RESUMEN – TRABAJO DE GRADO

AUTORES	**ANDREA CELENE RODRIGUEZ PAEZ** **KAREN JILENA SUMALABE CHINCHILLA**
FACULTAD	**FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONOMICAS**
PLAN DE ESTUDIOS	**ADMINISTRACION DE EMPRESAS**
DIRECTOR	**ELMAR JOSE CRIADO CASADIEGO**
TÍTULO DE LA TESIS	**DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL LABORATORIO CLÍNICO COFESALUD IPS LTDA DE LA CIUDAD DE OCAÑA.**

RESUMEN

(70 palabras aproximadamente)

EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ES UNA HERRAMIENTA QUE OFRECE A LAS ORGANIZACIONES UN MODELO DE TRABAJO COMO UTILIDAD PARA DISEÑAR, IMPLEMENTAR Y MEJORAR EL DESEMPEÑO EN SUS LABORES, PROTEGIENDO Y RESGUARDANDO LA INFORMACIÓN COMO ACTIVO PRIMORDIAL Y NECESARIO EN EL EJERCICIO DE SUS ACTIVIDADES. EL FIN PRINCIPAL POR EL CUAL SE DISEÑA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, ES CON EL PROPÓSITO DE CUIDAR LA CONFIABILIDAD, LA DISPONIBILIDAD Y LA INTEGRIDAD DE LA INFORMACIÓN PROCESADA Y GUARDADA POR EL LABORATORIO CLÍNICO CONFESALUD IPS LTDA.

CARACTERÍSTICAS

PÁGINAS: 142	PLANOS:	ILUSTRACIONES:	CD-ROM:1

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL LABORATORIO CLÍNICO CONFESALUD IPS LTDA DE LA CIUDAD DE OCAÑA

ANDREA CELENE RODRIGUEZ PAEZ
KAREN JILENA SUMALABE CHINCHILLA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONOMICAS
ADMINISTRACION DE EMPRESAS
OCAÑA
2014

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL LABORATORIO CLÍNICO CONFESALUD IPS LTDA DE LA CIUDAD DE OCAÑA

ANDREA CELENE RODRIGUEZ PAEZ
KAREN JILENA SUMALABE CHINCHILLA

Trabajo de Grado presentado para optar por el título de Administrador de Empresas.

Director del proyecto
ELMAR JOSE CRIADO CASADIEGO
Magister en Desarrollo y Gestión de empresas sociales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONOMICAS
ADMINISTRACION DE EMPRESAS
OCAÑA
2014

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE GRAFICAS

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCION

La información se ha constituido en uno de los principales activos que es necesario proteger dentro de las organizaciones. Las empresas se enfrentan a diario a situaciones que alteran el funcionamiento normal de sus actividades lo que representa inestabilidad y pérdidas significativas para las mismas.

El sistema de gestión de seguridad de la información es una herramienta que brinda a las empresas un modelo para diseñar, implementar y mejorar el desempeño de sus actividades, salvaguardando los activos de la información y orientado a las organizaciones a prestar mejor sus servicios y a mantenerse en la búsqueda de una mejora continua.
El propósito del proyecto de investigación planteado como el diseño de un sistema de gestión de seguridad de la información para el laboratorio clínico CONFESALUD IPS LTDA es el de proteger la confidencialidad, integridad y disponibilidad de la información que es utilizada, procesada y guardada por la empresa. Para ello fue necesario realizar un análisis y evaluación del manejo de la información, basados en la aplicación de la norma ISO 27001 para diseñar un sistema que se ajuste a la organización y que sirva como medio eficaz de protección.

Para llevar a cabo el cumplimiento del proyecto se plantearon objetivos específicos con el fin de diseñar el sistema de gestión de seguridad de la información, para lo que fue necesario realizar un diagnóstico de la situación actual de la seguridad de la información física y lógica del laboratorio clínico, indagando por medio de la aplicación de una encuesta dirigida al personal de la empresa, la aplicación de la lista de chequeo donde se observaron los factores que pueden colocar en riesgo la seguridad de la información dentro y fuera de la empresa y se analizó el alcance de los procesos de gestión de la organización.

Se plantea el manual de seguridad para el manejo de la información definiendo el alcance, los objetivos, las responsabilidades y las políticas de seguridad de la información, basadas en los controles ya establecidos en la norma ISO 27002.

Fue necesario establecer los parámetros para medir y evaluar los riesgos teniendo en cuenta la norma ISO 27005 en la que se especifica la gestión del riesgo en la seguridad de la información y que ayudaron a identificar las amenazas a las que se encuentra expuesta la información y las vulnerabilidades que pueden representar daños o alteraciones en el buen funcionamiento del laboratorio clínico, para contrarrestar dichos riesgos se aplicaron los controles adecuados que sirven de ayuda para mitigar o a eliminar los riesgos presentes en el sistema de información de la organización.

El planteamiento del sistema de gestión de seguridad de la información para el laboratorio clínico es un modelo plasmado en este documento para que la empresa obtenga las herramientas de manejo, prevención, acción y control que deberá implementar una vez decida aceptarlo y con el que puede lograr un mejor desempeño en los procesos de la seguridad de la información.

1. TITULO

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL LABORATORIO CLÍNICO CONFESALUD IPS LTDA DE LA CIUDAD DE OCAÑA.

1.1 PLANTEAMIENTO DEL PROBLEMA

CONFESALUD IPS LTDA es una entidad de salud con especialidad médica básica que presta a sus pacientes el servicio de laboratorio clínico en donde se realizan exámenes de rutina y pruebas especiales con el fin de ofrecer un diagnóstico y asistencia médica. La IPS como organización tiene el compromiso de ofrecer "salud con calidad" en los servicios prestados a la población de Ocaña y su provincia, utilizando tecnología de punta, precios justos y con los más altos estándares de calidad y servicio. [1]

La actividad a la que se dedica el laboratorio clínico genera constantemente una gran cantidad de información lo que conlleva a un manejo de datos confidenciales para la empresa y a una delicada administración de la información de los pacientes, razón por la cual se requiere un soporte en su gestión y mantenimiento pues el uso de esta información se podría convertir en un riesgo para la entidad al ser expuesta involuntariamente, al ser alterados los datos y resultados o al presentarse perdida o plagio de la misma. Por tal motivo la empresa necesita controlar de manera apropiada la información que procesa, guarda y suministra siendo esté uno de los activos más importantes que posee y del que depende para llevar a cabo sus funciones normales, convirtiéndose casi que en una obligación su protección ya que el peligro está inminente dentro y fuera de la organización y está en juego el funcionamiento de la empresa, su prestigio, buen nombre y la confianza de los usuarios.

Existen múltiples peligros en la seguridad de la información que acechan al laboratorio clínico en su labor de prestar un servicio de salud con calidad y en el desarrollo de su gestión; eventualidades que pueden ocasionar graves repercusiones sociales, económicas y legales en sus operaciones, como la falta de protección de información confidencial y de datos personales, el modo de uso o divulgación de la información que puede estar sujeta a sabotajes, robos, fraudes, falsificaciones y venta de información igualmente está expuesta a daños en el lugar donde se almacena, tales como: emergencias de incendios, inundaciones o actos vandálicos, lo que originaría un alto en las operaciones normales del laboratorio ocasionando altos costos, pérdidas económicas y retraso en las actividades y procesos. Por tal razón la información que la empresa posee se convierte en un activo valioso pero a la vez vulnerable a daños y peligros del ambiente.

[1] CONFESALUD IPS LTDA. Laboratorio Clínico exámenes de rutina y pruebas especiales. Ocaña: Portafolio de servicios, 2012. p.3.

Actualmente el laboratorio clínico no cuenta con un sistema de gestión que sirva como guía en la protección y manejo de la información, lo que constituye un riesgo y causa inseguridad en los directivos y administrativos de la entidad pues el principal propósito de la organización es la prestación del servicio con calidad destinado a dar a los pacientes la confianza en el cumplimiento de los requisitos que se exigen, y uno de estos requisitos es que la información de los pacientes sea tratada cuidadosamente, que los datos y resultados sean salvaguardados y suministrados de manera confidencial. El diseño de un modelo de gestión para establecer los controles de seguridad que protejan los activos de la información del laboratorio clínico, es un requerimiento que debe cumplir la organización para que los datos que se almacenan sean protegidos de manera segura, se evite algún tipo de anomalía que ponga en riesgo la credibilidad y funcionamiento normal de la entidad.

1.2 FORMULACION DEL PROBLEMA

¿El Diseño de un Sistema de gestión de seguridad de la información basado en las norma ISO/IEC 27000, constituye una guía para el manejo, protección y fortalecimiento de la seguridad de la información y como apoyo al desarrollo de los procesos internos y externos que se llevan a cabo dentro del laboratorio clínico Confesalud IPS Ltda de la ciudad de Ocaña?

1.3 OBJETIVOS

1.3.1 Objetivo general. Diseñar un Sistema de gestión de seguridad de la información para el laboratorio clínico Confesalud IPS Ltda. de la ciudad de Ocaña.

1.3.2 Objetivos específicos.

Diagnosticar la situación actual de la seguridad de la información física y lógica del laboratorio clínico Confesalud IPS Ltda.

Definir el manual de seguridad para el manejo de la información del laboratorio clínico Confesalud IPS Ltda.

Establecer los parámetros para medir el riesgo y proponer los controles para mitigarlos o eliminarlos.

Plantear el sistema de gestión de la seguridad de la información para el laboratorio clínico según las normas y estándares de la ISO 27000.

1.4 JUSTIFICACION

El laboratorio clínico Confesalud IPS Ltda. Para llevar a cabo sus actividades utiliza un software especializado en el área administrativa, llamado GESLAB que beneficia los

procesos que desarrolla para la prestación del servicio de exámenes y toma de pruebas, funciona sobre una base de datos que almacena la información de ensayos, pedidos, clientes, probetas, materiales, proveedores, calibraciones y conversiones de unidades a través de estadísticas y graficas de ensayos realizados y en general de todos los procesos que se realizan dentro del laboratorio.

Con la creación de un sistema de gestión de seguridad de la información se busca que la organización guarde los datos importantes de una manera eficaz y segura mitigando los riesgos eminentes que a diario se presentan dentro y fuera de la organización. Ante estas problemáticas las empresas han de establecer estrategias, controles y políticas que garanticen el adecuado manejo y resguardo de los activos pertenecientes a la organización principalmente la información ya que de esta depende en gran parte la normatividad y buen funcionamiento del negocio.

Proponer el diseño del sistema de gestión de seguridad de la información para el Laboratorio Clínico, le brinda a la entidad herramientas claras de las funciones y el desempeño que deben tener los administrativos y empleados en sus labores y de los controles que deben implementar con respecto a la información que manipulan, el fin primordial es aportar al laboratorio clínico la confidencialidad, integridad y disponibilidad de la información en el interior de la organización aunque esto no solo sirve de guía para el laboratorio también para todas las organizaciones que hacen parte de la región para que consigan implementar este sistema y puedan así proteger la información, la base de datos y demás activos importantes que permitan su buen funcionamiento.

Este diseño también será de importancia para la Universidad ya que servirá como modelo de aprendizaje hacia los estudiantes de las diferentes carreras que se vinculen con el tema y los afiancen más a los cambios que diariamente enmarcan el entorno laboral.

Como profesionales es importante la investigación y el desarrollo de este proyecto porque aporta las herramientas sólidas para tomar decisiones y manejar con mayor fluidez las organizaciones, logrando ser más competitivos y entrar así en el mundo de la globalización.

1.5 HIPOTESIS

Mediante el diseño de un sistema de gestión de seguridad que proteja la información de la empresa, se busca brindar a la entidad de salud una herramienta de apoyo que le permita tomar decisiones que beneficien la gestión y el uso de la información interna y externa del laboratorio clínico.

1.6 DELIMITACIONES

1.6.1 Delimitación Conceptual. Se tendrán en cuenta los conceptos relacionados con la Norma Técnica Colombiana ISO y los controles y estándares que hacen referencia a la seguridad de la información y al funcionamiento del laboratorio clínico como: Seguridad

del recurso humano, ataque, vulnerabilidad, factores de riesgo, riesgo, impacto, amenaza, disponibilidad, integridad, confidencialidad, información, gestión de activos, activo de la información, GESLAB, seguridad de la información, seguridad física, seguridad lógica, mecanismo de seguridad, sistema de gestión, manual de políticas, controles, políticas de seguridad, procedimiento, prueba analítica, historia clínica, documentación clínica y equipo de trabajo.

NTC ISO/IEC 27001 Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). 2005.

NTC ISO/IEC 27002 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. 2005.

NTC ISO/IEC 27005. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. 27005.

1.6.2 Delimitación Operativa. La recolección de información para el desarrollo del sistema de gestión de seguridad de la información se hará a través de la inspección, la observación, la elaboración de una encuesta y de listas de chequeo aplicadas en el laboratorio clínico ubicado en la ciudad de Ocaña.

1.6.3 Delimitación Temporal. El desarrollo del proyecto se llevara a cabo en un periodo de 5 meses a partir de la fecha de inicio de la elaboración del anteproyecto, de acuerdo a las actividades planteadas en el cronograma de actividades.

1.6.4 Delimitación Geográfica. El desarrollo del estudió se hará en el laboratorio clínico Confesalud IPS Ltda. Ubicado en la ciudad de Ocaña, N de S.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

Los laboratorios clínicos tienen poco más de 100 años de existencia durante los cuales han experimentado una gran evolución, que en los últimos 30 años puede calificarse de revolución. A comienzos de los años sesenta el número de determinaciones que se realizaban en los laboratorios clínicos era reducido. La mayoría de los reactivos se preparaban en el propio laboratorio y los métodos analíticos eran, en general, poco específicos, con gran cantidad de interferencias y errores. En esa época los clínicos utilizaban la máxima «si un resultado analítico no encaja con el cuadro clínico, hay un error del laboratorio».

Los laboratorios clínicos, que habían experimentado una lenta evolución durante las décadas precedentes, sufrieron un cambio profundo menos coincidente en el tiempo y relacionado: la producción industrial de equipos de reactivos y la automatización. El crecimiento de la demanda de pruebas como consecuencia de los mayores conocimientos de fisiopatología, así como el enorme desarrollo de la industria química que tuvo lugar en los primeros años sesenta, hizo que un gran número de compañías químicas comenzaran a fabricar reactivos con fines diagnósticos. La fabricación industrial de reactivos en grandes cantidades aseguraba la estandarización de las pruebas y garantizaba mejor su calidad. Como consecuencia de esto, surgieron los denominados equipos de reactivos (kit). Dos hechos clave en el desarrollo de los equipos de reactivos fueron la utilización como reactivos de las enzimas (métodos enzimáticos) y los anticuerpos (métodos inmunológicos). El uso de los anticuerpos adquirió una nueva dimensión con los anticuerpos monoclonales.

La automatización hizo posible procesar la gran cantidad de determinaciones que comenzaba a solicitarse a los laboratorios clínicos. Los primeros sistemas automáticos eran rudimentarios, producían gran cantidad de problemas y utilizaban volúmenes de muestra elevados. Pero, a pesar de estos inconvenientes, representaban un gran avance con relación a los métodos manuales.

Durante los años setenta y ochenta siguió creciendo el número de solicitudes por parte de los clínicos, así como su presión para reducir los tiempos de respuesta, lo que llevó a la construcción de equipos analíticos muy potentes con una elevada capacidad de proceso. Simultáneamente, se mejoraban los métodos analíticos y se hacía posible un número mayor de determinaciones diferentes en los analizadores automáticos. La automatización ha influido decisivamente en el desarrollo de nuevos métodos y pruebas, de forma que algunas de las técnicas actuales no hubieran sido posibles sin la automatización. También, en esta época comenzaron a aparecer sistemas automáticos para inmuno-análisis, lo que permitió incorporar determinaciones hormonales, proteínas específicas y marcadores tumorales a la rutina diaria automatizada. Durante los últimos años, la automatización se ha ido introduciendo técnicas han descendido en cuanto a complejidad y duración y los tiempos de

análisis son cada vez más cortos, lo que permite a la mayoría de los laboratorios en su catálogo.

La expansión de la industria del diagnóstico ha cambiado el lugar de desarrollo de la mayoría de las metodologías analíticas. En los primeros tiempos, los titulados superiores que trabajaban en los laboratorios, principalmente los de los hospitales, eran los encargados del desarrollo de los nuevos métodos, que posteriormente pasaban a la industria que los comercializaba.

Sin embargo, desde hace ya algunos años las compañías químicas son los lugares de desarrollo de las nuevas técnicas y metodologías. Los titulados superiores que trabajan en los laboratorios clínicos en la actualidad dedican su atención a la evaluación sobre el terreno de los equipos comerciales. Además, en los últimos años, las compañías dedicadas a la fabricación de equipos de reactivos diagnósticos asociadas con los fabricantes de los analizadores están lanzando al mercado equipos de reactivos cada vez más cerrados, de forma que sólo pueden utilizarse con un sistema específico, por lo que la modificación de estos equipos comerciales es cada vez más difícil. Este hecho tiene ventajas e inconvenientes, pero desde el punto de vista del análisis y las modificaciones que pudieran introducirse en el laboratorio clínico, es una limitación importante.

Las tendencias de los últimos años apuntan hacia laboratorios clínicos con gran capacidad de trabajo, ya que tienen muchas ventajas con relación a los pequeños. Generalmente, es menor el coste por prueba en los laboratorios grandes que procesen grandes lotes al ser menor la incidencia de los costes comunes de cada prueba. Las inversiones en garantía de calidad de los laboratorios grandes son mayores que las de los pequeños. Por todo lo apuntado, las tendencias actuales caminan hacia la fusión de pequeños laboratorios para crear laboratorios con gran capacidad de procesado.

En el mismo sentido que las ideas desarrolladas anteriormente, los últimos años han sido testigos de la introducción masiva de los ordenadores en los laboratorios clínicos. Aparte del control de la instrumentación analítica, principalmente los analizadores automáticos, los ordenadores son la piedra fundamental de los sistemas de gestión integral de los laboratorios clínicos.

Además de manejar todos los datos producidos en el laboratorio (admisión de pacientes, distribución de tareas, captación de resultados, control de calidad, edición de informes, archivos históricos), los sistemas informáticos de laboratorio permiten otras funciones, como la gestión de almacenes y la contabilidad analítica y presupuestaria. En este momento se está asistiendo a la creación de redes informáticas, donde las peticiones de pruebas analíticas se hacen directamente por el clínico a través de ordenador y los resultados se reciben también a través del ordenador. Así pues, los sistemas informáticos han permitido una mejor gestión de los laboratorios clínicos, con unos resultados espectaculares en cuanto

a la edición de informes, la consulta de archivos históricos y la contabilidad analítica y presupuestaria. [2]

El Laboratorio Clínico Confesalud IPS Ltda. Es una empresa resultado de una alianza entre profesionales comprometidos con su labor, inicio sus actividades en Septiembre del 2008. Están registrados en la Cámara de Comercio con Matrícula N: 00018857 e inscritos en el registro especial de prestadores de servicios en salud con código 0173501.

La misión fundamental del Laboratorio Clínico es proporcionar información necesaria que contribuya a la prevención, detección precoz, diagnóstico, pronóstico y seguimiento de las enfermedades, esta información proviene de los resultados de las magnitudes biológicas con interés clínico. El Laboratorio Clínico, ha venido experimentando un cambio acelerado a través de la historia, todo esto con el propósito de hallar las herramientas útiles y eficientes que documenten el estado de salud (Medicina Preventiva) o enfermedad (Medicina Curativa) de los pacientes. La comunidad para la que trabaja requiere más y mejores servicios fundamentados en alta calidad asistencial, concepto que asegura a cada paciente actos diagnósticos y terapéuticos conformes a estándares internacionales de aseguramientos de calidad.

Es particularmente la gestión de calidad destinada a dar al paciente la confianza de acercarse a un laboratorio que cumple con los requisitos que se exigen. La empresa se encuentra en un proceso de mejoramiento continuo, el personal que desempeña la atención se ha concientizado de la importancia de la calidad en la atención, para destacarse frente a las demás Instituciones prestadoras de servicios de salud y lograr la satisfacción de los usuarios.

Los valores como Calidad, Eficiencia, Excelencia, Calidez humana, Responsabilidad caracterizan la labor del personal, debido a esto los pacientes encontrarán en la Empresa un modelo en la prestación de servicios; el mayor interés es poder destacarse en el Sistema General de Seguridad Social, basándose en el cumplimiento de los Estándares de Calidad normativamente establecidos.

Los objetivos que persigue la Organización son:

1. Ofrecer servicios de laboratorio clínico de alta calidad, seguridad y confiabilidad.
2. Capacitación permanente del personal.
3. Satisfacer las necesidades de los usuarios
4. Mejorar permanentemente la eficacia del sistema de gestión de la calidad.

[2] AMERICA LAB SERVILOO SA, Un paseo por la Historia del laboratorio clínico. [en línea] Actualizado en el [citado el 12 de febrero de 2014] Disponible en internet en: http://www.americalab.net/latest/un-dia-en-el-laboratorio.html

Los servicios de exámenes y pruebas que ofrece el laboratorio clínico son:

Química: Acido Úrico, Albumina, Amilasa en sangre, Amilasa en orina, Bilirrubina diferenciales, Bilirrubina total, Bilirrubina directa, Calcio, Ck total, Ck mb, Cloro, Colesterol total, Colesterol HDL, Colesterol LDL, Creatinina, Curva de glicemia, Deshidrogenasa láctica, Fosfatasa alcalina, Glicemia pre, Glicemia postprandial, Got, Gpt, Hemoglobina glicosilada, Nitrógeno ureico, Proteínas totales, Proteinuria, Potasio, Sodio, Test de O'sullivan, Trigliceridos, Troponina.

Hematología, Coagulación y Hormonas: Cuadro hemático automatizado IV, Generación, Extendido sangre periférica, Células L.E., Hematocrito, Hemoglobina, Hemoclasificacion, Prueba de ciclaje, Reticulocitos, Recuento de plaquetas, Velocidad de sedimentación globular, Tiempo de coagulación, Tiempo de sangría, Tiempo de protrombina tp, Tiempo de tromboplastina tpt, Progesterona TSH, Prolactina LH, T3, FSH, T4

Parasitología: Coprologico, coprologico seriado, Coproparasitoscopico, hemoparasitos - gota gruesa, Prueba de guayaco, Test de Graham, Zn modificado en materia fecal, Antigeno para hepatitis B, Antiestreptolisina o Antigenos febrilesAntitoxaplasma igg, Antitoxoplasma igm, Citomegalovirus igg,, Citomegalovirus igm, Coombs directo, Coombs indirecto, Fta ABS, Helicobacter pylori, Herpes virus igg, Herpes virus igm, Hiv. Virus de inmunodeficiencia humana, Pcr proteina c reactiva, Prueba de embarazo, Ra test factor reumatoideo, Serología vdrl.

