# AUDITORÍA A LA PROTECCIÓN DE LOS DATOS SOBRE LA HISTORIA CLÍNICA ELECTRÓNICA DE LA E.S.E. MUNICIPAL MANUEL CASTRO TOVAR.

MAURICIO ANDRES NEUTA ARTUNDUAGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO - HUILA
2019

# AUDITORÍA A LA PROTECCIÓN DE LOS DATOS SOBRE LA HISTORIA CLÍNICA ELECTRÓNICA DE LA E.S.E. MUNICIPAL MANUEL CASTRO TOVAR.

MAURICIO ANDRES NEUTA ARTUNDUAGA

Proyecto aplicado presentado como requisito para optar al título de Especialista en Seguridad Informática

Asesor de proyecto:
Edgar Roberto Dulce

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO - HUILA
2019

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pitalito, 28 de Noviembre de 2019

## DEDICATORIA

Con este proyecto quiero darle la gloria y honra a Dios primeramente por darme la fortaleza y perseverancia cada día de seguir mis sueños y de poder ver realizados mis metas junto a mi familia, este logro sin lugar a dudas está dedicado a Él.

A mi amada esposa pos su amor, paciencia y apoyo incondicional que me brindo día tras día en el transcurso de este proceso académico.

A mi amado hijo Emiliano que con su ternura y dulzura me motiva y me anima para ir por cosas mayores.

Mauricio Andrés Neuta Artunduaga

## AGRADECIMIENTOS

Agradecer al Dios de la gloria por darme primeramente el don de la vida, y sobre todo por darme la capacidad y la fortaleza de poder ver realizado este triunfo más en mi vida, agradezco a mi familia por su comprensión y apoyo incondicional en el transcurso de este proceso profesional.

Al asesor asignado Edgar Roberto Dulce por su tiempo valioso y disposición en el momento que lo necesite para direccionarme hasta este punto.

A la Ingeniera Yolima Esther Mercado, tutora de la UNAD, por estar atenta a las inquietudes generadas en cada tarea del curso.

## RESUMEN

En estos últimos años se ha evidenciado en Colombia, con gran insistencia, temas de interés acerca de la protección de datos personales, en especial con la expedición de las normas que desarrollan el principio constitucional de protección de la intimidad y la información (ley 1266 de 2008 y ley 1581 de 2012). Aunque estas normas afectan especialmente al sector financiero, crediticio, comercial y de servicios, no son los únicos a quienes regulan estas normas, existe un sector con gran relevancia que maneja datos tan importantes y especiales que han sido denominados “datos sensibles” y precisamente se trata del sector salud.

A la luz de la ley 1581 de 2012, que regula el manejo y tratamiento de los datos personales, el artículo 5 indica como categoría de datos especiales a los datos sensibles, señalando que “se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación,….”[1], dentro de estos se incluyen los datos concernientes a la salud, por ende las historias clínicas y todos los datos relacionados con la salud de una persona son sensibles y de obligatoria protección por parte de las entidades responsables que tengan relación con dichos datos.



**Palabras Clave**: historias clínicas, salud, registros médicos, normativa, auditoría, control, estrategias, procesos, actividades, plan.


[1] Superintendencia de Industria y Comercio. Políticas de tratamiento de la información personal en la superintendencia de industria y comercio. Ley 1581 de 2012. P.2. Disponible en: http://www.sic.gov.co/sites/default/files/documentos/Politicas_Habeas_Data_0.pdf

## ABSTRACT

In recent years there has been much talk in Colombia about the protection of personal data, especially with the issuance of rules that develop the constitutional principle of protection of privacy and information (Law 1266 of 2008 and Law 1581 of 2012). Although these rules especially affect the financial, credit, commercial and services sectors, they are not the only ones to whom these regulations are regulated, there is a highly relevant sector that handles such important and special data that have been called "sensitive data" and precisely It deals with the health sector.

In light of Law 1581 of 2012, which regulates the handling and processing of personal data, Article 5 indicates as a category of special data sensitive data, noting that "sensitive data is understood to be those that affect the privacy of the owner or whose improper use can generate their discrimination, ... ", within these the health-related data are included, therefore the clinical histories and all the data related to the health of a person are sensitive and of obligatory protection on the part of the responsible entities that are related to said data.



**Keywords**: medical records, health, medical records, regulations, audit, control, strategies, processes, activities, plan.

**CONTENIDO**

Pag

## LISTADO DE FIGURAS

Pag.

## LISTADO DE TABLAS

Pag.

## ANEXOS

Pag.

## GLOSARIO

**CONFIDENCIALIDAD**: Método de seguridad que brinda a los sistemas de información, restringir el acceso de personas no autorizadas, con el fin de proteger sus datos.

**DISPONIBILIDAD**: Método de seguridad que brinda a los sistemas de información que los datos tratados sean accesibles únicamente a solicitud de los usuarios del sistema.

**INTEGRIDAD**: Método de seguridad que brinda a los sistemas de información, proteger la exactitud y conservación completa de los datos.

**VULNERABILIDADES**: Es la debilidad que presenta un control de seguridad y que por su susceptibilidad puede ser aprovechada por las diferentes amenazas.

**RIESGOS**: Es la posibilidad de que se presente una eventualidad e impacte de forma negativa sobre la información.

**AMENAZAS**: Es la acción que se presenta de forma inesperada con la capacidad de ocasionar consecuencias críticas al aprovecharse de las vulnerabilidades presentes en los sistemas de información.

**SGSI**: Sistema de Gestión de la Seguridad de la Información.

**HCE**: Historia Clínica Electrónica.

**CONTROL**: Es el método de salvaguardar o contrarrestar los posibles riesgos y amenazas presentadas en la organización. Permite dentro de la política de seguridad las buenas prácticas de uso de la información.

**POLÍTICA DE SEGURIDAD**: Son todos los mecanismos y procedimientos de seguridad que se utilizan dentro de la organización para hacerle frente a los diferentes riesgos y amenazas de seguridad que puedan surgir.

**SEGURIDAD DE LA INFORMACIÓN**: Es el mecanismo de seguridad para conservar la confidencialidad, integridad y disponibilidad de la información.

**EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Es toda condición que presenta un sistema de información y que indica una probabilidad de violación a los controles de seguridad.

**AUTENTICIDAD**: Es el proceso de verificación de identidad que la persona solicita a un recurso informático por medio de un sistema de control de acceso.

**ANÁLISIS DE RIESGOS**: Es el proceso de análisis e identificación para medir y estimar el riesgo.

**GESTIÓN DEL RIESGO**: Es el conjunto de todas las actividades sistemáticas para administrar y controlar el riesgo dentro de la organización.

**TRATAMIENTO DEL RIESGO:** Es el mecanismo de implementación de medidas de seguridad para reformar el riesgo.

**VALORACIÓN DEL RIESGO**: Es el procedimiento de análisis, verificación y evaluación de los riesgos.

# INTRODUCCIÓN

Un dato personal es toda aquella información concerniente a un individuo que lo identifica y caracteriza ante una sociedad y que puede tener trascendencia para su intimidad. A partir de esta premisa, un dato puede estar relacionado con: “datos de identificación, datos laborales, datos patrimoniales, datos académicos, datos ideológicos, datos de salud, características personales y físicas, vida y hábitos sexuales”[2]. Hay determinados datos que por su gran relevancia en cuanto a la confidencialidad y privacidad deben tener un tratamiento más amplio y estricto, estos datos son llamados “Datos sensibles”. Los datos sensibles, o también conocidos como datos especialmente protegidos, son una clase de datos que debido a su incidencia especial en la intimidad, pueden afectar las esferas más íntimas de las personas, y que su revelación clandestina puede causar daño al honor y la intimidad del individuo. Estos datos requieren mayor protección y la Ley establece un tratamiento especial.

La protección de los datos personales se ha venido constituyendo como un derecho fundamental en Colombia bajo disposiciones de normas legales (ley 1266 de 2008 y ley 1581 de 2012), que conlleva a una protección especial a los datos personales de los individuos en todas sus etapas, esto quiere decir, desde su recolección, almacenamiento, tratamiento hasta su transferencia. Esta ley cuida la información confidencial y privada registrada en cualquier base de datos o archivos, garantizando que la información estará segura y que personas malintencionadas no accederán a los datos vulnerando las condiciones de seguridad y privacidad de información de las personas.

El presente proyecto tiene como objetivo principal, establecer una auditoría a la red de datos en la gestión de la Historia Clínica Electrónica (HCE), en la E.S.E Municipal Manuel Castro Tovar de Pitalito. Cabe resaltar que en los últimos años se ha proporcionado gran importancia a la gestión de las Historias Clínicas, teniendo en cuenta que la información tratada por ser de tipo confidencial solicita de un tratamiento especial. Es así, que esta propuesta de trabajo se hace necesaria debido a que se logra evidenciar el aumento en la producción de información clínica sin el tratamiento documental pertinente.

Para el desarrollo del presente proyecto se tomará como referencia la norma ISO/IEC 27001:2013, ya que es una norma internacional establecida por la ISO

[2] Lawyou. 24 de octubre de 2017. Datos personales (LOPD). Disponible en https://lawyoulegal.com/datos-personales-lopd/

(Organización Internacional de Normalización) cuyo fin es la de proteger la información más importante de las organizaciones, además de dar a conocer los requisitos de implementación, mantenimiento y mejora continua de un SGSI (Sistema de Gestión de Seguridad de la información) en las empresas.

# 1. PLANTEAMIENTO DEL PROBLEMA

La historia clínica y los datos de salud están estrechamente relacionados con el estado íntimo y personal de un individuo, es así que dentro de la conservación, guarda, custodia y protección, las entidades de salud y las personas facultadas de su manejo y tratamiento deben aplicar controles y políticas que garanticen los principios fundamentales de la protección de datos personales.

Cuando las organizaciones no cuentan con un buen sistema de control que garantice la protección y seguridad de la información, comienza a emerger y a identificarse todas aquellas debilidades y amenazas que ponen en riesgo la información confidencial y privada de las personas, en este caso, los datos sensibles o datos de especial protección.

Es importante destacar que la Historia Clínica "es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley"[3]. Precisamente algunas de las falencias más relevantes que se pueden resaltar en la administración de los datos sensibles en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar, es que no existe un control adecuado en el tratamiento de la información ya que los registros almacenados son vulnerables por manejos inapropiados, enfrentándose a la falta de garantías en la seguridad y confidencialidad en la información.

Otros factores que afectan directamente la seguridad de la información en la Historia Clínica Electrónica de la empresa, es el libre acceso y sin restricciones por la mayoría de las dependencias tanto misionales como administrativas a los datos de caracterización y de atención de los usuarios, que por cierto, son los únicos dueño y propietarios de la información. Es precisamente este acceso sin restricciones que cualquier funcionario de la empresa puede tanto visualizar, revelar como imprimir los registros personales y de atenciones de los usuarios, violando así el principio de privacidad de la información.

[3] Ministerio de Salud. Resolución número 1995 de 1999. Artículo 1. (Julio 8). P.1. Disponible en: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

En seguridad informática la confidencialidad requiere de un principio, que la información sea accesible de forma única por las personas que se encuentran autorizadas. Esto quiere decir, que es requisito acceder a la información mediante autorización y control, con el fin de mantener en secreto determinada información o recursos.

Un aspecto más a resaltar es que se pierde el secreto profesional que es inviolable, la Ética Médica define lo siguiente: "Entiéndase por secreto profesional médico aquello que no es ético o lícito revelar sin justa causa. El médico está obligado a guardar el secreto profesional en todo aquello que por razón del ejercicio de su profesión haya visto, oído o comprendido, salvo en los casos contemplados por disposiciones legales."[4] Este hecho viola el principio de confidencialidad de la información.

Otra anomalía que viene presentándose en la historia clínica electrónica es la manipulación, alteración y/o modificación de los datos sin plena autorización, ocasionando de esta manera una violación al principio de integridad de la información.

Teniendo en cuenta la problemática planteada, se ha definido la siguiente pregunta de investigación:

¿Es posible mediante el proceso de la auditoria, respecto a la protección y manejo de confidencialidad de los datos sensibles que reposan en la Historia Clínica electrónica de los usuarios en la E.S.E. Municipal Manuel Castro Tovar, mejorar su seguridad de la información?

[4] Encolombia. Secreto Profesional. Ley 23 de 1981. Artículo 37. Disponible en: https://encolombia.com/medicina/guiasmed/mision-medica/modulo3misionmedica11/

## 2. JUSTIFICACIÓN

El tratamiento de los datos sensibles en el sector salud, requieren del compromiso, cuidado y responsabilidad absoluta de las entidades de salud y los profesionales que tienen acceso a ellos, por ende también de obligatorio cumplimiento para ellos la ejecución de manuales de controles y políticas de tratamiento de datos y en especial el establecimiento de los métodos necesarios para asegurar en los titulares de los datos y la información en salud la garantía constitucional de la protección de la intimidad y la información.

Incurrir en la violación de las normas de privacidad y seguridad puede perjudicar el buen nombre de una entidad y, en el peor de los casos, afectar la relación entre los pacientes de la entidad y los profesionales de la salud. Se ha podido evidenciar que los entes de control que vigilan la prestación de los servicios de salud en Colombia han imputado sanciones significativas a las empresas de salud que no han garantizado la protección de los datos básicos de los pacientes, teniendo en cuenta que esta situación puede afectar la privacidad de las personas.

La confidencialidad en nuestros tiempos actuales es el común denominador de los usuarios que en cierta forma sienten que su información privada y sensible es vulnerable, por consiguiente, se estima importante el análisis de la gestión de la Historia Clínica Electrónica, teniendo en cuenta que se está tratando información confidencial y que requiere de un manejo especial. Condiciones que están siendo perjudicadas debido a manejos inapropiados en las empresas que custodian y resguardan la información, implicando que los datos alojados en la historia clínica del paciente resulten afectados, manipulados, y en el peor de los casos, que la información termine en manos ajenas de sus propietarios.

El desarrollo de este proyecto involucra un conjunto de procesos y acciones de mejora, por lo que se ve la necesidad de generar nuevas procesos y métodos para la administración de los datos de la Historia Clínica Electrónica, ya que se superarían algunas brechas de seguridad que se hacen evidentes en el uso y manejo de esta información que se encuentra disponible en la historia.

Para medir el grado de privacidad de los datos sensibles de los usuarios, es relevante primeramente conocer el funcionamiento del sistema de información que administra actualmente la Historia Clínica Electrónica, debido a que cada vez más se está haciendo uso en las empresas que prestan servicios de salud este soporte electrónico, abandonando en cierta forma el proceso tradicional del

diligenciamiento de papel de la historia clínica. Con este plan de trabajo se quiere ahondar un poco más en la estructura del sistema de información que gestiona la información, para conocer de esta manera los factores y causas que están afectando los estandartes primordiales de la seguridad de la información, en otras palabras, que afectan negativamente la confidencialidad, integridad y accesibilidad de la información.

Es importante resaltar, que el dueño de la información es única y exclusivamente cada una de las personas o usuarios que voluntariamente facilitan sus datos para su respectivo y oportuno uso haciendo del individuo el mayor beneficiario, por ende, debe brindarse la confianza y seguridad de que la información de los usuarios está cien por ciento protegida, respetando los principios de seguridad en cuanto integridad y calidad de los datos.

Para el estudio de este caso, la auditoria es la mejor herramienta a implementar ya que por medio de este proceso se podrá planificar las diferentes tareas y los objetivos para lograr los resultados determinados; también se podrá implementar las acciones necesarias para alcanzar las mejoras trazadas; se podrá realizar un proceso de verificación que consiste en establecer un periodo de prueba para medir y valorar la efectividad de los cambios y por último, facilita el proceso de actuar sobre las correcciones y modificaciones necesarias, además que brinda la oportunidad de toma de decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Realizar una auditoría, relacionando la protección y manejo de confidencialidad de los datos sensibles que reposan en la Historia Clínica electrónica de los usuarios en la E.S.E. Municipal Manuel Castro Tovar.

## 3.2 OBJETIVO ESPECÍFICOS

- Analizar la eficiencia del sistema de información en cuanto a la protección de los datos sensibles de la Historia Clínica electrónica y verificar el cumplimiento de la norma en cuanto a la confidencialidad de los datos en la misma.

- Ejecutar un plan de auditoria, definiendo los métodos, procesos, técnicas, procedimientos, pruebas y solicitud de documentos para que este se lleve a cabo satisfactoriamente.

- Elaborar un informe final de la auditoria con los hallazgos y recomendaciones respectivas para que la E.S.E. Municipal establezca un plan de mejoramiento y un sistema de control adecuado.

# 4. MARCO REFERENCIAL

## 4.1 MARCO INSTITUCIONAL

"La E.S.E. Municipal MANUEL CASTRO TOVAR, es una entidad pública descentralizada, de carácter municipal y categoría especial, creada mediante Decreto 017 de 19 de marzo de 1999, emitido por el Despacho de la Alcaldía Municipal de Pitalito, en virtud de las facultades especiales otorgadas al Ejecutivo Municipal, por la Corporación Edilicia, como se acredita con los Acuerdos 039 de 1998 y 009 de 1999. De esta manera, mediante Acuerdo 009 de fecha 26 de Febrero de 1999, la Junta Directiva de la EMPRESA SOCIAL DEL ESTADO, denominó la misma como EMPRESA SOCIAL DEL ESTADO MUNICIPAL "MANUEL CASTRO TOVAR", denominación que subsiste"[5].

### La Misión

"Contribuir a mejorar la calidad de vida de los usuarios del Municipio de Pitalito, brindando servicios de salud de baja complejidad equitativos, oportunos, asequibles y con sentido humanitario. Logrando cobertura total en la promoción de la salud, prevención, tratamiento y cura de la enfermedad; con talento humano idóneo, tecnología adecuada y procesos de atención enfocados a loa satisfacción de las partes interesadas y el mejoramiento continuo de la Institución"[6].

### La Visión

"En el año 2020, seremos una ESE de baja complejidad de atención, reconocida en el sur del Departamento por la innovación en la implementación de los programas de promoción de la salud y prevención de la enfermedad con enfoque humanizado y de seguridad del paciente, aplicando estándares de mejoramiento continuo en todos los procesos Institucionales, con tecnología de punta, equipo humano altamente comprometido y una comunidad participativa para asegurar rentabilidad económica. Social y Desarrollo Empresarial"[7].

---

[5] E.S.E. Municipal Manuel Castro Tovar. 2017. Portafolio de servicios. Disponible en http://esemanuelcastrotovar.gov.co/wp-content/uploads/2017/07/Portafolio-de-Servicios-ESE-MCT.pdf. P.2.

[6] E.S.E. Municipal Manuel Castro Tovar. 2017. Portafolio de servicios. Disponible en http://esemanuelcastrotovar.gov.co/wp-content/uploads/2017/07/Portafolio-de-Servicios-ESE-MCT.pdf. P.3.

[7] E.S.E. Municipal Manuel Castro Tovar. 2017. Portafolio de servicios. Disponible en http://esemanuelcastrotovar.gov.co/wp-content/uploads/2017/07/Portafolio-de-Servicios-ESE-MCT.pdf. P.3.

**Política de Calidad**

"El compromiso Institucional de la ESE Manuel Castro Tovar es trabajar en la implementación de una cultura de atención humanizada resaltando la integridad, el respeto y la igualdad, con el propósito de dar respuesta a las necesidades del usuario, su grupo familiar y las partes interesadas, con personal altamente comprometido en el cumplimiento de estrategias innovadoras e incluyentes, que abanderen los valores y principios corporativos garantizando desde todas las áreas y servicios el cuidado de la salud, la solución efectiva de las enfermedades y la plena satisfacción de la comunidad laboyana"[8].

**Servicios Ofertados**

A continuación se presenta el portafolio de servicios ofertados por la E.S.E. Municipal Manuel Castro Tovar a todos sus beneficiarios.

- Medicina General.
- Odontología.
- Actividades de Protección Específica.
- Actividades de Detección Temprana.
- Laboratorio Clínico.
- Farmacia.
- Servicio de Ambulancia.
- PIC.
- Vigilancia Epidemiológica[9].

## 4.2 MARCO CONCEPTUAL

### 4.2.1 Historia Clínica Tradicional

Según la Resolución número 1995 de 1999 emanada por el Ministerio de Salud, define la Historia Clínica como "un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del

[8] E.S.E. Municipal Manuel Castro Tovar. 2017. Portafolio de servicios. Disponible en http://esemanuelcastrotovar.gov.co/wp-content/uploads/2017/07/Portafolio-de-Servicios-ESE-MCT.pdf. P.6.

[9] E.S.E. Municipal Manuel Castro Tovar. 2017. Portafolio de servicios. Disponible en http://esemanuelcastrotovar.gov.co/wp-content/uploads/2017/07/Portafolio-de-Servicios-ESE-MCT.pdf. P.11-16.

paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley"[10].

La historia clínica es una de las maneras de registro del proceder médico, cuyas aspectos más relevantes están implícitas en su elaboración y de las cuales se describen: Profesionalidad, hace referencia a que únicamente el profesional de salud se encuentran en la facultad de diligenciar una historia clínica adecuada; Ejecución típica, se refiere a que la medicina se practica teniendo en cuenta las normas de excelencia del momento; Objetivo, hace referencia al proceso de transcripción en la historia clínica; Licitud, hace referencia a que las mismas leyes o normas jurídicas amparan a la historia clínica como documento indispensable.

El proceso de registro de la Historia Clínica establece un documento primordial e imprescindible dentro de un sistema de información de salud, además, constituye el reporte completo del tratamiento en el transcurso de la atención prestada al paciente, es debido a esto su importancia como documento legal. La historia clínica ha estado reglamentada y regida por diferentes normas con base en la Ley General de Sanidad 14/1986; con la Ley 41/2002, donde infiere básicamente en la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Además, esta ley especifica textualmente la historia clínica, teniendo en cuenta sus múltiples funciones y usos, sus contenidos, soportes y preservación, de igual manera precisa las propiedades y características de custodia de la historia clínica, como también confidencialidad de la historia clínica.

Como característica principal, cada uno de los pacientes tiene obligatoriamente un único número de identificación, lo cual facilita el registro de toda la información asistencial que se le brinde en el transcurso de sus atenciones, como por ejemplo: consultas, servicio de urgencias y hospitalizaciones, entre otros. Toda esta información queda instantáneamente registrada y respectivamente con su número de identificación.

#### 4.2.1.1 Características de la Historia Clínica

Las características básicas son:

[10] Ministerio de Salud. Resolución número 1995 de 1999. Artículo 1. (Julio 8). P.1. Disponible en: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

- "**Integralidad**: La historia clínica de un paciente debe contener todos los datos concerniente a los aspectos técnicos y científicos que están estrechamente relacionados con la atención en salud, entre los cuales se mencionan: Promoción y Prevención, consultas asistenciales, impresión diagnóstica, tratamiento de la enfermedad, abordándolo en todas sus esferas como psicológico, social, personal, familiar y comunitaria.
- **Secuencialidad**: Toda la información resultante de la atención en salud del paciente debe quedar registrada y almacenada de forma cronológica en que ocurrió la atención.
- **Racionalidad científica**: Es la utilización de los conceptos científicos en el tratamiento de las acciones en salud ofrecidas al paciente, de tal forma que se evidencie clara y concisa, el procedimiento que se llevó a cabo en la atención de salud, esto quiere decir, impresión diagnostica y el plan de manejo.
- **Disponibilidad**: Es la posibilidad de acudir a la historia clínica cuando sea necesario teniendo en cuenta sus restricciones y privilegios de uso.
- **Oportunidad**: Es el oportuno diligenciamiento de la historia clínica una vez haya terminado la atención en salud del paciente"[11].

