticos, a los cuales pueden acceder a través de un nombre de usuario y autenticación por contraseña, lo cual garantiza confidencialidad, manejo y salvaguarda de la información; cada uno de los equipos tienen asignado usuario con perfiles acorde a las funciones, de esta manera se limita el acceso a información. Se soporta con el formato GSI-F-12 Formato Registro de Usuarios y Claves.

### 5.6 Evaluar y Mejorar los Sistemas Para Promover el Uso de Información Para el Cumplimiento de las Metas y de los Objetivos Organizacionales

El proceso de recursos informáticos de la entidad, tiene establecidos mecanismos para informar las fallas o las oportunidades de mejora de recopilación o procesamiento de los datos, relacionadas con las necesidades de información, para lo cual existe un formato GSI-F-032 Seguimiento Fallas en el Sistema de Información, posteriormente se recopilan las solicitudes realizadas, se priorizarán de acuerdo al riesgo, al costo y al beneficio para implementar las mejoras del sistema, verificando que se dio cumplimiento a los requerimientos realizados por los usuarios, los cuales son evaluados de forma continua.

#### 5.6.1 Evaluar la eficiencia y mejora del diseño y administración del sistema de información.

Se tomara una muestra de usuarios del sistema para evaluar el nivel de satisfacción con el sistema de información de Salud Sogamoso, de igual manera se medirá la oportunidad de respuesta frente a solicitudes de mejoras o nuevos requerimientos.

Aunado a lo anterior se evaluara planos de generación de informes, con el fin de mejorarlos o actualizarlos de acuerdo a los cambios que puedan surgir por necesidad o por cambios de la normatividad.

### 5.7 Análisis de la Información

La institución realiza análisis de la información que se obtiene de manera rutinaria de acuerdo a las herramientas utilizadas acorde a las necesidades de los procesos.

La información generada de acuerdo a las necesidades de los clientes internos o externos buscan estandarizar los datos de tal forma que sean el insumo de la toma de decisiones de tipo administrativo o asistencial, utilizando las técnicas de minería de datos la cual ayuda a predecir el comportamiento de indicadores que pueden incidir de forma negativa o positiva para la Empresa.

La ESE cuenta con la conformación institucional de comités como: PLANEACIÓN, SOGC, IAMI, COVE, FINANCIERO, HISTORIAS CLINICAS, entre otros, siendo estos los responsables de analizar y evaluar la información generada de forma sistémica, lo cual permite hacer mejoramiento continuo de la calidad de la información; es importante anotar que la

interpretación y el análisis de la información se realiza bajo la responsabilidad y directriz del líder de proceso y/o comité institucional.

Los resultados de los análisis sirven para la toma de decisiones estratégicas y apoyan el mejoramiento de las actividades cotidianas en busca de satisfacer necesidades y expectativas de los clientes y la sostenibilidad de la empresa.

Se evalúa la eficiencia de los sistemas de información y de los mecanismos para su análisis y difusión con el ánimo de mejorar la calidad en la interpretación e información de interés a socializar y publicar.
Salud Sogamoso E.S.E. cuenta con medios de difusión de información de interés de los clientes internos o externos, para lo cual se cuenta con los diferentes canales de comunicación entre los cuales encontramos: comités, Intranet, pagina web, sistema de perifoneo intramural, medios radiales, medios televisivos e impresos (boletines), entre otros descritos en el plan de comunicaciones de la entidad.

### 5.8. Seguridad de la Información

**5.8.1 Política de Seguridad:** Salud Sogamoso E.S.E. se compromete a un eficiente manejo de la información, utilizando recursos adecuados, apoyados en lineamientos que garanticen la confidencialidad, privacidad, seguridad y confiabilidad de la información.

Todo colaborador de la entidad es responsable de preservar la confidencialidad, integridad y disponibilidad de la información en cumplimiento de la presente política y de los procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.