Marcadores Tumorales: antígeno prostático específico psa , Hormona gonodatropina, corionica, Bhcg

Uroanálisis Microbiología Otros: Ácido úrico en orina de 24 horas, Calcio en orina, Creatinuria en 24 horas, Depuracion de creatinina, Parcial de orina, Potasio en orina de 24 horas, Proteinuria en orina de 24 horas, Antibiograma, Baciloscopia en esputo,, Baciloscopia en moco y linfa, Cultivo para germenes comunes, Coprocultivo, Frotis de garganta, Frotis de secrecion uretral, Frotis de secrecion vaginal, Gram, Hemocultivo, Koh para sarcoptes scabiei, Urocultivo recuento de colonias y antibiograma, Eosinofilos en moco nasal, Espermograma [3]

2.2 MARCO CONCEPTUAL

Activo de la Información. Se entiende por cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. Otra buena definición de Activo es todo aquello que tiene valor para su empresa. La ISO 27001 pide que todos los activos relevantes sean identificados e inventariados. Existe un poco de confusión porque se acostumbra a asociar la expresión "inventario de activos" al usual inventario de hardware y software. Cuando el adjunto es

[3] CONFESALUD IPS LTDA, op. cit, p.13-14.

seguridad de la información, por "inventario de activos" debemos comprender un conjunto más abarcativo de activos, que contempla sistemas, personas, ambientes físicos entre otros.[4]

Gestión de activos. Se relaciona con el mantenimiento y protección apropiados de todos los activos de la información.[5]

Información. Es uno de los activos más importantes de la empresa contenido en papeles y en sistemas de información. La información que posee la organización debe mantenerse protegida rigurosamente por tal motivo se deben tomar las precauciones necesarias para mantenerla bajo cuidado y preservarla dentro de la entidad y se deben tener en cuenta tres conceptos importantes: Confidencialidad, integridad y disponibilidad.[6]

Confidencialidad. Implica el acceso a la información por parte únicamente de quienes están autorizados.[7]

Integridad. Mantenimiento de la exactitud y cumplimiento de la información y sus métodos de proceso.[8]

Disponibilidad. Es el acceso a la información y a los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran.[9]

Amenaza. Evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.[10]

Impacto. Consecuencia que sobre un activo tiene la materialización de una amenaza.[11]

Riesgo. Posibilidad de que se produzca un impacto determinado en un activo en un dominio o en toda la organización.[12]

---

[4] REAL ISMS. Gestión de riesgos. Activos de la información. Guía de referencia de Uso. [en línea] Actualizado en el 2012. [citado el 12 de febrero de 2014] Disponible en: (https://sites.google.com/a/realiso.com/realisms-spa/gestao-de-risco/-3-3-ativos-de-informacao)

[5] SISTESEG. Servicio de seguridad de la información. [en línea] Actualizado en el 2013. [citado el 12 de febrero de 2014] Disponible en: (http://www.sisteseg.com/informatica.html)

[6] MUÑOZ CAÑABATE, Antonio. Grupo de investigación DIGIDOC. Sistemas de Información en las Empresas. [en línea] Actualizado en el 2003. [Citado el 12 de febrero de 2014] Disponible en: (http://www.upf.edu/hipertextnet/numero-1/sistem_infor.html)

[7] INTECO, Instituto Nacional de tecnologías de la comunicación. Implantación de un SGSI en la empresa. Conceptos básicos sobre seguridad de la información. España. P. 4.

[8] Ibíd., p.4.

[9] Ibíd., p.4.

[10] EAR/PILAR. Entorno de análisis de riesgos. España. 2011. Glosario de términos. p.4.

[11] Ibíd., p.14

[12] SOCIEDAD ESPAÑOLA DE INFORMATICA DE LA SALUD. Seguridad de la información en entornos sanitarios. Conceptos generales Primera edición España. 2008, p.19.

Factores de riesgo. Son los elementos, procedimientos y acciones presentes en el ambiente que ponen en riesgo el funcionamiento de la empresa.

Vulnerabilidad. Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema de información.[13]

Ataque. Evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.[14]

Seguridad del recurso humano. Busca asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles a desempeñar, minimizando los riesgos relacionados con el personal.[15]

Sistema de información. Es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de informacion no necesariamente incluye equipo electronico (hardware). El almacenamiento de informacion, el procesamiento de informacion y la salida de informacion.[16]

GESLAB. Software administrativo para laboratorios clínicos. Es un programa que aporta a agilizar los procesos en el laboratorio, disminuir el riesgo de error al digitar los resultados, transmisión de datos automáticamente, facilita el sistema de facturación, control del ingreso de los pacientes, cartera y abonos, datos de la historia clínica de los pacientes y en general le da a la empresa un control de los datos que utiliza para llevar a cabo sus actividades normales.[17]

SGSI (Sistema de gestión en la seguridad de la información). ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.[18]

Que incluye un SGSI. En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro

---

[13] INSTITUTO POLITECNICO NACIONAL. Seguridad física y planes de contingencia. Poli libro seguridad informática. [en línea] Actualizado en el 2005. [Citado en julio 22 de 2014] Disponible en: (http://148.204.211.134/polilibros../z_basura/HTML/UNIDAD%206/CONTENIDO/Con%20Unidad%206_1.htm)

[14] UNIVERSIDAD POLITECNICA SALESIANA. Definición de la normalización a emplear. Términos y definiciones de seguridad. 2004. Repositorio digital UPS. Cap.1.

[15] SISTESEG. Op. Cit. Disponible en: (http://www.sisteseg.com/informatica.html)

[16] COHEN, Daniel. Sistemas de información en la organización. Los sistemas de información. Definiciones. Cap.1. Mc.Graw-Hill. Colombia. 2000. p.4.

[17] BARRETO, Luis Carlos. Software administrativo para laboratorio Clínico. [en línea] Actualizado en el 2011. [citado el 12 de febrero de 2014] Disponible en: (http://barretosoftware.com/portafolio/geslabsoftware/)

[18] ICONTEC. NTC-ISO 27001. Sistema de Gestión de Seguridad de la Información. Bogotá D.C. 2006. P.25

niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

a) Documentos de Nivel 1. Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc. del SGSI.

b) Documentos de Nivel 2. Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

c) Documentos de Nivel 3. Instrucciones, checklists (lista de verificación o de chequeo) y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

d) Documentos de Nivel 4. Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.[19]

Seguridad de la información. Es el conjunto de métodos y herramientas destinados a proteger los activos de la información ante cualquier amenaza, se trata de un proceso en el cual participan personas. [20]

Seguridad Física. Este tipo de seguridad se asocia a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas entre otros. [21]

Seguridad Lógica. Es la protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía.[22]

Mecanismo de Seguridad. Procedimiento, herramienta o método para garantizar el cumplimiento de la política de seguridad.[23]

ISO/IEC. ISO, Organización Internacional de Normalización, e IEC, Comisión Electrotécnica Internacional. Forman en sistema especializado para la normalización mundial. Los organismos mundiales miembros de ISO e IEC, participan en el desarrollo de

[19] ISO27000.ES. Sistema de Gestión de Seguridad de la Información. España. 2009. p.4.
[20] UNIVERSIDAD POLITECNICA SALESIANA. op.cit, p.6.
[21] Ibíd., p.6.
[22] Ibíd., p.6.
[23] Ibíd., p.6.

las normas Internacionales a través de comités técnicos establecidos por la organización respectiva, para tratar con campos particulares de la actividad técnica. [24]

ISO/ IEC 27000. Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).[25]

ISO/IEC 27001. Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI, de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.[26]

ISO/IEC 27002. Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. [27]

ISO/IEC 27005. Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.[28]

---

[24] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Norma Técnica Colombina NTC-ISO 17025. Requisitos generales para la competencia de los laboratorios del ensayo y calibración. Bogotá D.C. 2005. p. 20

[25] ISO27000.ES. El portal de ISO 27001 en español. [en línea] Actualizado en el 2009. [Citado el 12 de febrero de 2014] Disponible en: (http://www.iso27000.es/iso27000.html)

[26] Ibíd., p.4.

[27] Ibíd., p.4.

[28] Ibíd., p.4.

Sistema de gestión. Un sistema de gestión es un esquema o marco de referencia para la administración de una entidad u organización basado en el desarrollo de políticas y acciones con los que la empresa pretende alcanzar sus objetivos y ofrecer bienestar social a la población a quien le presta el servicio.

Manual de políticas. Es el documento que denota el compromiso de la empresa con la seguridad de la información, contiene los parámetros y acciones a seguir por parte del recurso humano de la empresa para evitar errores, robos, fraudes o mal uso de las instalaciones, quipos y servicios.

Controles. Medios utilizados para manejar los riesgos y amenazas como la creación de políticas o procedimientos dentro de la organización que pueden ser administrativas, técnicas, de gestión o legales.[29]

Políticas de seguridad. Es el plan de acción para afrontar riesgos de seguridad**,** el conjunto de reglas para el mantenimiento de un adecuado nivel en las buenas prácticas para la seguridad de los equipos, las edificaciones y en si dentro de las organizaciones.

Procedimiento. Proceso en el que se llevan a cabo las etapas técnicas y administrativas necesarias para que el laboratorio clínico pueda producir información. [30]

Prueba Analítica. Unidad básica del laboratorio, conjunto de pasos necesarios para obtener un resultado final de las pruebas realizadas en un laboratorio clínico.

Historia Clínica. Registro de datos clínicos de un paciente, obtenidos de forma directa o indirecta.[31]

Documentación Clínica. Es aquella que se produce como consecuencia de la atención directa a los pacientes.

Equipo de trabajo. Cualquier máquina, instrumento o instalación utilizada en el trabajo.

2.3 MARCO TEÓRICO

La seguridad en la información es uno de los temas más polémicos que socialmente se ha extendido en nuestros tiempos, son muchas las empresas que están implementando sistemas de seguridad y aplicando herramientas dentro de sus organizaciones con el fin de salvaguardar los datos que hacen posible el curso normal de su trabajo ya que son conscientes de las amenazas y riesgos que corre la información.

---

[29] UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS. Seguridad de la información. 2003.p.15.
[30] LÓPEZ, Antonio. Sistema de información del laboratorio Clínico. SEIS. 2004. p.109.
[31] BRANDÉS, Fernando. Responsabilidad profesional y Laboratorio Clínico. Documento No 6 SEDIGLAC. Madrid. 1999. p.2.

La información ha logrado posicionarse como uno de los activos más importantes dentro de las organizaciones tanto públicas como privadas, cuanto más grande es la empresa mayor protección debe existir sobre este bien y no consiste solamente en crear usuarios y contraseñas, también es necesario crea políticas que garanticen la seguridad física y lógica de la información, asegurando la privacidad y la protección de las operaciones a ser vulnerados por daños causados con o sin intención.

Según algunos autores la seguridad en un sistema de información es un estado que nos indica que ese sistema está libre de peligro, daño o riesgo, entendiendo como peligro todo aquello que puede afectar su funcionamiento directo o los resultados que se obtienen del mismo.[32]

Para la mayoría de los expertos el concepto de seguridad en la información es utópico porque no existe un sistema cien por ciento seguro. Para que un sistema de seguridad funcione debe cumplir con ciertas características como la integridad en donde la información solo puede ser modificada por quien esté autorizado. La confidencialidad en donde la información solo puede ser vista por los autorizados y la disponibilidad que quiere decir que la información debe estar de manera disponible para cuando se necesite. [33]Algunos autores mencionan una cuarta característica que es la irrefutabilidad, donde no se puede negar la autoría, pero esto ocurre dependiendo la amenaza y puede dividirse en seguridad lógica y seguridad física.

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad de la información. La seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, perdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido es la información, el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

La seguridad de la información es un elemento imprescindible en la estrategia de negocio de cualquier empresa por esto es necesario identificar los riesgos que estén asociados a la información que maneja internamente la organización, identificar las herramientas de tecnología que apoyen y guíen a los empleados en las funciones que van a realizar y que dependan directamente del buen uso de la información, los controles a implementar como el manual de políticas cuyo fin es concientizar y dirigir a los empleados de acuerdo a cada rol que realice dentro de la entidad.

La seguridad en la información de una empresa debe catalogarse como un proceso integral, que garantice la protección en los aspectos físicos y lógicos e involucre el factor humano, es decir llevar a cabo un manejo unificado en contra de las amenazas.

[32] CONTRERAS, Pamela. Gestión de recursos informáticos. Unidad 5. Chile. 2004. p.1.
[33] MARQUEZ, Andrés. Las medidas de seguridad en la protección de datos. Microsoft. España. 2011. p.1

Para que este proceso sea integral se necesita diseñar e implementar unas políticas claras de seguridad de la información que orienten internamente a la empresa, definiendo las reglas generales de comportamiento para la interacción entre los usuarios y los activos de la misma. Las políticas son independientes de los ambientes propios de la organización y son la base del modelo de seguridad, dependen de la cultura de la organización, por esta razón deben elaborarse a la medida de los requerimientos propios de la Empresa. Como punto de partida para la definición de las políticas de seguridad de la información se tiene como referencia el análisis de riesgo realizado a partir de la observación y la aplicación de un instrumento de recolección de información y los controles de la ISO 27000

Responsabilidad del laboratorio clínico en la información y diagnóstico. La entidad debe ser responsable ante los pacientes de la información que suministra pues en cualquier ocasión puede ser visto como negligencia y llevar a un problema legal probando que hubo culpabilidad en cualquiera de sus formas: dolosa, quien tiene la intención, quiere hacer una cosa y sabe lo que hace ó imprudencia, cuando se omite la información y no se tienen los cuidados elementales.

Existe un código penal vigente que distingue entre imprudencia grave o profesional según las siguientes circunstancias:

a) Exista una acción u omisión en el ejercicio profesional.
b) La infracción supone no cumplir con el deber objetivo de cuidado.
c) La conducta imprudente determina un daño al paciente existiendo una relación causa-efecto.

Tras la denuncia, se sigue un proceso donde se reúnen pruebas para comprobar el delito, culpabilidad de los acusados, daños ocasionados al paciente y la relación causal con actuación profesional.

En caso de que la información manejada y obtenida a través de resultados hechos por las investigaciones en el laboratorio puedan ser manipulados de mala manera y traer consecuencias al paciente como:

a) Uso inadecuado de los datos analíticos obtenidos e informatizados, para los que el paciente debe expresar su consentimiento, pues la privacidad, deber de secreto y derecho de acceso a. la información deben estar contemplados.
b) Evitar que las pruebas de laboratorio realizadas, se utilicen con fines distintos a los que dieron su origen y fueron propuestos al interesado para obtener su consentimiento, como podrían ser mezclar los fines diagnósticos, con los epidemiológicos, ensayos clínicos, etc.
c) Informar adecuadamente al paciente a fin de salvaguardar sus derechos recogidos en la Ley General de Sanidad.
d) Correcta toma de muestras biológicas y transporte adecuado al laboratorio.

La metódica de trabajo y procesos a realizar dentro del laboratorio orienta a las siguientes recomendaciones:

a) Identificación correcta de la muestra biológica.
b) Salvaguardar la intimidad en su recogida, sin figurar los datos personales del interesado, siendo sustituidas por un sistema de códigos de identificación.
c) La cantidad de muestra obtenida para los análisis, debe contemplar la posibilidad de realizar no sólo métodos analíticos presuntivos sino también de confirmación.
d) Tanto el registro de los datos como su manejo, determinan importantes cambios en el uso que puede hacerse de información tan trascendente desde el punto de vista médico-legal, se involucra tanto al paciente como al sistema sanitario. El técnico debe pensar que los datos solicitados al laboratorio podrían ser utilizados posteriormente en la elaboración de diligencias judiciales.
e) El secreto profesional debe aceptar la existencia del secreto compartido. Es importante la constancia del consentimiento y finalidad de las pruebas analíticas a realizar.
f) La posibilidad de que los datos de la historia clínica pudieran ser utilizados contra el paciente y que éste no declare contra sí mismo.
g) Utilización de la historia clínica con fines distintos para los que el paciente dio su consentimiento.
h) Requerimiento de la Historia Clínica por la Administración de Justicia.

La documentación generada en este sentido, nos permite apuntar algunos elementos de reflexión médico-legal:

a) El informe de laboratorio aporta "resultados".
b) En la historia clínica podrían aparecer informes de laboratorio diversos para ser contrastados y correctamente interpretados.
c) Los informes de laboratorio realizados durante la atención "urgente", podrían ser requeridos posteriormente por la justicia, a fin de establecer causas y concausas de lesiones.

La realización de técnicas presuntivas, generalmente, deben estar adecuadamente validados; por ello, las concentraciones de corte incluyen a más de un componente de los supuestamente presentes en la muestra analizada. Resulta aconsejable que los laboratorios que pudieran disponer de tecnología y métodos analíticos capaces de realizar tanto las técnicas presuntivas como las de confirmación.

Una vez obtenido el resultado de los análisis y elaborado el informe correspondiente, pueden surgir algunas cuestiones médico-legales. Se hace pues necesario establecer algunas recomendaciones fundamentales, por su posible trascendencia médico legal:

a) Definir y constatar documentalmente los requisitos exigibles a los directores de laboratorio y personal técnico, responsable de realizar estos análisis.

b) Actualización y formación permanente del personal técnico relacionado con estas pruebas.
c) El laboratorio y sus responsables deben disponer de información adicional necesaria para asegurar el resultado final emitido en el informe correspondiente.
d) Uso indebido de los resultados: La informatización permite intercambio de resultados implementación de pruebas e incluso acceso a los datos, con finalidades distintas para las que el interesado dio su consentimiento.
e) Documentar su participación en programas de evaluación externa de la calidad.

El informe emitido debe contener básicamente:

a) Identificación de la muestra.
b) Informe cuantitativo, valores numéricos y criterios de corte utilizados, o informe cualitativo en su defecto.
c) Métodos analíticos utilizados.
d) Interpretación toxicológica de los resultados.
e) Firma del facultativo responsable.

Es importante considerar que el archivo y conservación de la muestra se haga adecuadamente porque, al solicitarla tiempo después del primer análisis, podría aportar resultados contradictorios, por no poner el cuidado y previsión necesario. Hay que tener presente que, en este tipo de intervenciones, el Laboratorio debe pensar en el paciente, quien tiene derechos tan bien definidos como el propio técnico, salvo que éste, también, presenta una serie de obligaciones respecto al usuario que se le hace la prueba solicitada; ya sea por él mismo o por requerimiento de la Justicia. [34]

2.4 MARCO LEGAL

Ley 10 de 1990, Artículo 8o. Por la cual se organiza el Sistema Nacional de Salud y se dictan otras disposiciones, determina que corresponde al Ministerio de Salud formular las políticas y dictar todas las normas científico- administrativas, de obligatorio cumplimiento por las entidades que integran el Sistema**.** [35]

Ley 100 de 1993. "La Seguridad Social Integral es el conjunto de instituciones, normas y procedimientos, de que disponen la persona y la comunidad para gozar de una calidad de vida, mediante el cumplimiento progresivo de los planes y programas que el Estado y la sociedad desarrollen para proporcionar la cobertura integral de las contingencias, especialmente las que menoscaban la salud y la capacidad económica, de los habitantes del

[34] BRANDÉS, Fernando. Op. Cit. p.2
[35] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Ley 10 de 1990. Bogotá. 1990.

territorio nacional, con el fin de lograr el bienestar individual y la integración de la comunidad.” [36]

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 y se dictan otras disposiciones”. [37]

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”.[38]

Ley 1581 de 2012. “La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”. [39]

Decreto 1377 de 2013. “Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas”. [40]

Resolución Nº 008430 de 1993. Por la cual se establecen las normas científicas, técnicas y administrativas para la investigación en salud. [41]

Decreto 77 de 1997. Artículo 2º. Objeto de los Laboratorios clínicos. El objeto de los laboratorios clínicos será el de prestar servicios para apoyar la atención integral en salud, de acuerdo con los principios de calidad, oportunidad y racionalidad lógico-científica. [42]

---

[36] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Ley 100 de 1993. Bogotá. 1993.
[37] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Ley 1266 de 2008. Bogotá. 2008.
[38] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Ley 1273 de 2009. Bogotá. 2009.
[39]SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Ley 1581 de 2012. Bogotá. 2012.
[40] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Decreto 1377 de 2013. Bogotá. 2013.
[41] REPUBLICA DE COLOMBIA. Ministerio de salud. Resolución No 008430 de 1993. Bogotá. 1993.
[42] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Decreto 77 de 1997. Bogotá. 1997.

Decreto 2323 de 2006. "El laboratorio clínico en Colombia es una entidad pública o privada en la cual se realizan los procedimientos de análisis de especímenes biológicos de origen humano, como apoyo a las actividades de diagnóstico, prevención, tratamiento, seguimiento, control y vigilancia de las enfermedades, de acuerdo con los principios básicos de calidad, oportunidad y racionalidad." [43]

Norma Técnica Colombiana NTC ISO/IEC 9000. Especifica los requisitos para un Sistema de gestión de la calidad (SGC) que pueden utilizarse para su aplicación interna por las organizaciones, sin importar si el producto o servicio lo brinda una organización pública o empresa privada, cualquiera que sea su tamaño, para su certificación o con fines contractuales.

El enfoque basado en hechos para la toma de decisiones que consiste en el análisis de datos y de la información que manejan las organizaciones. Que exista un control de los documento y de los datos de la empresa. [44]

Norma Técnica Colombiana NTC-ISO/IEC 27000. Evaluación y tratamiento del riesgo Evaluación de los riesgos de seguridad. La evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos. Puede ser necesario llevar a cabo el proceso de evaluación de los riesgos y la selección de controles varias veces para cubrir diferentes partes de la organización o sistemas individuales de información. Es recomendable que la evaluación de riesgos incluya el enfoque sistemático para estimar la magnitud de los riesgos (análisis del riesgo) y el proceso de comparación de los riesgos estimados frente a los criterios de riesgo para determinar la importancia de los riesgos (valoración del riesgo).