Considerando lo expuesto anteriormente, la Historia Clínica es un documento único e insustituible tanto para entidad prestadora de servicios de salud como para el paciente. En cuanto a la importancia de la Historia Clínica, se puede afirmar que este aspecto se debe precisamente a los datos que suministra el paciente al profesional de salud al momento de su atención, sin esta particularidad no habría un registro alguno de atención.

Ahora bien, su uso es obligatorio. Por ende, dentro de la historia clínica todas las atenciones que se lleven a cabo deben efectuarse su respectivo registro. Cabe recordar que es "irremplazable, es privada y pertenece al paciente." De igual manera es relevante resaltar que la historia clínica es la agrupación de varios atributos primordiales, como los son aspectos informativos, legales, funcionales y administrativos; claro está que, es necesario que cumpla con ciertos criterios normativos establecidos teniendo en cuenta su importancia y trascendencia.

#### 4.2.1.2 Función de la Historia Clínica

[11] Ministerio de Salud. Resolución número 1995 de 1999. (Julio 8). P.2-3. Disponible en: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf

La historia clínica es un elemento orientado primordialmente a brindar una asistencia apropiada al paciente. Teniendo en cuenta esta primicia es posible enumerar cinco funciones esenciales de la historia clínica: La primera función hace referencia a la asistencial, teniendo en cuenta que como documento reúne los aspectos de la impresión diagnóstica y el plan de manejo del paciente en el transcurso de su atención. La segunda función hace referencia a la docencia, ya que la historia clínica es un material fundamental para los pedagogos La tercera función hace referencia al área de la investigación, como base de partida para el estudio epidemiológico. La cuarta función hace referencia a la valoración de la calidad asistida del servicio, debido a que la historia clínica es un documento que permite determinar la calidad de la atención y sirve como soporte en los diferentes comités administrativos. Por último, está la función que hace referencia al documento médico legal, teniendo en cuenta que la información que tratada y procesada tiene un valor legal.

Además de estas funciones, existen otras que valen la pena resaltar: la historia clínica como fundamento para el planteamiento, ejecución y control en los procesos orientados a la recuperación y rehabilitación de la salud. Es indudable que la importancia de la historia clínica radica en que es un elemento esencial en el desarrollo de la atención valiéndose de respaldo y soporte en el cumplimiento de todas las actividades realizadas por el profesional, pues el mismo funcionario es el que tiene la obligación de consignar específicamente toda la información relacionadas con la atención del paciente dejando soporte y evidencia de dicha atención. Los datos registrados en la historia clínica se consideran como un argumento que posee gran peso y valor jurídico y que además debe preservarse en el transcurrir del tiempo. La historia clínica forma una línea ordenada de todos y cada uno de los sucesos y situaciones de la vida de un ser humano, por ende se le añade que tiene un compendio científico como soporte para la investigación médica.

La Ley 41/2002, en uno de sus apartados insta que la historia clínica tiene "como fin principal facilitar la asistencia sanitaria"[12]. Del mismo modo define otros usos legítimos de la historia clínica, como por ejemplo: fines legales, interviene en la salud pública, nexos epidemiológicos, en áreas de investigación, en el sector educación o docencia; para fines de procesos de calidad, procesos de acreditación, entre otros.

[12] Ley 41/2002. Artículo 15. (de 14 de noviembre). Ley de autonomía del paciente. Disponible en: http://www.auxiliar-enfermeria.com/lap_05.htm

#### 4.2.1.3 Componentes de la Historia Clínica

La historia clínica consta de diferentes componentes de información, esto quiere decir que los formularios son generados por medio de la atención del profesional de salud en el transcurso de la intervención. Algunos de los formularios o componentes que conforman la historia clínica son: informe de alta, que hace referencia al campo donde se hallan los datos relacionados con el lugar de atención, los datos personales del usuario y los datos que tienen que ver directamente con el proceso asistencial. De igual forma se encuentran los formularios del proceso clínico, notas de enfermería, las prescripciones hechas por el personal médico, resultados de paraclínicos, actividades realizadas por servicios, la hoja de referencia y contra referencia, formulario de autorización, y los componentes administrativos y operativos.

En el art.15 de la ley 41/2002 aborda temas acerca de la información mínima que la historia clínica que debe tener, por ejemplo: los soportes en relación al ingreso de la atención del servicio, reporte de urgencia, anamnesis y el examen físico, las órdenes médicas, reporte de interconsulta, el formulario del consentimiento informado obligatorio, el reporte de anestesia si es requerido, el reporte de la sala de parto si es requerido, la hoja evolución y asesoría de los buenos cuidados, soporte sobre los buenos hábitos alimenticios y de cuidado, y por último el informe clínico de alta.

Otros compendios puntualizan que los componentes de la historia clínica contienen la información considerada como relevante y vital sobre la realidad del estado actual de salud de los pacientes, tanto física como psicológica. Esta afirmación es importante, partiendo de la premisa que lo realmente trascendental y lo que al final importa, es que en los diferentes componentes de la historia clínica se encuentren todos los soporte y evidencias generadas en el transcurso de la atención y que efectivamente en estas hojas estén registrados absolutamente todos los datos concernientes al estado actual de salud de los pacientes, con el fin de que este proceso sea de utilidad como insumo a la hora de la impresión diagnostica oportuna y acertada, facilitando de esta manera la detección de posibles patologías por parte del personal misional.

#### 4.2.1.4 Tipos de Modelo de la Historia Clínica

Las historias clínicas son utilizadas acorde a cada centro de salud u hospital y teniendo en cuenta sus necesidades. Aun así, se pueden reconocer dos clases de historias clínicas: por un parte la historia estructurada teniendo como base las fuentes de información y por otro lado la historia estructurada teniendo como base la problemática de salud. Referente a la historia clínica estructurada teniendo

como base las fuentes de información también se le conoce como la famosa y conocida historia clínica tradicional. Dentro de sus aspectos a resaltar se tiene que la información que se registra en este tipo de historia se hace de manera cronológica sin excepción alguna. En cuanto a la historia clínica estructurada en base a la problemática de la salud, de igual manera se le conoce como el nuevo estilo. Al igual que la primera, esta historia se estructura de manera cronológica y los datos están previamente establecidos. Este tipo de historia clínica surge con el fin de que el profesional de salud tiene la responsabilidad de disponer sus historias de tal manera que al final resultara evidencia de la información básica obtenida en las atenciones de los pacientes.

Existe otro tipo de modelo de la historia clínica denominado ECOP (Expediente Clínico Orientado por Problemas). Este tipo de historia maneja la misma información que la historia tradicional, pero enfocado desde otra perspectiva. Sus partes son: implantación de información básica, generación de la problemática a resolver, impresión diagnostica, patología diagnóstico terminante, planes de manejo. De igual manera se dice que el ECOP puede determinar una mejor clasificación de los diagnósticos, brindado de esta forma optimizar las estadísticas de morbimortalidad, esto quiere decir que, ofrece y facilita una mejor planeación por la alta dirección y ayuda a la toma de decisiones acertadas.

### 4.2.2 Historia Clínica Electrónica

La Historia Clínica Electrónica tiene su punto de partida debido a que la Historia Clínica Tradicional, muestra ciertas deficiencias, que se pueden enumerar: el acopio y preservación que lleva al extravío de información, esta situación hace que la historia clínica no posea el atributo de integralidad. Hoy en día emergen grandes avances digitales que fortalecen la era de la información y la comunicación, por tal motivo la historia clínica electrónica surge como una respuesta al desarrollo tecnológico por su uso y aplicabilidad. De igual manera se destacan múltiples beneficios para la red de salud que pedía a gritos un proceso sistemático que facilite el tratamiento de la información en el sector salud. De los beneficios se pueden nombrar los siguientes: Presenta una estructura adecuada, los equipos tecnológicos facilitan el acceso a la información, optimizan las lecturas y análisis de los resultados, se elimina la legibilidad de los documentos, entre otros. Un aspecto importante es que aunque ofrece múltiples ventajas, demanda cuidado especial en el registro de la información.

Para el gran paso de la Historia Clínica Tradicional a las plataformas tecnológicas debe efectuar ciertas exigencias implantadas a partir de cinco niveles. El primer nivel siendo el más básico de todos. El segundo nivel es en base con la tecnología usada que brinda una mejoría visual de la información. El tercer nivel tiene que ver

con la usabilidad de redes sistemáticas en la entidad. El cuarto nivel encargado de almacenar todos los datos básicos de los pacientes en sus diferentes niveles de atención. El quinto y último nivel aparentemente como el más complejo, comprende gran cantidad de información, como por ejemplo: registros del estado de salud, antecedentes personales, hábitos y cuidados alimenticios, etc.

El objetivo primordial de la Historia Clínica Electrónica no es tan simple de que esté disponible para su uso, sino que en situaciones adversas se logre recuperar cuando así se requiera. Por ende, su conceptualización corresponde a que es aquella en donde la información puede ser capturada de manera digital, y cuyo soporte indudablemente es electrónico, lo que facilita y brinda el acopio, procesamiento y transmisión por sistemas informáticos.

### 4.2.3 Seguridad de la Información

En temas de protección y seguridad de los datos en la Historia Clínica Tradicional, se puede entrever una situación compleja en el momento de efectuar el cambio del documento físico al documento digital, de igual manera emerge resistencia en la aprobación de la historia digital por parte del cuerpo de profesionales de la salud. En lo mencionado ha sido posible determinar algunas barreras que impiden su implementación, ellas son: personal, económicas, tiempo, resistencia al cambio, administrativas, entre otras.

La esencia de la Historia Clínica Electrónica es “la confidencialidad de la información clínica” ya que este aspecto forma parte de los derechos de las personas, además de esto, es de obligatorio cumplimiento llevar a cabo un plan de seguridad que acate las normas concernientes a la protección de los datos personales, software, datos, etc.

Teniendo como base los métodos primordiales de seguridad se precisa los fines y mecanismos de los mismos: la identificación, se determina la persona al cual pertenece la atención; la confidencialidad, atributo que nos da la confianza que a la información solo se podrá acceder a ella con previa autorización; la integridad, atributo que garantiza que los datos no han sido alterados ni manipulados sino que se conservan tal cual como han sido generados; el no repudio, cuyo fin es el proceso probatorio de la participación en una comunicación del sistema; la autorización, atributo con la prominencia de establecer qué personas tienen la facultad de acceder a las diferentes actividades y tareas gestionadas a una persona; la auditoria, proceso en el cual se analiza, verifica y evalúa todas las acciones y conductas realizadas sobre los sistemas de información. Por último,

está la disponibilidad, atributo que permite acceder a los datos en el momento que se desee y por las personas autorizadas.

Existen ciertos requerimientos de seguridad que deben cumplirse para una buena gestión en el diligenciamiento de la Historia Clínica Electrónica, esto son: confidencialidad, integridad, disponibilidad, no repudio, autentificación y autorización.

### 4.2.4 Norma ISO/IEC 27001

La norma ISO/IEC 27001 es un estándar internacional que garantiza tanto la protección como la confidencialidad e integridad de la información. Esta norma determina las condiciones básicas para implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). Esta norma es un sistema activo cuyo objetivo principal consiste en analizar y gestionar los riesgos basados en los procesos de mejora continua, basado en el ciclo de calidad PHVA.

La norma ISO/IEC 27001 consta de 3 características que son los fundamentos de la seguridad informática y que garantizan su eficacia:

- **Confidencialidad**: Atributo que establece que la información no esté disponible ni se tenga acceso a ella por parte de los usuarios y/o procesos sin previa autorización.
- **Integridad**: Atributo que establece que la información debe permanecer completa, conservando su integridad y exactitud, salvaguardando los datos de cualquier tipo de manipulación, alteración o modificación.
- **Disponibilidad**: Atributo que establece que la información tenga la facultad de ser accesible por parte de los usuarios y/o procesos que estén previamente autorizados.

**¿A quién está dirigida la implementación de la norma ISO 27001?**

La implementación de la Norma ISO 27001 está dirigida a cualquier tipo de entidad sin tener en cuenta su tamaño y/o naturaleza. El aspecto más relevante para tener en cuenta a la hora de decidir sobre la puesta en marcha de un SGSI reside en la importancia que los activos de información tienen dentro de una empresa como elementos imprescindibles para la obtención de sus objetivos.

*Figura 1. Pilares de la Seguridad Informática*


Fuente: Propia del autor.

En la nueva versión de la Norma ISO/IEC 27001:2013 se incluye un nuevo componente conocida como el de las *partes interesadas,* que integra tanto a los propietarios de las organizaciones, como aquellos interesados que están directa e indirectamente en la empresa y desde luego las autoridades legales o reguladoras.

A continuación se describen los nuevos capítulos, su numeración y apartados:

*Tabla 1. Capítulos, numeración y apartados Norma ISO/IEC 27001:2013*

| Numeral | Capítulos | Apartados |
|---|---|---|
| 0 | Introducción | |
| 1 | Alcance | |
| 2 | Referencias Normativas | |
| 3 | Términos y Definiciones | |
| 4 | Contexto de la Organización | 4.1 Comprensión de la organización y su contexto.<br>4.2 Comprensión de las necesidades y expectativas de las partes interesadas.<br>4.3 Determinación del alcance del sistema de |

| | | |
|---|---|---|
| | | gestión de continuidad de negocios.<br>4.4 Sistema de Gestión de Continuidad de Negocios. |
| 5 | Liderazgo | 5.1 Liderazgo y compromiso.<br>5.2 Compromiso gerencial.<br>5.3 Política.<br>5.4 Roles, responsabilidades y autoridades de la organización. |
| 6 | Planificación | 6.1 Acciones para atender los riesgos y las oportunidades.<br>6.2 Objetivos de continuidad de negocios y planes para lograrlos. |
| 7 | Soporte | 7.1 Recursos.<br>7.2 Competencia.<br>7.3 Concientización.<br>7.4 Comunicación.<br>7.5 Información a documentar. |
| 8 | Operación | 8.1 Planificación y control operacional.<br>8.2 Análisis de impactos en los negocios y valuación de riesgos.<br>8.3 Estrategia de continuidad de negocios.<br>8.4 Establecimiento e implementación de los procedimientos de continuidad de negocios. |
| 9 | Evaluación del Desempeño | 9.1 Monitoreo, medición, análisis y evaluación.<br>9.2 Auditoría interna.<br>9.3 Revisión gerencial. |
| 10 | Mejora | 10.1 No conformidades y acciones correctivas.<br>10.2 Mejoramiento continuo. |

Fuente: SGSI. La norma ISO 27001:2013 ¿Cuál es su estructura? Disponible en https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

### 4.2.5 SGSI (Sistema de Gestión de la Seguridad de la Información)

**Alcance del SGSI**: Describe la extensión y los límites del SGSI. Acobija la selección de los elementos críticos a proteger. De igual manera el alcance relaciona las actividades principales que permiten efectuar con la misión y los objetivos generales de la organización.

**Políticas y objetivos de seguridad de la información**: Especifica el primordial objetivo del SGSI. La política de seguridad es el conjunto de reglas (en seguridad física, personal, administrativa y de la red) que se aplican a las actividades de un sistema y que pertenecen a una organización. Describe responsabilidades del usuario como por ejemplo las de proteger información confidencial. También refiere cómo se va a supervisar la eficacia de las medidas de seguridad.

El Sistema de Gestión de la Seguridad de la Información (SGSI) es una herramienta de gestión basada en la norma ISO/IEC 27001 que permite determinar, analizar y disminuir los riesgos que infringen la confidencialidad, integridad y disponibilidad de la información de la entidad. Gracias a la implementación de este sistema las organizaciones se benefician con el resguardo de los activos de información, la conservación de la conformidad reglamentaria, el salvaguardia de la imagen corporativa y la minimización de pérdidas por eventualidades de seguridad de la información.

**Implantación de un SGSI en una empresa**

Implantar un SGSI en una empresa supone:

- La adopción de procesos formales.
- La definición de responsabilidades de cara a la seguridad de la información.
- Establecimiento de políticas, planes y procedimientos para la seguridad de la información.
- Conservar y mantener información documentada como respaldo[13].

**¿Por qué implantar un Sistema de Gestión de la Seguridad de la Información?**

Abordar la seguridad de la información en una organización por medio de un sistema de gestión resulta bastante provechoso, lo cual se puede mencionar lo siguiente:

- Mejora continua.
- Ajustarse a las necesidades de cada empresa.
- Establecer controles pertinentes y oportunos para la seguridad de la información.
- Integración de sistemas de gestión[14].

[13] ISO 27001. Norma ISO 27001. ¿Qué significa la implantación de un SGSI en una empresa? Disponible en: https://normaiso27001.es/

[14] ISO 27001. Norma ISO 27001. ¿Por qué implantar un Sistema de Gestión de la Seguridad de la Información? Disponible en: https://normaiso27001.es/

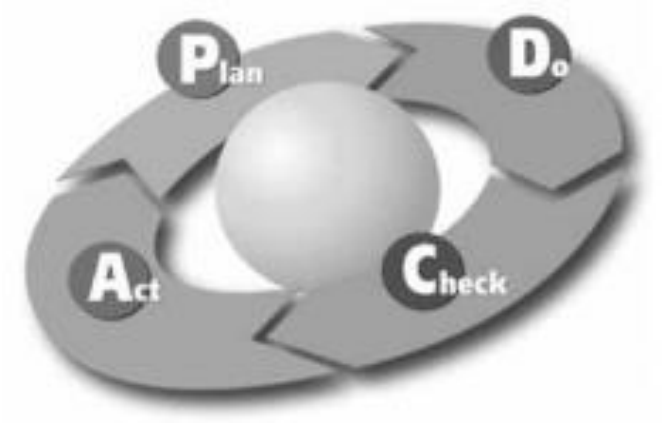
## Diseño del SGSI

Para el diseño del Sistema de Gestión de la Seguridad de la Información es imprescindible acoger un enfoque basado en procesos que facilite establecer, implementar, operar, mantener y mejorar el Sistema de Gestión acogido por la empresa mediante la ejecución del ciclo de la mejora continua PHVA (Planear, Hacer, Verificar y Actuar), esto quiere decir, la planificación de actividades, realizar acciones sobre lo planeado, la verificación de los resultados de dichas actividades y por último, actuar sobre los resultados previstos.

El ciclo PHVA consiste básicamente en:

- **Planear**: La esencia del ciclo de calidad está en que antes de emprender algún proceso siempre se realiza una adecuada planeación. El planear corresponde a la formulación de los objetivos o actividades del sistema, la definición de las metas y los mecanismos para lograrla, los recursos básicos para generar resultados, así como los índices que permiten monitorear el desarrollo posterior de lo definido en esta etapa. Por último permite identificar y abordar los riesgos y las oportunidades.
- **Hacer**: Este paso hace referencia al cumplimiento de lo planificado. Es aquí donde se lleva a cabo todo y cada una de las acciones programadas teniendo en cuenta las medidas implementadas, así como sea el plan de acción, del mismo modo debe ser el seguimiento sobre las actividades y respectivamente su responsable. Esto debe reflejar la capacidad de organización y de su talento humano para la toma oportuna y acertada de decisiones ideales a los diferentes procesos y trabajar en equipo y así poder asignar adecuadamente los requerimientos necesarios para alcanzar los objetivos.
- **Verificar**: Es la comparación de lo ejecutado versus lo planificado. Se valoran los resultados esperados y se determinan los problemas no solucionados. En esta fase se establecen en qué nivel se dio cumplimiento a lo programado. Para el proceso de verificar se puede realizar de dos formas: ya sea acción por acción o por cambio esperado que propone el plan de acción. Mientras se va efectuando el plan de acción se va valorando la efectividad de las acciones ejecutadas, esto quiere decir, que produzca los resultados que se esperan en las disposiciones concertadas, como por ejemplo: tiempo, costos, alcance, entre otros.
- **Actuar**: En esta fase se lleva a cabo las medidas correctivas necesarias para el logro de los objetivos. También se ejecutan las actividades básicas para contrarrestar las falencias manifestadas en la fase verificar. En el transcurso de esta fase frecuentemente emergen planes posteriores o recomendaciones que es el aspecto que nos dirige o direcciona hacia la mejora continua.

*Figura 2. Modelo PHVA aplicado a los procesos de SGSI*




Fuente: Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Disponible en file:///C:/Users/user/Downloads/202-Texto%20del%20art%C3%ADculo-417-1-10-20150612.pdf

*Tabla 2. Resumen del modelo PHVA aplicado a los procesos de SGSI*

| | |
|---|---|
| Planificar (establecer el SGSI) | Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización. |
| Hacer (implementar y operar el SGSI) | Implementar y operar la política, los controles, procesos y procedimientos del SGSI. |
| Verificar (hacer seguimiento y revisar el SGSI) | Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión. |
| Actuar (mantener y mejorar el SGSI) | Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI. |

Fuente: Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Disponible en file:///C:/Users/user/Downloads/202-Texto%20del%20art%C3%ADculo-417-1-10-20150612.pdf

### 4.2.6 Plan de auditoría

El plan de auditoria es el esquema metodológico más significativo y relevante del auditor informático. Consiste en la evaluación de los recursos tecnológicos mediante la implementación de un conjunto de técnicas de análisis y verificación de políticas y procesos de la organización para el buen funcionamiento y cumplimiento de los sistemas de información, ya que facilitan las medidas necesarias para que los sistemas sean fidedignos y contengan un buen nivel de protección.

**Metodologías para auditoría de SGSI**

El proceso de auditar un SGSI precisa de una metodología que ofrezca las orientaciones y/o pasos que permitan la revisión completa e intensiva de cada una de las medidas de seguridad implementadas de acuerdo a la normativa ISO/IEC 27001.

A continuación se mencionan algunas de las metodologías utilizadas para la auditoría de un SGSI.