Son determinante en la seguridad de la información:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información
- Su integridad, asegurando que la información registrada y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información según las funciones que desempeñe en Salud Sogamoso E.S.E
- La seguridad de la información se logra a través de la implementación, aplicación y control al procedimiento de Gerencia y Seguridad de la Información, por lo anterior es política de Salud Sogamoso E.S.E:

1. Realizar un análisis del riesgo de la seguridad de la información con acompañamiento de la área de control interno y de acuerdo a su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos en el MECI y plan anticorrupción.
2. Cumplir con los requisitos legales o reglamentarios en la entrega de información al cliente interno y externo.
3. Concientizar y entrenar en seguridad de la información a todo el personal.

4. Establecer los recursos informáticos necesarios para garantizar la continuidad de la prestación del servicio acorde a la Misión de la empresa.
5. Establecer sanciones conforme a la norma y procedimientos internos de la entidad, en los casos identificados y comprobados por mal uso de los recursos informáticos a los responsables.
6. Detectar anomalías, todo funcionario es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas a través de la Intranet o medios escritos.
7. Preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y procedimiento inherente a la Seguridad de la Información y normas de archivo.
8. Se establece diseño del Plan de Seguridad de la Información y Riesgos de la Seguridad de la Información incluidos en la Matriz de Riesgos del Proceso.
9. Hace parte de este manual el Plan de Seguridad Digital
10. El líder de recursos informáticos, como responsable directo de la Seguridad de la Información realizará la implementación y seguimiento.
11. Hace parte integral de este Manual el Plan de Seguridad Digital que incluye las políticas de: Políticas y Estándares de Seguridad Personal, Políticas Y Estándares de Seguridad Física y Ambiental, Políticas y Estándares de Control de Acceso Lógico, Políticas y Estándares de Seguridad Y Administración de Operaciones de Cómputo, Políticas y Estándares de Cumplimiento de Seguridad Informática

### 5.8.2 Compromiso de la dirección

La Gerencia de la entidad, expresa su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad, a través de:

- La revisión y aprobación de la Política de Seguridad de la Información contenida en este documento.
- Facilitar la divulgación a los colaboradores de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener la política de seguridad de la información.
- Promover la importancia de la seguridad de la información entre los funcionarios, personal con órdenes de prestación de servicios y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
- El proceso de Recursos Informáticos en apoyo de la alta gerencia debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información y uso adecuado de los recursos informáticos, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

### 5.8.3 Uso de equipos móviles

A continuación se provee las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso

de servicios o se requiera para el cumplimiento del objeto de contratos para cumplir con la misión y plan estratégico de Salud Sogamoso E.S.E. Así mismo, velará porque los colaboradores hagan uso responsable de los servicios y equipos proporcionados por la entidad.

### 5.8.3.1. Normas para uso de dispositivos móviles

- Los equipos móviles deben tener opciones de protección
- En los equipos móviles institucionales se debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para ser entregados a los usuarios, igualmente se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- En los equipos móviles según tecnología se debe activar la opción de cifrado de la memoria de almacenamiento haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- Los equipos de uso institucional se debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Los usuarios de cada dispositivo móvil institucional deben asociar la línea a una cuenta de correo electrónico para la solución de copias de seguridad de la información contenida en los dispositivos móviles institucionales.
- El proceso de Recursos Informáticos debe tener registro de los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

### 5.8.4 Uso de conexiones remotas

Por política de confidencialidad y seguridad de la información Salud Sogamoso E.S.E. Prohíbe el acceso desde conexiones remotas, salvo que por fuerza mayor o en casos excepcionales se requiera "factores externos que no permitan la movilidad de los colaboradores y requieran realizar teletrabajo la cual estará supervisada y monitoreada por el proceso de recursos informáticos atendiendo a los siguientes lineamientos":

1. El proceso de Recursos Informáticos determinara la o las herramientas de comunicaciones necesarias que garanticen la seguridad en el acceso a los equipos y software empresarial
2. Se informara a los colaboradores sobre el uso adecuado de las mismas.