Es conveniente realizar periódicamente las evaluaciones de riesgos para abordar los cambios en los requisitos de seguridad y en la situación de riesgo, por ejemplo en activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando se producen cambios significativos. Estas evaluaciones de riesgos se deberían efectuar de forma metódica que puedan producir resultados comparables y reproducibles. La evaluación de los riesgos de seguridad de la información debería tener un alcance definido claramente para que sea eficaz y debería incluir las relaciones con las evaluaciones de riesgos en otras áreas, según sea apropiado. El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil. En la norma ISO/IEC TR 13335-3 (Directrices para la seguridad de la tecnología de la información: técnicas para la gestión de

[43] SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. Decreto 2323 de 2006. Bogotá. 2006.
[44] ICONTEC INTERNACIONAL. Norma Técnica Colombiana. NTC-ISO/IEC.9000. Sistema de Gestión de Calidad. Colombia. 2005.

la seguridad de la tecnología de la información) se discuten ejemplos de metodologías para la evaluación del riesgo. Tratamiento de los riesgos de seguridad. Antes de considerar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar si se pueden aceptar o no los riesgos. Los riesgos se pueden aceptar si, por ejemplo, según la evaluación se considera el riesgo bajo o que el costo del tratamiento no es efectivo en términos financieros para la organización. Tales decisiones se deberían registrar. Para cada uno de los riesgos identificados después de la evaluación de riesgos es necesario tomar una decisión para su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) Aplicación de los controles apropiados para reducir los riesgos.
b) Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política de la organización y sus criterios para la aceptación del riesgo.
c) Evitación de los riesgos al no permitir acciones que pudieran hacer que éstos se presentaran.
d) Transferencia de riesgos asociados a otras partes, por ejemplo aseguradores o proveedores.

Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se deberían seleccionar e implementar de modo que satisfagan los requisitos identificados por la evaluación de riesgos. Los controles deberían garantizar la reducción de los riesgos hasta un nivel aceptable teniendo en cuenta los siguientes elementos:

a) Requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales.
b) Objetivos de la organización.
c) Requisitos y restricciones operativos.
d) Costo de la implementación y la operación con relación a los riesgos que se reducen, y que permanezca proporcional a los requisitos y restricciones de la organización.
e) Necesidad de equilibrar la inversión en la implementación y operación de los controles frente a la probabilidad del daño que resultará debido a las fallas de seguridad.

Los controles se pueden seleccionar a partir de esta norma, de otros conjuntos de controles, o se pueden diseñar controles nuevos que satisfagan las necesidades específicas de la organización. Es necesario reconocer que es posible que algunos controles no se puedan aplicar a todos los sistemas y entornos de información, y pueden no ser viables para todas las organizaciones. A modo de ejemplo, el numeral 10.1.3 describe la forma en que se pueden segregar las funciones para evitar fraude y error. Es posible que las organizaciones pequeñas no puedan segregar todas las funciones y que sean necesarias otras formas de lograr el mismo objetivo de control. En otro ejemplo, el numeral 10.10 describe la forma en que se puede monitorear el uso del sistema y recolectar evidencia. Los controles descritos, como el registro de eventos, pueden entrar en conflicto con la legislación correspondiente, como por ejemplo en la protección de la privacidad para los clientes o en el sitio de trabajo.

Los controles de seguridad de la información se deberían tener en cuenta en la especificación de los requisitos de sistemas y proyectos y en la fase de diseño. De lo contrario, se pueden originar costos adicionales y soluciones menos eficaces y, es posible, en el peor de los casos, la incapacidad de lograr una seguridad adecuada. Se debe recordar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización. 2.4.2.2 Capítulo 5: Política de seguridad de la información Objetivo: brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. Las directivas deberían establecer una dirección clara de la política según los objetivos del negocio y demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la política de seguridad de la información en toda la organización.

Documento de la política de seguridad de la información Control. La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes. Guía de implementación. El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

a) Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información.
b) Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio.
c) Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo.
d) Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización. Incluyendo los siguientes:

Cumplimiento de los requisitos legales, reglamentarios y contractuales. Requisitos de educación, formación y concientización sobre seguridad. Gestión de la continuidad del negocio. Consecuencias de las violaciones de la política de seguridad. Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información.

Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios. Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector. Información adicional. La política de seguridad de la información podría formar parte de un documento de política general. Si la política de

seguridad de la información se distribuye fuera de la organización, es necesario tener cuidado de no divulgar información sensible. [45]

Confidencialidad y seguridad. La Ley General de Sanidad y la Ley de Protección de Datos se ocupan de aspectos relacionados con la Seguridad y la Confidencialidad, pero el médico clínico tiene presente, desde que existe su profesión, el "Secreto Profesional".

El Código de ética y deontología de la profesión médica14 dedica los artículos 14 a 16 del capítulo IV al secreto profesional del médico. En síntesis el código fija la cuestión en los siguientes términos:

a) El secreto del médico, inherente al ejercicio de la profesión es un derecho del paciente que obliga a cualquier médico en su ejercicio y que no se extingue por el fallecimiento del paciente.
b) Es un deber del médico exigir el mismo secreto a sus colaboradores.
c) El ejercicio de la medicina en equipo supone el deber de secreto para todos los implicados y sobre todo el secreto.
d) Cuando ello sea imprescindible y con carácter restrictivo, se puede revelar el secreto en los siguientes casos: Por imperativo legal.
e) En las enfermedades de declaración obligatoria.
f) En las certificaciones de nacimiento y defunción.
g) Si el silencio diera lugar a un perjuicio del paciente, de otras personas o colectivo.
h) Cuando el médico se vea injustamente perjudicado por el secreto y el paciente permita la situación.
i) Cuando el médico se vea acusado ante el colegio o sea llamado a testificar en materia disciplinaria.
j) Cuando el paciente lo autorice, pero siempre con carácter restrictivo.

El código dedica además en el artículo 17 a los sistemas de información estableciendo que estos deben garantizar el derecho del paciente a la intimidad además establece que: En las instituciones sanitarias la documentación clínica y administrativa debe separarse. Los bancos de datos extraídos de las historias clínicas estarán bajo la responsabilidad de un médico. Se prohíbe la conexión de los bancos de datos médicos a una red informática no médica.[46]

[45] ICONTEC INTERNACIONAL. Norma Técnica Colombiana NTC-ISO 27000. Sistema de Gestión de seguridad de la información. Colombia. 2004. p. 30
[46] MAZON RAMOS Y GIMENEZ AZCARATE. La información de la documentación Clínica. Informe SEIS. Pamplona. 2000. p.13

3. DISEÑO METODOLOGICO

3.1 TIPO DE INVESTIGACION

El diseño del modelo de gestión de seguridad de la información del laboratorio clínico Confesalud Ltda. se realizó teniendo en cuenta la investigación descriptiva, pues el propósito es conocer la situación actual de la entidad prestadora de salud, analizar la información e interpretarla correctamente, de tal manera que se puedan mitigar los riesgos e implementar unas políticas adecuadas para el manejo de la información de la organización.

La propuesta para el diseño de un modelo de gestión se fundamentó en la investigación de metodologías de riesgo y buenas prácticas de seguridad y calidad de la información teniendo como referencia las normas técnicas NTC ISO 27001, NTC ISO 27002, NTC ISO 25000 e NTC ISO 9001.

3.2 POBLACION Y MUESTRA

La población objeto de estudio estuvo conformada por el personal que hace parte de la entidad de Salud Confesalud IPS Ltda. Cuenta con dos (2) bacteriólogas, una (1) bacterióloga auxiliar y dos (2) auxiliares de laboratorio.

Tomando como referente la información anterior y determinando que la cantidad de empleados con los que cuenta la empresa es un número mínimo, se tuvo en cuenta toda la población para recolectar la información necesaria.

3.3 TECNICAS E INSTRUMENTOS DE RECOLECCION DE INFORMACION

Fuentes primarias:

Observación. Se realizaron las visitas necesarias a las instalaciones de la entidad con el propósito de aplicar la técnica de observación e inspección del estado de la información física y lógica que posee la Empresa y si cumple con los requerimientos básicos en la seguridad de la misma. Esta técnica ayudó al desarrollo del primer objetivo específico del proyecto.

Encuesta. Para la recolección de la información se utilizó la encuesta como instrumento, para la que se elaboró un cuestionario dirigido al personal que hace parte de la organización con el objetivo de conocer aspectos relacionados con sus labores dentro del manejo de la información que posee la Empresa y uso que le están dando a la información con la que trabajan. El fin fue determinar la necesidad para el diseño y la implementación de las políticas para la seguridad de la información que maneja la entidad de Salud en

Ocaña. Esta técnica ayudó al desarrollo del primer objetivo específico del proyecto. (Anexo A)

Listas de chequeo. Se utilizaron listas de chequeo como herramienta para comprobar que la información obtenida es la efectiva para el control de los procesos. Esta técnica ayudó al desarrollo del primer objetivo específico del proyecto. (Anexo B)

Fuentes secundarias:

Libros y artículos. Fuentes que contengan la información necesaria que esté relacionada con la seguridad de la información y políticas de seguridad para la implementación del sistema de gestión de seguridad de la información dentro de una empresa. Esta técnica sirvió para llevar a cabo el cumplimiento del segundo y tercer objetivo específico del proyecto.

Normas. Leyes y reglamentaciones que regulen el manejo de la información y la implementación de políticas de seguridad de la información. Esta técnica sirvió para llevar a cabo el cumplimiento del segundo y tercer objetivo específico del proyecto.

4. RESULTADOS

4.1 DIAGNOSTICO DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN FISICA Y LÓGICA DEL LABORATORIO CLINICO CONFESALUD IPS LTDA

4.1.1 Alcance de los procesos de gestión de la empresa.

4.1.1.1 Estudio de la organización.

a) Organización. El Laboratorio clínico CONFESALUD IPS LTDA es una entidad prestadora de servicios de laboratorio, donde se realizan exámenes de rutina y pruebas especiales destinadas a dar a sus pacientes y al médico la confianza de acercarse a un laboratorio que cumple con los requisitos que se exigen.

Es una empresa comprometida con ofrecer a sus pacientes salud con calidad brindando los mejores servicios de la región de Ocaña y su provincia, con tecnología de punta, oportunidad, precios justos y con los más altos estándares de calidad y servicio.

Es una empresa que se creó como resultado de una alianza entre profesionales en el área de bacteriología, comprometidos con la labor de ofrecer un servicio de salud con calidad. Inicio sus actividades en el mes de septiembre del año 2008 y cuentan con todos los requerimiento legales como la cámara de comercio con matricula número 00018857 y se encuentran inscritos en el registro especial de prestadores de servicios de salud con código 0173501.

b) Misión. En nuestra empresa orientamos los esfuerzos en ofrecer los mejores servicios del laboratorio clínico, con tecnología de punta, con oportunidad, con altos estándares de calidad y de servicio para la satisfacción de las necesidades de nuestros usuarios.

Nuestra Misión es contribuir con nuestros esfuerzos al mejoramiento de la calidad de vida de la población Ocañera, prestando los mejores servicios de laboratorio clínico con el fin de satisfacer las exigencias de la medicina moderna, proporcionando a los usuarios el diagnóstico y los resultados confiables, íntegros y disponibles, y utilizando los más altos estándares en calidad, tecnología y servicio.

c) Visión. Nuestra empresa procurara el mejoramiento continuo, apoyados por nuestro talento humano altamente calificado y nuestra cultura de servicio en concepto de respeto por nuestros usuarios, buscando posicionarse como un laboratorio de referencia de la región de Ocaña.

Nos proyectamos para el año 2020 como una empresa con una trayectoria consolidada, siempre en búsqueda del mejoramiento continuo, y del reconocimiento en la región por la excelente calidad del servicio prestado, contando con el desarrollo profesional de nuestro recurso humano y fomentando el respeto por nuestros usuarios y pacientes.

d) Objetivos organizacionales.

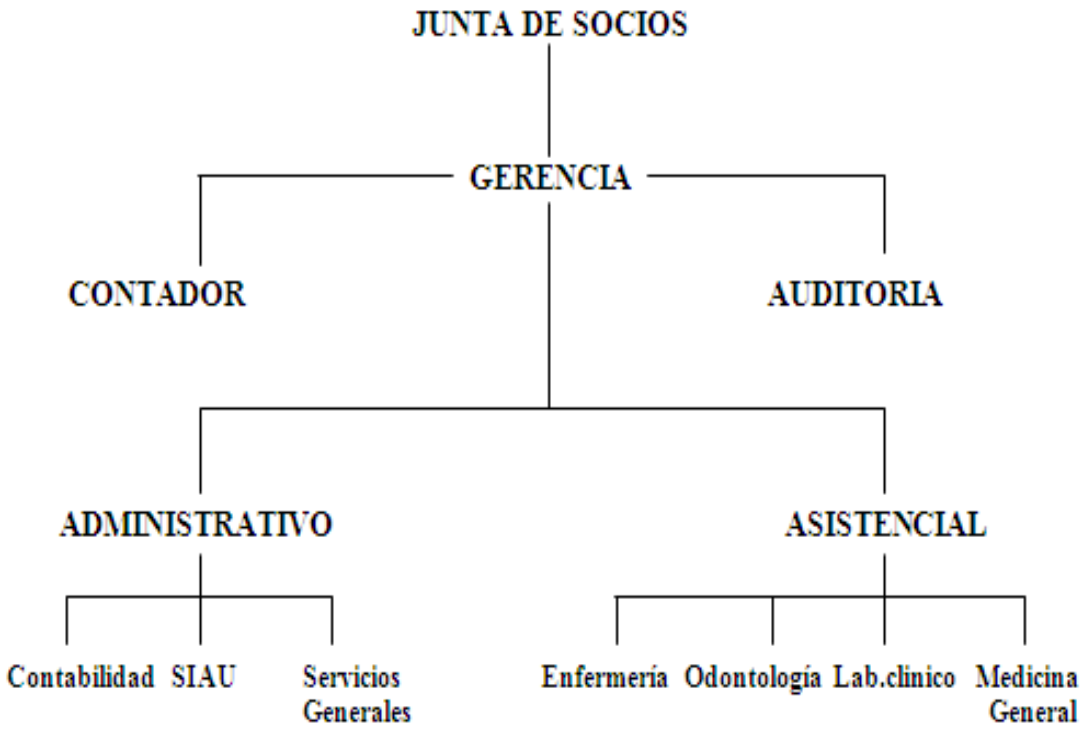
Ofrecer servicios de laboratorio clínico de alta calidad, seguridad y confiabilidad.
Capacitación permanente del personal.
Satisfacer las necesidades de nuestros usuarios.
Mejorar permanentemente la eficacia del sistema de gestión de la calidad.

e) Valores.

Calidad
Oportunidad.
Eficiencia.
Responsabilidad.
Honestidad.
Transparencia.
Respeto.´
Liderazgo.
Conocimiento.
Calidez humana.

f) Estructura organizacional.

FIGURA1. Estructura organizacional CONFESALUD IPS LTDA.



Fuente. Laboratorio clínico CONFESALUD IPS LTDA.

4.1.2 Identificación y valoración de los activos de la empresa.

4.1.2.1 Activos primarios. Los activos primarios de la empresa están compuestos por las actividades y procesos que se llevan a cabo dentro de la organización, pues estos hacen parte de la razón de ser de la empresa y se deben efectuar para cumplir con los objetivos y propósitos propuestos por la entidad y así llevar a cabo la misión principal del laboratorio clínico.

a) Actividades de la empresa. El laboratorio clínico CONFESALUD IPS LTDA realiza dentro de sus actividades más importantes la toma de muestras para la producción de exámenes de rutina y pruebas especiales tales como:

TABLA 1. Actividades del laboratorio clínico CONFESALUD IPS LTDA.

ACTIVIDADES	EXÁMENES Y PRUEBAS
QUÍMICA.	Acido Úrico.
	Albumina.
	Amilasa en sangre.
	Amilasa en orina.
	Bilirrubina diferencial.
	Bilirrubina total.
	Bilirrubina directa.
	Calcio.
	Ck total.
	Ck mb.
	Cloro.
	Colesterol total.
	Colesterol HDL.
	Colesterol LDL.
	Creatinina.
	Curva de glicemia.
	Deshidrogenasa láctica.
	Fosfatasa alcalina.
	Glicemia pre.
	Glicemia postprandial.
	Got.
	Gpt.
	Hemoglobina glicosilada.
	Nitrógeno ureico.
	Proteínas totales.
	Proteinuria.
	Potasio.

	Sodio.
	Test de O'sullivan.
	Trigliceridos.
	Troponina.
HEMATOLÓGICAS.	Cuadro hemático automatizado IV.
	Generación.
	Extendido sangre periférica.
	Células L.E.
	Hematocrito.
	Hemoglobina.
	Hemoclasificacion.
	Prueba de ciclaje.
	Reticulocitos.
	Recuento de plaquetas.
	Velocidad de sedimentación globular.
COAGULACIÓN.	Tiempo de coagulación.
	Tiempo de sangría.
	Tiempo de protrombina tp.
	Tiempo de tromboplastina tpt.
HORMONAS.	Progesterona TSH.
	Prolactina LH.
	T3.
	FSH.
	T4.
PARASITOLOGÍA.	Coprologico.
	Coprologico seriado.
	Coproparasitoscopico.
	Hemoparasitos - gota gruesa.
	Prueba de guayaco.
	Test de Graham.
	Zn modificado en materia fecal.
PRUEBAS DE INMUNOLOGÍAS.	Antígeno para hepatitis B,
	Antiestreptolisina o Antigenos febriles.
	Antitoxaplasma igg.
	Antitoxoplasma igm,
	Citomegalovirus igg.
	Citomegalovirus igm.
	Coombs directo.
	Coombs indirecto.
	Fta ABS.
	Helicobacter pylori.
	Herpes virus igg.
	Herpes virus igm.

	Hiv. Virus de inmunodeficiencia humana,
	Pcr proteina c reactiva.
	Prueba de embarazo.
	Ra test factor reumatoideo.
	Serología vdrl
MARCADORES TUMORALES.	Antígeno prostático específico psa.
	Hormona gonodatropina.
	Corionica.
	Bhcg.
URO ANÁLISIS.	Ácido úrico en orina de 24 horas.
	Calcio en orina.
	Creatinuria en 24 horas.
	Depuracion de creatinina.
	Parcial de orina.
	Potasio en orina de 24 horas.
	Proteinuria en orina de 24 horas.
MICROBIOLOGÍA.	Antibiograma.
	Baciloscopia en esputo.
	Baciloscopia en moco y linfa.
	Cultivo para germenes comunes.
	Coprocultivo.
	Frotis de garganta.
	Frotis de secrecion uretral.
	Frotis de secrecion vaginal.
	Gram.
	Hemocultivo.
	Koh para sarcoptes scabiei.
	Urocultivo recuento de colonias y antibiograma.
	Eosinofilos en moco nasal.
	Espermograma.

Fuente. Laboratorio Clínico CONFESALUD IPS LTDA.

b) Procesos de la empresa. El laboratorio clínico lleva a cabo los procesos teniendo en cuenta cada una de sus funciones la misión de la empresa y sus objetivos organizacionales para ofrecer a sus pacientes un trabajo con resultados con el nivel de seguridad y confiabilidad de la información trasmitida que le permitan tanto al paciente como al médico el diagnóstico y las conclusiones acertadas para tomar decisiones apropiadas.

TABLA 2. Procesos del laboratorio clínico CONFESALUD IPS LTDA.

PROCESOS	RESUMEN
PROCESO PREANALÍTICO.	Se denomina fase pre-analítica a la etapa previa a la realización de un análisis de laboratorio. Esta etapa incluye la preparación del paciente, la confección de la solicitud de análisis y los cuidados para la obtención de las muestras. La atención que el médico de asistencia y el personal del laboratorio concedan a este proceso determinará, en gran medida, la calidad de los resultados que se van a obtener. La calidad de los resultados y las prácticas clínicas y de laboratorio para optimizarla se hace con especial énfasis en las interferencias producidas por factores que dependen del paciente, del personal de salud o de ambos.
PROCESOS ANALÍTICOS.	Los procesos analíticos se desarrollan en el interior del propio laboratorio clínico. La selección, aplicación y evaluación de los diferentes procederes analíticos constituyen el factor fundamental que, como un marcador ultrasensible, se hace necesario revisar siempre, cuando se trata de conocer la calidad con que se desempeña el laboratorio clínico. El aseguramiento de la calidad, en sus dos variantes: interno y externo, constituye un aliado insustituible de los analistas para conocer el comportamiento del desempeño diario, dentro y fuera del laboratorio.
PROCESOS POSTANALITICOS.	Se considera proceso post-analítico a la etapa en que se confirman los resultados y el laboratorio redacta un informe. En este

	debe constar la interpretación, por parte del médico de asistencia, de los datos obtenidos, la evaluación del tiempo total que duró la obtención (turn-around-time) y la confidencialidad que se mantuvo. Se denomina inesperado un resultado que contradiga la información previa sobre el paciente. Por tanto, debe ser confirmado lo mismo si se encuentra dentro de los intervalos de referencia como fuera de ellos. En cuanto a la correcta interpretación de los resultados, es imprescindible tener en cuenta las unidades en que se expresan y el intervalo de referencia para estas unidades, la sensibilidad y especificidad no sográficas y el valor predictivo del parámetro que se analice. Por último, el tiempo total invertido en la realización de un análisis es un aspecto al cual se le presta cada vez mayor atención y constituye una medida de la eficiencia de un laboratorio.

Fuente. Laboratorio clínico CONFESALUD IPS LTDA.

c) Información. La función fundamental del laboratorio clínico es proporcionar información necesaria que contribuya a la prevención, detección precoz, diagnostico, pronostico y seguimiento de las enfermedades.

Esta información proviene de los resultados de las magnitudes biológicas con interés clínico. El laboratorio clínico ha venido experimentando un cambio acelerado a través de la historia, con el propósito de hallar las herramientas útiles y eficientes que documenten el estado de la salud (medicina preventiva) o enfermedad (medicina curativa) de los pacientes.

La comunidad para la que el laboratorio clínico trabaja requiere más y mejores servicios fundamentales de alta calidad asistencial, concepto que asegura a cada paciente actos diagnósticos y terapéuticos para la recepción satisfecha de información no solo de los usuarios sino de los médicos y de la misma empresa.

4.1.2.2 Activos de soporte. Los activos de soporte son todos aquellos de los que dependen los elementos primarios de alcance que consiste en los activos que tienen vulnerabilidades que son explotadas por las amenazas cuyo fin es deteriorar los activos primarios como el proceso de información del laboratorio clínico. Los activos de soporte son los siguientes:

a) Hardware. Son todos los elementos físicos que dan soporte a los procesos realizados por el laboratorio clínico.

TABLA 3. Equipos de cómputo del laboratorio clínico CONFESALUD IPS LTDA.