*Tabla 3. Metodologías para auditoría de SGSI*

| Metodologías Auditoría SGSI | Descripción |
|---|---|
| **OCTAVE** | • Administra y direcciona la evaluación de los riesgos por medio de un grupo de personas multidisciplinarios.<br>• Contiene los métodos de evaluación y gestión de riesgos.<br>• Involucra a todas las personas de la organización.<br>• Implica como partes de su modelo de evaluación: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. |
| **MAGERIT** | • Posee un resultado absoluto en la evaluación y gestión de riesgos.<br>• Contiene un gran compendio de inventarios |

| | |
|---|---|
| | en temas concernientes a recursos Informáticos, activos de información y amenazas.<br>• Facilita un análisis completo cualitativo y cuantitativo.<br>• De carácter Público.<br>• No demanda autorización previa para su uso.<br>• Contiene una buena base documental. |
| **MEHARI** | • Utiliza una técnica de evaluación de riesgos tanto cualitativo como cuantitativo.<br>• Se adapta a las necesidades de la norma ISO 27001, 27002<br>• Combina análisis y evaluación del riesgo.<br>• Detecta vulnerabilidades por medio de auditorías y analiza las situaciones de riesgo. |
| **NIST SP 800-30** | • Bajo costo frente al riesgo hallado.<br>• Provee una guía para la evaluación de riesgos de seguridad.<br>• Suministra herramientas para la valoración y minimización de riesgos.<br>• Se aplica en el análisis y la gestión de los riesgos.<br>• A partir de los resultados mejora la administración. |
| **CORAS** | • Utiliza herramientas de apoyo para el análisis de riesgos.<br>• Suministra reportes de vulnerabilidades halladas.<br>• Eficiente en el desarrollo y mantenimiento del sistema.<br>• Soportada en modelos de riesgos de sistemas de seguridad críticos. |
| **CRAMM** | • Se aplica a todo tipo de sistemas y redes de información.<br>• Se utiliza para establecer la seguridad y/o requerimientos de incidentes.<br>• Identifica y especifica todos los activos TI.<br>• Analiza el impacto organizacional.<br>• Identifica y evalúa amenazas y vulnerabilidades. |

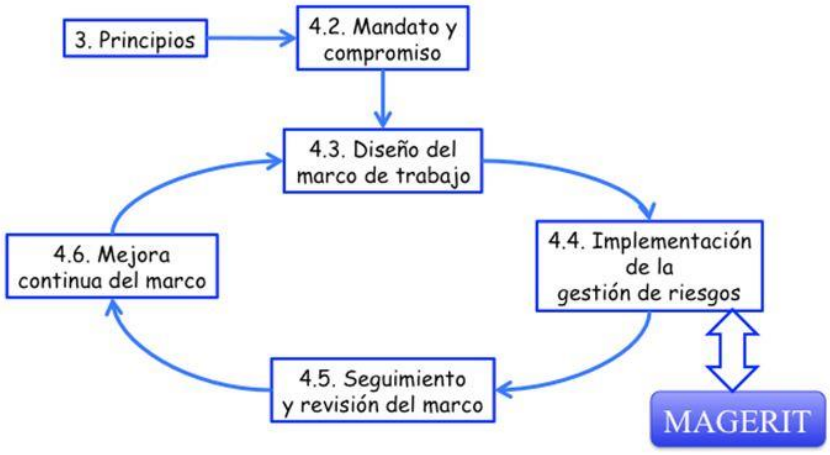
| | |
|---|---|
| **EBIOS** | • Compatible con las normas ISO 27001, 27002 y 31000.<br>• Se utiliza para varias finalidades y procedimientos de seguridad.<br>• Posee código libre y reutilizable.<br>• Involucra todas las áreas. |

Fuente: Propia del autor

**Metodología MAGERIT**: Esta metodología va dirigida a todos aquellos que están relacionados con la información digital y que constantemente tienen trato con ella. Si la información que se facilita es valiosa, MAGERIT ofrece la posibilidad de conocer el valor que está en juego y brindará la ayuda así mismo para protegerlo. Indudablemente percatarse del riesgo al que están expuestos los componentes de trabajo es, sencillamente, indispensable para tener la potestad de gestionarlos.

"MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo."[15]

*Figura 3. Marco de trabajo para la gestión de riesgos*




[15] Fuente: Catálogo de Elementos. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

Fuente: MAGERIT v.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Catálogo de Elementos. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

**Principios de auditoría**

El fundamento de la auditoria, incide en los requisitos que atienden como lineamientos en la ejecución de la misma, lo que permite suministrar resultados fidedignos, objetivos oportunos y eficientes para que la empresa logre la toma de decisiones concerniente a lo realizado.

A continuación se describen los principios de la auditoría:

- **Integridad**: Hace referencia a la conducta moral y ética profesional del auditor que implica su transparencia, imparcialidad, diligencia y responsabilidad, reflejando su idoneidad en el transcurso del proceso de la auditoría.
- **Presentación ecuánime**: Hace referencia al producto final de la auditoria (hallazgos, conclusiones e informes), lo cual debe evidenciar la autenticidad y precisión de la información que se expuso en el transcurso de la auditoria.
- **Debido cuidado profesional**: Hace referencia a la pericia que posee el auditor en el momento de formular los juicios de valor razonables en el trascurso de la auditoria.
- **Confidencialidad**: Hace referencia a la protección de la información, durante el proceso de la auditoria, garantizando que no se utilice de manera inadecuada.
- **Independencia**: Hace referencia a que la conducta del auditor se manifiesta en la soberanía de sus actos, libre de intereses personales. Este aspecto es el fundamento de la integridad y rectitud del resultado de la auditoria.
- **Enfoque basado en la evidencia**: Hace referencia a que la auditoria se fundamenta en la toma de evidencias de la información por el tiempo necesario establecido en todo el proceso de la auditoría.

**Fases de la auditoría**

El proceso de la auditoria consta de tres fases que se describen:

- **Planeación de la auditoría**: Se refiere a que todo proceso de auditoría se debe ejecutar al menos una vez en el año, aunque esta periodicidad tiene que ver directamente con las necesidades de la empresa. Durante esta etapa se efectúa la fase (planear) donde se establece aspectos como los recursos, los métodos y el tiempo para realizar el proceso de auditoría.

- **Implementación de la auditoría**: Es el proceso de preparación de la auditoría. Se da apertura con una reunión inicial, seguidamente una presentación de la metodología, tiempos y recursos a utilizar. Se recoge y evalúa la información soportando las acciones de mejora como las fortalezas halladas en la auditoría. Al cierre de la auditoría se presentan las conclusiones y con base a estos resultados se implementan las oportunidades de mejora adecuadas.
- **Monitoreo de la auditoria**: Para esta etapa, se lleva a cabo el seguimiento a la ejecución de los objetivos. La eficiencia de las oportunidades dará lugar a la mejora de la implantación del modelo de protección y confidencialidad de la información. Es recomendable que este seguimiento se realice de manera periódica para garantizar los progresos y determinar cualquier acción que facilite soportar y respaldar el cumplimiento de las metas.

Para obtener un informe de auditoría inicial sobre el cumplimiento de la norma podremos realizar un análisis de brechas o deficiencias GAP antes de iniciar el proyecto aplicado a los requisitos genéricos de la norma. Basado en un análisis de riesgos podremos mediante el análisis de cumplimiento de los controles, obtener el informe para establecer el plan de aplicación de los mismos y su estado de cumplimiento, además de ayudarnos en la elaboración de la Declaración de Aplicabilidad[16].

**Perfil del auditor de sistemas**

A continuación se describen algunas de las cualidades humanas, de gestor y de organizador que debe tener el auditor de sistemas:

- Eficiencia en su misión en la entidad.
- Ser diplomático.
- Manejo de pedagogía.
- Conocimiento de herramientas y métodos, para llegar al objetivo a alcanzar.
- Conocimiento en técnicas de auditoria[17].

### 4.2.7 Informe de auditoría

El informe de auditoría es el reporte que resulta de la ejecución de dicho proceso. Este informe es una técnica del sistema de gestión, el cual ofrece emprender más

[16] ISO 27001. Norma ISO 27001. FASE 1 AUDITORIA INICIAL ISO 27001 GAP ANALYSIS Disponible en: https://normaiso27001.es/

[17] MINTIC. Seguridad y Privacidad de la Información. Guía de Auditoria. P.15. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

oportunidades de mejora y no solo dar respuesta y correcciones de las no conformidades halladas. Todo proceso de toma de decisiones efectivo pasa por un procedimiento bien argumentado, por lo que es conveniente, necesario y trascendental emplear las mejores energías para un SGSI. Un sistema robusto permite obtener los registros necesarios para analizar las posibles razones de los inconvenientes y su impacto real en el sistema[18].

El informe final debe estar documentado con todas las evidencias halladas en el proceso de la auditoría. Para esto, es oportuno archivar todos los reportes de la caracterización de las no conformidades y las intervenciones que se han llevado a cabo para abordarlas así como de sus resultados esperados.

## 4.3 MARCO CONTEXTUAL

El proyecto se ejecutará específicamente en la E.S.E. Municipal Manuel Castro Tovar de la ciudad de Pitalito, ubicado geográficamente al sur de Colombia en el Departamento de Huila y sobre el valle del Magdalena a unos 188 Km de Neiva, siendo esta ciudad la Capital del Huila.

*Figura 4. Ubicación geográfica donde se desarrollara la auditoría*

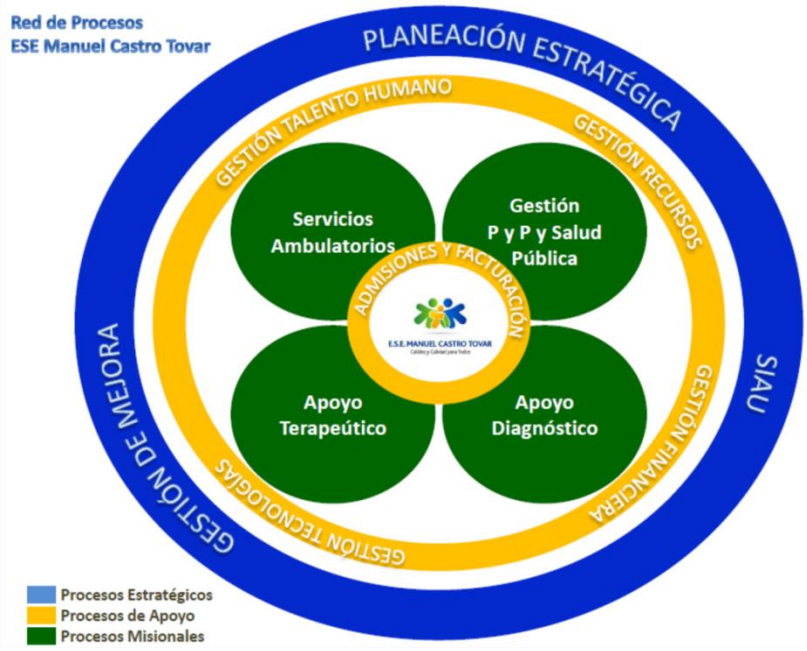

Fuente: Propia del autor.

[18] ISO 27001. Norma ISO 27001. Mejora en ISO 27001. Disponible en: https://normaiso27001.es/

**Mapa de procesos**

El mapa de procesos de la E.S.E Municipal Manuel Castro Tovar de Pitalito, se crea con el fin de dar respuesta a lo establecido en el Sistema de Gestión de Calidad, se rediseñó teniendo en cuenta los métodos para lograr los resultados trazados, implementando un modelo por procesos que brinde a la entidad, trabajadores y terceros enfocar todas sus quehaceres en una misma orientación, de tal forma que estén dirigidas a prestar servicios oportunos y eficientes para lograr la satisfacción de los clientes internos y externos, en cumplimiento de la misión, visión y objetivos de calidad.

*Figura 5. Red de Procesos E.S.E. Municipal Manuel Castro Tovar*




Fuente: Red de Procesos E.S.E. Municipal Manuel Castro Tovar. Disponible en http://esemanuelcastrotovar.gov.co/quienes-somos/

## 4.4 MARCO LEGAL

### 4.4.1 Normatividad de la Historia Clínica en Colombia

A continuación se mencionan algunas de las normas, leyes y decretos que regulan y controlan el manejo de la Historia Clínica, generadas y emitidas por el Ministerio de Salud y Protección Social necesarias para adoptar disposiciones en relación

con el manejo, custodia, tiempos de retención y conservación de las historias clínicas, así como con su disposición final.

A continuación se describen algunas de las normas aplicables al buen uso y aplicabilidad de la información en la historia clínica:

- La norma colombiana tiene sus principios en la Constituyente de 1991, en los cuales proceden de la legislación que cubre el desarrollo gubernamental.
- Ley 100 de 1993, en su artículo 22. Define sobre la calidad de los servicios en el Sistema de Salud.
- Resolución 2546 de 1998. Establece los datos mínimos; las responsabilidades y los flujos de información de prestadores de salud en el sistema de salud.
- Resolución 1995 de 1999, del Ministerio de Salud constituye las normas para el tratamiento de la historia clínica.
- Resolución 4144 de 1999. Por la cual se determinan los lineamientos en relación con el Registro Individual de Atención.
- Ley 23 de 1981. Artículos 33, 34, 35. Por la cual se establecen normas en materia de ética médica. Secreto profesional de la historia clínica.
- Decreto 3380 de 1981. El conocimiento que de la historia clínica que tengan los auxiliares del médico o de la institución en la cual éste labore, no son violatorios del carácter privado y reservado de ésta.
- Resolución 3374 de 2000 por la cual se reglamentan los datos básicos que deben reportar los prestadores de servicios de salud y las entidades administradoras de planes de beneficios sobre los servicios de salud prestados.

### 4.4.2 Normatividad en Seguridad Informática en Colombia

El aumento y uso de las nuevas tecnologías de la información ha instado y dispuesto la elaboración de un marco legal que se encargue y responsabilice de salvaguardar a todas y cada una de las partes interesadas en la utilización de estas técnicas digitales, además la reciprocidad y proceso de la información a través de estos mecanismos.

De igual manera resulta importante abarcar temas de trascendencia e interés como lo son los delitos informáticos, debido a que al transcurrir los días emergen nuevos fraudes y violaciones que pueden afectar negativamente la protección de la información en las organizaciones.

A continuación se mencionan las normas, leyes y decretos que regulan y controlan el manejo de la Seguridad Informática, emitidas por la Legislación Informática de Colombia obedeciendo la directriz de seguridad y de este modo evitar que se creen vulnerabilidades que impacten el negocio de la Entidad:

- Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, 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, entre otras disposiciones”.
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”[19].

[19] Las leyes y normas citadas en la lista anterior fueron tomadas del Manual de Normas y Políticas de Seguridad Informática. Disponible en: http://www.informatica-juridica.com/legislacion/colombia/

# 5. DESARROLLO DEL PROYECTO

En este capítulo se dará desarrollo a cada uno de los objetivos propuestos para la elaboración del proceso de auditoría, relacionando la protección y manejo de confidencialidad de los datos sensibles que reposan en la Historia Clínica electrónica de los usuarios en la E.S.E. Municipal Manuel Castro Tovar.

## 5.1 Análisis de la eficiencia del sistema de información en cuanto a la protección de los datos sensibles de la Historia Clínica electrónica.

Dinámica Gerencial Hospitalaria (DGH) es una plataforma desarrollada por la empresa SYAC S.A. orientada a administrar procesos específicos del sector salud, facilitando la gestión de las áreas administrativas y asistenciales, entre otras. DGH está compuesta por múltiples módulos que funcionan de forma integrados en donde el eje central es precisamente la Historia Clínica Electrónica, permitiendo a las instituciones la reducción en los tiempos de atención al usuario, ofreciendo oportunidad y eficacia para la toma de decisiones en tiempo real y además apoye el desarrollo de los procesos misionales de la entidad.

La información sensible de las personas está presente a lo largo y ancho de la empresa debido a que continuamente está siendo transmitida en diferentes dispositivos de la red. Partiendo de la premisa de que “el cifrado es el elemento fundamental de la seguridad de datos y es la forma más simple e importante de impedir que alguien robe o lea la información de un sistema informático con fines malintencionados”[20], es necesario, importante y trascendental tener en cuenta el cifrado de los datos por el valor que tiene para el negocio.

Como se mencionó líneas atrás, la información de los pacientes es sumamente importante y, de no poder garantizar la seguridad de la misma, las personas dejarán de confiar en la empresa, por eso, la implementación del cifrado de los datos garantiza que solo aquellos que posean la clave puedan descifrar el mensaje y acceder a su contenido. Una vez registrada y almacenada la información de los pacientes en la Historia Clínica Electrónica, los datos son transmitidos hacia el servidor de datos mediante el proceso de cifrado para impedir el uso no autorizado de la información. Para poder acceder a la información, el usuario debe hacerlo mediante el protocolo de autenticación, debido a que el servidor verificará la identidad digital del remitente de la

[20] Kaspersky. ¿Qué es el cifrado de datos? disponible en https://latam.kaspersky.com/resource-center/definitions/encryption

comunicación como una petición para conectarse. Si el usuario no posee las credenciales o los privilegios de acceso de ninguna manera podrán hacer contacto con la base de datos del sistema de información y se denegará su petición.

El formulario que presenta DGH para alimentar la Historia Clínica Electrónica, es diligenciado de forma manual cada vez que es solicitada la información al paciente, por ende, el profesional de salud es el único responsable de ingresar y validar la calidad del dato en el momento de la atención. La impresión diagnóstica parte de esta verdad, debido a que los datos que se registran en la Historia Clínica Electrónica, son de tipo texto únicamente, tanto el diagnostico final como los paraclínicos y la formulación de medicamentos.

Teniendo en cuenta que no existe una única Historia Clínica en Colombia, y que cada entidad de salud cuenta con su propio sistema de información para que administre todos los recursos del sistema, incluyendo la información registrada y almacenada en su debido momento, existen brechas en la atención de salud teniendo en cuenta que en el proceso de remisión del paciente, la remisión se tiene que hacer de forma manual, esto quiere decir que, se acude al viejo método del uso del papel debido a que la orden medica al nivel de complejidad que se remite, tiene que estar impresa, situación que merece toda la atención posible teniendo en cuenta que, en la impresión va registrado toda la atención de salud consignada en la Historia Clínica Electrónica.

Para evitar la pérdida de información del paciente, la entidad cuenta con un sistema de respaldo o backup que se lleva a cabo todos los días a media noche, teniendo en cuenta que el servidor de archivos esta previamente programado para que se lleve a cabo esta tarea y de esta manera se permita asegurar la disponibilidad e integridad de la información ante cualquier tipo de incidentes.

Aunque DGH es un software especializado en la automatización y manejo de información, se ha podido evidenciar una serie de irregularidades en el tratamiento y custodia de los datos que se manejan en la Historia Clínica Electrónica, dejándola vulnerable a posibles riesgos y amenazas que pueden causar un gran impacto negativo en cuanto a la clasificación de la información de acuerdo a su sensibilidad e importancia y desde luego al derecho constitucional de la protección de datos personales.

De igual manera, se evidencia que la gestión de la Historia Clínica Electrónica no brinda la confianza y seguridad para garantizar que los datos tratados cumplen

con los principios de privacidad y confidencialidad, teniendo en cuenta que la información procesada requiere de un tratamiento especial.

Al analizar la gestión de la Historia Clínica Electrónica, se verifica que no existen ningún tipo de controles o medidas para afrontar posibles incidentes en la seguridad de la información o por lo menos que regulen o mitiguen su impacto. No se han establecido políticas, normas o procesos orientados al uso apropiado y correcto de los datos sensibles de la Historia Clínica Electrónica en relación a su seguridad.

Otro aspecto a resaltar es que, no se evidencia una clasificación de la información adecuada teniendo en cuenta su confidencialidad y/o privacidad, a fin de poder establecer medidas de seguridad específicas que garanticen su protección. No se han establecido las restricciones estrictas y necesarias o en su defecto los accesos limitados a los recursos de la Historia Clínica Electrónica según perfiles determinados, facilitando que personas ajenas al proceso que está directamente asociado a los usuarios, puedan acceder a su información confidencial.

Aunque se han establecidos perfiles de acceso para el sistema de Información (Historia Clínica Electrónica) de forma que se restringa el acceso de los datos a la actividad o tarea específica a desarrollar, se evidencia que existen terceros que poseen las credenciales para el ingreso y tratamiento de la información.

El análisis realizado sobre la Historia Clínica Electrónica, permite vislumbrar el estado actual en cuanto a seguridad y privacidad de la información en la empresa, evidenciando una serie de vulnerabilidades que afectan directamente el principio de confidencialidad. El artículo 15 de la constitución política de Colombia hace mención a que “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”.[21] De acuerdo a la ley estatutaria 1581 de 2012, reglamentada por el decreto nacional 1377 de 2013, en su artículo 13, menciona que “los responsables del tratamiento deberán desarrollar sus políticas para el Tratamiento

[21] Constitución Política de Colombia 1991. Actualizada con los Actos Legislativos a 2016. Edición especial preparada por la Corte Constitucional. Artículo 15. Disponible en http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf. P.16.

de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas".[22]

## 5.2 Ejecución del plan de auditoría.

El desarrollo de este objetivo enmarca la elaboración del plan de auditoría, donde se incluye el alcance y la metodología escogida para hacer efectiva la investigación, los recursos tanto humanos como tecnológicos necesarios para llevarla a cabo, se estima un presupuesto aproximado para el proyecto, se plantea un cronograma de actividades, se exponen algunos controles del anexo A de la Norma ISO 27001:2013 que se tendrán en cuenta para la realización de la auditoría, y por último, se presenta el instrumento de recolección de información como fuente y base de partida para llevar a cabo el proceso de auditoría.

### 5.2.1 Alcance

La auditoría de sistemas abarcara las dos áreas de componen la empresa que tienen acceso a la Historia Clínica Electrónica:

- Área misional. Consultorios médicos y de enfermería.
- Área administrativa.

### 5.2.2 Metodología

Para la ejecución de la auditoría de sistemas se realizaran las siguientes actividades:

- La auditoría se aplicará específicamente sobre la Historia Clínica Electrónica en la E.S.E. Municipal Manuel Castro Tovar de la ciudad de Pitalito.
- Se tomará como población objeto a un grupo selecto de personas con diferentes perfiles (personal médico, enfermaría y administrativos) y que se ajustan al problema de investigación.
- Se aplicará una encuesta como instrumento de recolección de información que una vez sea empleada permita que los datos sean analizados y evaluados.

[22] MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto Número 1377 de 2013. 27 de Junio 2013. Artículo 13. Disponible en https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf. P.6.

- El procedimiento para aplicar la encuesta será por medio de entrevistas directas con la muestra ya mencionada y que han sido directamente seleccionadas.
- Una vez registrada la información en los formularios de encuesta se procederá a verificar la calidad de la información de los cuestionarios diligenciados, se depuraran los datos digitados y por último se tabularán.
- Se presentarán los resultados en un informe final de auditoría donde se evidenciarán tanto los hallazgos y causas que la originan como también los controles y procedimientos de seguridad adecuados para mitigarlos.

### 5.2.3 Recursos

**Talento Humano**

La auditoría de sistemas se llevará a cabo por el estudiante de la especialización en seguridad Informática:

- Mauricio Andrés Neuta Artunduaga.

También se contará con la colaboración de personal de la institución: Ingenieros del área de Gestión de las Tecnologías, personal médico, personal de enfermería, personal administrativo, tutor y asesor de proyecto.

**Recursos tecnológicos**

- 1 Computador portátil.
- Computadores en los consultorios.
- Computadores área administrativa.
- Impresora multifuncional.
- Dispositivos de almacenamiento USB.

**Software**

- Software institucional Dinámica Gerencial Hospitalaria (DGH).
- Procesadores de texto.