### 5.8.5 Reporte de talento humano en apoyo a seguridad de la información

"Desvinculación, licencias, vacaciones o cambio de labores de funcionarios, personal con órdenes de prestación de servicios y personal provisto por terceros"
Salud Sogamoso E.S.E. asegurará que sus funcionarios y/o colaboradores vinculados a la entidad por las diferentes modalidades de contratación, serán registrados al sistema de información a través de usuario y contraseña, de igual forma se garantiza su desvinculación o reasignación para la ejecución de nuevas labores de una forma ordenada, controlada y segura.
La líder de Gestión del talento Humano es la responsable de notificar a líder de Recursos informáticos las novedades de personal en cuanto a "desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros", con el fin de garantizar el cambio o generar ajustes a perfiles y accesos a los recursos informáticos de la entidad propiciando por la seguridad de la información.

### 5.8.6 Responsabilidad uso activos de información

Salud Sogamoso E.S.E. como propietario de la información física así como de la información generada, procesada, almacenada y transmitida en buen uso de las herramientas informáticas disponibles, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.
La información, archivos físicos, los recursos informáticos, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fax, entre otros) propiedad de Salud Sogamoso E.SE. , son activos de la institución y se proporcionan a los colaboradores autorizados, para contribuir con la Misión institucional.
Toda la información sensible, así como los activos donde ésta se almacena y se procesa se asigna a un responsable, inventariado y posteriormente clasificado acorde a las tablas de retención documental.

#### 5.8.6.1 Responsabilidad en los activos en Información

- Los colaboradores de la entidad deben actuar como propietarios de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Los colaboradores deben generar un inventario de activos para los procesos a los cuales pertenecen, acogiendo los lineamientos de Gestión documental designados por la empresa.
- Los colaboradores deben monitorear periódicamente la validez de los usuarios y perfiles de acceso a la información.
- Los colaboradores deben ser conscientes que los recursos de procesamiento de información se encuentran sujetos a auditorías por parte del área de control interno y a revisiones de cumplimiento en el buen uso.
- El área de Sistemas será quien autoriza y realiza la instalación, cambio o eliminación de componentes de los recursos informáticos
- El proceso de Recursos Informáticos debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- El proceso de Recursos Informáticos en acompañamiento con recursos físicos son los responsables del movimiento y preparación de las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.
- El proceso de Recursos Informáticos entregará la directriz para garantizar copias de seguridad de la información de los funcionarios a través del procedimiento GRI-P-005 COPIAS DE SEGURIDAD.
- Los recursos informáticos, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas y no deben ser utilizados para fines personales o ajenos al cumplimiento de los objetivos propuestos por Salud Sogamoso E.S.E.
- Los colaboradores no deben usar equipos de cómputo ni móviles personales para el desarrollo de las funciones empresariales.
- Los colaboradores no deben utilizar software no autorizado o de su propiedad en los equipos de Salud Sogamoso E.S.E.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo a Talento Humano y así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

### 5.8.7 Uso de Periféricos y Medios de Almacenamiento

El uso de periféricos y medios de almacenamiento (memorias usb, discos externos, cd, DVD) en los recursos informáticos (equipos de cómputo de escritorio y portable) dispuestos para el cumplimiento de las funciones será reglamentado por el proceso de Recursos Informáticos para los colaboradores de acuerdo a necesidad de uso.

#### 5.8.7.1 Normas uso de periféricos y medios de almacenamiento

- El proceso de Recursos Informáticos establece las condiciones e implementa los controles que regulen el uso de medios de almacenamiento externos acorde al procedimiento de copias de seguridad.
- El proceso de Recursos Informáticos debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la información, ya sea cuando estén en producción, cuando se tengan en Backup, cuando se re-asigne a un nuevo usuario o se determine para baja.

### 5.8.8 Acceso a Redes y Recursos de Red

Se debe propender porque las redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

#### 5.8.8.1 Acceso a redes y recursos de red

- EL proceso de Recursos Informáticos garantizará el mecanismo de autenticación y control para proteger el acceso a las redes de datos y los recursos de red de Salud Sogamoso E.S.E.
- El proceso de Recursos Informáticos debe asegurar que las redes inalámbricas de Salud Sogamoso E.S.E. cuenten con métodos de autenticación que evite accesos no autorizados.
- Los colaboradores antes de contar con acceso lógico por primera vez a la red de datos de Salud Sogamoso E.S.E., deben ser registrados en el formato registro de usuarios y claves.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de Salud Sogamoso E.S.E. deben cumplir con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

#### 5.8.8.2. Manejo y administración de internet

- El servicio de internet se presta dentro de la institución para el desarrollo de las labores administrativas

- Queda totalmente restringido el acceso a páginas de contenido ilícito o que atenten contra la dignidad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista. Pornográficas.

