FECHA DEL CAMBIO	DESCRIPCIÓN DEL CAMBIO	JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
25/01/2018	Elaboración del documento		1

1. OBJETIVO

Gestionar los riesgos que afectan la seguridad y confidencialidad de la información de la Ese Salud del Tundama, a través de un despliegue e implementación en todos los usuarios, así como las medidas que mitiguen o controlen los riesgos de confidencialidad de la información.

2. ALCANCE

Desde la identificación de riesgos asociados de la información hasta su control y mitigación.

3. RESPONSABLE O DUEÑO DEL PROCESO

Lider del proceso de sistemas de la información.

4. SOPORTE LEGAL Y DOCUMENTAL

- Ley 603 del 2000 por la cual se reglamenta la protección de los derechos de autor en Colombia.

- Ley 1273 del 5 de Enero de 2009 por la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- Ley 1341 del 30 de Julio de 2009 Por la cual se definen los 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 de Espectro y se dictan otras disposiciones.

- Ley 1581 de 2012 Por la cual se establece la protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-48 de 011 de la Corte Constitucional: Proyecto de Ley Estatutaria de Habeas Data y Protección de datos personales.

- Artículo 269A: Acceso abusivo a un sistema informático. El que sin autorización por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro de mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mensuales vigentes.

- Artículo 269B Obstaculización ilegítima de sistema informático o red de telecomunicación…incurrirá en pena de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios legales vigentes.

- Artículo 269C. Interceptación de datos informáticos. El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Artículo 269D: Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos o un sistema de tratamiento de información o sus partes componentes lógicos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos mensuales vigentes.

- Artículo 269E Uso de software malicioso. El que sin estar facultado para ello produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos vigentes.

- Artículo 269F: Violación de datos personales. El que sin estar facultado para ello con provecho propio o de un tercero, obtenga, compila, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos mensuales vigentes.

- Artículo 269G. suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programa o envíe páginas electrónicas, enlaces o ventanas emergentes incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses en multa de 100 a 1000 salarios mensuales legales vigentes.

- Resolución 1460 del 30 de octubre de 2015: Por la cual la ESE SALUD DEL TUNDAMA adopta la política de Confidencialidad y Seguridad de la Información.

- Resolución 302 del 06 de abril de 2016. Por la cual la Ese Salud Del Tundama adopta la política de Gestión Documental.

- Manual de Atención al usuario: aprobado 04/12/2014.

- Resolución 224 del 03 de marzo de 2015 por la cual la Ese Salud Del Tundama adopta la política de Gestión de la Tecnología.

- Plan anticorrupción y atención al ciudadano vigencia 2016 Ese Salud Del Tundama.

- Plan de Gestión Institucional Vigencia 2016-2020. Gestión administrativa.

- Norma ISO 27001: SO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa

5. DEFINICIONES

- **Amenaza:** Es una situación o acontecimiento que puede causar daño a los bienes informáticos físicos o magnéticos, puede ser una persona, un programa malicioso un suceso natural o de otra índole que representan los posibles atacantes o factores que inciden negativamente en la seguridad de la información.

- **Riesgo**: Probabilidad que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la entidad.
- **Análisis de riesgo:** Es un proceso dirigido a determinar la posibilidad que las amenazas se materialicen sobre los bienes informáticos ya sean físicos o magnéticos e implica la identificación de la información a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que pueden cause.

- **Bienes informáticos**: Elementos, componentes, documentos físicos y magnéticos que deben ser protegidos para evitar la ocurrencia de una amenaza.

- I**mpacto**: Es el daño producido por la materialización de una amenaza contra la seguridad de la información.

- **Riesgo aceptable**: El riesgo se encuentra en un nivel que se puede aceptar sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

- **Seguridad**: es usada para minimizar los riesgos a que están expuestos los bienes informáticos sean físicos o magnéticos.

- **Vulnerabilidad**: En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos fiables o atacables en el sistema de información y califican el nivel de riesgo del mismo.

6. DESARROLLO DEL PROGRAMA

Para garantizar y preservar la información

El programa de seguridad de la información se conforma de un conjunto de proyectos, iniciativas y actividades realizadas de manera coordinada para lograr una estrategia de seguridad, es decir, llevar a la práctica un plan trazado que busca alcanzar los objetivos de protección de una organización.