NUMERO	EQUIPO	MODELO	REFERENCIA
02	Computador	SAMSUNG	SYNCMASTERS 19B150
023	Computador	SAMSUNG	SYNCMASTERS 740 NW
024	Computador	SAMSUNG	
025	Hematología	BAYER	ADVIA 60
026	Marcadores cardiacos	ROCHE	COBASH 232
027	Electrolitos	ROCHE	AVL
028	Quimiolab	STAT FAX	3000
029	Quimiolab	STAT FAX	MULTIWASH III
030	Química clínica	BIOMÉDICA	ADC18

Fuente. Laboratorio Clínico COFESALUD IPS LTDA.

b) Software. Consiste en todos los programas que contribuyen al funcionamiento del conjunto de procesamiento de datos utilizado para el proceso de toma de muestras y de recopilación de información utilizado por el laboratorio clínico.

El software de gestión para laboratorios clínico utilizado por la organización para realizar sus actividades y procesos es **GESLAB.**

Es un Software administrativo para laboratorios clínicos, un programa que aporta a agilizar los procesos en el laboratorio, disminuir el riesgo de error al digitar los resultados, transmisión de datos automáticamente, facilita el sistema de facturación, control del ingreso de los pacientes, cartera y abonos, datos de la historia clínica de los pacientes y en general le da a la empresa un control de los datos que utiliza para llevar a cabo sus actividades normales.

c) Redes. Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores físicamente o los elementos de un sistema de información. Los medios de soporte y de red utilizados para la comunicación del laboratorio clínico son las redes de internet vía wifi.

d) Personal. Son todas las personas involucradas en el sistema de información pertenecientes al laboratorio clínico.

TABLA 4. Personal del laboratorio clínico.

N.	**CARGO**	**NOMBRE**
1.	BACTERIOLOGA ESPECIALISTA	IDANA CELENE PORTILLO.
2.	BACTERIOLOGA	YAMILE PACHECO.
3.	BACTERIOLOGA	XIMENA REYES.
4.	AUXILIAR DE LABORATORIO	CLAUDIA PACHECO
5.	AUXILIAR DE LABORATORIO	MARIA FERNANDA CELIS

Fuente. Laboratorio clínico CONFESALUD IPS LTDA.

e) Sitio. Comprende el lugar donde se encuentra ubicado y funciona el laboratorio clínico y los medios físicos que se requieren para llevar a cabo los procesos, se compone de dos factores:

Ambiente externo e instalaciones. Es el lugar que rodea a la empresa y en el cual no se puede aplicar los medios de seguridad de la organización. Esta limitado por un perímetro que se encuentra en contacto con el exterior

El laboratorio clínico CONFESALUD IPS LTDA se encuentra ubicado en la ciudad de Ocaña, Norte de Santander, en la carrera 16ª N. 11-45 Barrio San Agustín.

FIGURA 2. Imagen del laboratorio clínico CONFESALUD IPS LTDA.

Fuente. Laboratorio clínico Confesalud IPS LTDA.

Servicios públicos esenciales. Son todos los servicios que se requieren para el funcionamiento normal del laboratorio clínico y para el uso del sistema de información de la empresa. La organización utiliza como servicios esenciales el agua potable, instalaciones de luz eléctrica, servicio de teléfono fijo y teléfonos móviles, al igual que el servicio de internet wifi.

f) Estructura física de la organización. Constituye las instalaciones físicas del laboratorio clínico representado en un plano o mapa del lugar.

FIGURA 3. Estructura física primera planta CONFESALUD IPS LTDA.

Fuente. Laboratorio Clínico CONFESALUD IPS LTDA.

FIGURA 4. Estructura física segunda planta CONFESALUD IPS LTDA.

Fuente. Laboratorio Clínico CONFESALUD IPS LTDA.

4.1.3 Análisis de la información recolectada.

4.1.3.1 Análisis de los resultados de la encuesta aplicada. El diseño del sistema de gestión de seguridad de la información aplicado al Laboratorio Clínico CONFESALUD IPS LTDA parte de la información que se procesa dentro de la entidad de salud, el manejo que se le está dando y los riesgos a los que se encuentra expuesta esta información. Por tal motivo, se llevó a cabo el diseño de una encuesta aplicada al personal del laboratorio clínico de donde se obtuvieron resultados que sirven para conocer el uso de la información que es utilizada y procesada por los trabajadores y administrativos de la entidad de salud.

Los resultados que se muestran en las tablas y graficas presentadas a continuación son evidencias que ayudaran a identificar algunos de los riesgos claves que tiene la información que procesa la empresa y a los que se encuentra expuesta la empresa y que sirven para establecer cuáles son los controles más adecuados a implementar en el sistema de gestión de seguridad de la información que se está diseñando.

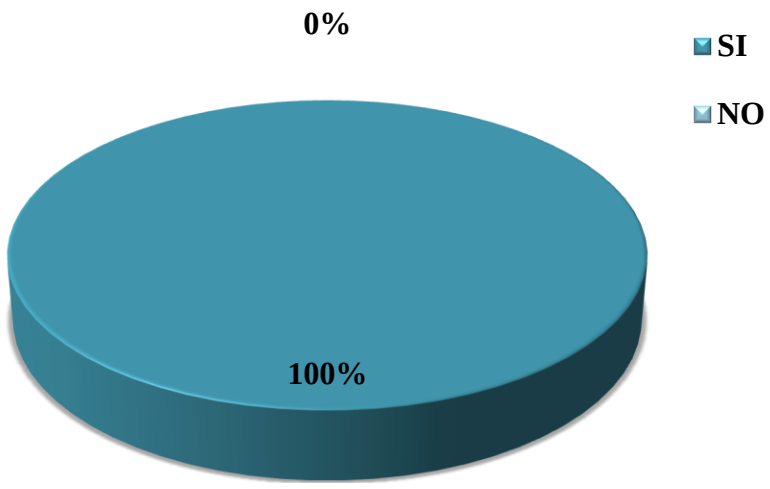
Además con la información suministrada por el personal que hace parte del laboratorio clínico se podrán identificar, analizar y evaluar los riesgos para realizar de la mejor manera le gestión de riesgos de seguridad de la información en la organización.

TABLA 5. Conocimiento del empleado sobre la existencia de políticas del manejo de la información confidencial en la empresa.

ITEMS	FRECUENCIA	PORCENTAJE
SI	5	100%
NO	0	0%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 1. Conocimiento del empleado sobre la existencia de políticas del manejo de la información confidencial en la empresa.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

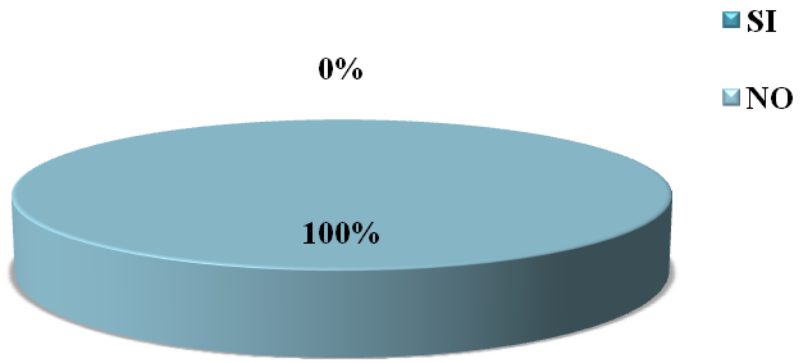
Con los resultados arrojados, los empleados en su totalidad afirman que la información suministrada en el lugar de trabajo la manejan de una manera confidencial e intransferible y aunque el laboratorio clínico no cuenta con un documento donde se especifiquen las responsabilidades y funciones en el tratamiento de la información plasmadas como políticas, anticipadamente la administración de la empresa se encargó de darles a conocer algunas pautas para llevar a cabo las operaciones realizadas por el laboratorio clínico CONFESALUD IPS LTDA de confidencialidad.

TABLA 6. Firma de contrato de confidencialidad.

ITEMS	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	5	100%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 2. Firma de contrato de confidencialidad.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA

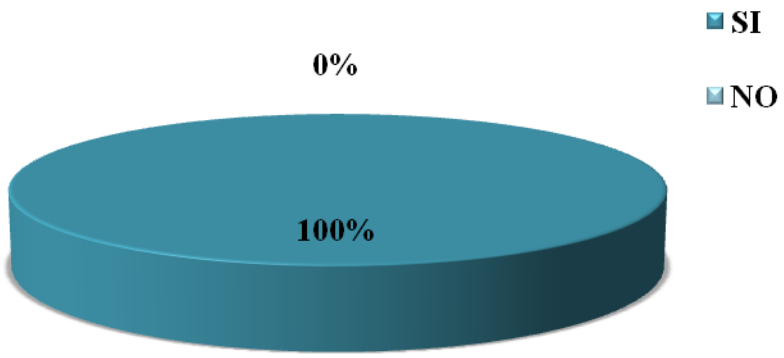
Con la información obtenida se evidencia que la organización no utiliza un contrato de confidencialidad para el uso responsable de la información procesada por parte de los empleados, es decir el 100% de los empleados al momento de ingresar a trabajar al laboratorio clínico CONFESALUD IPS LTDA no firman un acuerdo con la entidad de confidencialidad, y este documento es muy importante para poder comenzar a trabajar, tanto para tener el acceso al sistema como para el suministro de información, con esto se protege la empresa en caso de incidente, se compromete al empleado en sus funciones y de igual manera se genera fidelidad y confiabilidad a los usuarios en el momento que adquieren sus servicios.

TABLA 7. Acceso a los equipos que contienen información del laboratorio.

ITEMS	FRECUENCIA	PORCENTAJE
SI	5	100%
NO	0	0%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 3. Acceso a los equipos que contienen información del laboratorio.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

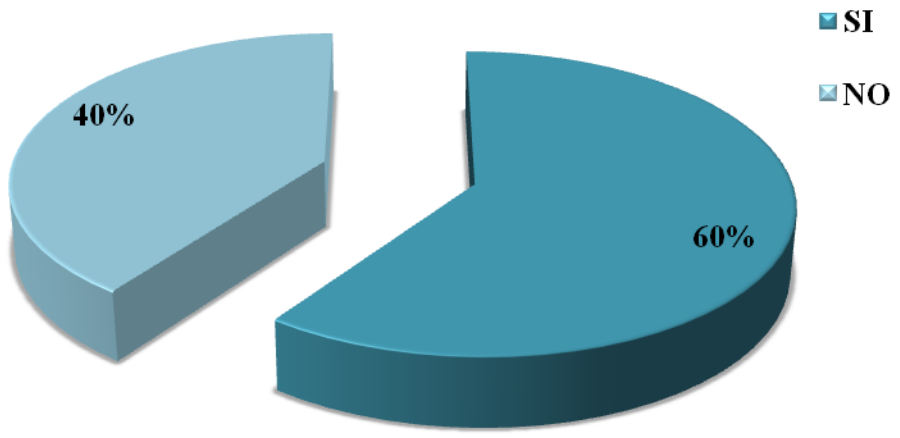
El 100% de los empleados del laboratorio clínico CONFESLUD IPS LTDA afirman que tienen acceso a los equipos para el procesamiento de información de la empresa, ya que algunas de sus funciones y labores se realizan utilizando estos medios pero es importante clasificar la información y ubicarla en equipos seguros para que solo personal autorizado tenga acceso a ella independientemente del cargo que tengan y de la información que contenga el equipo.

TABLA 8. Tiene clave de acceso para ingresar al sistema.

ITEMS	FRECUENCIA	PORCENTAJE
SI	3	60%
NO	2	40%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 4. Tiene clave de acceso para ingresar al sistema.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

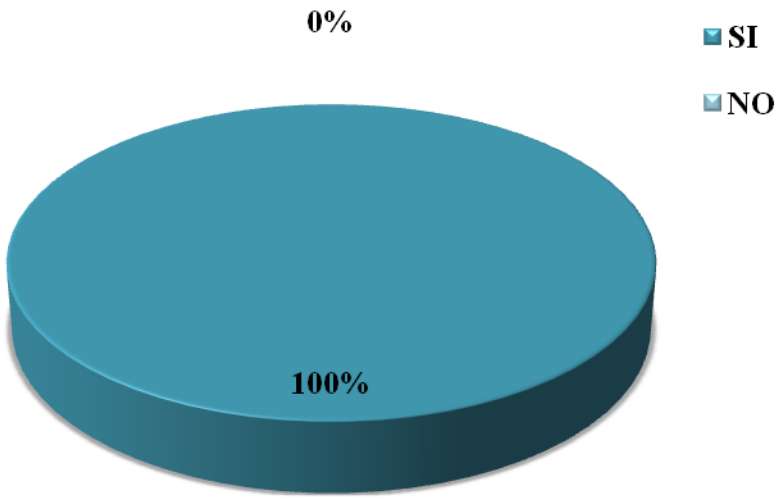
El 60% de los empleados encuestados afirman que para tener acceso a la información del laboratorio utilizan una clave o contraseña que les permite hacer uso de los datos e informes del laboratorio. El 40% restante aunque utilizan los equipos de información de la empresa no tienen acceso a la información relevante del laboratorio clínico por lo que se puede deducir que solo el 60% de los empleados tiene acceso a la información confidencial de la empresa. Se identifica también que cada empleado maneja la información de acuerdo al cargo que desempeña no en la totalidad de esta.

TABLA 9. Clave de acceso confiable.

ITEMS	FRECUENCIA	PORCENTAJE
SI	5	100%
NO	0	0%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 5. Clave de acceso confiable.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

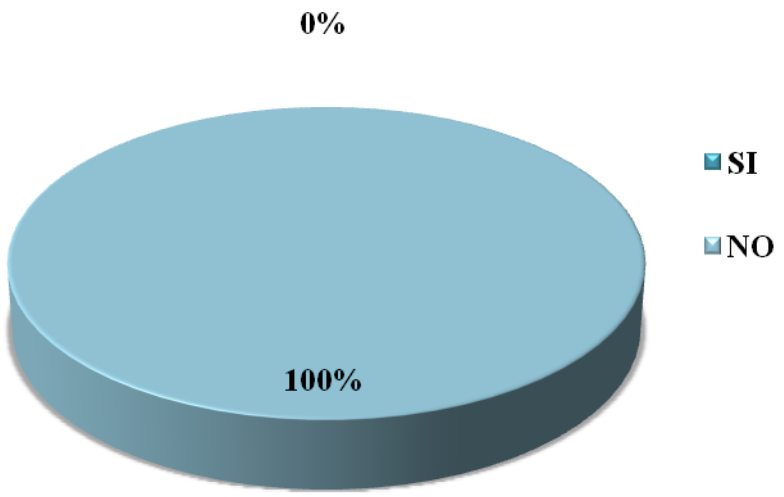
Cuando se manejan claves de acceso para ingresar a equipos que poseen información confidencial, estas deben ser altamente seguras para que no sean del dominio público ni puedan ser jaqueadas, las personas encuestadas del laboratorio clínico afirman que las claves manejadas para ingresar a los equipos de la empresa son confiables, esto indica que la información que está guardada es de conocimiento exclusivo del personal autorizado por la administración del laboratorio.

TABLA 10. Conocimiento de un plan de contingencia en caso de incidente.

ITEMS	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	5	100%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 6. Conocimiento de un plan de contingencia en caso de incidente.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

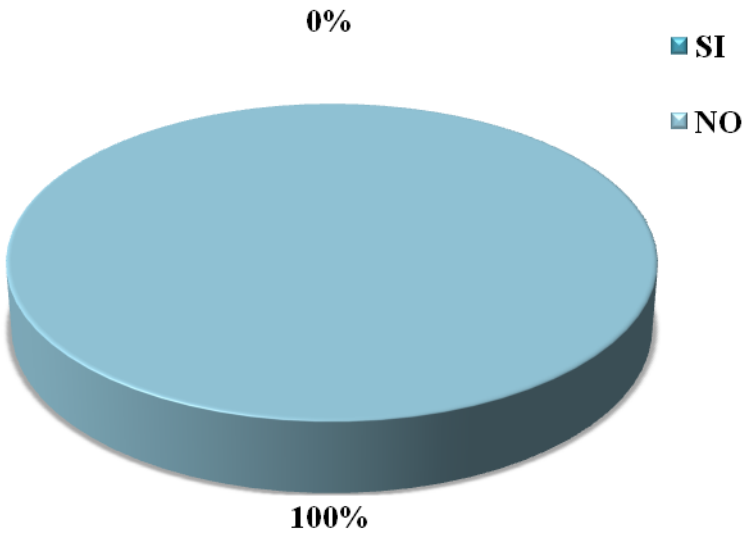
Los trabajadores en su totalidad afirman que el laboratorio no cuenta con un plan de contingencia con el que se pueda tomar acciones preventivas o correctivas para evitar incidentes de cualquier índole en el trabajo, algo muy grave, ya que estarían comprometidos con la seguridad de la información, de los activos, los empleados, los usuarios, las instalaciones y el funcionamiento de la organización en general.

TABLA 11. Facilitar información a terceros.

ITEMS	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	5	100%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 7. Facilitar información a terceros.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

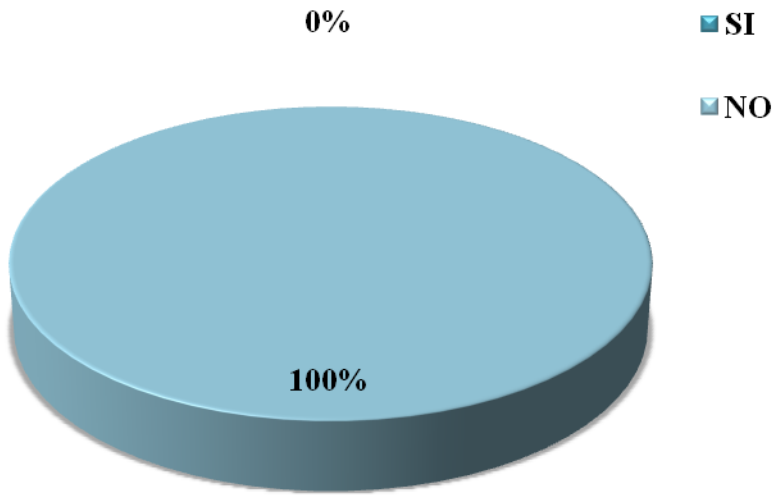
El 100% de los empleados consideran que facilitar información a terceros es responsabilidad de la administración del laboratorio clínico pues la información manejada y suministrada por las empresas, debe ser confidencial y debe ser manipulada por personal autorizado para una mayor seguridad, por eso los empleados responden que la información solo la manejan ellos y no están autorizados para transferirla por ningún medio o para entregarla para ser manipulada por personal ajeno al que está trabajando en el laboratorio clínico.

TABLA 12. Traslado de información fuera de la empresa.

ITEMS	FRECUENCIA	PORCENTAJE
SI	0	0%
NO	5	100%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 8. Traslado de información fuera de la empresa.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

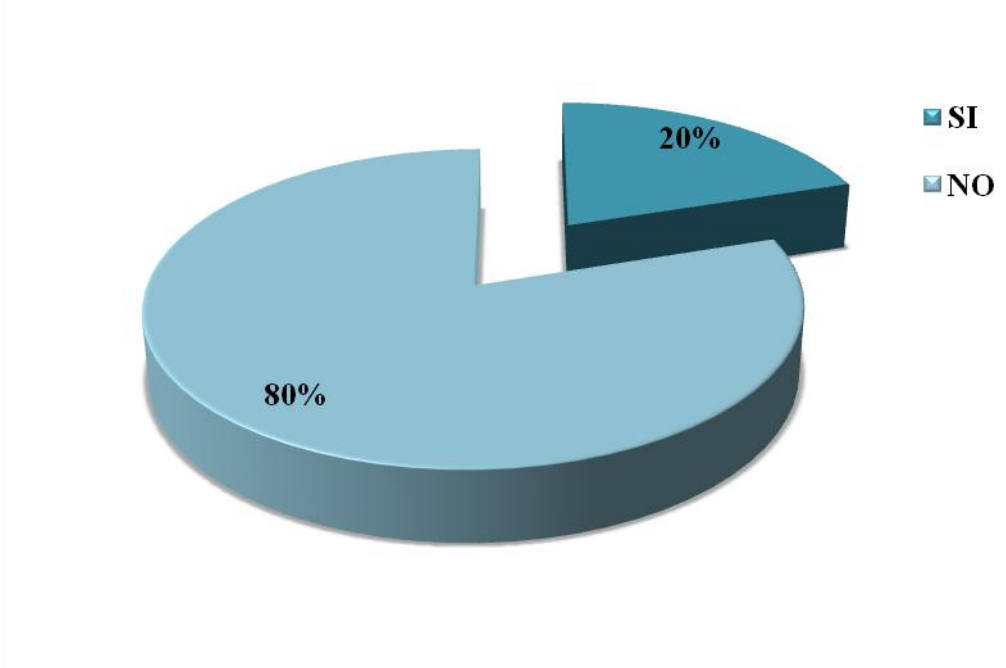
El personal del laboratorio en su totalidad responde que la información manejada y procesada por la empresa no es trasladada fuera del laboratorio clínico pues es necesario que la información de la organización cuando vaya a ser retirada del sitio por cualquier motivo, se haga bajo la autorización y supervisión de la administración del laboratorio y con la mayor precaución posible ya que esta puede ser extraviada o perdida, lo que afectaría el funcionamiento normal de la empresa.

TABLA 13. Transacciones comerciales en los equipos de la empresa.

ITEMS	FRECUENCIA	PORCENTAJE
SI	1	20%
NO	4	80%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 9. Transacciones comerciales en los equipos de la empresa.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

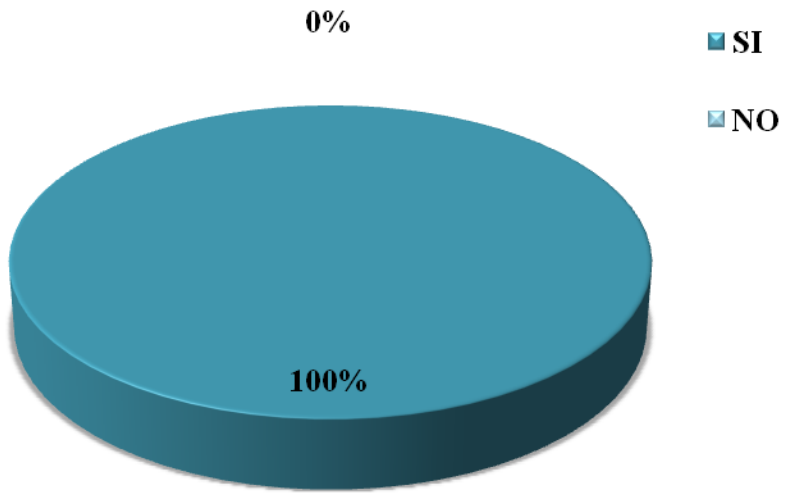
Solo el 20% de los empleados de la empresa, es decir la administración del laboratorio es la que se encarga de realizar transacciones comerciales, tales como: compra de insumos y tratos con clientes y proveedores, pagos de facturas o negocios en general, utilizando los equipos de la organización. Por esta razón se supone que el uso de los equipos para estas funciones se hace de manera responsable pues la tecnología facilita las funciones y hace más rápidas las transacciones comerciales para la organización, pero se debe ejecutar y manejar con mucha precaución ya que puede ser contraproducente a la hora de realizar pedidos, pagos etc. Se hace necesario utilizar medios electrónicos cuando todo el personal de la empresa tiene acceso a los equipos de la información. Los resultados a esta pregunta muestran que quienes fueron encuestados en su mayoría no utiliza los equipos para realizar dichas transacciones, es decir que para llevar a cabo las transacciones solamente lo realiza el personal administrativo de la empresa.