- El sistema de acceso a internet estará bajo constante monitoreo para verificar el buen uso y optimización del recurso. La institución generará los niveles de autorización sobre la navegación según las necesidades requeridas para cada uno de los tipos de usuarios.

**5.8.8.3.** Manejo y administración del correo institucional y chat institucionales.

El correo institucional es de uso exclusivamente laboral y no para uso personal, está por lo tanto prohibida la publicación de correos institucionales en portales públicos.

Está prohibido facilitar el acceso de la cuenta de correo electrónico (e-mail) a otras personas, su cuenta es personal e intransferible.

Está completamente prohibidas las siguientes actividades:

Utilizar el Correo Electrónico para cualquier propósito comercial o financiero.

No se debe participar en la propagación de mensajes en "cadenas", ni en esquemas piramidales de índole político, religioso o temas similares.

Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo electrónico. La información contenida en el correo electrónico hace parte de la confidencialidad de la Institución y todos los correos podrán ser monitoreados por parte de la institución, según sea requerido.

**5.8.9 Administración de Acceso a Usuarios**

Salud Sogamoso E.S.E. a través del proceso de Recursos Informáticos establecerá privilegios para el control de acceso lógico de cada colaborador a las redes de datos, los recursos tecnológicos y sistemas de información. Así mismo, velará porque los colaboradores autorizados tengan acceso únicamente a la información necesaria para el desarrollo de sus labores, ya que la asignación de los derechos de acceso está regulada por normas y procedimientos establecidos para tal fin y se describen a continuación.

- El proceso de Recursos Informáticos establece mediante procedimiento GRI-P-008 Administración de Usuarios en los Sistemas de Información se deja registro en el Formato GRI-F-008.
- El Colaborador realiza la solicitud al proceso de Recursos Informáticos, para la creación, modificación o retiro de usuarios.
- El líder de Sistemas recibe la solicitud autorizada por el líder del proceso al cual pertenece el colaborador y verifica si el requerimiento es de creación de cuentas, modificación, desactivación, bloqueo intencional, cambio de perfil o retiro de usuarios de las aplicaciones.
- Los usuarios con acceso a los servicios de red y los sistemas de información de Salud Sogamoso E.S.E. son responsables de las acciones realizadas, así como el uso adecuado de usuario y contraseña asignados para el acceso.
- Los colaboradores no deben compartir sus cuentas de usuario y contraseñas con otros colaboradores o con personal provisto por terceras partes.

**5.8.9 Privilegios Administrador de los Recursos Informáticos**

El proceso de gestión de recursos informáticos, velará porque los recursos Informáticos y los servicios de red de Salud Sogamoso E.S.E. sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores.

### 5.8.10.1 Uso de privilegios al administrador de los recursos informáticos

- El líder del proceso de gestión de recursos informáticos establece cuentas personalizadas con altos privilegios para los funcionarios responsables del manejo de los recursos tecnológicos, servicios de red y sistemas de información.
- Garantiza que los usuarios no puedan acceder a las bases de datos de los sistemas de información en producción.
- Asegura que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- Establece los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos y servicios de red, funcionarios, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información.
- Deshabilitarlas funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

La información que se maneja en el Sistema, se recopila y archiva en el servidor con IBM x 3650 el cual está configurado con un RAID-1 lo cual garantiza una copia espejo en tiempo real del sistema de información lo cual minimiza el riesgo de pérdida de información, la seguridad con la cual cuenta el servidor para el ingreso a la información se basa en la autenticación de un solo usuario con privilegios de administrador el cual tiene que autenticarse con una contraseña alfanumérica que cumple los requisitos para ser segura, el servidor no tiene conexión o acceso a través de internet lo cual minimiza el riesgo de ingreso a personal externo desde internet.

La información de insumo y formatos generada en base al sistema de información está salvaguardados adicionalmente en copias de seguridad que se almacenan fuera de la Sede Centro una vez por mes, lo cual garantiza el acceso o recuperación de la información en caso de una falla técnica.