La gestión del programa pretende dirigir, monitorear, evaluar y mejorar todas las actividades relacionadas con la seguridad, por lo que debe considerar y

utilizar los recursos de manera óptima, así como brindar información oportuna que permita tomar las mejores decisiones para la protección de la entidad, la información y otros activos.

El principal elemento que se debe tener en cuenta antes de la puesta en marcha del programa es el **respaldo de la alta dirección** con relación a las actividades de seguridad de la información. El soporte y compromiso de la alta dirección refleja un esfuerzo de toda la entidad para que todos sin excepción hablen el mismo idioma.

Es imprescindible contar con el apoyo de cada uno de los procesos y subprocesos creados en la entidad y la labor de los líderes es básica para lograr la colaboración y cooperación de todos los funcionarios y colaboradores.

En este sentido, una buena práctica consiste en desarrollar la estructura adecuada para la toma de decisiones en torno al programa, a través de la conformación de un **comité de seguridad de la información**, que permita la implementación de lo que se ha denominado gobierno de seguridad de la información, es decir, todas aquellas responsabilidades y acciones que ejerce la alta dirección en cuanto a la seguridad.

Estrategia:

El programa de seguridad es el resultado de una estrategia trazada para proteger a la organización y sus activos; por lo tanto, debe perseguir objetivos específicos que se desean alcanzar. Debe provenir de diferentes enfoques, por ejemplo, la alineación con los objetivos estratégicos de la empresa. Otro enfoque establece que puede tratarse del resultado de una evaluación de riesgos de seguridad.

Debemos ser cuidadosos a la hora de elegir nuestras contraseñas en nuestro computador del trabajo, existe información y se realizan operaciones cuya repercusión económica y personal es muy importante. Esto afecta los sistemas de la ESE Salud Del Tundama y equipos informáticos, así como a la privacidad del usuario.

- Se deben utilizar al menos 8 caracteres para crear la clave.
- Se recomienda utilizar en la contraseña dígitos, letras y caracteres especiales.

- Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas.
- Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado
- Cambiar las contraseñas con una cierta regularidad.

Se deben evitar la creación de contraseñas inseguras:

- No debe utilizar la misma contraseña siempre en todos los sistemas.
- No utilizar información personal en la contraseña.
- Hay que evitar utilizar secuencias básicas de teclado (por ejemplo:" qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
- No repetir los mismos caracteres en la misma contraseña.
- No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
- No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma.
- No enviar nunca la contraseña por correo electrónico o en un mensaje de texto.
- Cambiar las contraseñas por defecto proporcionadas por desarrolladores / fabricantes.

Asignación de claves para Prevenir accesos no autorizados

Previa solicitud por parte del líder del proceso o de talento humano, el proceso de sistemas de información asigna al personal de la institución que lo requiera clave personal para lo cual debe acercarse a la oficina y obtenerla, una vez realizado este proceso se obligara al usuario a que al primer ingreso al sistema la cambie para que solo él tenga en su poder la clave de su usuario de acceso al sistema de información.

Renovación de los equipos:

Ver Procedimiento para la Renovación de tecnologías.

Identificación de riesgos asociados

Este análisis lo realiza el Comité de Seguridad de la Información quienes acordarán planes de contingencia. En lugar de basarse en una evaluación

anual de los riesgos, gestiona el riesgo en sus redes desplegadas de forma continua. Las vulnerabilidades se investigan y se gestionan a diario. Las vulnerabilidades críticas que pudieran producir una revelación, alteración o destrucción de datos confidenciales se convierten en incidentes de seguridad de la información para lo cual se debe diligenciar el formato de incidentes de la información, los cuales deben ser investigados y analizados en el Comité de seguridad de la información.

Cómo prevenir la perdida de información

1- Conocimiento y aplicación de la política de seguridad de la ESE Salud del Tundama

Todos los colaboradores deben conocer la política de seguridad de la información con el objetivo de que todos los empleados conozcan cuán importante es la protección de la información para la empresa. El material debe ser entregado y debidamente explicado al empleado al momento de su ingreso en la institución. También se recomienda solicitar su compromiso para el cumplimiento de dichas normas a partir de la firma de un documento de consentimiento.

Para garantizar la confidencialidad de la información propia de la institución se debe realizar con la entrega del cargo o contrato el empalme con la entrega relacionada de la información, documentación propia del proceso que se recibe

2- Actualización automática de antivirus y anti spam

La ESE Salud Del Tundama através del proceso de sistemas de la información garantiza la correcta actualización del antivirus y las herramientas anti spam, con una periodicidad mensual, la cual depende del servidor antivirus.