### 5.2.4 Presupuesto

*Tabla 4. Presupuesto de auditoría*

| Cantidad | Descripción | Precio Unitario | Precio Total |
|---|---|---|---|
| 1 | Computador portátil. | $2.000.000 | $2.000.000 |
| 1 | Impresora multifuncional. | $1.000.000 | $1.000.000 |
| 1 | USB | $20.000 | $20.000 |
| 1 | Resma de papel carta | $8.000 | $8.000 |
| 1 | Documentos soportes | $100.000 | $100.000 |
| 1 | Auditor 1 (valor Mensual) | $2.000.000 | $10.000.000 |
| **Presupuesto Total** | | | $13.200.000 |

Fuente: Propia del autor

### 5.2.5 Cronograma de actividades

Teniendo en cuenta los objetivos propuestos en la auditoria de sistemas, se establece el siguiente cronograma de actividades.

*Tabla 5. Cronograma de actividades*

| ACTIVIDAD | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 |
| Solicitar los permisos necesarios para la aplicación de la auditoria de sistemas y los instrumentos a utilizar. | | | | | | | | | | | | | | | | |
| Vista preliminar de las áreas que serán evaluadas. | | | | | | | | | | | | | | | | |
| Selección del personal a encuestar. | | | | | | | | | | | | | | | | |
| Aplicar los instrumentos de recolección de información (encuestas) | | | | | | | | | | | | | | | | |
| Analizar la información y los resultados obtenidos en las encuestas. | | | | | | | | | | | | | | | | |
| Preparar el Informe final de auditoría. | | | | | | | | | | | | | | | | |
| Presentar el informe de auditoría a la alta gerencia evidenciando los resultados finales. | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Documentación. | | | | | | | | | | | | | | | | |

Fuente: Propia del autor

### 5.2.6 Programa de auditoría

En el programa se define el estándar que se va aplicar. Para el desarrollo de esta auditoría de sistemas se tomará como referencia la Norma ISO 27001:2013 y la ISO 27002:2013, se seleccionan los dominios dentro de los estándares y se asignan al grupo auditor para ser evaluados. A continuación se muestra la selección de los dominios que serán aplicados.

### 5.2.7 Dominios de la ISO 27001:2013

La versión 2013 del estándar describe catorce dominios principales, de los cuales se seleccionaron para el desarrollo de la auditoría los siguientes controles:

**A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
**A6.1 Organización interna**
6.1.1 Funciones y responsabilidades de la Seguridad de la información.
6.1.2 Separación de funciones.
6.1.3 Contacto con autoridades.

**A8. GESTION DE ACTIVOS**

**A8.1 Responsabilidad sobre los activos**
A8.1.3 Uso aceptable de los activos.
A8.1.4 Devolución de activos.
**A8.2 Clasificación de la información**
A8.2.1 Clasificación de la información.
A8.2.2 Etiquetado de la información.
A8.2.3 Manejo de los activos.
**A8.3 Manipulación de Soportes**
A8.3.1 Gestión de soportes extraíbles

**A9. CONTROL DE ACCESO**

**A9.1 Requisitos generales para el control de acceso**
A9.1.1 Política de control de acceso.
A9.1.2 Acceso a las redes y a los servicios de red.
**A9.2 Accesos de Usuario**

A9.2.1 Registro de usuarios y cancelación del registro.
A9.2.2 Gestión de acceso a los usuarios.
A9.2.3 Gestión de derechos de acceso privilegiados.
A9.2.4 Gestión de la información de autenticación secreta de los usuarios.
A9.2.5 Revisión de derechos de acceso de usuario.
A9.2.6 Remoción o ajuste de los derechos de acceso.

**A9.4 Control de acceso a sistemas y aplicaciones**

A9.4.1 Restricción de acceso a la información.
A9.4.2 Procedimientos de conexión (log-on) seguros.
A9.4.3 Sistema de gestión de contraseñas.

**A11. SEGURIDAD FÍSICA Y DEL ENTORNO**

**A11.1 Áreas de seguridad**

A11.1.2 Controles de acceso físico.
A11.1.3 Seguridad de oficinas, despachos e instalaciones.
A11.1.4 Protección contra amenazas externas y del ambiente.

**A12. SEGURIDAD EN LAS OPERACIONES**

**A12.1 Procedimientos y responsabilidades**

A12.1.1 Procedimientos documentados de operación.

**A12.3 Copias de seguridad**

A12.3.1 Respaldo de la información.

**A12.4 Registro y supervisión**

A12.4.1 Registro de eventos.
A12.4.2 Protección de la información de registros (logs)

**A12.6 Vulnerabilidad técnica**

A12.6.1 Gestión de vulnerabilidades técnicas.
A12.6.2 Restricciones en la instalación de software.

**A12.7 Auditorias de Sistemas de Información**

A12.7.1 Controles de auditoría de sistemas de información[23].

### 5.2.8 Instrumento de Recolección de Información

En esta etapa se aplica el instrumento de recolección de información que ha sido diseñado y que permite evaluar cada uno de los dominios con respecto a las vulnerabilidades, amenazas y riesgos existentes, así como para determinar el cumplimiento de los controles de acuerdo a la norma ISO/IEC 27001.

[23] MINTIC. Seguridad y Privacidad de la Información. Controles de Seguridad y Privacidad de la Información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Para la elaboración de la encuesta, se efectuara por medio de un muestreo por conveniencia. “El muestreo por conveniencia es una técnica de muestreo no probabilístico utilizada para crear muestras de acuerdo a la facilidad de acceso, la disponibilidad de las personas de formar parte de la muestra, en un intervalo de tiempo dado o cualquier otra especificación práctica de un elemento particular”[24]. Por otro lado, el muestreo por conveniencia es la técnica de uso más común, debido a sus ventajas ofrecidas como: rapidez para obtener resultados, simplicidad, económica y, además, los integrantes de por sí, están disponibles y accesibles para conformar la muestra.

A continuación se presenta el formato de encuesta aplicada al grupo de funcionarios de la empresa que fueron seleccionadas según la técnica de conveniencia, profesionales de diferentes áreas que laboran en la institución, para indagar sobre los diferentes aspectos de confidencialidad y privacidad de los datos sensibles en la Historia Clínica Electrónica.

**Diseño de instrumento de recolección de información**
**Instrumento de cumplimiento de controles ANEXO A ISO 27001:2013 – ISO 27002:2013**[25]

| | **AUDITORÍA A LA PROTECCIÓN DE LOS DATOS SOBRE LA HISTORIA CLÍNICA ELECTRÓNICA DE LA E.S.E. MUNICIPAL MANUEL CASTRO TOVAR** | **REF.** | | |
|---|---|---|---|---|
| | | | | |
| **AREA** | | **D** | **M** | **A** |
| | | | | |
| **Encuesta a la confidencialidad y privacidad de los datos sensibles de la Historia Clínica Electrónica** | | | | |
| **OBJETIVO:** | | | | |
| Evaluar la confidencialidad y privacidad de los datos sensibles de los usuarios en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar para determinar las vulnerabilidades, amenazas y riesgos que existen en el tratamiento | | | | |

[24] QuestionPro. ¿Qué es el muestreo por conveniencia? Disponible en https://www.questionpro.com/blog/es/muestreo-por-conveniencia/

[25] MINTIC. Seguridad y Privacidad de la Información. Controles de Seguridad y Privacidad de la Información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf. P.10-17.

y custodia de la información de acuerdo a los estándares de control establecidos en la Norma ISO/27001:2013 - ISO/27002:2013.

**Nota aclaratoria**: Para el desarrollo de esta encuesta **NO** se solicita ninguna información de carácter personal, debido a que los datos requeridos, corresponden exclusivamente para efectos académicos.

**Cuestionario inicial**

| No. | ÌTEM | SI | NO |
|---|---|---|---|
| 1 | ¿Conoce la política de protección de datos personales? | | |
| 2 | ¿Conoce la clasificación de los datos personales e implicaciones legales? | | |
| 3 | ¿Conoce la definición de “Dato sensible”? | | |
| 4 | ¿Conoce la definición de “Dato privado”? | | |
| 5 | ¿Conoce la definición de “Confidencialidad”? | | |
| 6 | ¿Conoce la política de delitos informáticos? | | |

**Cuestionario - Organización de la Seguridad de la Información**
**Dominio A6 - Subdominio A6.1 - A6.2**

| No. | ÌTEM | SI | NO |
|---|---|---|---|
| 7 | ¿Considera que la gestión de la Historia Clínica Electrónica brinda la confianza y seguridad para garantizar que los datos manejados cumplen con los principios de privacidad y confidencialidad? | | |
| 8 | ¿Se han asignado y definido las responsabilidades de los usuarios de la Historia Clínica Electrónica sobre la seguridad de la Información en los distintos procesos, tareas o actividades de la empresa? | | |
| 9 | ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos a la Historia Clínica Electrónica? | | |
| 10 | ¿Existe un procedimiento establecido para informar ante el área competente los incidentes relacionados con la Seguridad de la Información? | | |
| 11 | ¿Existe controles para afrontar posibles eventualidades sobre la seguridad de la información en la gestión de la Historia Clínica Electrónica? | | |

**Cuestionario - Gestión de Activos**
**Dominio A8 - Subdominio A8.1 - A8.3**

| No. | ÌTEM | SI | NO |
|---|---|---|---|
| 12 | ¿Se han establecido políticas, normas o procesos para el uso apropiado de los datos sensibles de la Historia Clínica Electrónica en relación a su seguridad? | | |
| 13 | ¿Existe un proceso para la devolución de la información privada cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato? | | |
| 14 | ¿Se clasifica la información según su confidencialidad o su privacidad a fin de establecer medidas de seguridad especificas? | | |
| 15 | ¿Los datos recogidos en la Historia Clínica Electrónica son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación? | | |
| 16 | ¿Existen procedimientos para el manejo y trato de la información de acuerdo a su clasificación? | | |
| 17 | ¿Existen controles o procedimientos establecidos para aplicar a soportes extraíbles o externos para proteger su seguridad?<br>-Uso<br>-Borrado<br>-Cifrado<br>-Impresión.<br>-Transferencia<br>-Etc. | | |
| **Cuestionario – Control de Acceso<br>Dominio A9 - Subdominio A9.1 – A9.4** | | | |
| **No.** | **ÌTEM** | **SI** | **NO** |
| 18 | ¿Existe una política, norma o proceso que defina los controles de acceso a los datos sensibles de la Historia Clínica Electrónica y que tengan en cuenta el acceso selectivo a la información según las necesidades de cada área o puesto de trabajo? | | |
| 19 | ¿Están establecidos las restricciones o accesos limitados a los recursos de la Historia Clínica Electrónica según perfiles determinados? | | |
| 20 | ¿Existen procesos formales de registros de usuarios a la Historia Clínica Electrónica? Usuario y contraseña. | | |
| 21 | ¿Existen procesos formales para asignación de perfiles de acceso a la Historia Clínica Electrónica? | | |
| 22 | ¿Existe un proceso específico para la asignación y autorización de permisos especiales para el acceso y manejo de los datos sensibles de la Historia Clínica | | |

| | | | |
|---|---|---|---|
| | Electrónica? | | |
| 23 | ¿Se ha establecido una política específica para el manejo de información clasificada como secreta o privada? | | |
| 24 | ¿Se ha establecido periodos concretos para renovación de permisos de acceso a la Historia Clínica Electrónica? | | |
| 25 | ¿Existe un proceso establecido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos? | | |
| 26 | ¿Se establecen perfiles específicos de acceso para el sistema de Información (Historia Clínica Electrónica) de forma que se restringa la información a la actividad o tarea específica a desarrollar? | | |
| 27 | ¿Se han implementado procesos de acceso seguro para el inicio de sesión de la Historia Clínica Electrónica considerando limitaciones de intentos de acceso para evitar la suplantación y uso inapropiado de la información? | | |
| 28 | ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras? | | |
| **Cuestionario – Seguridad Física y del Entorno<br>Dominio A11 - Subdominio A11.1 – A11.2** | | | |
| **No.** | **ÌTEM** | **SI** | **NO** |
| 29 | ¿Existen controles de acceso de personas no autorizadas en áreas restringidas y con acceso al sistema de información? | | |
| 30 | ¿Se han establecidos medidas de seguridad para zonas seguras (consultorios) para proteger la información privada y sensible a personal externo? | | |
| 31 | ¿Se controla o supervisa la actividad de personal que accede a áreas seguras y que tienen acceso al sistema de información? | | |

| | | | |
|---|---|---|---|
| Elaborado por: | Mauricio A. Neuta A. | Revisado por: | Mauricio A. Neuta A. |
| Entrevistado: | | Firma del entrevistado: | |

Como se puede observar, el formato de la encuesta contiene varios campos que pueden describirse de la siguiente manera:

*Tabla 6. Campos que conforman la encuesta*

| CAMPO | DESCRIPCIÓN |
|---|---|
| **REF**: | Identificación de la encuesta. |
| **AREA:** | Nombre del área a la cual se aplica la auditoría. |
| **FECHA**: | Día en el que se realizó la encuesta. |
| **OBJETIVO**: | Propósito por el cual se realiza la encuesta. |
| **NO:** | Orden de las preguntas encuestadas. |
| **ITEM**: | Preguntas que estructuran la encuesta. |
| **SI – NO:** | Opciones de respuesta. |
| **ELABORADO POR**: | Nombre del auditor. |
| **REVISADO POR**: | Nombre del auditor. |
| **ENTREVISTADO**: | Nombre de la persona a quien se le aplicó la encuesta. |
| **FIRMA DEL ENTREVISTADO**: | Firma de la persona a quien se le aplicó la encuesta. |

Autor: Propia del autor

**Cuestionario cuantitativo**. Contiene una serie de preguntas formuladas y objetivas utilizadas para obtener información detallada de los encuestados sobre un tema de investigación. Dichas preguntas son cerradas, es decir, sólo tienen dos opciones de respuesta: SI y NO.

El cuestionario cuantitativo, también permite establecer el porcentaje de riesgo y para ello se usa la siguiente fórmula:

$$\% \text{ de Riesgo} = \frac{\text{Sumatoria Respuestas SI} * 100}{\text{Total Encuesta}}$$

Fuente: Formula tomada del estudio de investigación realizada a la "S*eguridad de la red de datos del instituto departamental de salud de Nariño*". Disponible en https://repository.unad.edu.co/bitstream/handle/10596/11986/12749865.pdf?sequence=1

Una vez se calcule dicho porcentaje, se determina el nivel de riesgo total, para lo cual se tiene en cuenta la siguiente categorización:

*Tabla 7. Niveles de riesgo*

| Rango | Nivel de Riesgo | Descripción |
|---|---|---|
| 1% - 30% | Bajo | Deficiencias fáciles de solucionar a largo plazo. |
| 31% - 70% | Medio | Deficiencias que requieren de medidas de solución o mejora a corto plazo. |
| 71% - 100% | Alto | Deficiencias que requieren soluciones inmediatas para reducir el riesgo. |

Fuente: Formula tomada del estudio de investigación realizada a la "S*eguridad de la red de datos del instituto departamental de salud de Nariño*". Disponible en https://repository.unad.edu.co/bitstream/handle/10596/11986/12749865.pdf?sequence=1

Finalmente se calcula el porcentaje de riesgo total aplicando la fórmula:

% Riesgo Total = 100 - % de Riesgo

Fuente: Formula tomada del estudio de investigación realizada a la "S*eguridad de la red de datos del instituto departamental de salud de Nariño*". Disponible en https://repository.unad.edu.co/bitstream/handle/10596/11986/12749865.pdf?sequence=1

Con éste resultado se podrá concluir sobre el funcionamiento del proceso evaluado, teniendo como soporte, el conjunto de pruebas que permiten verificar los resultados de la encuesta.

### 5.2.9 Fuentes de recolección de información

Las fuentes de información que se tienen en cuenta para la realización del proyecto se pueden catalogar en información primaria.

**Fuentes de información primaria**: Las fuentes primarias están constituidas por la información original suministrada por los profesionales del área de la salud que laboran en la entidad y que están involucrados o que tienen relación directa con la Historia Clínica Electrónica. Se tomó una muestra de veinte (20) personas de la población total; entre los perfiles encuestados se encuentran médicos, enfermeras

jefes, psicólogos y auxiliares de enfermería, debido a que son el personal más idóneo y que califican para dar respuesta a todas y cada de las preguntas evaluadas.

### 5.2.10 Resultados de la encuesta

A continuación se muestran los resultados obtenidos una vez aplicada la encuesta al personal debidamente seleccionada.

| | **AUDITORÍA A LA PROTECCIÓN DE LOS DATOS SOBRE LA HISTORIA CLÍNICA ELECTRÓNICA DE LA E.S.E. MUNICIPAL MANUEL CASTRO TOVAR** | **REF.** | | |
|---|---|---|---|---|
| **AREA** | | **D** | **M** | **A** |
| | | | | |

**Encuesta a la confidencialidad y privacidad de los datos sensibles de la Historia Clínica Electrónica**

**OBJETIVO:**

Evaluar la confidencialidad y privacidad de los datos sensibles de los usuarios en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar para determinar las vulnerabilidades, amenazas y riesgos que existen en el tratamiento y custodia de la información de acuerdo a los estándares de control establecidos en la Norma ISO/27001:2013 - ISO/27002:2013.

**Nota aclaratoria**: Para el desarrollo de esta encuesta **NO** se solicita ninguna información de carácter personal, debido a que los datos requeridos, corresponden exclusivamente para efectos académicos.

**Cuestionario inicial**

| **No.** | **ÌTEM** | **SI** | **NO** |
|---|---|---|---|
| 1 | ¿Conoce la política de protección de datos personales? | 7 | 13 |
| 2 | ¿Conoce la clasificación de los datos personales e implicaciones legales? | 9 | 11 |
| 3 | ¿Conoce la definición de “Dato sensible”? | 7 | 13 |
| 4 | ¿Conoce la definición de “Dato privado”? | 13 | 7 |
| 5 | ¿Conoce la definición de “Confidencialidad”? | 18 | 2 |

| | | | |
|---|---|---|---|
| 6 | ¿Conoce la política de delitos informáticos? | 8 | 12 |
| **Cuestionario - Organización de la Seguridad de la Información Dominio A6 - Subdominio A6.1 - A6.2** | | | |
| **No.** | **ÌTEM** | **SI** | **NO** |
| 7 | ¿Considera que la gestión de la Historia Clínica Electrónica brinda la confianza y seguridad para garantizar que los datos manejados cumplen con los principios de privacidad y confidencialidad? | 5 | 15 |
| 8 | ¿Se han asignado y definido las responsabilidades de los usuarios de la Historia Clínica Electrónica sobre la seguridad de la Información en los distintos procesos, tareas o actividades de la empresa? | 7 | 13 |
| 9 | ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos a la Historia Clínica Electrónica? | 7 | 13 |
| 10 | ¿Existe un procedimiento establecido para informar ante el área competente los incidentes relacionados con la Seguridad de la Información? | 5 | 15 |
| 11 | ¿Existe controles para afrontar posibles eventualidades sobre la seguridad de la información en la gestión de la Historia Clínica Electrónica? | 5 | 15 |
| **Cuestionario - Gestión de Activos Dominio A8 - Subdominio A8.1 - A8.3** | | | |
| **No.** | **ÌTEM** | **SI** | **NO** |
| 12 | ¿Se han establecido políticas, normas o procesos para el uso apropiado de los datos sensibles de la Historia Clínica Electrónica en relación a su seguridad? | 7 | 13 |
| 13 | ¿Existe un proceso para la devolución de la información privada cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato? | 5 | 15 |
| 14 | ¿Se clasifica la información según su confidencialidad o su privacidad a fin de establecer medidas de seguridad especificas? | 5 | 15 |
| 15 | ¿Los datos recogidos en la Historia Clínica Electrónica son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación? | 7 | 13 |
| 16 | ¿Existen procedimientos para el manejo y trato de la información de acuerdo a su clasificación? | 7 | 13 |
| 17 | ¿Existen controles o procedimientos establecidos para aplicar a soportes extraíbles o externos para proteger su seguridad? | 7 | 13 |

| | | | |
|---|---|---|---|
| | -Uso<br>-Borrado<br>-Cifrado<br>-Impresión.<br>-Transferencia<br>-Etc. | | |
| **Cuestionario – Control de Acceso<br>Dominio A9 - Subdominio A9.1 – A9.4** | | | |
| **No.** | **ÌTEM** | **SI** | **NO** |
| 18 | ¿Existe una política, norma o proceso que defina los controles de acceso a los datos sensibles de la Historia Clínica Electrónica y que tengan en cuenta el acceso selectivo a la información según las necesidades de cada área o puesto de trabajo? | 7 | 13 |
| 19 | ¿Están establecidos las restricciones o accesos limitados a los recursos de la Historia Clínica Electrónica según perfiles determinados? | 9 | 11 |
| 20 | ¿Existen procesos formales de registros de usuarios a la Historia Clínica Electrónica? Usuario y contraseña. | 14 | 6 |
| 21 | ¿Existen procesos formales para asignación de perfiles de acceso a la Historia Clínica Electrónica? | 13 | 7 |
| 22 | ¿Existe un proceso específico para la asignación y autorización de permisos especiales para el acceso y manejo de los datos sensibles de la Historia Clínica Electrónica? | 9 | 11 |
| 23 | ¿Se ha establecido una política específica para el manejo de información clasificada como secreta o privada? | 6 | 14 |
| 24 | ¿Se ha establecido periodos concretos para renovación de permisos de acceso a la Historia Clínica Electrónica? | 4 | 16 |
| 25 | ¿Existe un proceso establecido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos? | 6 | 14 |
| 26 | ¿Se establecen perfiles específicos de acceso para el sistema de Información (Historia Clínica Electrónica) de forma que se restringa la información a la actividad o tarea específica a desarrollar? | 7 | 13 |
| 27 | ¿Se han implementado procesos de acceso seguro para el inicio de sesión de la Historia Clínica Electrónica considerando limitaciones de intentos de acceso para evitar la suplantación y uso inapropiado de la información? | 6 | 14 |
| 28 | ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras? | 9 | 11 |

| Cuestionario – Seguridad Física y del Entorno<br>Dominio A11 - Subdominio A11.1 – A11.2 | | | |
|---|---|---|---|
| **No.** | **ÌTEM** | **SI** | **NO** |
| 29 | ¿Existen controles de acceso de personas no autorizadas en áreas restringidas y con acceso al sistema de información? | 8 | 12 |
| 30 | ¿Se han establecidos medidas de seguridad para zonas seguras (consultorios) para proteger la información privada y sensible a personal externo? | 6 | 14 |
| 31 | ¿Se controla o supervisa la actividad de personal que accede a áreas seguras y que tienen acceso al sistema de información? | 6 | 14 |

| | | | |
|---|---|---|---|
| Elaborado por: | Mauricio A. Neuta A. | Revisado por: | Mauricio A. Neuta A. |
| Entrevistado: | | Firma del entrevistado: | |

$$\% \text{ de Riesgo} = \frac{239 * 100}{620}$$

$$\% \text{ de Riesgo} = 38.5$$

$$\% \text{ Riesgo Total} = 100 - 38.5$$

$$\% \text{ Riesgo Total} = 61.5$$

Fuente: Formula tomada del estudio de investigación realizada a la "S*eguridad de la red de datos del instituto departamental de salud de Nariño*". Disponible en https://repository.unad.edu.co/bitstream/handle/10596/11986/12749865.pdf?sequence=1

**Riesgo Parcial**: El Riesgo Parcial da como resultado al multiplicar las 239 respuestas que marcaron SI en la encuesta, por el 100%, y se divide por el total de respuestas evaluadas (620).