## 5.9. Manejo de los Equipos de Cómputo

- En el proceso de Inducción y re inducción a colaboradores se incluirá un ítem donde se hable de la responsabilidad y uso adecuado de los equipos de cómputo y elementos electrónicos.
- Los equipos de cómputo son asignados por el proceso de Recursos Físicos que van a ser utilizados en labores inherentes a las funciones para las cuales fueron contratados
- Se informa que el cuidado y limpieza externa de los equipos de cómputo son responsabilidad exclusiva del custodio del bien.
- Los equipos deben permanecer encendidos solamente en horas laborables, para evitar el consumo innecesario de energía
- El equipo de cómputo asignado es exclusivamente para uso laboral y no para uso personal. La información que se encuentre en los equipos de cómputo es de la institución y podrá ser auditada según sea requerido por la institución. El usuario a quien se le ha asignado un equipo de cómputo es responsable de su seguridad y de su buen uso. Es responsabilidad del usuario a quien se le asignó el equipo de cómputo informar, oportunamente, del mal funcionamiento del mismo a través de la INTRANET Formulario de Solicitud de mantenimiento https://www.saludsogamoso.gov.co/sp/intranet/mantenimiento_nueva_solicitud.php.
- Solo quienes pertenecen al proceso de Recursos Informáticos están autorizados para dar mantenimiento de software y hardware a los equipos de cómputo.
- Ninguna persona diferente a quienes pertenecen al proceso de recursos informáticos está autorizado para dar mantenimiento a un equipo o realizar cambio o reemplazo de sus partes. Sólo los funcionarios del proceso de recursos informáticos están autorizados para realizar formateo de discos duros, reconfiguración de opciones o cambio de las características del software operativo de los equipos de cómputo.

- Se mantendrá un fondo de pantalla institucional predeterminado para todos los equipos de cómputo pertenecientes a la institución, el funcionario no deberá de ningún modo alterarlo, ni modificarlo.

- Para garantizar el normal funcionamiento de los equipos de cómputo, impresoras, escáner, y periféricos se realizará el mantenimiento acorde al plan de mantenimiento programado y entregado a la secretaria de salud departamental según el procedimiento.

- Las unidades para la recarga de impresión (tóner, cintas y cartuchos de tinta) son entregadas al colaborador que las solicite previa presentación de la unidad recién acabada.

## 6. PROCEDIMEINTO PARA DILIGENCIAMIENTO DEL FORMATO DE NECESIDADES DE INFORMACIÓN

El formato está diseñado para describir las necesidades de información de cada uno de los procesos y unificar en una sola herramienta, con el objeto de tener un consolidado que permita la elaboración y/o adquisición de herramientas informáticas para la solución adecuada.

El alcance va desde la identificación de la necesidad que debe ser registrada por el Líder del equipo independiente del usuario que la solicite hasta la entrega de la solución a satisfacción por el Proceso responsable.

El formato es publicado usando la herramienta de google docs. Alojada en el drive asociado al correo saludsogamoso.sistemas@gmail.com con perfiles de edición a los usuarios, de esta forma estará en línea para los líderes de proceso y será la única herramienta de verificación para los efectos de cumplimiento.

El formato también lo deben tener en sus archivos de gestión de cada proceso y esto permite que los titulares puedan editar en sus PC y luego copiar o pegar en el archivo en línea.

Pasos para el diligenciamiento adecuado

I. Campo columna A: Proceso/Área en este campo de debe identificar el proceso a referenciar que está involucrado en la necesidad de información y debe hacer parte del mapa de procesos de la empresa.

II. Campo Columna B: Descripción del Informe, se debe registrar en forma corta y precisa la necesidad de información a solicitar. En este se debe anexar al correo del Líder de Proceso que tenga que entregar la solución un documento que lleve la estructura y datos o variables requeridas para dar la interpretación adecuada y evitar reprocesos al momento de generar la información, en caso que se requiera información específica que contenga códigos determinados se debe anexar el listado de los mismos. "Ejemplo Códigos CIE10, Códigos CUPS, Cuentas Contables, rubros presupuestales"

III. Campo columnas C y D: Medio de entrega de la información, se va diligenciar si es magnética o física, se asignará uno (1) si se requiere y cero (0) si no se requiere. En caso de requerir de ambas formas se debe colocar 1 en ambas casillas.