3- Bloqueo de los códigos maliciosos

Evitar instalar programas no autorizados o descargar contenidos innecesarios ya que estos pueden acarrear malware - acrónimo de malicioso software, es decir, software malicioso- que conlleva a la vulnerabilidad del equipo y de la información contenida en ellos.

4- Precaución en el transporte y almacenamiento de la información

Se debe tener cuidado con la información importante y relevante de la ESE Salud Del Tundama, no se puede dejar a la mano de cualquier persona o en carpetas de acceso público en los equipos o en medios extraíbles (USB, CD, DVD, etc.), ya que estas pueden pasar de una a otra persona y la información puede caer en manos no autorizadas.

5- Contraseñas fuertes y seguras

Se debe garantizar utilizar contraseñas seguras es decir debe ser fácil de recordar y difícil de descifrar, se recomienda no utilizar las mismas contraseñas en los aplicativos institucionales y personales y no almacenar las claves en algún lugar visible o de fácil acceso, una vez creada la(s) clave(s) de acceso a los software institucional el usuario deberá cambiarla para que sea él, el único en tener las contraseñas de acceso a los sistemas.

6- Evitar correos electrónicos que no provengan de un remitente de confianza

Para minimizar problemas de virus en red se recomienda no abrir en los equipos de la ESE Salud Del Tundama, correos que no se conozca el remitente, o el envió de correos masivos de cadenas o similares, de este modo se minimizará la posibilidad de infectarse con códigos maliciosos y ser víctima de casos de robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza.

7- Cuidar la información de la empresa incluso fuera del ámbito corporativo

Cuando se trasladan documentación y papeles de importancia para trabajar fuera de la ESE Salud Del Tundama, se debe tener especial cuidado en lo que respecta al robo o pérdida de los mismos. Además, tales documentos deben ser manipulados teniendo en cuenta el nivel de confidencialidad que requieren. En caso de que se utilicen dispositivos de almacenamiento USB o CD, DVD, etc., siempre es necesario realizar un análisis con un antivirus al momento de insertarlos en el equipo.

8- Realizar copia de seguridad de su información

Verificar que el área de sistemas de información este realizando las respectivas copias de seguridad de los archivos importantes y de confidencialidad de la Ese Salud Del Tundama, para que ante cualquier avería en sus dispositivos (PC, USB, CD, DVD, etc.) se cuente con un respaldo de su información.

9 – Proceso de backup y a que se le realiza backup

Los backups se realizan a la información de vital importancia de la ESE Salud del Tundama y a las bases de datos de los softwares institucionales que se tengan.

Backup de archivos de Colaboradores (Archivos utilizados por el personal de la ESE Salud Del Tundama, de carácter laboral).

1. Backup del Software Institucional, backup de los Datos y de estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, tablespaces, usuarios, roles y todo archivo necesario para el funcionamiento de los Sistemas de Información de la ESE Salud del Tundama para la pronta recuperación de los mismos en caso de fallas).

    1. Backups archivos colaboradores.

El proceso de backups de equipos de los colaboradores se realiza a todos los equipos del área administrativa, y en el área asistencial a los que cada líder de proceso determine como importantes o susceptibles de realizar el respaldo de la información. En la tabla 1 se describe el procedimiento para generar los backups de los colaboradores.

Tabla 1. Procedimiento backups archivos colaboradores

Nº	Actividad	Responsable	Documento
1	Se determinan e identifican los archivos a respaldar en los equipos en las diferentes áreas. Solo se deben almacenar los archivos correspondientes a información vital de la ESE Salud Del Tundama, nada archivos de música o fotos y videos personales.	Funcionarios o colaboradores a cargo del equipo y que maneja archivos institucionales importantes.	