**El Riesgo Total**: El Riesgo Total da como resultado al restar el 100%, menos el resultado previamente arrojado por el Riesgo Parcial (38.5).

Según el resultado obtenido en el Riesgo Total, indicara el Nivel de Riesgo en que se encuentra involucrada y comprometida la seguridad de la información en la Historia Clínica Electrónica.

*Tabla 8. Resultado niveles de riesgo*

| Resultado del Riesgo | Rango | Nivel de Riesgo | Descripción |
|---|---|---|---|
| 61.5 | 31% - 70% | Medio | Deficiencias que requieren de medidas de solución o mejora a corto plazo. |

Fuente: Formula tomada del estudio de investigación realizada a la "S*eguridad de la red de datos del instituto departamental de salud de Nariño*". Disponible en https://repository.unad.edu.co/bitstream/handle/10596/11986/12749865.pdf?sequence=1

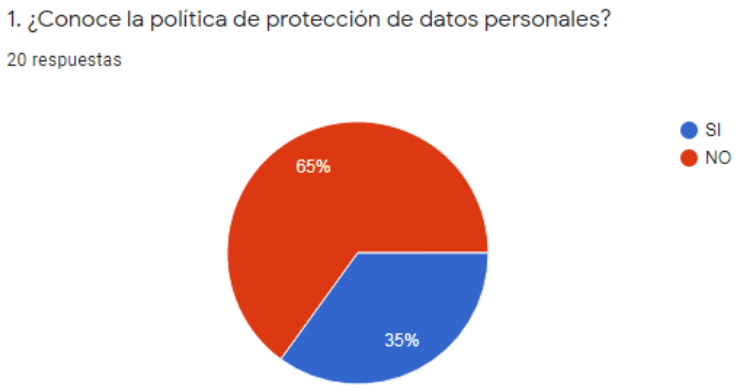
**RIESGO:**

Porcentaje de Riesgo Parcial: = 38.5 %
Porcentaje de Riesgo Total= 61.5
Impacto según relevancia del proceso: Riesgo Medio

### 5.2.11 Análisis de las respuestas resultante de la encuesta

Las siguientes gráficas muestran los resultados de las encuestas aplicadas a los funcionarios de la institución E.S.E. Municipal Manuel Castro Tovar sobre la protección de los datos en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar:

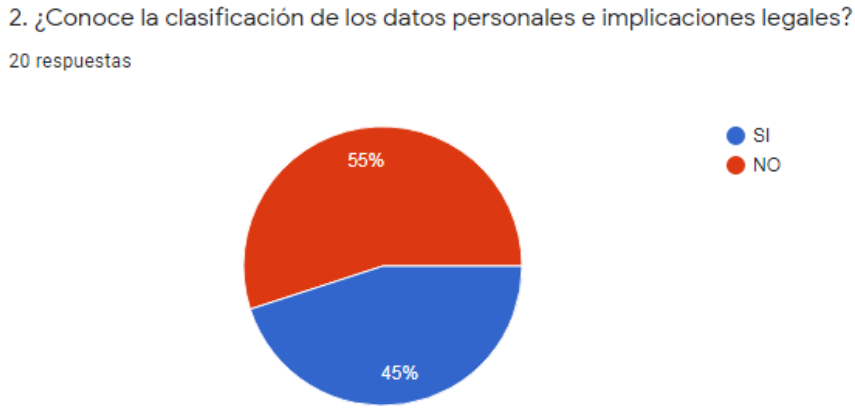
Gráfica 1.




Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica indica que un 65%, correspondiente a 13 personas, NO conocen la política de protección de datos personales, y un 35%, correspondiente a 7 personas, SI conocen la política.

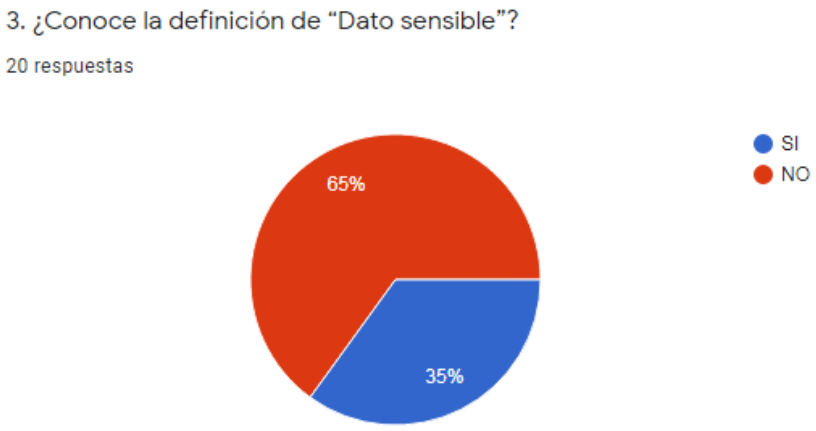
Gráfica 2.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en la gráfica, un 55%, correspondiente a 11 personas, calificaron este ítem de evaluación como, NO conocen la clasificación de los datos personales e implicaciones legales, y un 45%, correspondiente a 9 personas, calificaron diciendo, SI conocen la clasificación e implicaciones legales.

Gráfica 3.

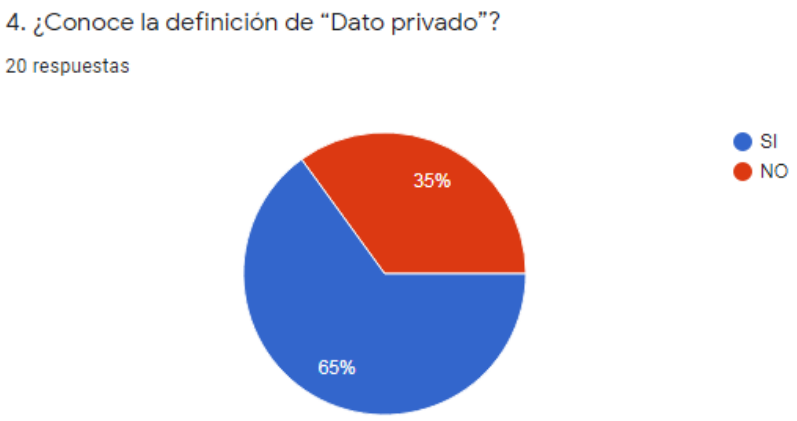



Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 3, un 65%, correspondiente a 13 personas, manifiestan que NO conocen la definición

de “Dato sensible”, y un 35%, correspondiente a 7 personas, asimilan o expresan que SI conocen su definición.

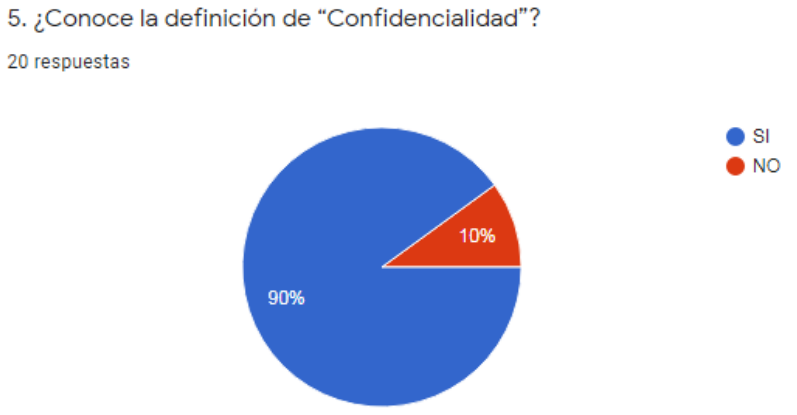
Gráfica 4.




Fuente: Propia del autor

De un total de 20 personas encuestadas, se puede observar en la gráfica que, un 35%, correspondiente a 7 personas, manifiestan que NO conocen la definición de “Dato privado”, y un 65%, correspondiente a 13 personas, del mismo modo asimilan o expresan que SI conocen su definición.

Gráfica 5.




Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 5 indica que, un 10%, correspondiente a 2 personas, manifiestan que NO conocen la definición de

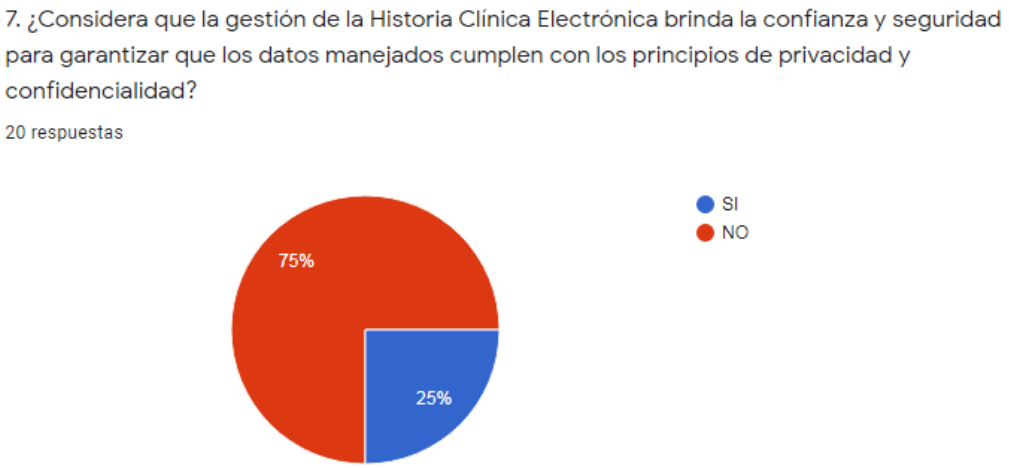
“Confidencialidad”, y un 90%, correspondiente a 18 personas, claramente dejan expuesto que SI conocen su definición.

Gráfica 6.


Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en esta gráfica, un 60%, correspondiente a 12 personas, calificaron este ítem de evaluación como, NO conocen la política de delitos informáticos, y un 40%, correspondiente a 8 personas, calificaron diciendo, SI conocen la clasificación e implicaciones legales

Gráfica 7.




Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 7, un 75%, correspondiente a 15 personas, manifiestan que NO consideran que la

gestión de la Historia Clínica Electrónica brinda la confianza y seguridad para garantizar que los datos manejados cumplen con los principios de privacidad y confidencialidad, y un 25%, correspondiente a 5 personas, asimilan o expresan que SI se brinda la confianza y seguridad.

Gráfica 8.


Fuente: Propia del autor

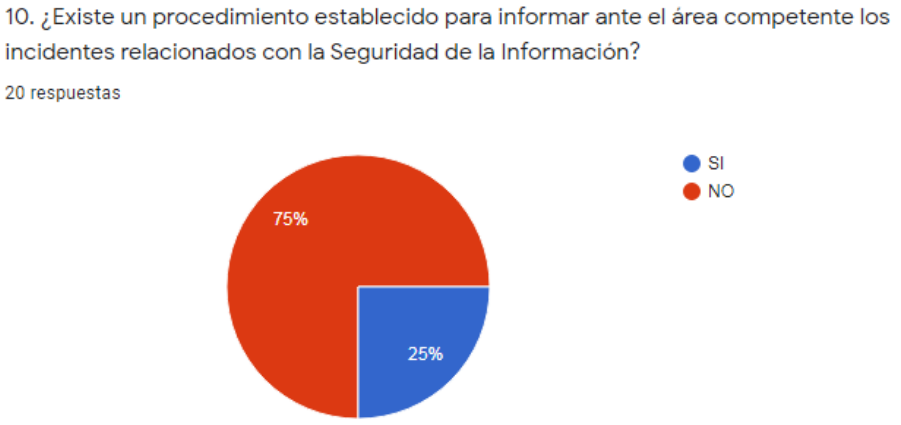
De un total de 20 personas encuestadas, se puede observar en la gráfica 8 que, un 65%, correspondiente a 13 personas, manifiestan que NO se han asignado y definido las responsabilidades de los usuarios de la Historia Clínica Electrónica sobre la seguridad de la Información en los distintos procesos, tareas o actividades de la empresa, y un 35%, correspondiente a 7 personas, del mismo modo asimilan o expresan que SI se han designado las diferentes responsabilidades.

Gráfica 9.


Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 9 indica que, un 65%, correspondiente a 13 personas, manifiestan que NO se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos a la Historia Clínica Electrónica, y un 35%, correspondiente a 7 personas, claramente dejan expuesto que SI se han segregado las áreas de responsabilidades.

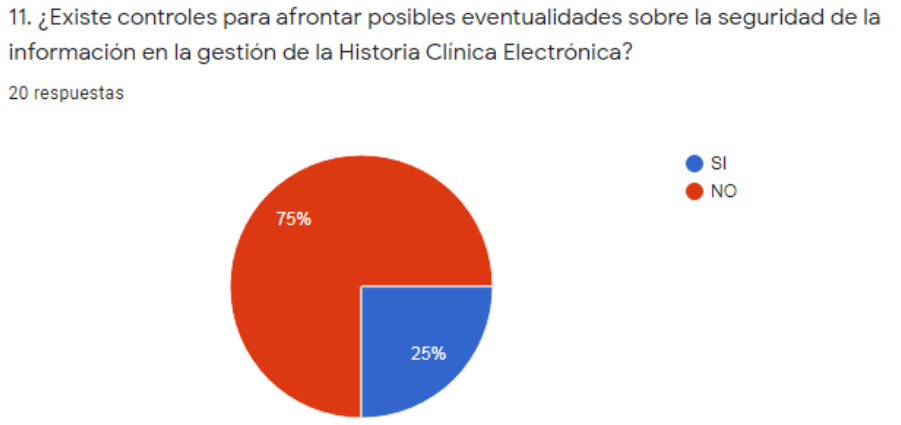
Gráfica 10.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en esta gráfica, un 75%, correspondiente a 15 personas, calificaron este ítem de evaluación como, NO existe un procedimiento establecido para informar ante el área competente los incidentes relacionados con la Seguridad de la Información, y un 25%, correspondiente a 5 personas, calificaron diciendo, SI existe tales procedimientos.

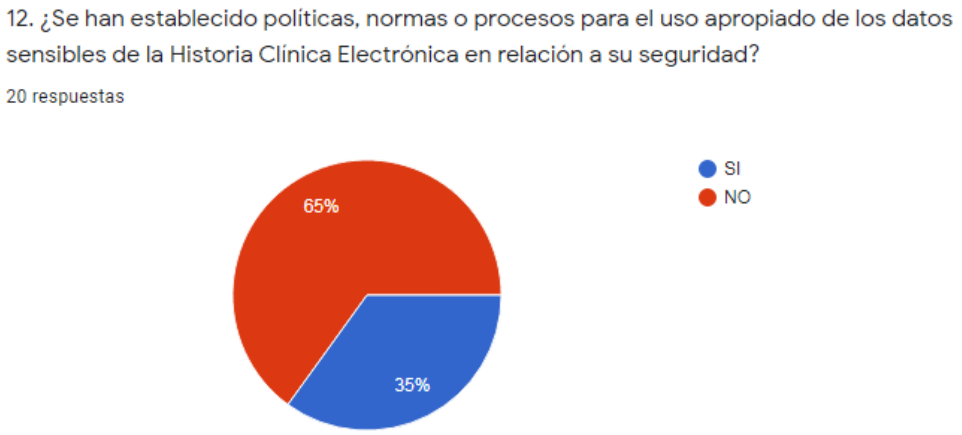
Gráfica 11.




Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 11, un 75%, correspondiente a 15 personas, manifiestan que NO existen controles para afrontar posibles eventualidades sobre la seguridad de la información en la gestión de la Historia Clínica Electrónica, y un 25%, correspondiente a 5 personas, asimilan o expresan que SI existen controles para posibles eventualidades.

Gráfica 12.




Fuente: Propia del autor

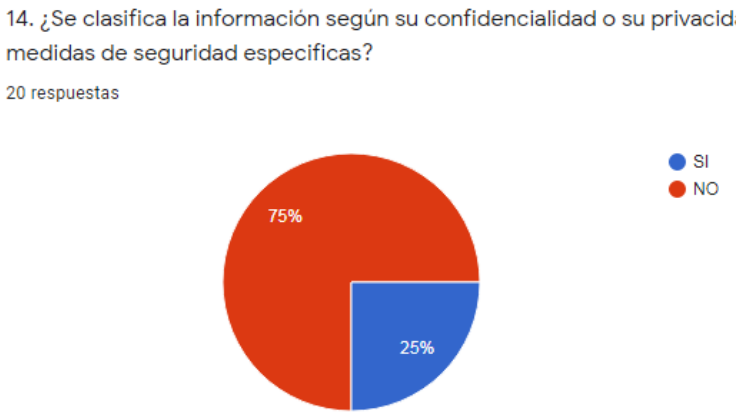
De un total de 20 personas encuestadas, se puede observar en la gráfica 12 que, un 65%, correspondiente a 13 personas, manifiestan que NO se han establecido políticas, normas o procesos para el uso apropiado de los datos sensibles de la Historia Clínica Electrónica en relación a su seguridad, y un 35%, correspondiente a 7 personas, asimilan o expresan que SI se han establecidos políticas.

Gráfica 13.


Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 13 indica que, un 75%, correspondiente a 15 personas, manifiestan que NO existe un proceso para la devolución de la información privada cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato, y un 25%, correspondiente a 5 personas, claramente dejan expuesto que SI existe el proceso en mención.

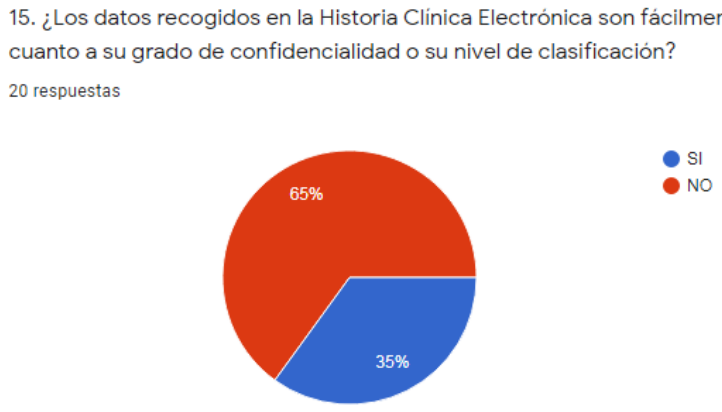
Gráfica 14.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en esta gráfica, un 75%, correspondiente a 15 personas, calificaron este ítem de evaluación como, NO se clasifica la información según su confidencialidad o su privacidad a fin de establecer medidas de seguridad específicas, y un 25%, correspondiente a 5 personas, calificaron diciendo, SI se clasifica la información.

Gráfica 15.




Fuente: Propia del autor

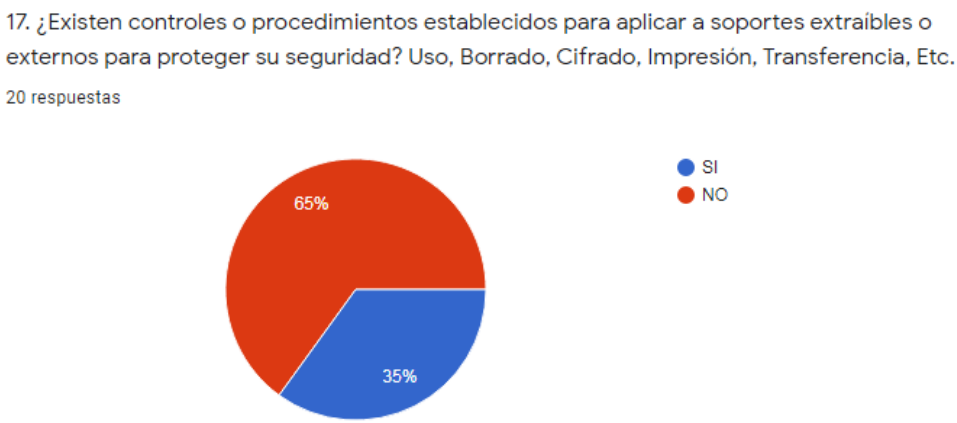
De un total de 20 personas encuestadas, según el ítem de evaluación número 15, un 65%, correspondiente a 13 personas, manifiestan que los datos recogidos en la Historia Clínica Electrónica NO son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación, y un 35%, correspondiente a 7 personas, asimilan o expresan que los datos recogidos, SI son fácilmente identificables en cuanto a su grado de confidencialidad.

Gráfica 16.


Fuente: Propia del autor

De un total de 20 personas encuestadas, se puede observar en la gráfica 16 que, un 65%, correspondiente a 13 personas, manifiestan que NO existen procedimientos para el manejo y trato de la información de acuerdo a su clasificación y un 35%, correspondiente a 7 personas, asimilan o expresan que SI existen procedimientos para su manejo.

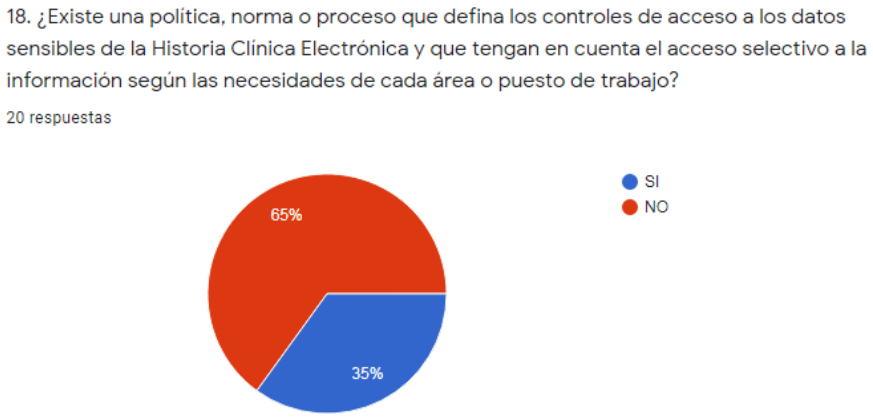
Gráfica 17.




Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 17 indica que, un 65%, correspondiente a 15 personas, manifiestan que NO existen controles o procedimientos establecidos para aplicar a soportes extraíbles o externos para proteger su seguridad: Uso, Borrado, Cifrado, Impresión, Transferencia, Etc. y un 25%, correspondiente a 5 personas, claramente dejan expuesto que SI existen controles o procedimientos establecidos.

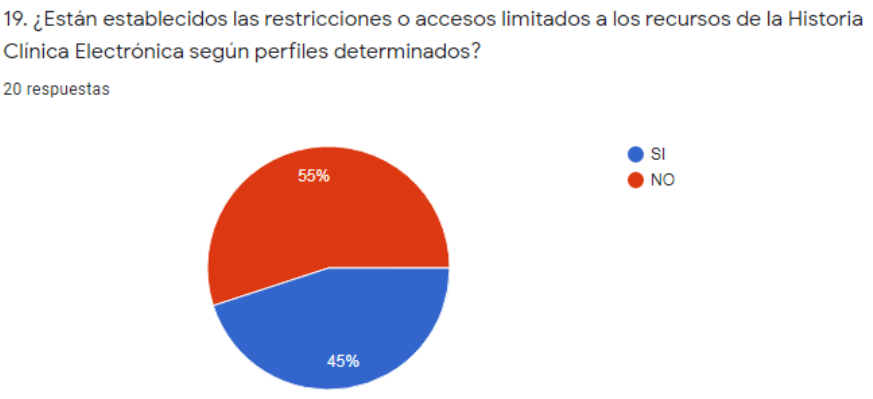
Gráfica 18.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en esta gráfica, un 65%, correspondiente a 13 personas, calificaron este ítem de evaluación como, NO existe una política, norma o proceso que defina los controles de acceso a los datos sensibles de la Historia Clínica Electrónica y que tengan en cuenta el acceso selectivo a la información según las necesidades de cada área o puesto de trabajo, y un 35%, correspondiente a 7 personas, calificaron diciendo, SI existe una política que defina los controles de acceso a los datos.