TABLA 14. Acceso a la información importante de la empresa.

ITEMS	FRECUENCIA	PORCENTAJE
SI	5	100%
NO	0	0%
TOTAL	**5**	**100%**

Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

GRAFICA 10. Acceso a la información importante de la empresa.



Fuente. Personal del laboratorio clínico CONFESALUD IPS LTDA.

El 100% de los empleados del laboratorio clínico tiene acceso a toda la información sin restricción alguna, esto puede llegar a ser contraproducente para la organización ya que no todos los empleados necesitan toda la información para poder realizar sus funciones, cada uno de ellos tiene actividades distintas pues la información que ellos manejen debe ser la que su actividad dentro de la organización requiera.

4.1.3.1 Análisis de los resultados de la lista de chequeo. Se elaboró una lista de chequeo como método para llevar a cabo la inspección en los procesos de la seguridad de la información del laboratorio clínico CONFESALUD IPS LTDA y establecer las posibles amenazas que ponen en riesgo la seguridad de la información dentro y fuera de la empresa.

Con la información adquirida a partir de la aplicación de la lista de chequeo se podrán conocer las características y riesgos que existen y afecten a las instalaciones, equipos, archivos, documentos, personal de trabajo y usuarios de la entidad prestadora de salud, además se podrán identificar los hallazgos que podrían ocasionar inconvenientes en el tema de seguridad de la información que la institución posee.

TABLA 15. Hallazgos.

Nº	HALLAZGO	PLAN DE ACCION	PROCESOS AFECTADOS	RIESGO
1.	El laboratorio clínico actualmente no cuenta con un sistema de seguridad establecido donde se definan los procedimientos y las normas a seguir para la protección de la información que se procesa y se suministra a los pacientes en el laboratorio.	Es importante para el laboratorio clínico proteger la información con la que trabaja implementando un sistema de seguridad ya que la entidad maneja un sin número de información confidencial tanto para ella como para sus pacientes. Un sistema de seguridad haría más fiable preservar la confidencialidad de los datos de la empresa, conservar la integridad de los mismos y lograr que la información protegida se encuentre disponible.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Daño físico, Eventos naturales, Perdida de servicios esenciales, Perturbación de vida a la radiación, Compromiso de la información, Fallas técnicas, Acciones no autorizadas, compromiso de las funciones.
2.	La empresa no maneja dentro de sus documentos un contrato para los empleados que ingresan a laborar en	La creación de un contrato o acuerdo de confidencialidad sirve para que los empleados mantengan en total discreción la información	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio	Compromiso de la información, acciones no autorizadas, compromiso

	el laboratorio o que hacer parte del mismo, que indique cuales son las cláusulas de confidencialidad en el manejo de la información reservada y privada del laboratorio.	que se está manipulando y se evitan mal entendidos entre las partes implicadas y malos manejos de la información para fines particulares. Para ello es necesario definir las condiciones del contrato teniendo en cuenta: la responsabilidad de cada una de las partes, las definiciones, excepciones y posibles sanciones.	clínico.	de las funciones.
3.	La mayor parte de los empleados del laboratorio clínico cuentan con el acceso a los equipos que contienen la información que se guarda y se procesa, aunque no todos tienen un usuario y una contraseña para acceder directamente a dicha información, existe el riesgo indirecto de que esta información sea manipulada por terceros ajenos a la empresa.	El laboratorio deberá mantener la información más relevante y confidencial en equipos que sean de uso exclusivo por personal autorizado y su protección se hará por medio del ingreso de contraseñas y en un lugar donde el acceso sea sumamente restringido pues no se descarta la mala intención por terceros de tener acceso a información de interés personal, así que lo recomendable para la empresa es que mantenga los archivos físicos y equipos que contienen la información estrictamente protegidos.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Compromiso de la información, acciones no autorizadas, Compromiso de las funciones.
4.	La empresa no tiene previsto un plan de contingencia en caso de ocurrir algún incidente ambiental o de tipo social	Es necesario para el laboratorio clínico diseñar un plan de contingencia para actuar correctamente ante cualquier eventualidad que ocurra	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio	Daño físico, Eventos naturales, Perdida de los servicios esenciales,

	ocasionado por situaciones ajenas al manejo interno de la organización.	con el fin de evaluar, mantener y mejorar los procedimientos de protección de la información que puedan ser afectados por la situación de riesgo y que permitan mitigar los daños potenciales antes que un desastre ocurra.	clínico.	perturbación debida a la radiación, compromiso de la información, fallas técnicas, Compromiso de las funciones.
5.	Los equipos y archivos en donde se almacena la información general y confidencial del laboratorio clínico están ubicados en las oficinas y dentro del laboratorio pero no se encuentran exentos de ser dañados o de sufrir algún deterioro por factores de uso, mantenimiento o de tipo ambiental.	El laboratorio clínico deberá tener presente la realización a menudo del mantenimiento requerido por los equipos y lugares que contienen la información importante de la empresa con el fin de mantenerlos en buen estado procurando darles el mejor uso para que su tiempo de vida útil sea mayor y su estado permanezca aceptable para el almacenamiento y el cuidado de la información de la empresa.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Daño físico, Eventos naturales, Compromiso de la información.
6.	El laboratorio Clínico no cuenta con un sistema de vigilancia constante que esté pendiente tanto de movimientos extraños dentro de la entidad como de posibles amenazas que puedan ocasionar la pérdida	Es importante que la organización evalué la posibilidad de implementar un medio por el cual pueda vigilar la información del laboratorio, ya sea contratando vigilancia privada, ubicando cámaras de seguridad dentro de la empresa o adquiriendo una protección con una entidad	Afecta a los procesos Pre-analíticos, Analíticos y post- analíticos del laboratorio clínico.	Compromiso de la información, Acciones no autorizadas, Compromiso de las funciones.

	o robo de la información, solo tiene una alarma de seguridad ubicada en la entrada de la IPS utilizado exclusivamente en la noche, y durante el día se encuentra el personal de la empresa laborando y ellos la cuidan.	aseguradora que se encargue de mantener a salvo tanto la información de la empresa como todo lo que la compone. Esto sería una gran ventaja para la empresa porque además de cuidar la información protegería a la empresa en todas tus áreas y se tendría un mayor control.		
7.	La empresa mantiene copias de seguridad de sus archivos para evitar algún tipo de anomalía que afecte el buen funcionamiento de la empresa, pero estas copias están guardadas en los equipos donde se encuentran los demás archivos.	Se le recomienda a la empresa guardar las copias de seguridad que son muy importantes para la organización en una unidad de disco duro externa, en una nube o en un dispositivo guardado en lugar seguro donde sea menor el riesgo de sufrir alteraciones.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Compromiso de la información, fallas técnicas, Compromiso de las funciones.
8.	Dentro de la entidad de salud no se aplica un control para el uso de contraseñas, para la autenticación del usuario y para la limitación del tiempo de acceso al sistema de los funcionarios que pueda hacer del sistema un método de almacenamiento y acceso más seguro	El uso de contraseñas por parte de los empleados es indispensable para el manejo de la información dentro del laboratorio por tal motivo es recomendable que se estén cambiando periódicamente y que se utilice un método que ayude a verificar que el usuario es quien está ingresando verdaderamente al sistema.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Compromiso de la información, Compromiso de las funciones.

	efectivo en el control de la información.			
9.	La entrega de información a los pacientes podría sufrir el riesgo de ser cambiada o alterada pues no se cuenta con un método eficiente para verificar que esta información concuerde, más que la atención puesta y el trabajo de identificarlo y suministrarlo por el personal del laboratorio.	Es importante implementar una manera apropiada para verificar la información que se entrega a los pacientes y así evitar incidentes y disminuir el margen de error que pueda ocasionar malentendidos o problemas legales para la empresa.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Compromiso de la información, acciones no autorizadas y compromiso de las funciones.
10	El laboratorio clínico no cuenta con un método eficiente para eliminar información, que ya no sea utilizada por la empresa pero que no deja de ser un riesgo para la entidad por el uso inadecuado que se le pueda dar por parte de terceros.	La información tiene un proceso que consiste en crearla, guardarla, utilizarla, compartirla, archivarla y destruirla, cuando la información llega a este último punto es porque ha cumplido con toda su utilidad para la empresa por esto es importante que sea destruida de una manera prudente de tal manera que no quede ninguna evidencia que pueda originar inconvenientes para la empresa.	Afecta a los procesos Pre-analíticos, Analíticos y post-analíticos del laboratorio clínico.	Compromiso de la información.

Fuente. Laboratorio Clínico CONFESALUD IPS LTD

4.1.4 Diagnostico de la seguridad física y lógica del laboratorio clínico. El laboratorio clínico CONFESALUD IPS LTDA es una entidad prestadora del servicio de toma de muestras y pruebas médicas, que realiza sus actividades con el fin de prestar a la comunidad un servicio con calidad. El uso, procesamiento y trasmisión de información es considerado por la empresa como una de las labores más importantes para su funcionamiento, lo que hace de la información procesada uno de los activos más importantes para cumplir con la misión y los objetivos empresariales trazados por la organización.

En la recopilación de datos que se realizó a partir del estudio de la organización y la aplicación de los instrumentos correspondientes, se obtuvo información importante que arrojo resultados claves para conocer cuál es la situación actual en la que se encuentra el laboratorio clínico, frente al manejo que se le da a la seguridad física y lógica de los activos de la información utilizados por la empresa.

El motivo más importante a resaltar y por el cual se está desarrollando esta investigación, es porque el laboratorio clínico actualmente no cuenta con un sistema de seguridad establecido, donde se definan los procedimientos y las normas a seguir para la protección de la información que se procesa y se suministra a los pacientes en el laboratorio.

Uno de los resultados obtenidos, es que la empresa aún no cuenta con unas políticas establecidas para guiar a la empleados en sus funciones y responsabilidades, en el manejo de la información y en la seguridad que se debe tener con esta, pese a que en el momento de ingresar a la empresa se les orienta y se les dan las pautas para realizar sus labores, es necesario crear este documento para que de manera formal se les dé a conocer las responsabilidades y deberes que cada uno debe cumplir con respecto al cuidado y protección de la información de la empresa.

Otro dato importante que fue suministrado por el laboratorio clínico, es que no utilizan un contrato de confidencialidad o un documento legal que haga constar la responsabilidad que asumen los trabajadores del cuidado y discreción que deben mantener con la información con la que trabajan, este es un aspecto bastante importante para mejorar, ya que la implementación de un contrato para la iniciación o continuación de labores del recurso humano en la empresa, le brinda a la organización una herramienta más para proteger la información.

Se encontró que los empleados en su totalidad tienen acceso a los equipos donde se recopila y almacena la información utilizada por la empresa, aunque no todos tienen acceso directo a la información confidencial de la misma pues no poseen una cuenta de usuario ni una contraseña para ingresar a los archivos donde se encuentra resguardada, es posible que esta sea una amenaza para tener en cuenta, ya que con solo tener la opción de uso de los equipos, puede presentarse algún incidente en el que se vea afectada la información importante allí almacenada.

Un factor muy importante encontrado es que la organización no cuenta con un plan de contingencia y en caso de presentarse alguna eventualidad que pueda causar daños físicos, no solo a la información sino también al personal y las instalaciones del laboratorio clínico, no se tiene un plan de acción definido, ni para prevenir la situación, ni tampoco para tomar decisiones adecuadas o acciones correctivas.

Los empleados del laboratorio clínico demostraron tener un sentido de responsabilidad claro con la información con la que trabajan, ya que procuran mantener a salvo dicha información, manejando contraseñas seguras y cambiándolas con regularidad para evitar alteraciones, aunque se reconoce que la empresa no aplica un control para el uso de contraseñas que ayuden en la autenticación del usuario y para la limitación del tiempo de acceso al sistema de los funcionarios que pueda hacer del sistema un método de almacenamiento y acceso más seguro y efectivo en el control de la información.

De igual manera los empleados no suministran información de la empresa a terceros sin tener la debida autorización de la administración del laboratorio clínico, ni se traslada información confidencial fuera de las instalaciones de la organización para evitar cualquier incidente como pérdida, robo o mal uso. Para realizar la entrega de información a los pacientes, no se cuenta con un método eficiente para verificar que esta información no sea alterada, solamente se tiene la atención del personal puesta en los documentos y resultados con el fin de identificarlos y suministrarlos de la mejor manera.

El uso de las redes y del sistema para realizar tratos comerciales con clientes y proveedores le corresponde única y exclusivamente a personal administrativo, ya que este es considerado un riesgo también para el sistema de información de la empresa.

Los equipos y archivos en donde se almacena la información general y confidencial del laboratorio clínico se encuentran: Algunos ubicados en las oficinas y otros al interior del área restringida o segura del laboratorio clínico, aun así no se tiene una total cobertura para la seguridad de los activos de la información pues estos no se encuentran exentos de ser dañados o de sufrir algún deterioro por factores de uso, mantenimiento o de tipo ambiental.

Uno de los hallazgos importantes es que el laboratorio Clínico no cuenta con un sistema de vigilancia constante en el que se disponga de cámaras de seguridad o de personal preparado en el área de seguridad, para que esté pendiente y al tanto de movimientos extraños dentro de la entidad o alrededor del perímetro en donde se encuentra ubicada, teniendo la responsabilidad de cuidarla de posibles amenazas que puedan ocasionar daños a la empresa en general y en especial a la información, como la pérdida o robo de la misma.

La IPS solo tiene una alarma de seguridad ubicada en la entrada de Las instalaciones, utilizado exclusivamente en la noche, y durante el día se encuentra el personal de la empresa laborando y ellos sin los encargados de cuidarla.

Es bueno resaltar que por precaución al daño de la información, la empresa siempre mantiene copias de seguridad de sus archivos para evitar algún tipo de anomalía que afecte el buen funcionamiento de la empresa, pero estas copias están guardadas en los equipos donde se encuentran los demás archivos, así que sigue siendo un riesgo la protección de los equipos.

Finalmente se pudo encontrar que el laboratorio clínico no cuenta con un método eficiente para eliminar información que ya no es utilizada por la empresa pero que no deja de ser un riesgo para la entidad por el uso inadecuado que se le pueda dar por parte de terceros si llegase a su poder, lo que ocasionaría graves consecuencias para la entidad.

4.2 DEFINICIÓN DEL MANUAL DE SEGURIDAD PARA EL MANEJO DE LA INFORMACIÓN DEL LABORATORIO CLÍNICO CONFESALUD IPS LTDA

4.2.1 Manual de seguridad de la información. Para establecer el sistema de gestión de seguridad de la información dentro del laboratorio clínico CONFESALUD IPS LTDA es necesario definir un manual de seguridad teniendo en cuenta la información recopilada a través de los instrumentos aplicados (la encuesta y la lista de chequeo) y la información general obtenida de la empresa (las características de la organización, la ubicación, los activos que posee y la tecnología) para fijar los objetivos, directrices y principios para la acción con relación a la seguridad de la información.

Esta guía o manual está basado en las normas NTC ISO/IEC 27001 Y 27002 las cuales contienen las políticas y los controles que permiten diseñar la estructura para dirigir las acciones y procesos de acuerdo con las necesidades del laboratorio clínico.

El documento diseñado será presentado como el manual de políticas de seguridad de la información del laboratorio clínico CONFESALUD IPS LTDA para que la administración de la empresa lo analice y evalué con el fin de ser aprobado para ser implementado y utilizado como guía en los procesos y actividades llevadas a cabo en la organización. (Anexo C)

4.3 PARÁMETROS PARA MEDIR EL RIESGO Y CONTROLES PARA MITIGARLOS O ELIMINARLOS

4.3.1 Análisis del riesgo. Para analizar los riesgos a los que se encuentra expuesta la información que hace parte del Laboratorio Clínico CONFESALUD IPS LTDA se tienen en cuenta las posibles amenazas que afectan a la organización y la vulnerabilidad que estos tienen dentro de la probabilidad de ocurrencia de riesgos potenciales que puedan generar aun mayor amenaza y obstaculizar el desarrollo normal de las funciones dentro de la entidad. Para determinar los riesgos se hace necesario elaborar un listado de las amenazas y las vulnerabilidades, teniendo en cuenta las actividades y procesos que se llevan a cabo en la empresa y priorizándolos según el grado en que afecten las funciones, la misión y los

objetivos organizacionales del laboratorio clínico. Los factores más importantes a identificar son los siguientes:

4.3.1.1 Identificación del riesgo. Para identificar los riesgos se deben determinar los sucesos que podrían causar una perdida potencial a la empresa, comprendiendo el cómo, el dónde y el por qué podría ocurrir está perdida. Es necesario recolectar los datos importantes de la empresa, e identificar las amenazas y las vulnerabilidades que puedan alterar los procesos que se llevan a cabo dentro del Laboratorio Clínico. Para ello se identifican los siguientes factores:

a) Identificación de los activos. Un activo es todo aquello que tiene valor para la organización y que por lo tanto requiere de protección. Para identificar los activos es necesario tener en cuenta que el sistema de información consta de software, hardware y también de información física de la empresa lo que ayudara a realizar una lista de los activos que van a estar sometidos a la gestión del riesgo y una lista de los procesos del negocio relacionados con los activos y su importancia.

TABLA 16. Identificación de los activos.

HADWARE	Computador	SAMSUNG	SYNCMASTERS 19B150
	Computador	SAMSUNG	SYNCMASTERS 740 NW
	Computador	SAMSUNG	
	Hematología	BAYER	ADVIA 60
	Marcadores cardiacos	ROCHE	COBASH 232
	Electrolitos	ROCHE	AVL
	Quimiolab	STAT FAX	3000
	Quimiolab	STAT FAX	MULTIWASH III
	Química clínica	BIOMÉDICA	ADC18
SOFTWARE	Programa administrativo para laboratorios	GESLAB	

RED	Red WIFI	TELEFONICA MOVISTAR	
PERSONAL	BACTERIOLOGA ESPECIALISTA	IDANA CELENE PORTILLO.	
	BACTERIOLOGA	YAMILE PACHECO.	
	BACTERIOLOGA	XIMENA REYES.	
	AUXILIAR DE LABORATORIO	CLAUDIA PACHECO	
	AUXILIAR DE LABORATORIO	MARIA FERNANDA CELIS	
LUGAR	INSTALACIONES	Perímetros de ubicación del laboratorio clínico.	Ocaña, Norte de Santander, carrera 16ª N. 11-45 Barrio San Agustín.
	SERVICIOS PUBLICOS ESENCIALES	Agua potable	
		Luz eléctrica	
		Telefonía fija	
		Telefonía Móvil	
		Internet wifi	
ORGANIZACIÓN	ESTRUCTURA FISICA DE LA EMPRESA	Plano físico de la empresa.	

Fuente. Laboratorio Clínico CONFESALUD IPS LTDA.

b) Identificación de las amenazas. Una amenaza tiene el potencial de causar daño a los activos de la información, a los procesos, a los sistemas y por ende a toda la

organización como tal. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Para identificar a profundidad las amenazas para la seguridad de la información del laboratorio clínico se tendrá como referencia el catalogo de amenazas citado en la NTC ISO/IEC 27005:2008 y la información recolectada a partir de la aplicación de la encuesta y la lista de chequeo en el laboratorio clínico CONFESALUD IPS LTDA para luego realizar una lista de amenazas a las que se encuentra directamente expuesta la organización.

La siguiente tabla presenta las amenazas comunes que pueden ser utilizadas durante el proceso de evaluación de las amenazas que pueden catalogarse como deliberadas, accidentales o ambientales. Para cada uno de los tipos de amenazas se indica de esta manera:

D: Deliberadas. Tienen como objetivo los activos de la información.
A: Accidentales. Se utilizan para las acciones humanas que pueden dañar accidentalmente los activos de la información.
E: Ambientales. Se utiliza para los incidentes que no se basan en las acciones humanas.

TABLA 17. Amenazas más comunes.

TIPO	AMENAZA	ORIGEN
DAÑO FISICO	Fuego.	A,D,E.
	Daño por agua.	A,D,E.
	Contaminación.	A,D,E.
	Daño importante.	A,D,E.
	Destrucción del equipo o los medios.	A,D,E.
	Polvo, corrosión, congelamiento.	A,D,E.
EVENTOS NATURALES	Fenómenos climáticos.	E.
	Fenómenos sísmicos.	E.
	Fenómenos Volcánicos.	E.
	Fenómenos meteorológicos.	E.
	Inundación.	E.
PERDIDA DE LOS SERVICIOS ESENCIALES	Falla en el sistema de suministro de agua o de aire acondicionado.	A,D.
	Perdida del suministro de energía.	A,D.E
	Falla en el equipo de comunicaciones.	A,D.
PERTURBACION DEBIDA A LA RADIACIÓN	Radiación electromagnética.	A,D,E.
	Radiación térmica.	A,D,E.
	Impulsos electromagnéticos.	A,D,E.
	Interceptación de señales de interferencia comprometedoras.	D.
	Espionaje remoto.	D.

COMPROMISO DE LA INFORMACIÓN	Escucha subrepticia	D.
	Hurto de medios o documentos.	D.
	Hurto de equipos	D.
	Recuperación de medios reciclados o desechados.	D.
	Divulgación.	A,D.
	Datos provenientes de fuentes no confiables.	A,D.
	Manipulacion de hardware.	D.
	Manipulación de software.	A,D.
	Detección de la posición.	D.
FALLAS TECNICAS	Falla del equipo.	A.
	Mal funcionamiento del equipo.	A.
	Saturación del sistema de información.	A,D.
	Mal funcionamiento del software.	A.
	Incumplimiento en el mantenimiento del sistema de información.	A,D.
ACCIONES NO AUTORIZADAS	Uso no autorizado del equipo.	D
	Copia fraudulenta del software.	D
	Uso del software falso o copiado.	A,D.
	Corrupción de los datos.	D.
	Procesamiento ilegal de los datos.	D.
COMPROMISO DE LAS FUNCIONES	Error en el uso.	A.
	Abuso de derechos.	A,D.
	Falsificación de derechos.	D.
	Negación de acciones.	D.
	Incumplimiento en la disponibilidad del personal.	A,D,E.