2	Los funcionarios o colaboradores colocan la información institucional importante, critica y confidencial en una única carpeta habilitada para tal fin, la cual se les da a conocer una vez ingresan a la institución.	Funcionarios o colaboradores a cargo del equipo y que maneja archivos institucionales importantes.	Carpeta creada en el equipo de cada colaborador
3	Se verifica que la información que los colaboradores o funcionarios están almacenando en la carpeta, sea la correcta, se realizan filtros aleatorios para verificar y garantizar la información a respaldar.	Oficina De Sistemas De Información.	
4	Se verifica que el programa de creación de copias de seguridad las esté realizando correctamente.	Oficina De Sistemas De Información.	Personal backup programa para la copia de seguridad
5	La periodicidad de las copias de seguridad de los equipos de los colaboradores se realiza todos los días al arranque del equipo de trabajo.	Oficina De Sistemas De Información.	
6	Se realiza semanalmente copias de seguridad, de los archivos de los equipos de los colaboradores a un disco externo.	Oficina De Sistemas De Información.	
7	Fin		

Nota: Para copias grandes se usan discos externos, los archivos que tengan el mismo nombre se eliminaran automáticamente y quedara el más reciente.

Tiempo de respaldo de archivos en medio magnético.

2. Backup bases de datos software institucional.

En la actualidad se realiza copias de seguridad al software institucionales como se muestra en la tabla 2.

Softwars institucionales

- Panacea – Histórico de historias clínicas.
- Dinámica Gerencial - Histórico de historias clínicas.

- ASÍS – Software institucional actual para el manejo de la parte asistencial.
- Génesis – Software para el manejo de la parte presupuestal y contable de la Ese Salud del tundama.
- Almera: Software de gestión de la calidad.

Tabla 2. Procedimiento backup bases de datos software institucional

Nº	Actividad	Responsable	Documento
1	Verificación de las bases de datos de los diferentes softwares institucionales que se tiene en la ESE Salud Del Tundama y a los cuales se les debe realizar copia de seguridad.	Oficina De Sistemas De Información	
2	Creación de tarea programada para la realización de las diferentes copias de seguridad de las bases de datos	Oficina De Sistemas De Información	
3	Se realiza copia de seguridad todos los días en horas de la noche. En horas del medio día será hará una copia incremental de lo realizado en horas de la mañana.	Oficina De Sistemas De Información (Técnico Operativo)	Se llena formato REGISTRO COPIA DE RESPALDO BASE DE DATOS, registrando la correcta creación de la copia de seguridad.
4	Verificación de la correcta creación de las copias de seguridad del software institucionales.	Oficina De Sistemas De Información	
5	Semanalmente se extrae la copia más reciente y se almacena en disco externo, para en caso de emergencia realizar la respectiva restauración de la misma.	Oficina De Sistemas De Información	
6	Fin		

11. Cláusula de confidencialidad y manejo de la información

Ver POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACIÓN**.**

12. Uso de los equipos

Los equipos sólo pueden ser manipulados por personal VINCULADO MEDIANTE CONTRATO de prestación de servicios o de planta entrenada y capacitada que cumplan los siguientes requisitos que deben estar estipulados en el contrato de servicios, a saber:

- Personas idóneas, capacitadas y entrenadas en el correcto uso de los diferentes equipos a su cargo.
- Que cumplan con el código de ética
- Cláusula sobre manejo de la información y seguridad de la misma.
- Adherirse a la política de confidencialidad de la información de la Ese Salud del Tundama.

7. ESTRATEGIAS DE SENSIBILIZACIÓN

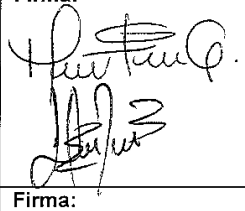
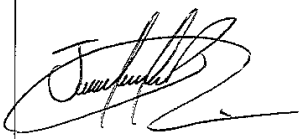
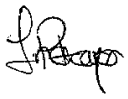
- Acordadas con líder de comunicaciones.

8. INDICADORES

Los estipulados en el tablero de mando de indicadores de gestión (Ver software institucional).

9. DOCUMENTOS REFERENCIA

Estándares de seguridad ISO 27000

Elaborado por:	**Cargo:**	**Fecha:**	**Firma:**
María Fernanda Gallo Pesca Edwin Andrés Romero Agudelo	Miembros Equipo de autoevaluación de Estándares de Gerencia de la información	25/01/2018	
Revisado por:	**Cargo:**	**Fecha:**	**Firma:**
Diana Carolina Azula	Asesora Acreditación	19/02/2018	
Jenith Lorena López	Líder Mejoramiento Continuo	16/03/2018	
Lina Patarroyo	Profesional de apoyo Gestión de Mejoramiento Continuo	22/03/2018	
Aprobado por:	**Cargo:**	**Fecha:**	**Firma:**
Claudia Marina García Fernández	Gerente	02/04/2018