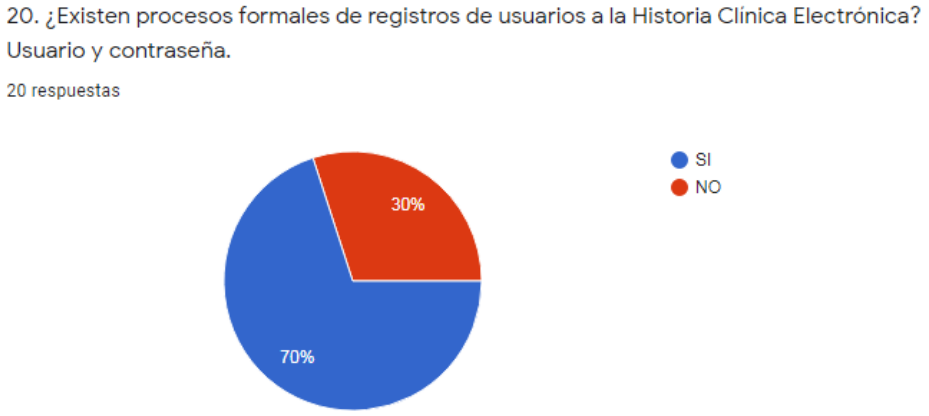
Gráfica 19.




Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 19, un 55%, correspondiente a 11 personas, manifiestan que NO están establecidas las restricciones o accesos limitados a los recursos de la Historia Clínica Electrónica según perfiles determinados, y un 45%, correspondiente a 9 personas, asimilan o expresan que SI están establecidas los accesos limitados mencionados.

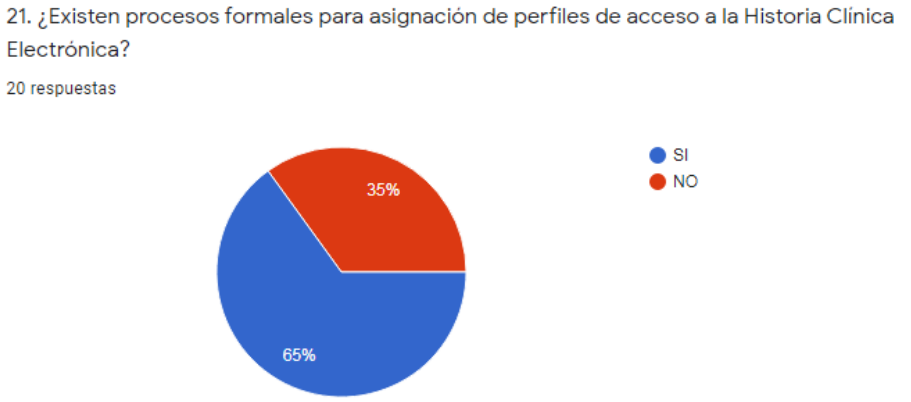
Gráfica 20.




Fuente: Propia del autor

De un total de 20 personas encuestadas, se puede observar en la gráfica 20 que, un 30%, correspondiente a 6 personas, manifiestan que NO existen procesos formales de registros de usuarios a la Historia Clínica Electrónica: Usuario y contraseña, y un 70%, correspondiente a 14 personas, asimilan o expresan que SI existen procesos formales de registros de usuarios.

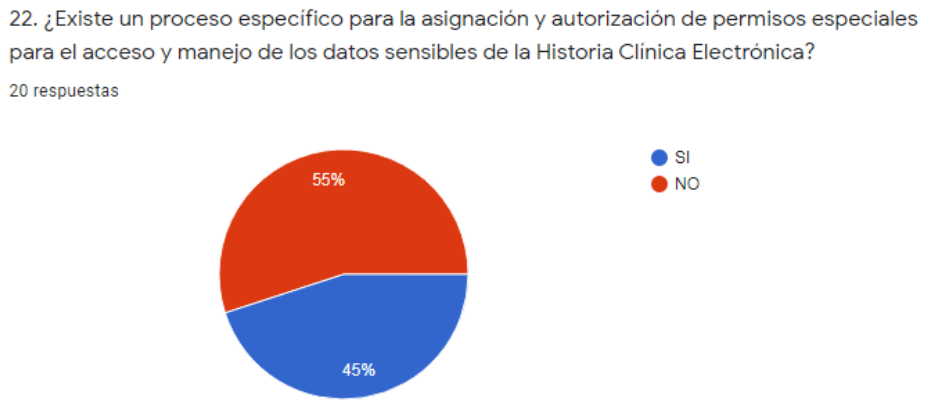
Gráfica 21.




Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 21 indica que, un 35%, correspondiente a 7 personas, manifiestan que NO Existen procesos formales para asignación de perfiles de acceso a la Historia  Clínica Electrónica, Etc. y un 65%, correspondiente a 13 personas, claramente dejan expuesto que SI existen procesos formales.

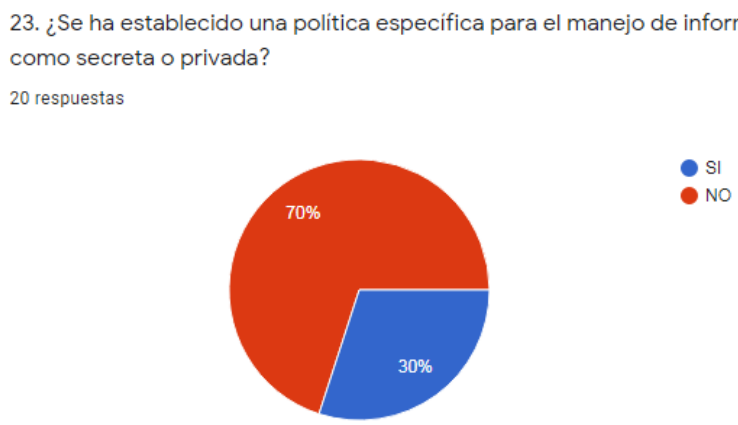
Gráfica 22.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en esta gráfica, un 55%, correspondiente a 11 personas, calificaron este ítem de evaluación como, NO existe un proceso específico para la asignación y autorización de permisos especiales para el acceso y manejo de los datos sensibles de la Historia  Clínica Electrónica, y un 45%, correspondiente a 9 personas, calificaron diciendo, SI existe el proceso específico para la asignación de permisos especiales.

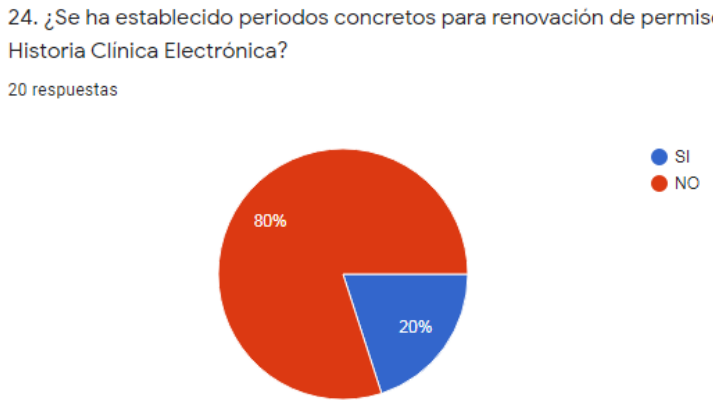
Gráfica 23.




Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 23, un 70%; correspondiente a 14 personas, manifiestan que NO se ha establecido una política específica para el manejo de información clasificada como secreta o privada, y un 30%, correspondiente a 6 personas, asimilan o expresan que SI se ha establecido la política.

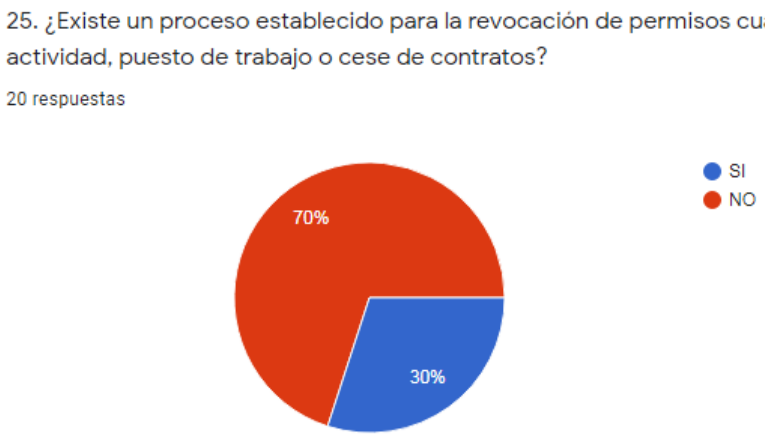
Gráfica 24.




Fuente: Propia del autor

De un total de 20 personas encuestadas, se puede observar en la gráfica 24 que, un 80%, correspondiente a 16 personas, manifiestan que NO se ha establecido periodos concretos para renovación de permisos de acceso a la Historia Clínica Electrónica, y un 20%, correspondiente a 4 personas, asimilan o expresan que SI existen los periodos concretos mencionados.

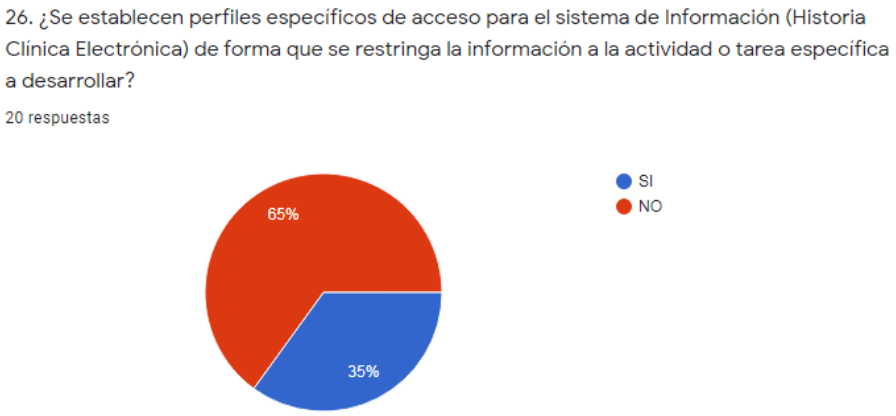
Gráfica 25.




Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 25 indica que, un 70%, correspondiente a 14 personas, manifiestan que NO existe un proceso establecido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos, y un 30%, correspondiente a 6 personas, claramente dejan expuesto que SI existen procesos para la revocación de permisos

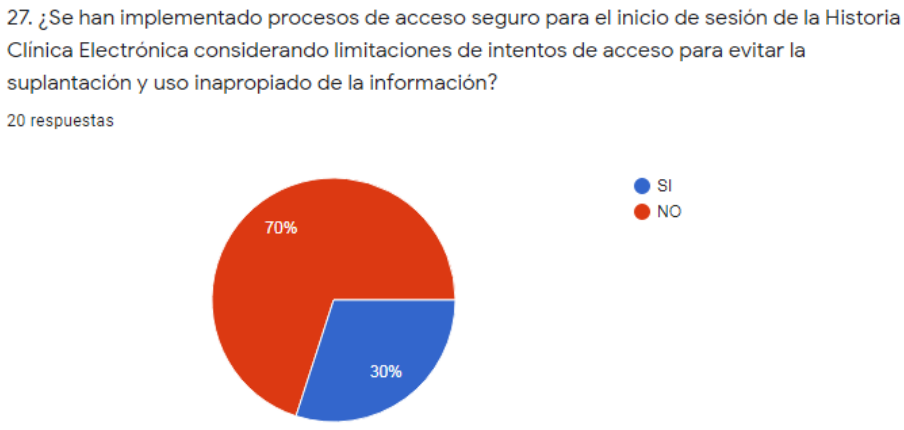
Gráfica 26.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede observar en esta gráfica, un 65%, correspondiente a 13 personas, calificaron este ítem de evaluación como, NO se establecen perfiles específicos de acceso para el sistema de Información (Historia Clínica Electrónica) de forma que se restringa la información a la actividad o tarea específica a desarrollar, y un 35%, correspondiente a 7 personas, calificaron diciendo, SI están establecidos los perfiles de acceso.

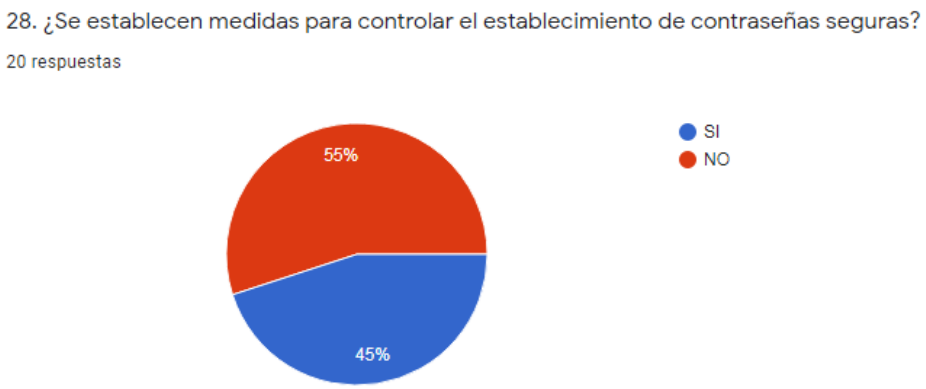
Gráfica 27.




Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 27, un 70%, correspondiente a 14 personas, manifiestan que NO se han implementado procesos de acceso seguro para el inicio de sesión de la Historia Clínica Electrónica considerando limitaciones de intentos de acceso para evitar la suplantación y uso inapropiado de la información, y un 30%, correspondiente a 6 personas, asimilan o expresan que SI están implementado los procesos de acceso seguro.

Gráfica 28.




Fuente: Propia del autor

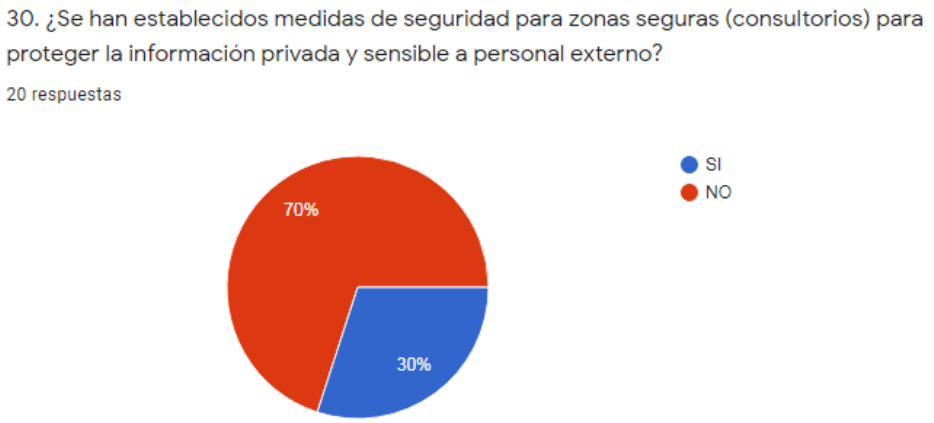
De un total de 20 personas encuestadas, se puede observar en la gráfica 28 que, un 55%, correspondiente a 11 personas, manifiestan que NO se establecen medidas para controlar el establecimiento de contraseñas seguras y un 45%, correspondiente a 9 personas, asimilan o expresan que SI existen las medidas establecidas..

Gráfica 29.


Fuente: Propia del autor

De un total de 20 personas encuestadas, la gráfica 29 indica que, un 60%, correspondiente a 12 personas, manifiestan que NO existen controles de acceso de personas no autorizadas en áreas restringidas y con acceso al sistema de información, y un 40%, correspondiente a 8 personas, claramente dejan expuesto que SI existen dichos controles de acceso.

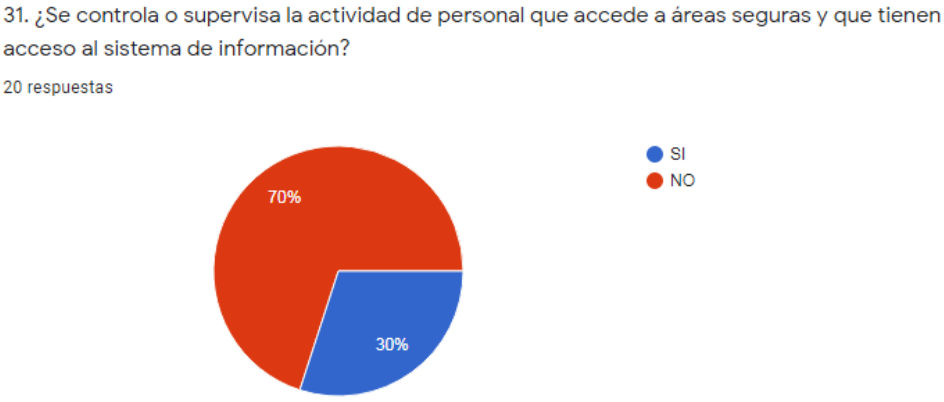
Gráfica 30.




Fuente: Propia del autor

De un total de 20 personas encuestadas, como se puede apreciar en esta gráfica, un 70%, correspondiente a 14 personas, calificaron este ítem de evaluación como, NO Se han establecidos medidas de seguridad para zonas seguras (consultorios) para proteger la información privada y sensible a personal externo, y un 30%, correspondiente a 6 personas, calificaron diciendo, SI están establecidas las medidas de seguridad de áreas seguras.

Gráfica 31.




Fuente: Propia del autor

De un total de 20 personas encuestadas, según el ítem de evaluación número 31, un 70%, correspondiente a 14 personas, manifiestan que NO se controla o supervisa la actividad de personal que accede a áreas seguras y que tienen acceso al sistema de información, y un 30%, correspondiente a 6 personas, asimilan o expresan que SI se controla el acceso a las zonas en mención.

## Análisis y Gestión de Riesgos

"El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo".[26]

## Metodología de Evaluación de Riesgo

Para este proyecto se empleó la Metodología MAGERIT por su experiencia en el análisis y gestión de los riesgos, y además porque presenta las siguientes características:

- MAGERIT permite analizar el impacto que puede resultar para una entidad la violación de la seguridad de la información, identificando y clasificando las amenazas y vulnerabilidades presentes en esta.
- MAGERIT comprende toda una guía absoluta que específica el paso a paso sobre la manera de efectuar el análisis de riesgos.
- MAGERIT tiene una visión estratégica general de la Seguridad de los Sistemas de Información ISO 27001.

MAGERIT persigue los siguientes Objetivos:

- "Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso." [27]

[26] Wikipedia. (13 noviembre 2019 ) Análisis de riesgo informático. Disponible en https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

[27] Catálogo de Elementos. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

MAGERIT funciona bajo los siguientes pasos:

*Tabla 9. Pasos Metodología MAGERIT*

| Pasos | Descripción |
|---|---|
| Paso 1 | Inventario y Valoración de Activos. |
| Paso 2 | Identificación y Valoración de Amenazas y Vulnerabilidades. |
| Paso 3 | Medición del impacto. |
| Paso 4 | Medición del Riesgo. |

Fuente: MAGERIT v.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

**Identificación de Amenazas**

A continuación, se observa las tablas de dimensiones de seguridad y las amenazas que se pueden presentar según la metodología MAGERIT.

*Tabla 10. Dimensiones de seguridad según MAGERIT*

| Dimensiones de Seguridad a valorar | Identificación |
|---|---|
| Autenticidad | A |
| Confidencialidad | C |
| Integridad | I |
| Disponibilidad | D |
| Trazabilidad | T |

Fuente: MAGERIT v.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

*Tabla 11. Tipos de amenazas*

| Identificación de las Amenazas | |
|---|---|
| [N] | Desastres naturales |
| [I] | De Origen Industrial |
| [E] | Errores y fallos no intencionados |
| [A] | Ataques intencionados |

Fuente: MAGERIT v.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

A continuación se presenta un catálogo de amenazas posibles según la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT v3.0.

*Tabla 12. Catálogo de amenazas según metodología MAGERIT*

| Ítem | Tipo de Amenaza | Descripción |
|---|---|---|
| A001 | [N] Desastres Naturales. | Se incluyen:<br>[N.1] Fuego.<br>[N.2] Daños por agua. |
| A002 | [I] De origen Industrial. | Se incluyen:<br>[I.1] Fuego.<br>[I.2] Daños por agua.<br>[I.*] Desastres industriales.<br>[I.3] Contaminación mecánica.<br>[I.4] Contaminación electromagnética.<br>[I.5] Avería de origen físico o lógico.<br>[I.6] Corte del suministro eléctrico.<br>[I.7] Condiciones inadecuadas de temperatura o humedad.<br>[I.8] Fallo de servicios de comunicaciones.<br>[I.9] Interrupción de otros servicios o suministros esenciales.<br>[I.10] Degradación de los soportes de almacenamiento de la información.<br>[I.11] Emanaciones electromagnéticas |
| A003 | [E] Errores y fallos no intencionados. | Se incluyen:<br>[E.1] Errores de los usuarios.<br>[E.2] Errores del administrador.<br>[E.3] Errores de monitorización (log).<br>[E.4] Errores de configuración.<br>[E.7] Deficiencias en la organización.<br>[E.8] Difusión de software dañino.<br>[E.9] Errores de re-encaminamiento.<br>[E.10] Errores de secuencia.<br>[E.14] Fugas de información.<br>[E.15] Alteración de la información.<br>[E.16] Introducción de falsa |

| | | |
|---|---|---|
| | | información.<br>[E.17] Degradación de la información.<br>[E.18] Destrucción de la información.<br>[E.19] Divulgación de información.<br>[E.20] Vulnerabilidades de los programas (software).<br>[E.21] Errores de mantenimiento / actualización de programas (software).<br>[E.23] Errores de mantenimiento / actualización de equipos (hardware).<br>[E.24] Caída del sistema por agotamiento de recursos.<br>[E.25] Pérdida de equipos.<br>[E.28] Indisponibilidad del personal. |
| A004 | [A] Ataques intencionados. | Se incluyen:<br>[A.4] Manipulación de la configuración.<br>[A.5] Suplantación de la identidad del usuario.<br>[A.6] Abuso de privilegios de acceso.<br>[A.7] Uso no previsto.<br>[A.8] Difusión de software dañino.<br>[A.9]Re-encaminamiento de mensajes<br>[A.10] Alteración de secuencia.<br>[A.11] Acceso no autorizado.<br>[A.12] Análisis de tráfico.<br>[A.13] Repudio.<br>[A.14] Interceptación de información (escucha).<br>[A.15] Modificación de información.<br>[A.16] Introducción de falsa información<br>[A.17] Corrupción de la información.<br>[A.18] Destrucción de la información.<br>[A.19] Divulgación de información.<br>[A.22] Manipulación de programas.<br>[A.24] Denegación de servicio.<br>[A.25] Robo de equipos.<br>[A.26] Ataque destructivo.<br>[A.27] Ocupación enemiga.<br>[A.28] Indisponibilidad del personal.<br>[A.29] Extorsión.<br>[A.30] Ingeniería social (picaresca). |

Fuente: MAGERIT v.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos (.pdf). Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xdv-8pNKjcc

**Evaluación de las vulnerabilidades, riesgos y amenazas según los controles contemplados en los dominios del Anexo A de la norma ISO 27001:2013.**

Para este proyecto solo se aplicarán los dominios definidos a continuación debido a que en estos las vulnerabilidades, riesgos y amenazas encontradas afectan de manera considerable a la organización.