Fuente. NTC ISO/IEC 27005:2008

c) Identificación de las vulnerabilidades. Las vulnerabilidades deben ser identificadas teniendo en cuenta las amenazas por causa en daños de los activos o de la misma organización en general. Para ellos se observa la situación y el uso que se le está dando a la organización, los procesos, el personal, el ambiente físico, el hardware, software y equipos de comunicaciones y a cada dependencia del laboratorio clínico.

La presencia sola de la vulnerabilidad no causa daño, dado que es necesario que exista una amenaza presente para que ocurra la situación de riesgo. Para identificar las vulnerabilidades latentes en el laboratorio clínico CONFESALUD IPS LTDA se elaboró un listado de posibles escenarios que pueden causar incidentes.

TABLA 18. Vulnerabilidades más comunes.

TIPO	VULNERABILIDADES
HARDWARE	Mantenimiento insuficiente.
	Susceptibilidad a la humedad, al polvo y a la suciedad.
	Sensibilidad a la radiación electromagnética.
	Falta de control de cambio con configuración eficiente.
	Susceptibilidad a las variaciones de tención.
	Susceptibilidad a las variaciones de temperatura.
	Almacenamiento sin protección.
	Falta de cuidado en la disposición final.
	Copia no controlada.
SOFTWARE	Falta de insuficiencia de la prueba del software.
	Defectos bien conocidos en el software.
	Falta de "terminación de sesión cuando se abandona la estación de trabajo".
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.
	Falta de pruebas de auditoría.
	Distribución errada de los derechos de acceso.
	Software de distribución amplia.
	Utilización de los programas de aplicación a los datos errados en los términos de tiempo.
	Interface de usuario complicada.
	Falta de documentación.
	Configuración incorrecta de parámetros.
	Fechas incorrectas.
	Falta de mecanismos de identificación y autenticación.
	Tablas de contraseñas sin protección.
	Gestión deficiente de contraseñas.
	Habilitación de servicios innecesarios.
	Software nuevo o inmaduro.
	Especificaciones incompletas o no claras para los desarrolladores.
	Falta de control eficaz del cambio.
	Descarga y uso no controlado de software.
	Falta de copias de respaldo.
	Falta de protección física de las puertas y ventanas de la edificación.
	Falla en la producción de informes de gestión.

RED	Falta de prueba del envío o la recepción de mensajes.
	Líneas de comunicación sin protección.
	Trafico sensible sin protección.
	Conexión deficiente de los cables.
	Punto único de falla.
	Falta de identificación y autenticación de emisor y receptor.
	Arquitectura insegura de la red.
	Transferencia de contraseñas autorizadas.
	Gestión inadecuada de la red.
	Conexiones de red pública sin protección.
PERSONAL	Ausencia de personal.
	Procedimientos inadecuados de contratación.
	Entrenamiento insuficiente en seguridad.
	Uso incorrecto de software y hardware.
	Falta de conciencia acerca de la seguridad.
	Falta de mecanismos de monitoreo.
	Trabajo no supervisado del personal externo o de limpieza.
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.
LUGAR	Uso inadecuado o descuidado del control de accesos físicos a las edificaciones y los recintos.
	Ubicación en un área susceptible de inundación.
	Red energética inestable.
	Falta de protección física de las puertas y ventanas de la edificación.
ORGANIZACIÓN	Falta de procedimientos formal para el retiro del registro de usuarios.
	Falta de proceso formal para revisión de los derechos de acceso.
	Falta o insuficiencia de disposiciones en los contratos con los clientes y/o terceras partes.
	Falta de procedimientos de monitoreo de los recursos de procesamientos de información.
	Falta de supervisiones regulares.
	Falta de procedimientos de identificación y evaluación de riesgos.
	Falta de reportes sobre fallas incluidos en los registros de administradores y operadores.
	Respuesta inadecuada de mantenimiento del servicio.
	Falta o insuficiencia en el acuerdo a nivel de servicio.
	Falta de procedimiento de control de cambios.

	Falta de procedimientos formal para el control de la documentación del SGSI.
	Falta de procedimiento formal para la supervisión del registro del SGSI.
	Falta de procedimiento formal para la autorización de la información disponible al público.
	Falta de asignación adecuada de responsabilidades en la seguridad en la información.
	Falta de planes de continuidad.
	Falta de políticas sobre el uso del correo electrónico.
	Falta de procedimientos para la introducción del software en los sistemas operativos.
	Falta de registros en las bitácoras de administrador y operario.
	Falta de procedimientos para el manejo de información clasificada.
	Falta de responsabilidades en la seguridad de la información en la descripción de los cargos.
	Falta o insuficiencia en las disposiciones en los contratos con los empleados.
	Falta de los procesos disciplinarios definidos en el caso de incidentes de seguridad en la información.
	Falta de política formal sobre la utilización de computadores portátiles.
	Falta de control de los activos que se encuentran fuera de las instalaciones.
	Falta o insuficiencia de políticas sobre limpieza de escritorio y de pantalla.
	Falta de autorización de los recursos de procesamiento de la información.
	Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad.
	Falta de revisiones regulares por parte de la gerencia.
	Falta de procedimientos para la presentación de informes sobre las debilidades en la seguridad.
	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.

Fuente. NTC ISO/IEC 27005:2008

4.3.1.2 Estimación del riesgo. La estimación del riesgo se puede realizar de diferentes maneras, todo depende de las amenazas que tengan los activos y la amplitud de las vulnerabilidades. Este análisis se puede ejecutar utilizando las metodología de estimación cualitativa, cuantitativamente o con una combinación de ambas.

La forma de análisis deberá ser consistente con los criterios de evaluación del riesgo por esta razón se aplicara la metodología cuantitativa para conocer por medio de una escala de valores numéricos las probabilidades de amenaza y de vulnerabilidad en la que se encuentra el laboratorio clínico. La calidad de este análisis depende de lo completos y exactos que sean los valores numéricos.

La estimación se mide en una escala de 0 - 4, teniendo en cuenta que:

0 = Muy bajo.
1 = Bajo.
2 = Medio.
3 = Alto.
4 = Muy alto.

TABLA 19. Estimación cuantitativa de la amenaza.

Vulnerabilidad / **Amenaza**	**Activos de la información.**				
	Hardware	**Software**	**Redes**	**Personal**	**Sitio**
Daño físico.	4	4	2	1	4
Eventos naturales.	3	3	4	4	4
Perdida de los servicios esenciales.	3	3	4	3	4
Perturbación debida a la radiación.	2	2	3	2	2
Compromiso de la información.	4	4	3	4	3
Fallas técnicas.	4	4	2	3	2
Acciones no autorizadas.	4	4	2	4	1
Compromiso de las funciones.	2	3	2	4	1

Fuente. Estudiantes.

TABLA 20. Estimación cuantitativa de la vulnerabilidad.

Vulnerabilidad / Amenaza	Activos de la información.				
	Hardware	**Software**	**Redes**	**Personal**	**Sitio**
Daño físico.	4	3	1	1	3
Eventos naturales.	4	2	2	2	4
Perdida de los servicios esenciales.	2	1	3	2	4
Perturbación debida a la radiación.	3	1	1	1	1
Compromiso de la información.	4	4	4	4	4
Fallas técnicas.	3	3	4	2	2
Acciones no autorizadas.	4	4	4	4	3
Compromiso de las funciones.	2	3	2	4	3

Fuente. Estudiantes

4.3.2 Evaluación de riesgos. La evaluación del riesgo permite la definición de las prioridades y de los sucesos en un orden según las acciones que se realicen para atender los riesgos más críticos que se presentan. El proceso de evaluación de los riesgos en la seguridad de la información implica la identificación y evaluación de los activos, la evaluación de las amenazas para los activos y la evaluación de las vulnerabilidades. Los resultados se utilizan para evaluar los riegos y luego identificar su tratamiento.

4.3.2.1 Matriz con los valores predefinidos. Esta matriz resulta de la consideración de la probabilidad de un escenario de incidente, graficado frente al impacto estimado en la empresa. La probabilidad de un escenario de incidente está dada por una amenaza que explota una vulnerabilidad con una probabilidad determinada. El riesgo resultante se mide en una escala de 0 a 8.

0-2	**Riesgo bajo**
3-5	**Riego medio**
6-8	**Riesgo alto**

TABLA 21. Matriz de valores predefinidos.

	Probabilidad del escenario de incidente	Muy baja (muy improbable)	Baja (improbable)	Media (posible)	Alta (probable)	Muy alta (frecuente)
Impacto en el negocio	**Muy bajo**	**0**	**1**	**2**	**3**	**4**
	Bajo	**1**	**2**	**3**	**4**	**5**
	Media	**2**	**3**	**4**	**5**	**6**
	Alta	**3**	**4**	**5**	**6**	**7**
	Muy alta	**4**	**5**	**6**	**7**	**8**

Fuente. NTC ISO/ IEC 27005:2008

Fórmula aplicada.

RIESGO = AMENAZA + VULNERABILIDAD.

4.3.2.1 Resultados de la evaluación del riesgo.

TABLA 22. Resultado de la evaluación del riesgo.

Vulnerabilidad / **Amenaza**	**Activos de la información.**				
	Hardware	**Software**	**Redes**	**Personal**	**Sitio**
Daño físico.	8	7	3	2	7
Eventos naturales.	7	5	6	6	8
Perdida de los servicios esenciales.	5	4	7	5	8
Perturbación debida a la radiación.	5	3	4	3	3
Compromiso de la información.	8	8	7	8	7
Fallas técnicas.	7	7	6	5	4
Acciones no autorizadas.	8	8	6	8	4
Compromiso de las funciones.	4	6	4	8	4

Fuente. Estudiantes.

4.3.2.2 Resultados de los riesgos identificados de la empresa.

TABLA 23. Identificación de los riesgos de la seguridad de la información en el laboratorio clínico CONFESALUD IPS LTDA.

AMENAZA	VULNERABILIDAD	RIESGO
Incumplimiento del sistema de información.	Mantenimiento insuficiente. Falta de procedimientos del control de cambios.	Daño físico, compromiso de la información, fallas técnicas.
Hurto de medios o documentos.	Almacenamiento sin protección. Copia no controlada. Falta de cuidado en la disposición final. Falta de mecanismos de monitoreo establecidos en la seguridad. Trabajo no supervisado del personal externo o de limpieza.	Compromiso de la información, acciones no autorizadas, compromiso de las funciones.
Abuso de derechos	Falta de la terminación de sesión cuando se abandona el puesto. Disposición de los medios de almacenamiento sin borrado adecuado. Falta en el monitoreo de los recursos de procesamiento de la información. Falta de disposiciones en los contratos con clientes o terceras partes. Falta del proceso formal para la revisión de los derechos de acceso.	Compromiso de las funciones, compromiso de la información.

Error de uso	Falta de documentación. Fechas incorrectas. Entrenamiento insuficiente en seguridad. Uso incorrecto del software y hardware. Falta de conciencia acerca de la seguridad. Falta de políticas y procedimientos para el manejo de información clasificada. Falta de responsabilidades en la seguridad de información en la descripción de los cargos.	Compromiso de la información, Compromiso de las funciones.
Hurto de equipos	Falta de control de los activos. Falta de políticas formales sobre el uso de equipos. Falta de procesos disciplinarios. Falta de protección física de las puertas y ventanas de la edificación.	Compromiso de la información, acciones no autorizadas, compromiso de las funciones.
Uso no autorizado de equipos	Falta de revisiones regulares por parte de la gerencia. Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería. Conexiones de red pública sin protección. Falla en la producción de informes de gestión.	Compromiso de la información, acciones no autorizadas y compromiso de las funciones.
Procesamiento ilegal de datos.	Falta o insuficiencia en las disposiciones en los contratos con los empleados. Falta de mecanismos de monitoreo.	Compromiso de las funciones, acciones no autorizadas y compromiso de la información.

Falla del equipo	Falta de planes de continuidad.	Daño físico, compromiso de la información, fallas técnicas.
Corrupción de datos	Falta de procedimiento formal para el control de los documentos.	Acciones no autorizadas, compromiso de la información.
Incumplimiento de la disponibilidad del personal.	Ausencia del personal	Compromiso de las funciones.
Saturación del sistema de información	Gestión inadecuada de la red.	Compromiso del sistema de información.
Espionaje remoto	Arquitectura insegura de la red. Transferencia de contraseñas autorizadas.	Compromiso de las funciones, compromiso de la información.
Escucha subrepticia	Líneas de comunicación sin protección. Trafico sensible sin protección.	Compromiso de la información
Manipulación del software	Falta de copias de respaldo.	Compromiso de la Información.
Falsificación de derechos	Falta de mecanismos de identificación y autentificación del usuario. Contraseñas sin protección. Gestión deficiente de las contraseñas.	Compromiso de las funciones.

Fuente. Estudiantes.

4.3.3 Tratamiento del riesgo en la seguridad de la información. Para darle el tratamiento adecuado al riesgo se deberán seleccionar los controles adecuados y las opciones con las que se puede manejar el riesgo de manera que se tenga un control sobre ya sea reducirlos, retenerlos, evitarlos o transferirlos, igualmente es importante definir un plan de tratamiento para los riesgos identificados.

Las opciones para el tratamiento del riesgo se deben seleccionar teniendo en cuenta los resultados que se dieron en la evaluación del riesgo anteriormente realizada, el costo esperado para implementar las opciones y los beneficios que pueden resultar a partir de la implementación. La dirección o administración del laboratorio clínico será la encargada de tomar en consideración los riesgos identificados que con la aplicación de los controles debidos podrán ser tratados para que se cumpla con la continuidad del negocio.

Las cuatro opciones utilizadas para llevar a cabo el tratamiento del riesgo no se excluyen mutuamente en ocasiones puede ser necesita la combinación de varias para obtener mejores resultados en el tratamiento del riesgo.

4.3.3.1. Selección de controles para el tratamiento del riesgo. Es necesario seleccionar los controles más apropiados para que se pueda dar un mejor manejo y tratamiento a los riesgos determinados en la evaluación hecha del manejo de la información del laboratorio clínico.

a) Controles para la seguridad de la información. Los controles de la seguridad de la información son códigos en los que se indican las buenas prácticas para la seguridad de la información es por esto que para llevar a cabo el proceso de tratamiento de los riesgos se deben identificar como primera medida los controles adecuados para contrarrestar los riesgos ya identificados.

Estos controles se encuentran plasmados en la norma ISO 27002 (Anexo D)

4.3.3.2 Opciones para el tratamiento del riesgo.

a) Reducción del riesgo. El nivel del riesgo se debe reducir mediante la selección de controles que sean los más adecuados y justificados para contrarrestar las posibles amenazas y vulnerabilidades. En general, los controles pueden brindar uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y concienciación. Para reducir el riesgo es necesario realizar los siguientes pasos:

Selección de controles para reducir los riesgos. Para seleccionar los controles se tienen en cuenta los riesgos identificados en el resultado de la evaluación realizada y se analizan teniendo pensando en cuáles serían los más apropiados para reducir los riesgos.

TABLA 24. Identificación de controles para la reducción del riesgo.

RIESGO/AMENAZA	CONTROLES
Incumplimiento del sistema de información.	1. Emplazamiento y control de equipos. 2. Instalaciones y suministros. 3. Seguridad del cableado. 4. Mantenimiento de los equipos. 5. Seguridad de los equipos fuera de las instalaciones. 6. Reutilización o retirada segura de equipos.
Hurto de medios o documentos.	1. Perímetro de seguridad física. 2. Controles físicos de entrada. 3. Seguridad de oficinas, despachos e instalaciones. 4. Protección contra amenazas externas y de origen ambiental. 5. Trabajo en áreas seguras. 6. Áreas de acceso público y de carga y descarga. 7. Identificación de los riesgos derivados del acceso de terceros. 8. Tratamiento de la seguridad en relación a los clientes. 9. Tratamiento de la seguridad en contratos con terceros.
Abuso de derechos	1. Política de control de acceso. 2. Registro de usuario. 3. Gestión de privilegios. 4. Gestión de contraseñas de usuario. 5. Revisión de los derechos de acceso de usuario. 6. Uso de contraseñas. 7. Equipo de usuario desatendido. 8. Política de puesto de trabajo despejado y pantalla limpia. 9. Procedimientos seguros de inicio de sesión. 10. Identificación y autenticación de usuario. 11. Sistema de gestión de contraseñas. 12. Uso de los recursos del sistema. 13. Desconexión automática de sesión. 14. Limitación del tiempo de conexión.

Error de uso	1. Documento de política de seguridad de la información. 2. Revisión de la política de seguridad en la información. 3. Compromiso de la dirección con la seguridad en la información. 4. Coordinación de la seguridad en la información. 5. Asignación de responsabilidades relativas a la seguridad de la información. 6. Proceso de autorización de recursos para el tratamiento de la información. 7. Acuerdos de confidencialidad. 8. Identificación
Hurto de equipos	1. Inventario de activos. 2. Propiedad de los activos. 3. Uso aceptable de los equipos. 4. Perímetro de seguridad física. Controles físicos de entrada. 5. Seguridad de oficinas, despachos e instalaciones. 6. Trabajo en áreas seguras.
Uso no autorizado de equipos	1. Revisión de la política de seguridad de la información. 2. Política de uso de los servicios de red. 3. Autenticación de usuario para conexiones externas. 4. Identificación de los equipos en las redes. 5. Protección de los puertos de diagnóstico y configuración remotos. 6. Segregación de las redes. 7. Control de conexión a la red. 8. Control de encaminamiento (routing) de red.
Procesamiento ilegal de datos.	1. Funciones y responsabilidades. 2. Investigación de antecedentes. 3. Términos y condiciones de contratación. 4. Revisión independiente de la seguridad en la información.
Falla del equipo	1. Emplazamientos y protección de equipos.

	2. Instalaciones de suministro. 3. Seguridad en el cableado. 4. Mantenimiento de los equipos. 5. Seguridad de los equipos fuera de las instalaciones. 6. Reutilización o retirada segura de los equipos. 7. Retirada de materiales propiedad de la empresa. 8. Control de vulnerabilidades técnicas.
Corrupción de datos	1. Identificación de los riesgos derivados del acceso a terceros. 2. Tratamiento de la seguridad en la relación con los clientes. 3. Tratamiento de la seguridad en contratos con terceros. 4. Áreas de acceso público y de carga y descarga. 5. Trabajo en áreas seguras. 6. Seguridad en oficinas, despachos e instalaciones. 7. Controles físicos de entrada. 8. Copias de seguridad. 9. Controles contra el código malicioso. 10. Controles de red. 11. Seguridad de los servicios de red. 12. Fugas de información.
Incumplimiento de la disponibilidad del personal.	1. Funciones y responsabilidades. 2. Investigación de antecedentes. 3. Términos y condiciones de contratación. 4. Responsabilidades de la dirección. 5. Concienciación, formación y capacitación en seguridad de la información. 6. Responsabilidad del cese o cambio. 7. Devolución de activos. 8. Retirada de los derechos de acceso. 9. Uso de contraseñas. 10. Equipo de usuario desatendido. 11. Política de puesto de trabajo despejado. 12. Ausencia del personal.
Saturación del sistema de información	1. Comercio electrónico. 2. Transacciones en línea. 3. Información públicamente disponible.

	4. Política de uso de los servicios en red. 5. Autenticación de usuario para conexiones externas. 6. Identificación de los equipos en las redes. 7. Control de conexión en la red.
Espionaje remoto	1. Funciones y responsabilidades. 2. Políticas de control de acceso. 3. Registro de usuario. 4. Uso de contraseñas. 5. Equipo de usuario desatendido. 6. Política segura de los servicios en red. 7. Autenticación de usuario para conexiones externas. 8. Identificación de los equipos en las redes. 9. Control de la conexión a la red. 10. Procedimientos seguros de inicio de sesión. 11. Identificación y autenticación de usuario. 12. Sistema de gestión de contraseñas. 13. Desconexión automática de sesión. 14. Limitación del tiempo de conexión.
Escucha subrepticia	1. Restricción del acceso a la información. 2. Aislamientos de sistemas sensibles. 3. Controles contra el código malicioso. 4. Controles contra el código descargado en el cliente.
Manipulación del software	1. Copias de seguridad en la información.
Falsificación de derechos	**1.** Políticas de control de acceso. **2.** Registro de usuario. **3.** Gestión de contraseñas de usuario. **4.** Revisión de los derechos de acceso de usuario. **5.** Uso de contraseñas. **6.** Equipo de usuario desatendido. **7.** Procedimientos seguros de inicio de sesión. **8.** Identificación y autenticación de usuario. **9.** Sistema de gestión de contraseñas. **10.** Uso correcto del sistema. **11.** Desconexión automática de sesión. **12.** Restricción del acceso de información.

Fuente. Estudiantes

Restricciones. Existen muchas restricciones que puede afectar la selección de los controles y para reconocerlas y aplicarlas es conveniente considerar varias restricciones al seleccionar los controles. Al suponer las restricciones que generan ventajas y soporte para la reducción de riesgos se deberían tener en cuenta las siguientes:

Restricciones de tiempo: Pueden existir muchos tipos de restricción del tiempo. Por ejemplo, se deberían implementar controles dentro de un periodo de tiempo aceptable para los directores de la organización. Otro tipo de restricción del tiempo es si un control se puede implementar durante la vida activa de la información o del sistema. Un tercer tipo puede ser el periodo de tiempo que los directores de la organización deciden que es aceptable para estar expuestos a un riesgo particular.

Restricciones financieras: Los controles no deberían ser más costosos en su implementación o mantenimiento que el valor de los riesgos que van a proteger, excepto cuando la conformidad es obligatoria (por ejemplo con la legislación). Se deberían hacer todos los esfuerzos para no excederlos presupuestos asignados y lograr la ventaja financiera a través del uso de los controles. Sin embargo, en algunos casos, puede no ser posible alcanzar la seguridad que se buscan el nivel de aceptación del riesgo debido a las restricciones de presupuesto. Por lo tanto, esta se convierte en una decisión de los directores de la organización para resolver esta situación. Se recomienda tener mucho cuidado si el presupuesto reduce la cantidad o la calidad de los controles que se van a implementar dado que esto puede llevar a la retención implícita de un riesgo mayor a la planificada. El presupuesto establecido para los controles se debería utilizar únicamente como un factor limitante con cuidado considerable.

