

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, confiable hasta el análisis y toma de decisiones para el mejoramiento continuo.

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.


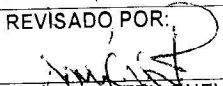
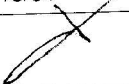
En teoría, una computadora no es necesariamente un ingrediente de un Sistema de Información Gerencial (SIG), pero en la práctica es poco probable que exista un SIG complejo sin las capacidades de procesamiento de las computadoras.

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.

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente

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.

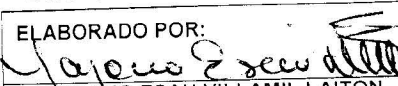
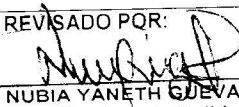
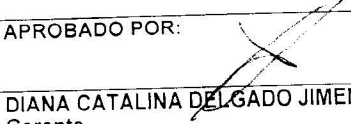
3.8 Centro de cómputo: Zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los 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.

4. RESPONSABLES

Gerencia
 Líder de Gestión de Recursos Informáticos
 Líderes de Proceso

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente

 Salud Sogamoso E.S.E.	GERENCIA Y SEGURIDAD DE LA INFORMACION	Código. GSI-P-36
		Versión. 02
		Fecha. 12/06/2017
		Página. 3 de 16

5. PROCEDIMIENTO

5.1 IDENTIFICACION 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 GSI-F-013 VERSION 2**", 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.


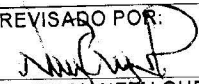
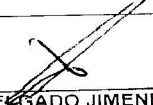
Para las nuevas necesidades de información, los clientes internos deben solicitar en el formato preestablecido al área de Sistemas de Información para que se establezca: Fuente de la Información, Método de recolección. Información específica requerida, forma de presentación de la información (Cualitativa, 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 Enterprice, Ventanilla Única de correspondencia, Página Web e Intranet, Tablero de Indicadores estratégicos, Control de UVR producidas, Medición de Adherencia a Guías entre Otros).

De no existir la herramienta es evaluado por el área de sistemas 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 HERRAMIENTAS INFORMÁTICAS

ELABORADO POR:  LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	REVISADO POR:  NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	APROBADO POR:  DIANA CATALINA DELGADO JIMENEZ Gerente
---	--	--

 Salud Sogamoso E.S.E. <small>Entidad Especializada en Salud</small>	GERENCIA Y SEGURIDAD DE LA INFORMACION	Código. GSI-P-36
		Versión. 02
		Fecha. 12/06/2017
		Página. 4 de 16

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, entre otras) que permite la centralización y almacenamiento de la 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.

Se tiene Herramienta Informática de ventanilla única de correspondencia que permite llevar el control en la entrada y salida de correspondencia interna y externa.

De acuerdo al formato de necesidades de información el área de sistemas de la ESE 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 RECOPIACIÓN DE INFORMACIÓN Y MANEJO EFICIENTE

La recopilación de información al sistema de información de Salud Sogamoso ESE 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.

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.

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Lider de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente

 Salud Sogamoso E.S.E.	GERENCIA Y SEGURIDAD DE LA INFORMACION	Código. GSI-P-36
		Versión. 02
		Fecha. 12/06/2017
		Página. 5 de 16

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.

5.6 EVALUAR Y MEJORAR LOS SISTEMAS PARA PROMOVER EL USO DE INFORMACIÓN PARA EL CUMPLIMIENTO DE LAS METAS Y DE LOS OBJETIVOS ORGANIZACIONALES

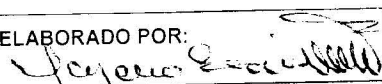
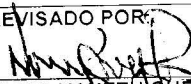

El proceso de recursos informáticos de la entidad, tiene establecidos mecanismos para informar las fallas o las oportunidades de mejora de recopilación o procesamiento de los datos, relacionadas con las necesidades de información, para lo cual existe un formato GSI-F-032 Seguimiento Fallas en el Sistema 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

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Lider de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



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.

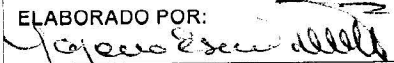
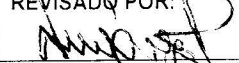

Los resultados de los análisis sirven para la toma de decisiones estratégicas y apoyan el mejoramiento de las actividades cotidianas en busca de satisfacer necesidades y expectativas de los clientes y la sostenibilidad de la empresa.


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.

7. SEGURIDAD DE LA INFORMACIÓN

7.1 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.

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Lider de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente

 Salud Sogamoso E.S.E.	GERENCIA Y SEGURIDAD DE LA INFORMACION	Código. GSI-P-36
		Versión. 02
		Fecha. 12/06/2017
		Página. 7 de 16

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:

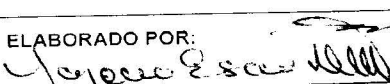
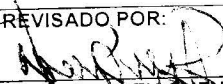

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información
- Su integridad, asegurando que la información registrada y sus métodos de proceso son exactos y completos.
- Su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información 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 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.
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.

El líder de recursos informáticos, como responsable directo de la Seguridad de la Información realizará la implementación y seguimiento del procedimiento de seguridad de la información.

7.2 COMPROMISO DE LA DIRECCIÓN

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente

 Salud Sogamoso E.S.E. <small>Entidad Especializada en Salud</small>	GERENCIA Y SEGURIDAD DE LA INFORMACION	Código. GSI-P-36
		Versión. 02
		Fecha. 12/06/2017
		Página. 8 de 16

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.
- La Gerencia debe 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 área de Sistemas 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.