*Tabla 13. Evaluación de las vulnerabilidades, riesgos y amenazas según los controles del dominio A6 ISO 27001:2013*[28]

| **Dominio:** | | **Controles:** | |
|---|---|---|---|
| **A6. Organización de la seguridad de la información.** | | 6.1.1 Funciones y responsabilidades de la Seguridad de la información.<br>6.1.2 Separación de funciones.<br>6.1.3 Contacto con autoridades. | |
| **Vulnerabilidades** | **Riesgos** | **Tipos de Amenazas** | **Controles de mitigación** |
| • No se han definido las responsabilidades de los empleados o puestos de trabajos en relación a la Seguridad de la información que conllevan un riesgo de mal uso, accidental o deliberado, si | • Uso inadecuado de la información sensible de la HCE.<br>• Manejo de información sin previo conocimiento de sus responsabilidades y funciones. | [E.14] Fugas de información.<br>[E.15] Alteración de la información.<br>[E.19] Divulgación de información.<br>[A.28] Indisponibilidad del personal. | • Adicionar a las funciones de cada empleado o puesto de trabajo aquellas funciones que tengan que ver con la seguridad de la información.<br>• Comunicar a cada persona implicada en la Seguridad de |

[28] Norma Técnica Colombiana. (2007-11-16). NTC-ISO 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

| | | | |
|---|---|---|---|
| son compartidas por una misma persona.<br>• No se evidencia un reporte de incidentes de seguridad al área encargada de la seguridad. | | | la Información sus roles y responsabilidades.<br>• En caso de incidentes en la seguridad de la información, mantener informado al área inmediatamente encargada del control y seguridad de la información. |

Fuente: Propia del autor

*Tabla 14. Evaluación de las vulnerabilidades, riesgos y amenazas según los controles del dominio A8 ISO 27001:2013*[29]

| **Dominio:** | | **Controles:** | |
|---|---|---|---|
| **A8. Gestión de activos.** | | A8.1 Responsabilidad sobre los activos.<br>A8.1.3 Uso aceptable de los activos.<br>A8.1.4 Devolución de activos.<br>A8.2 Clasificación de la información.<br>A8.2.1 Clasificación de la información.<br>A8.2.2 Etiquetado de la información.<br>A8.2.3 Manejo de los activos.<br>A8.3 Manipulación de Soportes.<br>A8.3.1 Gestión de soportes extraíbles. | |
| **Vulnerabilidades** | **Riesgos** | **Tipos de Amenazas** | **Controles de mitigación** |
| • No se ha documentado | • El uso aceptable de | [E.14] Fugas de información. | • Establecer y/o documentar |

[29] Norma Técnica Colombiana. (2007-11-16). NTC-ISO 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

| | | | |
|---|---|---|---|
| el uso apropiado de la información que describa los requisitos de seguridad de la información.<br>• No se evidencia un control adecuado para que los empleados devuelvan los activos de información una vez finalizado el periodo de su utilización o contrato.<br>• No se evidencia una clasificación de la información según su nivel de protección necesario: Criticidad y sensibilidad en cuando a su divulgación o modificación no autorizada o accidental.<br>• Ausencia de procedimientos claros para el manipulado de la información de acuerdo a su clasificación. | información que puede incluir aspectos relacionados con la difamación, la suplantación de identidad, entre otros.<br>• La mala clasificación de la información puede incurrir en la divulgación de datos que puede causar daño, incomodidad o un impacto significativo en la organización.<br>• La transferencia o comunicación irregular de información puede incurrir en la pérdida de datos. | [E.15] Alteración de la información.<br>[A.16] Introducción de falsa información.<br>[E.18] Destrucción de la información.<br>[E.19] Divulgación de información.<br>[A.17] Corrupción de la información. | normas para el uso de información en relación a su seguridad.<br>• Establecer procedimientos transferencia y borrado de información de forma segura en el caso que sea pertinente.<br>• La clasificación de la información debe alinearse con la política de control de acceso.<br>• Mantener un registro actualizado de autorizaciones de uso o acceso a los activos. |

Fuente: Propia del autor

*Tabla 15. Evaluación de las vulnerabilidades, riesgos y amenazas según los controles del dominio A9 ISO 27001:2013*[30]

| **Dominio:** | | **Controles:** | |
|---|---|---|---|
| **A9. Control de acceso.** | | A9.1 Requisitos generales para el control de acceso.<br>A9.1.1 Política de control de acceso.<br>A9.1.2 Acceso a las redes y a los servicios de red.<br>A9.2 Accesos de Usuario.<br>A9.2.1 Registro de usuarios y cancelación del registro.<br>A9.2.2 Gestión de acceso a los usuarios.<br>A9.2.3 Gestión de derechos de acceso privilegiados.<br>A9.2.4 Gestión de la información de autenticación secreta de los usuarios.<br>A9.2.5 Revisión de derechos de acceso de usuario.<br>A9.2.6 Remoción o ajuste de los derechos de acceso.<br>A9.4 Control de acceso a sistemas y aplicaciones.<br>A9.4.1 Restricción de acceso a la información.<br>A9.4.2 Procedimientos de conexión (log-on) seguros.<br>A9.4.3 Sistema de gestión de contraseñas. | |
| **Vulnerabilidades** | **Riesgos** | **Tipos de Amenazas** | **Controles de mitigación** |
| • Ausencia de requisitos para definir las | • Si no hay permisos o privilegios | [E.14] Fugas de información.<br>[E.15] Alteración | • Establecer, documentar y revisar la |

[30] Norma Técnica Colombiana. (2007-11-16). NTC-ISO 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

| | | | |
|---|---|---|---|
| reglas de control de acceso a la información, o los derechos y restricciones de acceso a la información.<br>• No existe una política establecida para el manejo de información clasificada como secreta, restringida para ciertas áreas autorizadas.<br>• No se ha definido un control adecuado para establecer una revisión periódica de los permisos de accesos de los usuarios al sistema de información.<br>• No se evidencia el uso de contraseñas seguras para el inicio de sesión del sistema de información. | establecidos en la organización, los usuarios del sistema pueden realizar tareas que no les está permitido.<br>• Acceso a información confidencial y de un alto nivel de criticidad.<br>• Exposición de los datos sensibles a usuarios no autorizados.<br>• Posible suplantación para el acceso a los datos clasificados como privados.<br>• El uso de contraseñas de baja calidad, contraseñas débiles, posibilitan la opción de ser descifradas. | de la información.<br>[A.16] Introducción de falsa información.<br>[E.18] Destrucción de la información.<br>[E.19] Divulgación de información.<br>[A.17] Corrupción de la información.<br>[A.28] Indisponibilidad del personal.<br>[A.30] Ingeniería social (picaresca). | política de control de acceso periódicamente, lo que significa que una política documentada es obligatoria.<br>• Asignación de roles específicos.<br>• Asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo.<br>• Establecer un control para garantizar que se modifican los derechos de acceso al cambiar de puesto de trabajo dentro de la organización si así se requiere.<br>• El acceso al sistema de información debe contar con la validación de intentos fallidos para protegerse contra accesos |

| | | | |
|---|---|---|---|
| | | | forzosos o no permitidos. |

Fuente: Propia del autor

*Tabla 16. Evaluación de las vulnerabilidades, riesgos y amenazas según los controles del dominio A11 ISO 27001:2013*[31]

| **Dominio:** | | **Controles:** | |
|---|---|---|---|
| **A11. Seguridad física y del entorno.** | | A11.1 Áreas de seguridad<br>A11.1.2 Controles de acceso físico.<br>A11.1.3 Seguridad de oficinas, despachos e instalaciones. | |
| **Vulnerabilidades** | **Riesgos** | **Tipos de Amenazas** | **Controles de mitigación** |
| • No están establecidas las medidas de seguridad en las zonas de oficinas para proteger la información en pantallas en áreas accesibles a personal externo. | • El acceso de personal externo en áreas restringidas, puede generar que información susceptible ante cualquier actividad maliciosa. | [E.14] Fugas de información.<br>[E.19] Divulgación de información.<br>[A.28] Indisponibilidad del personal.<br>[A.30] Ingeniería social (picaresca). | • Establecer medidas de control físicas para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas. |

Fuente: Propia del autor

[31] Norma Técnica Colombiana. (2007-11-16). NTC-ISO 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

*Tabla 17. Evaluación de las vulnerabilidades, riesgos y amenazas según los controles del dominio A12 ISO 27001:2013*[32]

| **Dominio:** | | **Controles:** | |
|---|---|---|---|
| **A12. Seguridad en las operaciones.** | | A12.1 Procedimientos y responsabilidades<br>A12.1.1 Procedimientos documentados de operación.<br>A12.3 Copias de seguridad<br>A12.3.1 Respaldo de la información.<br>A12.6 Vulnerabilidad técnica<br>A12.6.1 Gestión de vulnerabilidades técnicas.<br>A12.6.2 Restricciones en la instalación de software.<br>A12.7 Auditorias de Sistemas de Información<br>A12.7.1 Controles de auditoría de sistemas de información. | |
| **Vulnerabilidades** | **Riesgos** | **Tipos de Amenazas** | **Controles de mitigación** |
| • No se dispone de un procedimiento para evaluar el impacto en la seguridad de la información.<br>• Se evidencia ausencia de controles para la instalación de software no autorizado por parte de los usuarios del sistema. | • La falta de formación y concienciación sobre los procedimientos en el tratamiento de la información y su cuidado, incurre en la injerencia de su custodia.<br>• La falta de controles para la instalación de aplicaciones | [E.14] Fugas de información.<br>[E.15] Alteración de la información.<br>[E.18] Destrucción de la información.<br>[E.19] Divulgación de información.<br>[A.28] Indisponibilidad del personal.<br>[A.30] Ingeniería social (picaresca). | • Documentar los procedimientos que abarcan aquellas actividades que afectan al procesamiento de la información y aquellas que la protegen.<br>• Fortalecer el proceso de respaldo para evitar la |

[32] Norma Técnica Colombiana. (2007-11-16). NTC-ISO 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información. Disponible en http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

| | | | |
|---|---|---|---|
| • No se evidencia mecanismos de auditorías de medidas de seguridad del sistema de información. | o software puede incurrir en daños irreparables en los activos de la información.<br>• La falta de procesos de auditorías puede crear una brecha de seguridad marcada, tratamiento inadecuado de la información y una mala gestión de los datos. | | pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.<br>• Establecer restricciones para la instalación de software por parte de los usuarios.<br>• Establecer protocolos específicos para el desarrollo de auditorías considerando su impacto en los sistemas. |

Fuente: Propia del autor

### 5.3 Elaboración del informe final de la auditoría.

Informe de auditoría del proceso realizado a la protección y manejo de confidencialidad de los datos sensibles que reposan en la Historia Clínica electrónica de los usuarios en la E.S.E. Municipal Manuel Castro Tovar.

## TABLA DE CONTENIDO

# INTRODUCCIÓN

El presente documento muestra los resultados obtenidos del proceso de auditoria realizado a la protección y manejo de confidencialidad de los datos sensibles que reposan en la Historia Clínica electrónica de los usuarios en la E.S.E. Municipal Manuel Castro Tovar.

La importancia de la realización de este proyecto, contribuirá de manera significativa a la E.S.E. Municipal Manuel Castro Tovar, para brindar una perspectiva del funcionamiento y trabajo de la actual Historia Clínica Electrónica y así tomar acciones que garanticen la mejora y el cumplimiento de los controles de seguridad.

El proyecto se ha basado principalmente en el análisis y verificación del cumplimiento de los controles de seguridad que brinda la norma ISO 27001:2013 en su anexo A, en cuanto al acceso y tratamiento de los datos en el sistema de información; esto con el fin de eliminar o mitigar el riesgo informático y salvaguardar activos de información para la mejora continua de la entidad.

Finalmente se registran los hallazgos y recomendaciones como insumo para las políticas de seguridad informática y de Información acorde a las actividades de la E.S.E. Municipal Manuel Castro Tovar, para ser aprobadas, difundidas y aplicadas en la misma.

## OBJETIVO

Conocer el estado actual de la seguridad de la Información en cuanto a los datos sensibles que reposan en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar, con el fin de determinar los riesgos, vulnerabilidades y amenazas a los que se encuentra expuesta la entidad y así determinar los controles de Seguridad conforme a los requisitos de la norma ISO/IEC 27001:2013.

## ALCANCE

Determinar a través de los hallazgos encontrados, los controles y las recomendaciones adecuadas para proteger y salvaguardar los datos sensibles en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar, de acuerdo a lo establecido por la norma ISO27001:2013 en su anexo A.

## DICTAMEN

1. Se ha auditado la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar, y evaluado el nivel de riesgo presente en los datos sensibles de la misma, con los hallazgos y recomendaciones anexos que se adjuntaron.

2. Para la ejecución del proyecto se utilizó la norma ISO 27001:2013 y la Metodología de Análisis y Gestión de Riesgos Magerit versión 3.0, las cuales permitieron determinar los riegos, las vulnerabilidades y las amenazas presentes en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar, con el fin de tomar medidas preventivas y correctivas que ayuden a eliminar los riesgos asociados o en su defecto minimizarlos al máximo.

En el desarrollo del proyecto se realizó lo siguiente:

- Para obtener información relevante se utilizó el método de la encuesta, por ser una técnica eficaz para obtener datos relevantes y significativos, con el fin de obtener una opinión personalizada de los profesionales de la salud y quienes son los responsables del uso y tratamiento de los datos.
- Se aplicó una encuesta que fue contestada por 20 personas. La encuesta permitirá determinar el conocimiento que tenían los usuarios del sistema sobre las políticas de seguridad de la información.
- Se indagó sobre la existencia de documentación en cuanto a políticas, normas y/o procedimientos de seguridad para determinar los roles y responsabilidades en el manejo de la información.
- Se verificó la existencia de controles de seguridad de la información de acuerdo a la norma ISO/IEC 27001 aplicando los dominios de seguridad establecidos en el Anexo A.
- Se plantearon nuevos controles de seguridad de acuerdo a los resultados obtenidos del proceso aplicado anteriormente.

3. Este dictamen tiene como fin mejorar la eficiencia en el manejo de los datos sensibles en la Historia Clínica Electrónica, minimizar los riesgos asociados en la misma y asegurar que se cumplan los controles de seguridad establecidos en la norma ISO 27001:2013.

## HALLAZGOS Y RECOMENDACIONES

En el presente trabajo de acuerdo a las encuestas realizadas dentro del proceso de la auditoría se encontró lo siguiente:

**Hallazgo 1:**
Frente a los controles de la norma ISO 27001:2013. Dominio A6. Organización de la seguridad de la información.

- No se han definido con claridad las responsabilidades de cada uno de los empleados o puestos de trabajos en relación a la seguridad de la información que conllevan un riesgo de mal uso, accidental o deliberado, si son compartidas por una misma persona.
- No se evidencian formatos de reportes de incidentes de seguridad al área encargada de la seguridad.

**Recomendación:**

- Adicionar a las funciones de cada empleado o puestos de trabajos aquellas funciones que tengan que ver con la seguridad de la información.
- Comunicar a cada persona implicada en la Seguridad de la Información sus roles y responsabilidades.
- En caso de incidentes en la seguridad de la información, mantener informado al área inmediatamente encargada del control y seguridad de la información.

**Hallazgo 2:**
Frente a los controles de la norma ISO 27001:2013. Dominio A8. Gestión de activos.

- No se ha documentado el uso apropiado de la información que describa los requisitos de seguridad de la información.
- No se evidencia un control adecuado para que los empleados devuelvan los activos de información una vez finalizados sus periodos laborales o contratos.
- No se evidencia una clasificación de la información según sus niveles de protección necesarios: Criticidad y sensibilidad en cuando a su divulgación o modificación no autorizada o accidental.
- Ausencia de procedimientos claros para el manipulado de la información de acuerdo a su clasificación.

**Recomendación:**

- Establecer y/o documentar normas para el uso de información en relación a su seguridad.
- Establecer procedimientos tales como transferencia y borrado de información de forma segura en el caso que sea pertinente.
- La clasificación de la información debe alinearse con la política de control de acceso.
- Mantener un registro actualizado de autorizaciones de uso o acceso a los activos.

**Hallazgo 3:**
Frente a los controles de la norma ISO 27001:2013. Dominio A9. Control de acceso.

- Ausencia de requisitos para definir las reglas de control de acceso a la información, o los derechos y restricciones de acceso a la información.
- No existe una política establecida para el manejo de información clasificada como secreta, restringida para ciertas áreas autorizadas.
- No se ha definido un control adecuado para establecer una revisión periódica de los permisos de accesos de los usuarios al sistema de información.
- No se evidencia el uso de contraseñas seguras para el inicio de sesión del sistema de información.

**Recomendación:**

- Establecer, documentar y revisar la política de control de acceso periódicamente, lo que significa que una política documentada es obligatoria.
- Asignación de roles específicos.
- Asignar los permisos de accesos limitados solamente a la información necesaria para hacer un trabajo.
- Establecer controles para garantizar que se modifican los derechos de acceso al cambiar de puesto de trabajo dentro de la organización si así se requiere.
- El acceso al sistema de información debe contar con la validación de intentos fallidos para protegerse contra accesos forzosos o no permitidos.

**Hallazgo 4:**
Frente a los controles de la norma ISO 27001:2013. Dominio A11. Seguridad física y del entorno.

- No están establecidas las medidas de seguridad en las zonas de oficinas para proteger la información en pantallas en áreas accesibles al personal externo.

**Recomendación:**

- Establecer medidas de controles físicos para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas.

**Hallazgo 5:**
Frente a los controles de la norma ISO 27001:2013. Dominio A12. Seguridad en las operaciones.

- No se dispone de un procedimiento para evaluar el impacto en la seguridad de la información.
- Se evidencia ausencia de controles para la instalación de software no autorizado por parte de los usuarios del sistema.
- No se han definido procesos de auditorías a las medidas de seguridad del sistema de información.

**Recomendación:**

- Documentar los procedimientos que abarcan aquellas actividades que afectan al procesamiento de la información y aquellas que la protegen.
- Fortalecer el proceso de respaldo para evitar la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.
- Establecer restricciones para la instalación de software por parte de los usuarios.
- Establecer protocolos específicos para el desarrollo de auditorías considerando su impacto en los sistemas.

# 6. CONCLUSIONES

- En el desarrollo del proyecto se evidenció que la norma ISO 27001/2013 es una excelente herramienta para realizar una auditoría de la información debido a que permite identificar los riesgos a las que están expuestas las Historias Clínicas Electrónicas, y determinar los controles de seguridad adaptados a cada una de las necesidades que requieran las mismas, todo esto con el fin de garantizar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la E.S.E. Municipal Manuel Castro Tovar.

- Se aplicó la Metodología de análisis de riesgo Magerit versión 3.0 en el presente proyecto para garantizar la seguridad de los datos sensibles de la empresa, con el fin de contrarrestar los riesgos, las vulnerabilidades y las amenazas a las que está expuesta la E.S.E. Municipal Manuel Castro Tovar.

- Los datos sensibles de la Historia Clínica Electrónica presentan un grado considerable de riesgos informáticos debido a que la información se ve muy expuesta en cuanto a su confidencialidad, integridad y disponibilidad, esto gracias a la identificación riesgos, vulnerabilidades y amenazas de seguridad existentes.

- El personal de salud de la E.S.E. Municipal Manuel Castro Tovar conoce algunas pocas políticas de seguridad para la protección de los datos sensibles, sin embargo se evidencia que no se aplica a cabalidad para mitigar el riesgo al que están expuestos.

- Se plantearon y diseñaron algunos controles de seguridad de acuerdo a la norma ISO 27001:2013 y Magerit versión 3.0, con el que se obtuvieron una serie de diagnósticos que permite ver el estado de madurez en que se encuentra la Historia Clínica Electrónica frente a la gestión de la seguridad informática.

- La realización de la auditoría permitió determinar los riesgos, las amenazas y las vulnerabilidades que pueden atentar contra la seguridad de la información, las cuales permitieron proporcionar políticas y controles para mitigar dichos eventos adversos.

- En todo el proceso de la auditoría, donde se formularon procedimientos y controles de seguridad para los datos sensibles de la Historia Clínica Electrónica, fue trascendental e importante el apoyo y respaldo recibido por parte de la alta dirección, debido al compromiso adquirido para que se implementen en un futuro las recomendaciones planteadas.

# 7. RECOMENDACIONES

- Capacitar al personal en cuanto a las políticas de seguridad de la información permitiendo con ello minimizar las márgenes de riesgo de los datos sensibles en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar.

- Realizar campañas de concienciación a los funcionarios de la E.S.E. Municipal Manuel Castro Tovar, tanto del personal misional u operativo como del personal administrativo, con la finalidad de que ellos comprendan:

    - ✓ Que es información confidencial, secreta, sensible o clasificada, y porque dicha información está catalogada de esta forma.
    - ✓ Conozcan las implicaciones legales que puedan tener si comparten, copian o divulgan dicha información, en las que se pueden presentar consecuencias desde una amonestación, el despido o incluso la cárcel.
    - ✓ Hacer revisiones periódicas en sus funciones o actividades para verificar que dichas actividades cuentan con la confidencialidad y protección de los datos.

- Se recomienda que haya una revisión periódica de los riesgos y amenazas en el sistema de información, ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas.

- Se deben implementar las políticas y procedimientos para la protección de los datos sensibles, con el fin de mantener la seguridad de la información, teniendo en cuenta que la información, es el activo más importante de la empresa.

- El sistema de información y los componentes que las soportan, son activos muy importantes y valiosos, teniendo en cuenta que a través de ellos viaja la información, por tal razón es importante la creación y mantenimiento de planes de contingencia en caso de producirse una eventualidad que atente contra su normal funcionamiento.

- Cuando se realice la implementación de las políticas y procedimientos de seguridad para el sistema de información, deben estar consignados en un documento, además ser acatadas por el personal de la oficina de sistemas y todo el personal que tenga injerencia sobre la red, en caso contrario se deben aplicar las sanciones del caso, de acuerdo al impacto que se cause sobre los activos de información.

- Es importante contar con los medios necesarios para identificar los riesgos, las vulnerabilidades y las amenazas a los cuales puedan estar expuestos los datos

sensibles de la Historia Clínica Electrónica, teniendo en cuenta que se pueden aprovechar estas debilidades para afectar la confidencialidad, integridad y disponibilidad de la información.