Restricciones técnicas: Los problemas técnicos, como la compatibilidad de programas o hardware, se pueden evitar fácilmente si se tienen en cuenta durante la selección de los controles. Además, la implementación retrospectiva de controles para un proceso o un sistema existentes a menudo está obstaculizada por restricciones técnicas. Estas dificultades pueden desplazar la balanza de controles hacia aspectos físicos y de procedimiento de la seguridad. Puede ser necesario revisar el programa de seguridad de la información con el fin de lograr los objetivos de seguridad. Esto puede suceder cuando los controles no satisfacen los resultados esperados en la reducción de riesgos sin disminuir la productividad.

Restricciones operativas: Las restricciones operativas, como por ejemplo la necesidad de trabajar 24 horas durante los siete días de la semana y aun así realizar copia de soporte, pueden dar como resultado una implementación costosa y compleja de los controles, a menos que ellos se construyan en el diseño desde el principio.

Restricciones culturales: Las restricciones culturales para la selección de los controles pueden ser específicas para un país, un sector, una organización o incluso un departamento dentro de una organización. No todos los controles se pueden aplicar en todos los países. Los aspectos culturales no se pueden ignorar porque muchos controles dependen del

soporte activo del personal. Si el personal no entiende la necesidad del control o no lo encuentra culturalmente aceptable, el control se volverá ineficaz con el paso del tiempo.

Restricciones éticas: Las restricciones éticas pueden tener implicaciones importantes en los controles dado que la ética cambia con base en las normas sociales. Esto puede evitar la implementación de controles tales como la exploración del correo electrónico en algunos países. La privacidad de la información también se puede hacer dependiente de la ética de la región o del gobierno.

Restricciones ambientales: Los factores ambientales pueden influir en la selección de los controles tales como la disponibilidad del espacio, las condiciones climáticas extremas, la geografía urbana y natural del entorno.

Restricciones legales: Factores legales tales como la protección de datos personales o las disposiciones de códigos criminales para el procesamiento de la información podrían afectar la selección de controles. El cumplimiento legal y reglamentario puede determinar algunos tipos de controles, que incluyen la protección de datos y las auditorías financieras; también pueden evitar el uso de algunos controles, por ejemplo la codificación.

Facilidad en el uso: Una interfaz entre tecnología - humano deficiente resultará en un error humano y puede hacer que el control sea inútil. Los controles se deberían seleccionar de modo que brinden facilidad óptima en el uso al tiempo que alcanzan un nivel aceptable de riesgo residual para el negocio. Los controles que son difíciles de utilizar tendrán impacto en su eficacia, ya que los usuarios pueden intentar burlarlos o ignorarlos en la medida de lo posible. Los controles de acceso complejo dentro de una organización podrían alentar a los usuarios a encontrar métodos de acceso alternos, no autorizados.

Restricciones de personal: La disponibilidad y el costo de salario de habilidades especializadas para implementar los controles, y la capacidad para trasladar al personal entre los lugares en condiciones de operación adversa, se deberían tomar en consideración. La experiencia puede no estar fácilmente disponible para implementar controles planificados o puede sobrepasar los costos de la organización. Otros aspectos tales como la tendencia de parte del personal a discriminar a otros miembros del personal que no se han seleccionado para la seguridad pueden tener implicaciones importantes para las políticas y prácticas de seguridad. De igual modo, la necesidad de contratar a las personas correctas para el trabajo y hallar a las personas correctas, puede resultar en la contratación antes de finalizar la clasificación de la seguridad. El requisito para completar la clasificación de seguridad antes de la contratación es la práctica normal y más segura.

Restricciones para integrar controles nuevos y existentes: La integración de controles nuevos en la infraestructura existente y las interdependencias entre los controles a menudo se pasan por alto. Los controles nuevos pueden no ser implementados fácilmente si hay incongruencia o incompatibilidad con los controles existentes. Por ejemplo, un plan para utilizar fichas geométricas para el control del acceso físico puede causar conflictos con un sistema existente basado en teclados numéricos (PIN-pad) para el control del acceso. El

costo del cambio de los controles existentes por los controles planificados debería incluir elementos que se van a adicionar al costo total del tratamiento del riesgo. Puede no ser posible implementar un control seleccionado debido a la interferencia con controles actuales.

Tratamiento por medio de la reducción del riesgo. Observando las amenazas concluidas a partir de la evaluación del riesgo identificado, junto con la aplicación de los controles adecuados para el tratamiento del riesgo y teniendo en cuenta las restricciones anteriormente enunciadas se elabora un cuadro donde se identifican cada uno de los factores para resaltar en el tratamiento adecuado de la reducción del riesgo para el laboratorio clínico.

TABLA 25. Tratamiento de reducción del riesgo.

RIESGO/AMENAZA	CONTROLES	RESTRICCIONES
Incumplimiento del sistema de información.	Emplazamiento y control de equipos. Instalaciones y suministros. Seguridad del cableado. Mantenimiento de los equipos. Seguridad de los equipos fuera de las instalaciones. Reutilización o retirada segura de equipos.	RESTRICCIONES TECNICAS.
Hurto de medios o documentos.	Perímetro de seguridad física. Controles físicos de entrada. Seguridad de oficinas, despachos e instalaciones. Protección contra amenazas externas y de origen ambiental. Trabajo en áreas seguras. Áreas de acceso público y de carga y descarga. Identificación de los riesgos derivados del acceso de terceros. Tratamiento de la seguridad en relación a los clientes. Tratamiento de la seguridad en contratos con terceros.	RESTRICCIONES FINANCIERAS. RESTRICCIONES DE TIEMPO. RESTRICCIONES AMBIENTALES.

Abuso de derechos	Política de control de acceso. Registro de usuario. Gestión de privilegios. Gestión de contraseñas de usuario. Revisión de los derechos de acceso de usuario. Uso de contraseñas. Equipo de usuario desatendido. Política de puesto de trabajo despejado y pantalla limpia. Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas. Uso de los recursos del sistema. Desconexión automática de sesión. Limitación del tiempo de conexión.	RESTRICCIONES CULTURALES RESTRICCIONES OPERATIVAS
Error de uso	Documento de política de seguridad de la información. Revisión de la política de seguridad en la información. Compromiso de la dirección con la seguridad en la información. Coordinación de la seguridad en la información. Asignación de responsabilidades relativas a la seguridad de la información. Proceso de autorización de recursos para el tratamiento de la información. Acuerdos de confidencialidad. Identificación	RESTRICCIONES DE PERSONAL. RESTRICCIONES LEGALES. RESTRICCIONES ETICAS. RESTRICCIONES OPERATIVAS.
Hurto de equipos	Inventario de activos. Propiedad de los activos. Uso aceptable de los equipos. Perímetro de seguridad física. Controles físicos de entrada.	RESTRICCIONES DE TIEMPO. RESTRICCIONES FINANCIERAS.

	Seguridad de oficinas, despachos e instalaciones. Trabajo en áreas seguras.	
Uso no autorizado de equipos	Revisión de la política de seguridad de la información. Política de uso de los servicios de red. Autenticación de usuario para conexiones externas. Identificación de los equipos en las redes. Protección de los puertos de diagnóstico y configuración remotos. Segregación de las redes. Control de conexión a la red. Control de encaminamiento (routing) de red.	RESTRICCIONES LEGALES. RESTRICCIONES TECNICAS. RESTRICCIONES DE TIEMPO.
Procesamiento ilegal de datos.	Funciones y responsabilidades. Investigación de antecedentes. Términos y condiciones de contratación. Revisión independiente de la seguridad en la información.	RESTRICCIONES LEGALES. RESTRICCIONES FINANCIERAS.
Falla del equipo	Emplazamientos y protección de equipos. Instalaciones de suministro. Seguridad en el cableado. Mantenimiento de los equipos. Seguridad de los equipos fuera de las instalaciones. Reutilización o retirada segura de los equipos. Retirada de materiales propiedad de la empresa. Control de vulnerabilidades técnicas.	RESTRICCIONES TECNICAS. RESTRICCIONES FINANCIERAS. RESTRICCIONES DE TIEMPO.
Corrupción de datos	Identificación de los riesgos derivados del acceso a terceros.	RESTRICCIONES FINANCIERAS.

	Tratamiento de la seguridad en la relación con los clientes. Tratamiento de la seguridad en contratos con terceros. Áreas de acceso público y de carga y descarga. Trabajo en áreas seguras. Seguridad en oficinas, despachos e instalaciones. Controles físicos de entrada. Copias de seguridad. Controles contra el código malicioso. Controles de red. Seguridad de los servicios de red. Fugas de información.	RESTRICCIONES LEGALES. RESTRICCIONES CULTURALES. RESTRICCIONES ETICAS.
Incumplimiento de la disponibilidad del personal.	Funciones y responsabilidades. Investigación de antecedentes. Términos y condiciones de contratación. Responsabilidades de la dirección. Concienciación, formación y capacitación en seguridad de la información. Responsabilidad del cese o cambio. Devolución de activos. Retirada de los derechos de acceso. Uso de contraseñas. Equipo de usuario desatendido. Política de puesto de trabajo despejado. Ausencia del personal.	RESTRICCIONES LEGALES. RESTRICCIONES DE TIEMPO. RESTRICCIONES DE PERSONAL. RESTRICCIONES TECNICAS. RESTRICCIONES OPERATIVAS.
Saturación del sistema de información	Comercio electrónico. Transacciones en línea. Información públicamente disponible. Política de uso de los servicios en red. Autenticación de usuario para conexiones externas. Identificación de los equipos en las	RESTRICCIONES LEGALES. RESTRICCIONES FINANCIERAS. FACILIDAD EN EL USO.

	redes. Control de conexión en la red.	RESTRICCIONES PARA INTEGRAR CONTROLES NUEVOS Y EXISTENTES.
Espionaje remoto	Funciones y responsabilidades. Políticas de control de acceso. Registro de usuario. Uso de contraseñas. Equipo de usuario desatendido. Política segura de los servicios en red. Autenticación de usuario para conexiones externas. Identificación de los equipos en las redes. Control de la conexión a la red. Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas. Desconexión automática de sesión. Limitación del tiempo de conexión.	RESTRICCIONES DE TIEMPO. RESTRICCIONES TECNICAS. RESTRICCIONES FINANCIERAS. FACILIDAD DE USO. RESTRICCIONES ETICAS.
Escucha subrepticia	Restricción del acceso a la información. Aislamientos de sistemas sensibles. Controles contra el código malicioso. Controles contra el código descargado en el cliente.	RESTRICCIONES TECNICAS.
Manipulación del software	Copias de seguridad en la información.	RESTRICCIONES LEGALES. RESTRICCIONES OPERATIVAS.
Falsificación de derechos	Políticas de control de acceso. Registro de usuario.	RESTRICCIONES OPERATIVAS.

	Gestión de contraseñas de usuario. Revisión de los derechos de acceso de usuario. Uso de contraseñas. Equipo de usuario desatendido. Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas. Uso correcto del sistema. Desconexión automática de sesión. Restricción del acceso de información.	

Fuente. Estudiantes.

b) Retención del riesgo. Una vez realizada la evaluación del riesgo el laboratorio clínico debe tomar las decisiones adecuadas sobre la opción aplicar para el tratamiento del riesgo, si decide retener el riesgo se debe aceptar la pérdida o ganancia proveniente de un riesgo particular siempre y cuando se tengan en cuenta las políticas de seguridad de la información de la organización y la aceptación del riesgo considerada por la administración del laboratorio.

c) Evitación del riesgo. Cuando los riesgos identificados en la evaluación realizada se consideran muy altos o si los costos exceden los beneficios, el laboratorio debe tomar decisiones para evitar por completo el riesgo, esto lo haría mediante el retiro de la actividad o las actividades existentes o realizando cambios en las condiciones en las que se ejecutan la actividad afectada.

d) Transferencia del riesgo. El riesgo se transferirá a terceras partes que estén especializadas en manejar eficazmente y darle un mejor tratamiento particular al riesgo determinado en la evaluación realizada. La transferencia del riesgo debe ser una decisión tomada por la administración del laboratorio en la que le otorgan el poder a entidades externas quienes pueden modificar los riesgos o darle un tratamiento adicional. Es importante destacar que es posible transferir la responsabilidad para la gestión del riesgo pero no es posible transferir la responsabilidad del impacto y esto sería decisión del manejo de la seguridad del laboratorio clínico.

4.3.3.3 Plan de tratamiento del riesgo. Al seleccionar la reducción de riesgos dentro de las opciones mencionadas anteriormente para darle un mejor tratamiento a los riesgos identificados, se debe crear un plan de acción que ayude a establecer las estrategias para darle un manejo integral y adecuado a los riesgos y se debe realizar un análisis costo-beneficio teniendo como base el costo que genera para la empresa la implementación de

los controles enunciados en el tratamiento del riesgo frente al beneficio que obtendrá la empresa si decide implementar el control recomendado.

TABLA 26. Plan de tratamiento del riesgo.

RIESGO/ AMENAZA	CONTROLES	ESTRATEGIAS DE ACCION
Incumplimiento del sistema de información.	Emplazamiento y control de equipos. Instalaciones y suministros. Seguridad del cableado. Mantenimiento de los equipos. Seguridad de los equipos fuera de las instalaciones. Reutilización o retirada segura de equipos.	Aplicación y cumplimiento del manual de políticas de la seguridad de la información en los procesos y actividades del laboratorio clínico. Divulgación de las políticas de seguridad de la información a todo el personal de la empresa.
Hurto de medios o documentos.	Perímetro de seguridad física. Controles físicos de entrada. Seguridad de oficinas, despachos e instalaciones. Protección contra amenazas externas y de origen ambiental. Trabajo en áreas seguras. Áreas de acceso público y de carga y descarga. Identificación de los riesgos derivados del acceso de terceros. Tratamiento de la seguridad en relación a los clientes. Tratamiento de la seguridad en contratos con terceros.	Adquisición del servicio de seguridad privada por medio de entidades especializadas o un outsourcing. Implementación y ubicación de cámaras de seguridad en el interior exterior de las instalaciones del laboratorio clínico. Elaborar un contrato de confidencialidad para empleados, proveedores y clientes.
Abuso de derechos	Política de control de acceso. Registro de usuario. Gestión de privilegios. Gestión de contraseñas de usuario.	Implementación de un sistema de autenticación de usuario y de contraseñas para protección de la información.

	Revisión de los derechos de acceso de usuario. Uso de contraseñas. Equipo de usuario desatendido. Política de puesto de trabajo despejado y pantalla limpia. Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas. Uso de los recursos del sistema. Desconexión automática de sesión. Limitación del tiempo de conexión.	Utilizar sistemas y técnicas criptográficos para proteger la información sometida a riesgos. Aplicación de la política de seguridad de la información del laboratorio clínico.
Error de uso	Documento de política de seguridad de la información. Revisión de la política de seguridad en la información. Compromiso de la dirección con la seguridad en la información. Coordinación de la seguridad en la información. Asignación de responsabilidades relativas a la seguridad de la información. Proceso de autorización de recursos para el tratamiento de la información. Acuerdos de confidencialidad. Identificación	Aplicación de la política de seguridad de la información del laboratorio clínico. Elaborar un contrato de confidencialidad para empleados, proveedores y clientes. Utilizar métodos de detección y corrección de errores de la trasmisión de información para que sea eficaz y se llegue a cero errores en el sistema de información. Se deben destruir los documentos o equipos que contengan información importante y que ya no se encuentren en uso por parte del laboratorio clínico.
Hurto de equipos	Inventario de activos. Propiedad de los activos. Uso aceptable de los equipos.	Mantener totalmente restringida para terceros el área donde se encuentran los activos de la

	Perímetro de seguridad física. Controles físicos de entrada. Seguridad de oficinas, despachos e instalaciones. Trabajo en áreas seguras.	información del laboratorio clínico. Custodiar los equipos de la empresa por medio de cámaras de seguridad o con la instalación de alarmas en los lugares donde están ubicados.
Uso no autorizado de equipos	Revisión de la política de seguridad de la información. Política de uso de los servicios de red. Autenticación de usuario para conexiones externas. Identificación de los equipos en las redes. Protección de los puertos de diagnóstico y configuración remotos. Segregación de las redes. Control de conexión a la red. Control de encaminamiento (routing) de red.	Restringir el uso de elementos, programas y aplicaciones no permitidos en el sistema de información del laboratorio clínico utilizando contraseñas para configurar el sistema.
Procesamiento ilegal de datos.	Funciones y responsabilidades. Investigación de antecedentes. Términos y condiciones de contratación. Revisión independiente de la seguridad en la información.	Elaborar un contrato de confidencialidad para empleados, proveedores y clientes. La administración del laboratorio clínico deberá asegurarse haciendo una minuciosa investigación de los antecedentes de los empleados, clientes y proveedores antes de hacer cualquier contrato con ellos.
Falla del equipo	Emplazamientos y protección de equipos. Instalaciones de suministro. Seguridad en el cableado. Mantenimiento de los equipos. Seguridad de los equipos fuera de las instalaciones.	La empresa deberá cerciorarse de hacer los mantenimientos requeridos tanto a los equipos como las actualizaciones de los programas para mantener la función óptima de los computadores y equipos de información del laboratorio.

	Reutilización o retirada segura de los equipos. Retirada de materiales propiedad de la empresa. Control de vulnerabilidades técnicas.	Hacer una Revisión frecuente del sistema eléctrico y de redes de las instalaciones del laboratorio clínico.
Corrupción de datos	Identificación de los riesgos derivados del acceso a terceros. Tratamiento de la seguridad en la relación con los clientes. Tratamiento de la seguridad en contratos con terceros. Áreas de acceso público y de carga y descarga. Trabajo en áreas seguras. Seguridad en oficinas, despachos e instalaciones. Controles físicos de entrada. Copias de seguridad. Controles contra el código malicioso. Controles de red. Seguridad de los servicios de red. Fugas de información.	Elaborar un contrato de confidencialidad para empleados, proveedores y clientes. Mantener totalmente restringida para terceros el área donde se encuentran los activos de la información del laboratorio clínico. El sistema debe estar constantemente monitoreado con el fin de realizar las actualizaciones necesarias en los antivirus y evitar algún daño en el sistema.
Incumplimiento de la disponibilidad del personal.	Funciones y responsabilidades. Investigación de antecedentes. Términos y condiciones de contratación. Responsabilidades de la dirección. Concienciación, formación y capacitación en seguridad de la información. Responsabilidad del cese o cambio. Devolución de activos. Retirada de los derechos de acceso. Uso de contraseñas.	Elaborar un contrato de confidencialidad para empleados, proveedores y clientes. La administración del laboratorio clínico deberá asegurarse haciendo una minuciosa investigación de los antecedentes de los empleados, clientes y proveedores antes de hacer cualquier contrato con ellos. La empresa deberá capacitar a los empleados en el tema de la seguridad de la información para que ellos conozcan como realizar

	Equipo de usuario desatendido. Política de puesto de trabajo despejado. Ausencia del personal.	sus labores de la mejor manera y aporten soluciones.
Saturación del sistema de información	Comercio electrónico. Transacciones en línea. Información públicamente disponible. Política de uso de los servicios en red. Autenticación de usuario para conexiones externas. Identificación de los equipos en las redes. Control de conexión en la red.	Restringir el uso de elementos, programas y aplicaciones no permitidos en el sistema de información del laboratorio clínico utilizando contraseñas para configurar el sistema. Proteger la información que está expuesta públicamente a través de páginas web o redes de información. La empresa puede optar por tomar la decisión almacenar la información más importante y confidencial en un modelo de servicio llamado nube y tienen acceso a esta información a través de la red.
Espionaje remoto	Funciones y responsabilidades. Políticas de control de acceso. Registro de usuario. Uso de contraseñas. Equipo de usuario desatendido. Política segura de los servicios en red. Autenticación de usuario para conexiones externas. Identificación de los equipos en las redes. Control de la conexión a la red. Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas. Desconexión automática de sesión.	Implementación de un sistema de autenticación de usuario y de contraseñas para protección de la información. Utilizar sistemas y técnicas criptográficos para proteger la información sometida a riesgos. Utilizar aplicaciones que permitan limitar el tiempo de conexión al sistema de información del laboratorio clínico.

	Limitación del tiempo de conexión.	
Escucha subrepticia	Restricción del acceso a la información. Aislamientos de sistemas sensibles. Controles contra el código malicioso. Controles contra el código descargado en el cliente.	Implementación de un sistema de autenticación de usuario y de contraseñas para protección de la información. Utilizar sistemas y técnicas criptográficos para proteger la información sometida a riesgos. El sistema debe estar constantemente monitoreado con el fin de realizar las actualizaciones necesarias en los antivirus y evitar algún daño en el sistema.
Manipulación del software	Copias de seguridad en la información.	Utilizar medios de almacenamiento como un disco duro que se puede guardar en un lugar seguro y que sea extraíble, para tener otra opción más, que proteja la información y ubicarlo en un lugar aparte de las copias de seguridad creadas y guardadas en los equipos.
Falsificación de derechos	Políticas de control de acceso. Registro de usuario. Gestión de contraseñas de usuario. Revisión de los derechos de acceso de usuario. Uso de contraseñas. Equipo de usuario desatendido. Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas.	Aplicación y cumplimiento del manual de políticas de la seguridad de la información en los procesos y actividades del laboratorio clínico. de autenticación de usuario y de contraseñas para protección de la información. Utilizar sistemas y técnicas criptográficos para proteger la información sometida a riesgos.

	Uso correcto del sistema. Desconexión automática de sesión. Restricción del acceso de información.	

Fuente. Estudiantes.

a) Análisis del costo-beneficio. Una vez se identifican las estrategias de acción para darle un tratamiento al riesgo se deberán definir las responsabilidades y los recurso necesarios para medir cual sería el costo- beneficio que le otorgaría a la empresa la realización y aplicación de las estrategias planteadas.

TABLA 27. Análisis costo-beneficio.

ESTRATEGIAS	RESPONSABILIDADES	RECURSOS
Aplicación y cumplimiento del manual de políticas de la seguridad de la información en los procesos y actividades del laboratorio clínico.	Administración y empleados del laboratorio clínico.	Se requiere únicamente la responsabilidad y el compromiso del recurso humano para dar cumplimiento al manual de seguridad de la información del laboratorio clínico.
Divulgación de las políticas de seguridad de la información a todo el personal de la empresa.	Administración del laboratorio clínico.	Facilitar una copia del manual de seguridad de la información a cada uno de los empleados del laboratorio para que tengan acceso a las políticas elaboradas.
Adquisición del servicio de seguridad privada por medio de entidades especializadas o un outsourcing.	Dirección Administrativa de Confesalud IPS Ltda. Entidad prestadora del servicio de seguridad.	Es necesario utilizar recurso financiero para la inversión en el servicio adquirido.