7.3 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.

7.3.1. Normas para uso de dispositivos móviles



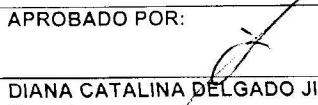
- Los equipos móviles deben tener opciones de protección
- En los equipos móviles institucionales se debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para ser entregados a los usuarios, igualmente se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITÓN Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



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 una cuenta de correo electrónico para la solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de ICETEX; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
- El área de sistemas 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.

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

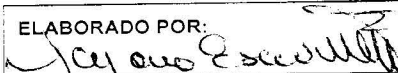
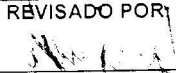
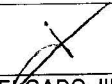
7.4 USO DE CONEXIONES REMOTAS

Salud Sogamoso E.S.E. establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas para el desarrollo de actividades propias en cumplimiento de las funciones o actividades contratadas; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

7.4.1 Normas para uso de conexiones remotas

- El Área de Control Interno, de manera conjunta con el Área de Sistemas, deben analizar y aprobar los métodos de conexión remota.
- El Área de Sistemas debe implementar los métodos y controles de seguridad para establecer conexiones remotas para el acceso al sistema de Información.
- El Área de Sistemas restringe las conexiones remotas a los recursos informáticos de la empresa, únicamente se permite acceso a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- El área de sistemas verifica la efectividad de los controles aplicados sobre las conexiones remotas a los recursos informáticos de manera permanente.
- El Área de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implementados para las conexiones remotas a los recursos informáticos de la empresa.
- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los recursos informáticos de Salud Sogamoso E.S.E. y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores de entidades públicas, de hoteles o cafés internet, entre otros.

7.5 REPORTE DE TALENTO HUMANO EN APOYO A SEGURIDAD DE LA INFORMACION

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



"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.

7.6 RESPONSABILIDAD USO ACTIVOS DE INFORMACIÓN


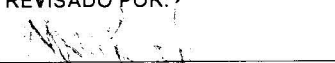
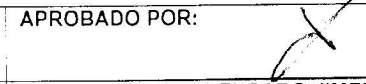
Salud Sogamoso E.S.E. como propietario de la información física así como de la información generada, procesada, almacenada y transmitida en buen uso de las herramientas informáticas disponibles, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices 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.S.E., 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.

7.6.1 Responsabilidad en los activos en Información

- Los colaboradores de la entidad deben actuar como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Lider de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

- Los colaboradores deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo los lineamientos de Gestión documental designados por la empresa.
- Los colaboradores deben monitorear periódicamente la validez de los usuarios y sus 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 área de Sistemas 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 área de Sistemas 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 área de Sistemas entregará la directriz para garantizar copias de seguridad de la información de los funcionarios.
- 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

ELABORADO POR: 	REVISADO POR: 	APROBADO POR:
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente

 Salud Sogamoso E.S.E. <small>Secretaría de Salud - Sogamoso</small>	GERENCIA Y SEGURIDAD DE LA INFORMACION	Código: GSI-P-36
		Versión: 02
		Fecha: 12/06/2017
		Página: 13 de 16

recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

7.7 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 computo de escritorio y portable) dispuestos para el cumplimiento de las funciones será reglamentado por el área de sistemas para los colaboradores de acuerdo a necesidad de uso.

7.7.1 Normas uso de periféricos y medios de almacenamiento

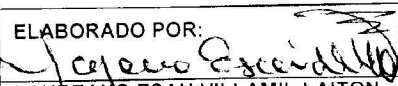
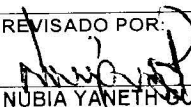
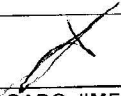
- El área de Sistemas establece las condiciones e implementa los controles que regulen el uso de medios de almacenamiento externos.
- El área de sistemas debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la información, ya sea cuando estén en producción,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

7.8 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.

7.9.1 Acceso a redes y recursos de red

- EL área de sistemas 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 área de sistemas 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.

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH QUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



7.9 ADMINISTRACIÓN DE ACCESO A USUARIOS

Salud Sogamoso E.S.E. a través del área de sistemas establecerá privilegios para el control de acceso lógico de cada usuario 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.

7.9.1 Administración de Acceso de Usuarios

- El área de sistemas establece mediante procedimiento GSI-P-012 administración de Usuarios en los Sistemas de Información.
- El Colaborador realiza la solicitud al área de Sistemas, 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.

7.10 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.

7.11.1 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

ELABORADO POR: 	REVISADO POR: 	APROBADO POR:
LAUREANO ESAU VILLAMIL LAITON Lider de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



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.
- Establecer 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.
- Deshabilitar las 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 están 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.

ELABORADO POR: 	REVISADO POR: 	APROBADO POR:
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente



BIBLIOGRAFIA

Ley 1341 de 2009 (Uso espectro) Par 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


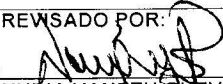
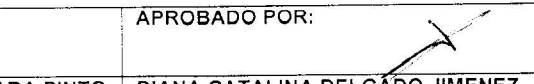
Resolución No 839 de 2017(Custodia HCL)

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

ELABORADO POR: 	REVISADO POR: 	APROBADO POR: 
LAUREANO ESAU VILLAMIL LAITON Líder de Recursos Informáticos	NUBIA YANETH GUEVARA PINTO Coordinadora de Calidad	DIANA CATALINA DELGADO JIMENEZ Gerente