IV. Campo columna E: Responsable de solicitud de la información, se escribe el área o dependencia que la solicita.

V. Campo columna F: Responsable de generación de la información, se escribe la dependencia, área o responsable de producir la información, en el caso de quien solicita la información no pueda identificar quien la debe generar debe solicitar apoyo al proceso de recursos informáticos o a las subgerencias.

VI. Campo Columna G: En este campo se edita únicamente datos numéricos acorde al comentario descrito y se relaciona a continuación; Si el informe es diario de debe colocar el 1, si el informe es semanal se debe colocar 2, si el informe es cada quince días se debe colocar 3, si el informe es mensual se debe colocar 4, si el informe es bimestral de debe colocar 5, si el informe es trimestral se debe colocar 6, si el informe es cuatrimestral se debe colocar 7, si el informe es semestral se debe colocar 8, si el

informes es anual se debe colocar 9. Esto permite la identificación adecuada para seguimientos.

VII. Campo Columna H: Fecha de Solicitud al Proceso Responsable de generar la información, este campo permite identificar la fecha inicial desde cuando se programa a necesidad de la información.

VIII. Campo Columna I: Fecha Probable de Entrega de Solución, este campo lo registra el proceso responsable de realizar la entrega de la información de acuerdo al análisis y datos entregados según lo registrado en el Campo Columna B descripción del Informe.

IX. Campo Columna J: Fecha de Entrega por Parte del Proceso Responsable, se debe escribir la fecha de entrega del primer informe al área o funcionario que solicito la información, en caso de requerir ajustes se deben solicitar en el campo observaciones, si es aceptado se debe dejar registro y en adelante para los casos que se pueden programar reportes del sistema de información se tomara las frecuencias descritas en la columna G periodicidad.

X. Campo Columnas k, L, M: Destino de la Información, se debe registrar en la casilla que aplique interna o externa o si es para ambas, en todos los casos se marca uno (1) si aplica o cero (0) si no aplica, no deben quedar celdas en blanco. Cuando aplica para Destino Externo se debe diligenciar la celda siguiente con el nombre del ente externo que la requiere.

XI. Campo Columna N: Área, dependencia o comité encargado del análisis, generación de resultados envió al destino final y seguimiento, en este campo se debe colocar el responsable de darle todo el trámite a la información hasta la entrega al destinatario final, en todos los casos se debe aplicar el procedimiento establecido por el proceso de gestión documental para el control de documentos.

XII. Campo Columnas O y P: Ubicación de la información, los procesos que intervienen deben tener definido el lugar físico y magnético donde va almacenar la información de gestión mientras pasa a archivo por transferencias documentales, en caso que haya marcado 1 en el campo medio de entrega de la información física columna D se debe diligenciar el campo de la columna P de lo contrario debe quedar 0.

XIII. Campo Columna Q: Flujo de Información, se debe colocar la secuencia a seguir desde que se genera la información, hasta la entrega final.

XIV. Campo Columna R: Indicador, Días trascurridos desde la fecha probable de entrega de la solución hasta la fecha de entrega, no puede ser negativo. Este campo muestra la efectividad de respuesta y se mide desde la fecha probable de entrega hasta el primer envió al proceso solicitante.

**XV.** Campo Columna S: Observación, este campo permite colocar todas las observaciones al registro tanto del solicitante como del proceso que entrega resultados.

Estas observaciones hacen parte del libro dispuesto para el formato y estarán en una hoja adicional.