## 8. VIDEO PRESENTACIÓN DEL ESCENARIO PROPUESTO

A continuación se adjunta la dirección electrónica acerca del video evidenciando el funcionamiento del escenario para el proyecto aplicado, en este caso, el proceso de auditoría frente a la protección y manejo de confidencialidad de los datos sensibles que reposan en la Historia Clínica electrónica de los usuarios en la E.S.E. Municipal Manuel Castro Tovar.

Link del video: https://www.youtube.com/watch?v=k5sP8MBAbps

# 9. ANEXOS

*1. Anexo. Formulario de respuesta de la encuesta*

## Encuesta a la confidencialidad y privacidad de los datos sensibles de la Historia Clínica Electrónica de la E.S.E.Municipal Manuel Castro Tovar

Objetivo:

Evaluar la confidencialidad y privacidad de los datos sensibles de los usuarios en la Historia Clínica Electrónica de la E.S.E. Municipal Manuel Castro Tovar para determinar las vulnerabilidades, amenazas y riesgos que existen en el tratamiento y custodia de la información de acuerdo a los estándares de control establecidos en la Norma ISO/27001:2013 - ISO/27002:2013.

Nota aclaratoria: Para el desarrollo de esta encuesta NO se solicita ninguna información de carácter personal, debido a que los datos requeridos, corresponden exclusivamente para efectos académicos.

*Obligatorio

1. ¿Conoce la política de protección de datos personales? *

- ○ SI
- ◉ NO

2. ¿Conoce la clasificación de los datos personales e implicaciones legales? *

- ○ SI
- ◉ NO

3. ¿Conoce la definición de "Dato sensible"? *

- ○ SI
- ◉ NO

4. ¿Conoce la definición de “Dato privado”? *

- ○ SI
- ◉ NO

5. ¿Conoce la definición de “Confidencialidad”? *

- ◉ SI
- ○ NO

6. ¿Conoce la política de delitos informáticos? *

- ○ SI
- ◉ NO

7. ¿Considera que la gestión de la Historia Clínica Electrónica brinda la confianza y seguridad para garantizar que los datos manejados cumplen con los principios de privacidad y confidencialidad? *

- ○ SI
- ◉ NO

8. ¿Se han asignado y definido las responsabilidades de los usuarios de la Historia Clínica Electrónica sobre la seguridad de la Información en los distintos procesos, tareas o actividades de la empresa? *

- ○ SI
- ◉ NO

9. ¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos a la Historia Clínica Electrónica? *

- ○ SI
- ◉ NO

10. ¿Existe un procedimiento establecido para informar ante el área competente los incidentes relacionados con la Seguridad de la Información? *

- ○ SI
- ◉ NO

11. ¿Existe controles para afrontar posibles eventualidades sobre la seguridad de la información en la gestión de la Historia Clínica Electrónica? *

- ○ SI
- ◉ NO

12. ¿Se han establecido políticas, normas o procesos para el uso apropiado de los datos sensibles de la Historia Clínica Electrónica en relación a su seguridad? *

- ○ SI
- ◉ NO

13. ¿Existe un proceso para la devolución de la información privada cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato? *

- ○ SI
- ◉ NO

14. ¿Se clasifica la información según su confidencialidad o su privacidad a fin de establecer medidas de seguridad especificas? *

- ○ SI
- ◉ NO

15. ¿Los datos recogidos en la Historia Clínica Electrónica son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación? *

- ○ SI
- ◉ NO

16. ¿Existen procedimientos para el manejo y trato de la información de acuerdo a su clasificación? *

- ○ SI
- ◉ NO

17. ¿Existen controles o procedimientos establecidos para aplicar a soportes extraíbles o externos para proteger su seguridad? Uso, Borrado, Cifrado, Impresión, Transferencia, Etc. *

- ○ SI
- ◉ NO

18. ¿Existe una política, norma o proceso que defina los controles de acceso a los datos sensibles de la Historia Clínica Electrónica y que tengan en cuenta el acceso selectivo a la información según las necesidades de cada área o puesto de trabajo? *

- ○ SI
- ◉ NO

19. ¿Están establecidos las restricciones o accesos limitados a los recursos de la Historia Clínica Electrónica según perfiles determinados? *

- ○ SI
- ◉ NO

20. ¿Existen procesos formales de registros de usuarios a la Historia Clínica Electrónica? Usuario y contraseña. *

- ◉ SI
- ○ NO

21. ¿Existen procesos formales para asignación de perfiles de acceso a la Historia Clínica Electrónica? *

- ◉ SI
- ○ NO

22. ¿Existe un proceso específico para la asignación y autorización de permisos especiales para el acceso y manejo de los datos sensibles de la Historia Clínica Electrónica? *

- ○ SI
- ◉ NO

23. ¿Se ha establecido una política específica para el manejo de información clasificada como secreta o privada? *

- ○ SI
- ◉ NO

24. ¿Se ha establecido periodos concretos para renovación de permisos de acceso a la Historia Clínica Electrónica? *

- ○ SI
- ◉ NO

25. ¿Existe un proceso establecido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos? *

- ○ SI
- ◉ NO

26. ¿Se establecen perfiles específicos de acceso para el sistema de Información (Historia Clínica Electrónica) de forma que se restringa la información a la actividad o tarea específica a desarrollar? *

- ○ SI
- ◉ NO

27. ¿Se han implementado procesos de acceso seguro para el inicio de sesión de la Historia Clínica Electrónica considerando limitaciones de intentos de acceso para evitar la suplantación y uso inapropiado de la información? *

- ○ SI
- ◉ NO

28. ¿Se establecen medidas para controlar el establecimiento de contraseñas seguras? *

- ○ SI
- ◉ NO

29. ¿Existen controles de acceso de personas no autorizadas en áreas restringidas y con acceso al sistema de información *

- ◉ SI
- ○ NO

30. ¿Se han establecidos medidas de seguridad para zonas seguras (consultorios) para proteger la información privada y sensible a personal externo? *

- ○ SI
- ◉ NO

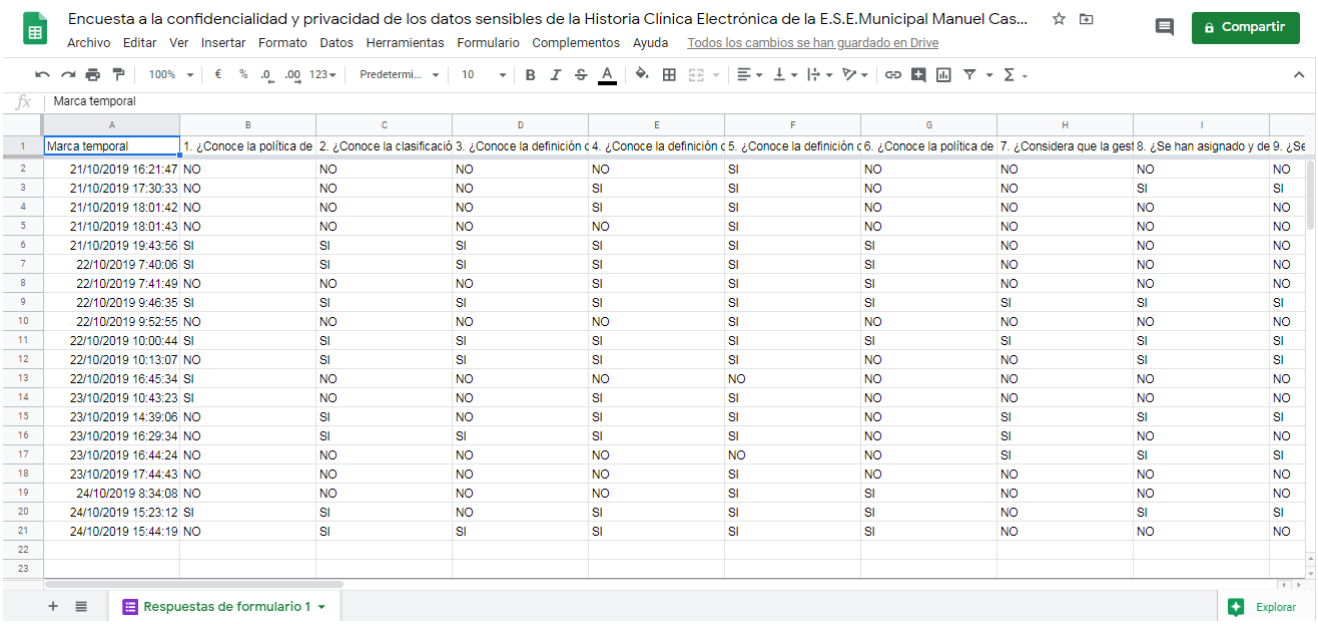
31. ¿Se controla o supervisa la actividad de personal que accede a áreas seguras y que tienen acceso al sistema de información? *

- ○ SI
- ◉ NO

Enviar

Página 1 de 1

## *2. Anexo. Respuestas en hojas de cálculo*



Encuesta a la confidencialidad y privacidad de los datos sensibles de la Historia Clínica Electrónica de la E.S.E.Municipal Manuel Cas...

Archivo Editar Ver Insertar Formato Datos Herramientas Formulario Complementos Ayuda Todos los cambios se han guardado en Drive

Compartir

Marca temporal

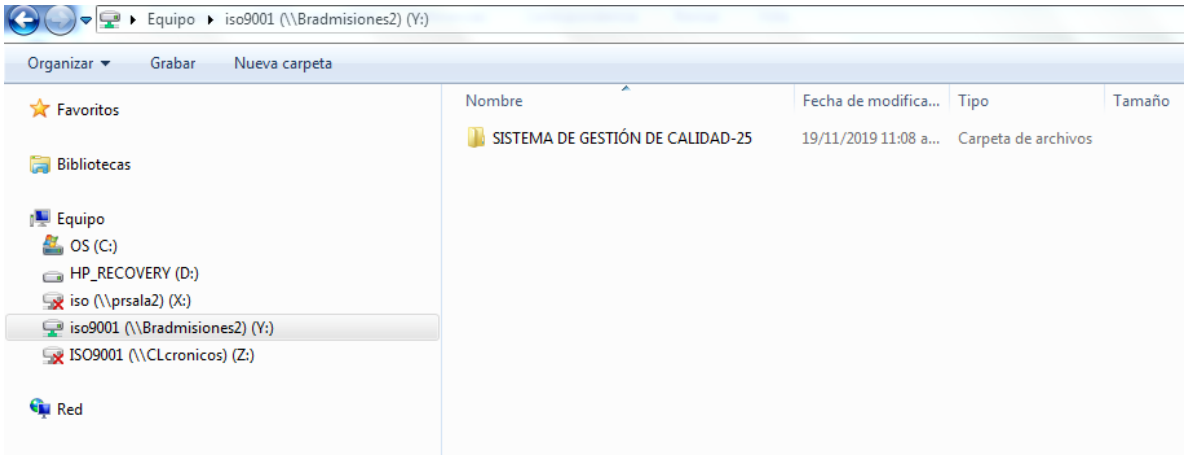
| | A | B | C | D | E | F | G | H | I | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Marca temporal | 1. ¿Conoce la política de | 2. ¿Conoce la clasificació | 3. ¿Conoce la definición c | 4. ¿Conoce la definición c | 5. ¿Conoce la definición c | 6. ¿Conoce la política de | 7. ¿Considera que la gest | 8. ¿Se han asignado y de | 9. ¿Se |
| 2 | 21/10/2019 16:21:47 | NO | NO | NO | NO | SI | NO | NO | NO | NO |
| 3 | 21/10/2019 17:30:33 | NO | NO | NO | SI | SI | NO | NO | SI | SI |
| 4 | 21/10/2019 18:01:42 | NO | NO | NO | SI | SI | NO | NO | NO | NO |
| 5 | 21/10/2019 18:01:43 | NO | NO | NO | NO | SI | NO | NO | NO | NO |
| 6 | 21/10/2019 19:43:56 | SI | SI | SI | SI | SI | SI | NO | NO | NO |
| 7 | 22/10/2019 7:40:06 | SI | SI | SI | SI | SI | SI | NO | NO | NO |
| 8 | 22/10/2019 7:41:49 | NO | NO | NO | SI | SI | SI | NO | NO | NO |
| 9 | 22/10/2019 9:46:35 | SI | SI | SI | SI | SI | SI | SI | SI | SI |
| 10 | 22/10/2019 9:52:55 | NO | NO | NO | NO | SI | NO | NO | NO | NO |
| 11 | 22/10/2019 10:00:44 | SI | SI | SI | SI | SI | SI | SI | SI | SI |
| 12 | 22/10/2019 10:13:07 | NO | SI | SI | SI | SI | NO | NO | SI | SI |
| 13 | 22/10/2019 16:45:34 | SI | NO | NO | NO | NO | NO | NO | NO | NO |
| 14 | 23/10/2019 10:43:23 | SI | NO | NO | SI | SI | NO | NO | NO | NO |
| 15 | 23/10/2019 14:39:06 | NO | SI | NO | SI | SI | NO | SI | SI | SI |
| 16 | 23/10/2019 16:29:34 | NO | SI | SI | SI | SI | NO | SI | NO | NO |
| 17 | 23/10/2019 16:44:24 | NO | NO | NO | NO | NO | NO | SI | SI | SI |
| 18 | 23/10/2019 17:44:43 | NO | NO | NO | NO | SI | NO | NO | NO | NO |
| 19 | 24/10/2019 8:34:08 | NO | NO | NO | NO | SI | SI | NO | NO | NO |
| 20 | 24/10/2019 15:23:12 | SI | SI | NO | SI | SI | SI | NO | SI | SI |
| 21 | 24/10/2019 15:44:19 | NO | SI | SI | SI | SI | SI | NO | NO | NO |
| 22 | | | | | | | | | | |
| 23 | | | | | | | | | | |

Respuestas de formulario 1

Explorar

## *3. Anexo. Formatos existentes Área Gestión de las Tecnologías*

Carpeta ISO9001. Sistema de Gestión de Calidad. Versión 25



Equipo ▸ iso9001 (\\Bradmisiones2) (Y:)

Organizar Grabar Nueva carpeta

Favoritos

Bibliotecas

Equipo

OS (C:)

HP_RECOVERY (D:)

iso (\\prsala2) (X:)

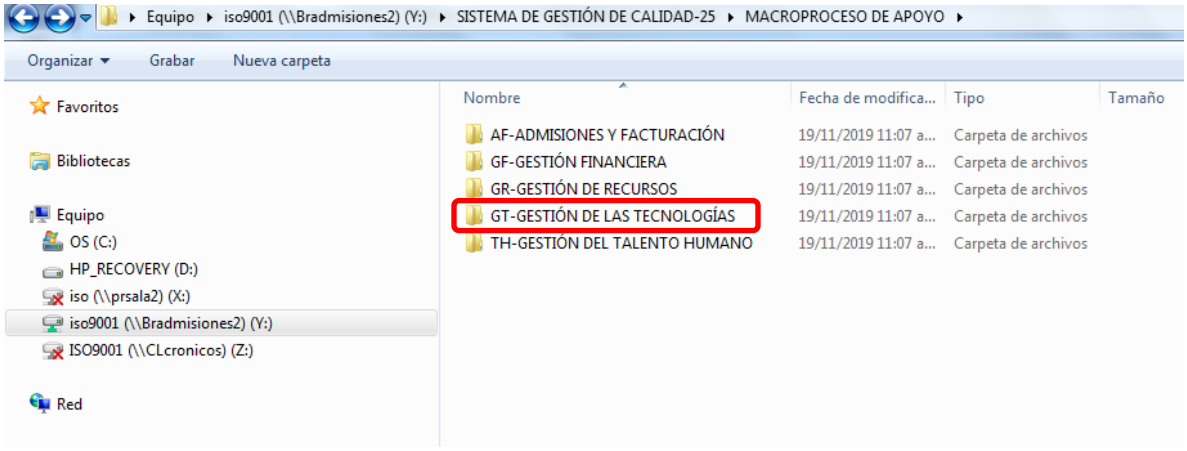
iso9001 (\\Bradmisiones2) (Y:)

ISO9001 (\\CLcronicos) (Z:)

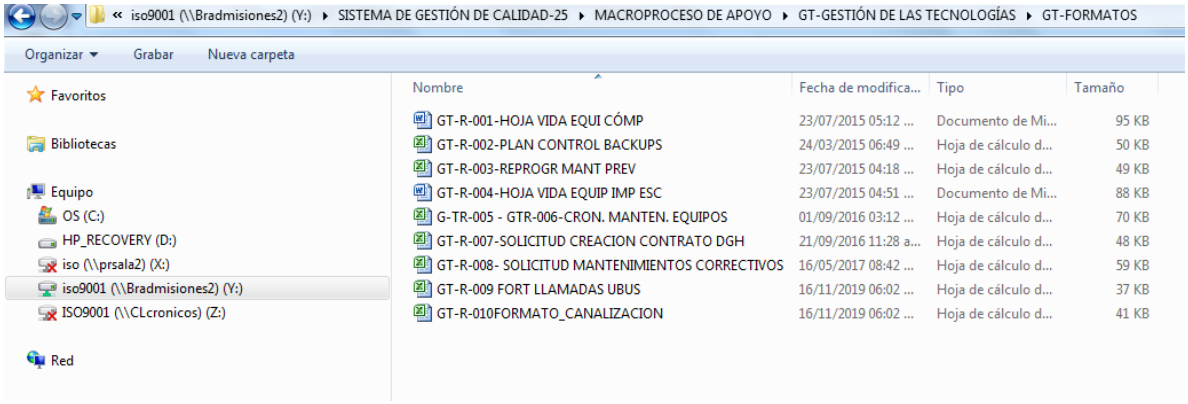
Red

| Nombre | Fecha de modifica... | Tipo | Tamaño |
|---|---|---|---|
| SISTEMA DE GESTIÓN DE CALIDAD-25 | 19/11/2019 11:08 a... | Carpeta de archivos | |

Carpeta GT-Gestión de las Tecnologías




Carpeta GT-Formatos




Formato cronograma de mantenimiento – Equipos de cómputo.

E.S.E. MANUEL CASTRO TOVAR
Calidez y Calidad para Todos

CRONOGRAMA DE MANTENIMIENTO
**EQUIPOS DE COMPUTO**
AÑO _____

SIGLAS: (P) Programado (OK) Ejecutado (R) Reprogramado (EJ) Reprogramado ejecutado

| | PROGRAMACION 3 PERIODOS EN EL AÑO DE 4 meses cada uno. | | | | 1 Periodo | | | | 2 Periodo | | | | 3 Periodo | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ID | NOMBRE EQUIPO | ESTADO | SEDE | AREA | ENE | FEB | MAR | ABR | MAY | JUN | JUL | AGO | SEP | OCT | NOV | DIC |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |

Formato Mantenimiento Preventivo.

E.S.E. MUNICIPAL MANUEL CASTRO TOVAR
Calidez y Calidad para Todos
NIT. 813.005.295-8

**REPROGRAMACION DE MANTENIMIENTO PREVENTIVO**

**PROCESO: GESTION DE LAS TECNOLOGIAS**

| NOMBRE EQUIPO | AREA | SEDE | JUSTIFICACION | FECHA PROGRAMADA | FECHA REPROGRAMADA | RESPONSABLE |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |



Formato Mantenimiento Correctivo.

E.S.E. MANUEL CASTRO TOVAR
Calidez y Calidad para Todos

**SOLICITUD DE MANTENIMIENTO CORRECTIVO**

| FECHA SOLICITUD | SEDE | AREA | EQUIPO COMPUTO/IMPRESORA | ID/PLACA/SERIAL | BREVE DESCRIPCION DE LA FALLA | AFECTA PRESTACION SERVICIO | | SOLICITADA POR |
|---|---|---|---|---|---|---|---|---|
| | | | | | | SI | NO | |
| | | | | | | | | |
| | | | | | | | | |

# 10. BIBLIOGRAFÍA


SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Políticas de tratamiento de la información personal en la superintendencia de industria y comercio. {En línea}. {15 Octubre de 2019}. Disponible en: (http://www.sic.gov.co/sites/default/files/documentos/Politicas_Habeas_Data_0.pdf )

MINISTERIO DE SALUD. Resolución número 1995 de 1999. Artículo 1. (Julio 8). {En línea}. {15 Octubre de 2019}. Disponible en: (https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf)

ENCOLOMBIA. Secreto Profesional. Ley 23 de 1981. Artículo 37. {En línea}. {15 Octubre de 2019}. Disponible en (https://encolombia.com/medicina/guiasmed/mision-medica/modulo3misionmedica11/)

E.S.E. MUNICIPAL MANUEL CASTRO TOVAR. Portafolio de servicios. {En línea}. {15 Octubre de 2019}. Disponible en: (http://esemanuelcastrotovar.gov.co/wp-content/uploads/2017/07/Portafolio-de-Servicios-ESE-MCT.pdf)

LEY 41/2002. Ley de autonomía del paciente. {En línea}. {30 Octubre de 2019} Disponible en: (http://www.auxiliar-enfermeria.com/lap_05.htm)

NORMA TECNICA COLOMBIANA. NTC-ISO/IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. {En línea}. {30 Octubre de 2019}. Disponible en: (http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf)

ISO 27001. ¿Qué significa la implantación de un SGSI en una empresa? {En línea}. {30 Octubre de 2019}. Disponible en: (https://normaiso27001.es/)

NORMA TECNICA COLOMBIANA. NTC-ISO/IEC 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Practica para la Gestión de la Seguridad de la Información. {En línea}. {30 Octubre de 2019}. Disponible en: http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=00000001070&ruta=/documentacion/0000001358/0000000107

PAE. Portal Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. {15 Noviembre de 2019}. Disponible en:

(https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XaX0NJJKjcc)

MINTIC. Seguridad y Privacidad de la Información. Guía de Auditoria. {En línea}. {15 Noviembre de 2019}. Disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf)

LEY 1581 DE 2012 DECRETO 1377 DE 2013. Colombia Digital. {En línea}. {15 Noviembre de 2019}. Disponible en: (http://www.colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html)

LEY 527 DE 1999. {En línea}. {15 Noviembre de 2019}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

LEY 1273 DE 2009. {En línea}. {15 Noviembre de 2019}. Disponible en: (http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf)

KASPERSKY. ¿Qué es el cifrado de datos? {En línea}. {15 Noviembre de 2019}. Disponible en (https://latam.kaspersky.com/resource-center/definitions/encryption)

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991. {En línea}. {20 Noviembre de 2019}. Disponible en (http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf)

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto Número 1377 de 2013. {En línea}. {20 Noviembre de 2019}. Disponible en (https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf)

MINTIC. Seguridad y Privacidad de la Información. Controles de Seguridad y Privacidad de la Información. {En línea}. {20 Noviembre de 2019}. Disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

QUESTIONPRO. ¿Qué es el muestreo por conveniencia? {En línea}. {20 Noviembre de 2019}. Disponible en (https://www.questionpro.com/blog/es/muestreo-por-conveniencia/)

Médicos Generales Colombianos. Leyes y Normas en Salud. {En línea}. {20 Noviembre de 2019}. Disponible en https://medicosgeneralescolombianos.com/index.php?option=com_content&view=article&id=77:normas-relacionadas-con-la-historia-clinica-y-la-formula-medica&catid=33&Itemid=22