## DETECCIÓN DE DISFUNCIONES EN EL SISTEMA DE INFORMACIÓN.

El manejo de los errores en el SQL Server nos da un control sobre el código Transact-SQL. Cuando surgen disfunciones en los datos, se tiene la oportunidad de realizar seguimientos al respecto y probablemente poder hacerlo de nuevo. El manejo de errores de SQL Server puede ser tan fácil como simplemente registrar que algo sucedió (Cliente interno o externo) o podría ser el área de recursos informáticos intentando poder corregir un error. Incluso se puede estar traduciendo el error al lenguaje SQL, ya que recursos informáticos sabe cómo los mensajes de error técnicos de SQL Server podrían no tener sentido y ser difíciles de entender. Pero afortunadamente, se tiene la oportunidad de poder traducir esos mensajes y convertirlos en algo más significativo para transmitir a los usuarios interno y externos de la institución.
Para minimizar las disfunciones del sistema de información, se analizara más de cerca la instrucción TRY…CATCH la sintaxis, su aspecto, su funcionamiento y lo que se puede hacer cuando se produce un error. A parte de eso, el método se explicará en un caso de SQL Server utilizando un grupo de sentencias / bloques T-SQL, que es simplemente la forma en que SQL Server maneja los errores. Esta es una manera muy sencilla pero estructurada de hacerlo.
Adicionalmente de eso, existe la función RAISERROR que se puede utilizar para poder generar nuestros propios mensajes de error personalizados, que es una excelente forma de traducir los mensajes de error confusos en algo un poco más significativo que la gente pueda entender.

### MANEJANDO ERRORES USANDO TRY… CATCH

Así es la sintaxis. Tenemos dos bloques de código:

```
BEGIN TRY
    --code to try
END TRY
BEGIN CATCH
    --code to run if error occurs
--is generated in try
END CATCH
```

Cualquier cosa entre BEGIN TRY y END TRY es el código que queremos monitorear para detectar un error. Entonces, si se hubiera producido un error dentro de esta sentencia TRY, el control se habría transferido inmediatamente a la instrucción CATCH y luego habría empezado a ejecutar el código línea por línea.

Ya mismo, dentro de la declaración CATCH, se puede tratar de corregir el error, informar el error o incluso poder registrar el error para saber cuándo ocurrió, quién lo hizo al registrar el nombre de usuario, todo lo que es útil. Además se tiene acceso a algunos datos especiales que solo están disponibles dentro de la declaración CATCH:

ERROR_NUMBER – Devuelve el número interno del error
ERROR_STATE – Devuelve la información sobre la fuente
ERROR_SEVERITY – Devuelve la información sobre cualquier cosa, desde errores informativos hasta errores que el usuario de DBA puede corregir, etc.
ERROR_LINE – Devuelve el número de línea en el que ocurrió un error
ERROR_PROCEDURE – Devuelve el nombre del procedimiento almacenado o la función
ERROR_MESSAGE – Devuelve la información más esencial y ese es el mensaje de texto del error
Es todo lo que se requiere cuando se trata acerca del manejo de errores de SQL Server. Todo se puede realizar con una simple instrucción TRY y CATCH y la única parte cuando puede tornar difícil es cuando estamos lidiando con transacciones. Es que, si hay un COMIENZO DE TRANSACCIÓN, siempre debe terminar con una transacción COMPROMISO o ROLLBACK. El problema es si se genera un error después de que comencemos, pero antes de confirmar o revertir. En este caso peculiar, existe una función especial que se puede usar en la declaración CATCH que permite verificar si una transacción está en un estado comprometible o no, lo que nos permite tomar la decisión de revertir o cometerla.

## 7. INDICADORES DE CONTROL.

Incidencia de restauración de copias de seguridad del sistema de Información de CNT en el Año debe ser menor o igual 1.

Incidencia de restauración de copias de seguridad del sistema de Información de ventanilla única en el Año debe ser menor o igual 1.

Incidencia en el acceso al sistema de información de usuarios no autorizados o ataques externos al sistema de información CNT deber ser 0.

## 8. DOCUMENTOS DE REFERENCIA

- Ley 1341 de 2009 (Uso espectro) Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones

- Ley 100 de 1993
- Ley 1122 de 2007
- Resolución No 839 de 2017(Custodia HCL)
- ISO 27001
- Resolución 0123 de 2012
- http://www.monografias.com/trabajos24/informacion-gerencial/informacion-gerencial.shtml#defin#ixzz3K5PeEHwh
- https://es.wikipedia.org/wiki/Seguridad_de_la_información