Implementación y ubicación de cámaras de seguridad en el interior y en el exterior de las instalaciones del laboratorio clínico.	Dirección Administrativa de Confesalud IPS Ltda.	Es necesario utilizar recurso financiero para la inversión en el servicio adquirido.
Elaborar un contrato de confidencialidad para empleados, proveedores y clientes.	Administración del laboratorio clínico.	Recibir la asesoría de un abogado para la elaboración del contrato y así hacer el acuerdo de manera legal.
Implementación de un sistema de autenticación de usuario y de contraseñas para protección de la información.	Administración del laboratorio clínico.	Adquisición e Implementación de un método de autenticación: -Sistema basado en una señal personal. - Sistema basado en una posesión; tarjeta de identidad, firma electrónica. -Sistema basado en características físicas; Identificación de voz, huellas o patrones oculares.
Utilizar sistemas y técnicas criptográficos para proteger la información sometida a riesgos.	Administración del laboratorio clínico.	Se deberá implementar una técnica criptográfica de seguridad tales como: -Acuerdo de claves. Clave secreta con comunicación cifrada. -Autenticación. Permite verificar que quien utiliza el sistema es quien dice ser. -Firma electrónica. Permite que se autentique a través de la firma personal.
Utilizar métodos de detección y corrección de	Administración del laboratorio clínico.	Utilizar métodos para la verificación de los

errores de la trasmisión de información para que sea eficaz y se llegue a cero errores en el sistema de información.		resultados con el propósito de disminuir errores en los resultados de las pruebas analizadas.
Se deben destruir los documentos o equipos que contengan información importante y que ya no se encuentren en uso por parte del laboratorio clínico y que representen un riesgo para la información	Administración del laboratorio clínico.	Se deberán utilizar métodos para eliminar la información tales como: -Información física. Maquinas triturados de papel. -Información lógica. Formatear sistemas operativos.
Mantener totalmente restringida para terceros el área donde se encuentran los activos de la información del laboratorio clínico.	Administración del laboratorio clínico. Empleados de la empresa.	Identificar y señalizar el área restringida con el fin mantenerla asegurada para no permitir el acceso no autorizado a terceras personas.
Custodiar los equipos de la empresa por medio de cámaras de seguridad o con la instalación de alarmas en los lugares donde están ubicados.	Administración del laboratorio clínico.	Inversión en tecnología de seguridad para la adquisición de cámaras y de alarmas.
Restringir el uso de elementos, programas y aplicaciones no permitidos en el sistema de información del laboratorio clínico utilizando contraseñas para configurar el sistema.	Administración del laboratorio clínico.	Configurar el sistema de información utilizado por la empresa con la utilización de contraseñas seguras que sean de conocimiento exclusivo de la administración.
La administración del	Administración del	Para tener acceso a esta

laboratorio clínico deberá asegurarse haciendo una minuciosa investigación de los antecedentes de los empleados, clientes y proveedores antes de hacer cualquier contrato con ellos.	laboratorio clínico.	información legal, la empresa deberá realizar un pago a la entidad gubernamental encargada de suministrar esta información a las empresas.
La empresa deberá cerciorarse de hacer los mantenimientos requeridos tanto a los equipos como las actualizaciones de los programas para mantener la función óptima de los computadores y equipos de información del laboratorio.	Administración del laboratorio clínico.	Se debe contratar una persona especializada en realizar el mantenimiento adecuado, tanto a los equipos de la empresa como a los programas y al sistema de información, esta persona debe ser 100% confiable pues tendrá acceso a la información del laboratorio clínico.
Hacer una Revisión frecuente del sistema eléctrico y de redes de las instalaciones del laboratorio clínico.	Administración del laboratorio clínico.	La revisión de las instalaciones de los servicios públicos deberá hacerla un técnico especializado particular contratado por la empresa o por las mismas empresas prestadoras de servicios.
La empresa deberá capacitar a los empleados en el tema de la seguridad de la información para que ellos conozcan como realizar sus labores de la mejor manera y aporten soluciones.	Administración del laboratorio clínico.	Contratar a una persona especializada en el tema de seguridad de la información que imparta la formación necesaria a los empleados y les brinde una capacitación completa.
El sistema debe estar constantemente monitoreado con el fin de realizar las actualizaciones	Administración del laboratorio clínico. Empleados de la empresa.	Renovar o actualizar el antivirus para protección del sistema operativo de los equipos de la empresa, cada

necesarias en los antivirus y evitar algún daño en el sistema		vez que el sistema requiera.
Proteger la información que está expuesta públicamente a través de páginas web o redes de información.	Administración del laboratorio clínico.	Si se sube información en las redes para hacerla pública se debe proteger de tal manera que no pueda ser modificada ni descargada.
La empresa puede optar por tomar la decisión de almacenar la información más importante y confidencial en un modelo de servicio llamado nube y tienen acceso a esta información a través de la red.	Administración del laboratorio clínico. Proveedor del servicio.	La empresa deberá asumir los costos del uso del servicio para adquirir la protección de la información tales como memoria, procesamiento y almacenamiento de datos.
Utilizar aplicaciones que permitan limitar el tiempo de conexión al sistema de información del laboratorio clínico.	Administración del laboratorio clínico.	Se deberá implementar una aplicación diseñada para limitar el tiempo de conexión de los usuarios al sistema con el fin de proteger la información.
Utilizar medios de almacenamiento como un disco duro que se puede guardar en un lugar seguro y que sea extraíble, para tener otra opción más, que proteja la información y ubicarlo en un lugar aparte de las copias de seguridad creadas y guardadas en los equipos.	Administración del laboratorio clínico. Empleados del laboratorio clínico.	Adquirir un medio diferente a los equipos de la empresa para almacenar información, tales como discos duros, blueray o firewall.

Fuente. Estudiantes.

4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL LABORATORIO CLÍNICO SEGÚN LAS NORMAS Y ESTÁNDARES DE LA ISO 27000

De manera específica, ISO 27001 indica que un SGSI debe estar formado por:

4.4.1 Alcance del SGSI. Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

4.4.2 Política y objetivos de seguridad. Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

4.4.3 Procedimientos y mecanismos de control que soportan al SGSI. Aquellos procedimientos que regulan el propio funcionamiento del SGSI.

4.4.4 Enfoque de evaluación de riesgos. Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

4.4.5 Informe de evaluación de riesgos. Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

4.4.6 Plan de tratamiento de riesgos. Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

4.4.7 Procedimientos documentados. Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

5. CONCLUSIONES

Durante el desarrollo de la investigación, se realizó como primera medida el diagnóstico de la situación en la que se encuentra el Laboratorio Clínico CONFESALUD IPS LTDA con respecto a la seguridad de la información, con el objetivo de conocer el uso que los empleados le dan a la información de la empresa y de establecer las posibles amenazas y vulnerabilidades que ponen en riesgo la información tanto dentro como fuera de la organización, lo que arrojó datos importantes para diseñar el sistema de gestión de la seguridad de la información de la empresa.

Uno de las principales herramientas que se debe crear en el proceso del diseño del sistema de gestión de seguridad de la información es el manual de seguridad. Este documento guía se elaboró teniendo en cuenta la información recopilada de la empresa y los controles a aplicar según la norma, con el fin de definir el alcance, los objetivos, las responsabilidades y la política de seguridad de la información de la empresa.

Se establecieron los parámetros para realizar la gestión del riesgo en la seguridad de la información del laboratorio clínico, para ellos se realizó un análisis en donde se identificaron los riesgos teniendo en cuenta los activos de la empresa, las amenazas y las vulnerabilidades. El siguiente paso consistió en evaluar los riesgos identificados a través de la aplicación de una matriz con valores predeterminados con el fin de conocer cuáles son los riesgos más críticos y por ultimo darles el tratamiento adecuado seleccionando los controles apropiados para reducirlos al máximo.

Con toda la información anteriormente establecida se planteó el Diseño del sistema de Gestión de la seguridad de la información para el Laboratorio Clínico CONFESALUD IPS LTDA, con el propósito de que la empresa le dé a la información que recibe, procesa, almacena y suministra, el uso adecuado y la mantenga bajo los estándares y normas de seguridad, salvaguardada y protegida de incidentes que pueden afectar el normal funcionamiento para la continuidad de la empresa.

6. RECOMENDACIONES

Es recomendable que el laboratorio clínico diseñe un plan de contingencia con el propósito de garantizar la continuidad de las actividades normales de la empresa y definir un plan preventivo, de acción y de reacción, creando estrategias que involucren a todo el personal de la organización y que beneficien las operaciones, para controlar cualquier situación de emergencia y que se logren minimizar las consecuencias negativas.

Una buena alternativa para incluir y hacer parte a los empleados de la empresa en el proceso del sistema de gestión de la seguridad de la información del laboratorio clínico, es sensibilizarlos sobre la magnitud de la responsabilidad que cada uno tiene frente al cuidado de los activos y de los documentos que pertenecen a la entidad, para esto es bueno darles charlas y capacitaciones que los orienten en como manipular de manera correcta la información que procesan.

La administración del laboratorio clínico podría estudiar la posibilidad de proteger a la organización contra daños de responsabilidad civil pues no está exenta de verse involucrada en una demanda con responsabilidad civil profesional y estas demandas pueden presentarse por negligencia o por errores cometidos en el proceso de gestión o sencillamente por omisión en la prestación del servicio lo que podría costarle a la empresa mucho dinero y hasta la posibilidad de seguir funcionando.

Una recomendación importante para la organización, es la creación de un comité encargado de tratar los temas de seguridad de la información del laboratorio clínico, y quien será el encargado de asignar responsabilidades, actividades y tomar las decisiones apropiadas para mantener segura la información de la empresa en la búsqueda de una mejora continua en el sistema de gestión de seguridad de la información diseñado para la empresa.

BIBLIOGRAFÍA

BRANDÉS, Fernando. Responsabilidad profesional y Laboratorio Clínico. Sociedad Española de Dirección y Gestión de los Laboratorios Clínicos. Documento No. 6. SEDIGLAC. Madrid. 1999.

COHEN, Daniel. Sistemas de información en la Organización. Cap.1. Los sistemas de información. Definiciones. Mc. Graw-Hill, Colombia.2000.

CONFESALUD IPS LTDA. Portafolio de Servicios. Ocaña. 2012. 15 pág.

CONTRERAS, Pamela. Gestión de recursos informáticos. Unidad 5 Seguridad Informática. Chile. 2004.

ICONTEC INTERNACIONAL. Norma Técnica Colombiana NTC-ISO 9000. SISTEMAS DE GESTIÓN DE LA CALIDAD. Bogotá D.C. (22 de 12 de 2005).

ICONTEC INTERNACIONAL. Norma Técnica Colombiana NTC-ISO 27000. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION. Bogotá D.C. 2004.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, Norma Técnica NTC-ISO/IEC Colombiana 27001. Tecnología de la información. Técnicas de Seguridad Sistema de Gestión de Seguridad de Información (SGSI) Requisitos. Bogotá D.C. ICONTEC. 2006.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica NTC-ISO/IEC Colombiana 17025. Requisitos generales para la competencia de los laboratorios de ensayo y calibración. Bogotá D.C. ICONTEC. 2005.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Implantación de un SGSI en la empresa. Conceptos Básicos sobre seguridad de la información. España. INTECO, 2010.

LÓPEZ, Antonio. Manual de salud electrónica para directivos de servicios y sistemas de salud. Capítulo IV. Sistema de información del laboratorio clínico. Sociedad Española de informática de salud. Barcelona.2004.

MARQUEZ, Andrés. Artículos y recursos empresariales. Las medidas de seguridad en la protección de datos. Microsoft. España.2011.

MAZON RAMOS, Pilar. & GIMENEZ DE AZCÁRATE, Javier. La informatización de la documentación clínica: Oportunidad de mejora de la práctica clínica y riesgos para la seguridad de la confidencialidad. Informe Seis. Pamplona. 2000.

MINISTERIO DE PROTECCION SOCIAL. (12 de 06 de 2006). Decreto 2323 de 2006.

REPUBLICA DE COLOMBIA, Ministerio de Salud. (04 de 10 de 1993). Resolución Nº 008430 DE 1993. Normas científicas, técnicas y administrativas para la investigación en salud.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Ley 1273 de 2009 Nivel Nacional. Ley 1273 de 2009. Bogotá D.C. Colombia: Diario Oficial 47.223 de enero 5 de 2009.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Decreto 1377 de 2013 Nivel Nacional. Decreto 1377 de 2013. Bogotá D.C. Colombia: Diario Oficial 48834 del 27 de junio de 2013.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Decreto 77 de 1997 Nivel Nacional. Decreto 77 de 1997. Bogotá D.C. Colombia.: Diario Oficial 42965 de enero 23 de 1997.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Ley 10 de 1990 Nivel Nacional. Ley 10 de 1990. Bogotá D.C. Colombia: Diario Oficial 39137 de enero 10 de 1990.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Ley 100 de 1993 Nivel Nacional. Ley 100 de 1993. Bogotá D.C. Colombia: Diario Oficial 41.148 del 23 de Diciembre de 1993.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Ley 1266 de 2008 Nivel Nacional. Ley 1266 de 2008. Bogotá D.C. Colombia.: Diario Oficial 47.219 de diciembre 31 de 2008.

SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTÁ D.C. Ley 1581 de 2012 Nivel Nacional. LEY ESTATUTARIA 1581 DE 2012. Bogotá D.C., Colombia: Diario Oficial 48587 de octubre 18 de 2012.

SOCIEDAD ESPAÑOLA DE INFORMATICA DE LA SALUD. Navarra de gestión para la administración S.A. Seguridad de la información en entornos sanitarios. Primera edición. Marzo de 2008. España. 20 p.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS. Seguridad de la información, Política de seguridad de la información de la Universidad Distrital Francisco José de Caldas. Versión 0.0.0.11. Bogotá D.C. 2003.

FUENTES ELECTRONICAS

AMERICA LAB SERVILOO SA, Un paseo por la Historia del laboratorio clínico. [en línea] Actualizado en el [citado el 12 de febrero de 2014] Disponible en internet en: http://www.americalab.net/latest/un-dia-en-el-laboratorio.html

BARRETO, Luis Carlos. Software administrativo para laboratorio Clínico. [en línea] Actualizado en el 2011. [citado el 12 de febrero de 2014] Disponible en: (http://barretosoftware.com/portafolio/geslabsoftware/)

EAR/PILAR. Entorno de Análisis de Riesgos. Glosario de términos. (En línea) 24 de marzo de 2011 (2014) Disponible en: (https://www.ccn-cert.cni.es/publico/herramientas/pilar5/doc/glossary/index.html)

INSTITUTO POLITECNICO NACIONAL. Seguridad física y planes de contingencia. Poli libro de seguridad informática. [En línea] Actualizado en el 2005 [citado en marzo 1 de 2014] Disponible en: http://148.204.211.134/polilibros../z_basura/HTML/UNIDAD%206/CONTENIDO/Con%20Unidad%206_1.htm.

ISO27000.ES. El portal de ISO 27001 en español. [en línea] Actualizado en el 2009. [Citado el 12 de febrero de 2014] Disponible en: (http://www.iso27000.es/iso27000.html)

ISO27000.ES. Sistema de Gestión de Seguridad de la Información (En línea). 2009. (2014) Disponible en: (http://www.iso27000.es/download/doc_sgsi_all.pdf)

MUÑOZ CAÑABATE, Antonio. Grupo de investigación DIGIDOC. Sistemas de Información en las Empresas. [en línea] Actualizado en el 2003. [Citado el 12 de febrero de 2014] Disponible en: http://www.upf.edu/hipertextnet/numero-1/sistem_infor.html

REAL ISMS. Gestión de riesgos. Activos de la información. Guía de referencia de Uso. [en línea] Actualizado en el 2012. [Citado el 12 de febrero de 2014] Disponible en: https://sites.google.com/a/realiso.com/realisms-spa/gestao-de-risco/-3-3-ativos-de-informacao

SISTESEG. Servicio de seguridad de la información. [En línea] Actualizado en el 2013. [Citado el 12 de febrero de 2014] Disponible en: http://www.sisteseg.com/informatica.html

UNIVERSIDAD POLITÉCNICA SALESIANA. Definición de la normalización a emplear. Términos y definiciones de seguridad. (En línea) 2004 (2014). Repositorio Digital-UPS. Disponible en: (http://dspace.ups.edu.ec/bitstream/123456789/573/3/CAPITULO1.pdf).

ANEXOS

ANEXO A. Encuesta aplicada a los empleados del laboratorio Clínico CONFESALUD IPS LTDA.

	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA **FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONOMICAS** **ADMINISTRACION DE EMPRESAS**	
	EMPRESA	
	LABORATORIO CLINICO CONFESALUD IPS LTDA.	

ENCUESTA			
Nombre :			
Cargo que desempeña:			
Fecha:			
Objetivo: Conocer el uso de la información por parte de los empleados de la empresa.			
PREGUNTAS		SI	NO
1. ¿Sabe usted si la empresa tiene políticas establecidas para el manejo de la información?			
2. ¿Cuándo ingresó a la empresa, firmó algún acuerdo de confidencialidad?			
3. ¿Tiene usted acceso a los equipos de información del laboratorio para el desempeño de sus funciones?			
4. ¿Tiene clave de acceso para ingresar al sistema de información de la empresa?			
5. ¿Considera que la clave de acceso que maneja es confiable para mantener la información segura?			
6. ¿Conoce usted si la empresa cuenta con un plan de contingencia en caso de presentarse algún incidente que pueda ocasionar un daño a la información?			
7. ¿Facilita información a terceros por medio de dispositivos como memorias USB, correos electrónico o redes?			
8. ¿Traslada usted información o equipos fuera de las instalaciones de la empresa?			
9. ¿Realiza algún movimiento o transacción comercial de la empresa a través de equipos o dispositivos electrónicos?			
10. ¿tiene acceso a la información de pacientes, cliente, proveedores, resultados de pruebas e información general de la empresa?			

ANEXO B. Lista de chequeo**.**

	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA **FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONOMICAS** **ADMINISTRACION DE EMPRESAS**	
	EMPRESA	
	LABORATORIO CLINICO CONFESALUD IPS LTDA.	

LISTA DE CHEQUEO	
Realizado por:	
Fecha:	
Objetivo:	Establecer las posibles amenazas que ponen en riesgo la seguridad de la información dentro y fuera de la empresa.

N.	ITEM	SI	NO	OBSERVACIONES
1.	Existe un inventario que evidencia los Activos que posee la Empresa.			
2.	Actualmente la empresa cuenta con un sistema de seguridad de la información.			
3.	La empresa cuenta con un documento legal que especifique las condiciones de confidencialidad al momento de efectuar un contrato laboral.			
4.	Se suministra a los empleados de la empresa equipos o dispositivos para el uso de información.			
5.	En el momento de ocurrir un incendio, perdida, robo o amenaza ambiental la empresa cuenta con un sistema de protección de la información que le permita recuperarla o tenerla a salvo.			
6.	La Empresa mantiene la información confidencial en una zona segura y con acceso restringido			
7.	La ubicación física donde se almacena la información está expuesta a alguna amenaza externa o de tipo ambiental.			
8.	La información que no se encuentra sistematizada está guardada en un archivo o sitio seguro.			

9.	La empresa cuenta con personal de vigilancia y seguridad capacitado para cualquier eventualidad que ponga en riesgo el estado de la información.			
10.	Los equipos que contienen la información general de la empresa están ubicados en un lugar seguro.			
11.	Los equipos de la empresa tienen actualizados los antivirus.			
12.	La empresa mantiene copias de seguridad de la información que procesa en un lugar donde este salvaguardada de amenazas.			
13.	Existe información pública disponible en la red.			
14	La empresa cuenta con algún sistema interno de información para la comunicación entre empleados.			
15.	Se aplica un control para el uso de contraseñas, autenticación del usuario y limitación de tiempo de acceso al sistema.			
16.	La información que entrega La empresa a los usuarios es verificada con anterioridad para evitar incidentes.			
17.	Los archivos del sistema están guardados bajo seguridad.			
18.	Los procesos que se realizan en el laboratorio tienen el control requerido para que no se dé una fuga de información.			
19.	Se utilizan métodos seguros para eliminar la información que no se utiliza, pero que puede ser un riesgo para la empresa.			
20.	Se realiza el mantenimiento adecuado a los equipos de la empresa.			

ANEXO C. Políticas del sistema de seguridad de la información laboratorio clínico CONFESALUD IPS LTDA.

1. INTRODUCCION

La información es un activo que tiene un valor muy importante para el funcionamiento normal del laboratorio Clínico pues con ella se llevan a cabo los procesos pre-analíticos, analíticos y post-analíticos concernientes a los servicios de toma de muestras, análisis de muestras y entrega de resultados, por esta razón la información debe estar debidamente protegida para garantizar la continuidad en el sistema de la información utilizado por la empresa con el fin de minimizar las amenazas y riesgos que puedan ocasionar daños y mejorar la gestión del Laboratorio.

Para que el manual de seguridad de la información pueda ser aplicado en forma correcta y funcione efectivamente, es necesario trazar las políticas de seguridad que protejan la información del laboratorio clínico y sobre todo que las directrices sean acogidas por la empresa como parte del marco organizacional vinculando a todo el personal de la entidad para que de la misma manera sea adquirido el compromiso de todos en la difusión, fortalecimiento y cumplimiento del mismo.

El laboratorio clínico CONFESALUD IPS LTDA con la necesidad de obtener una guía para mantener salvaguardada la información decide implementar sus propias políticas de seguridad de la información con el propósito de realizar de manera organizada y cuidadosa las actividades y procesos que realiza siendo orientados por la NTC ISO/IEC 27001:2008 y aplicando los controles de la NTC ISO/IEC 27002:2005.

2. ALCANCE

El manual de políticas de seguridad de la información aquí establecido se dicta en cumplimiento de las disposiciones del laboratorio clínico CONFESALUD IPS LTDA y con el propósito de gestionar adecuadamente el sistema de la información y proteger los activos de la información que hacen parte de la empresa.

Las políticas establecidas deben ser divulgadas en la organización, de modo que sean conocidas y cumplidas por todos los empleados y administrativos del laboratorio clínico. Igualmente deben ser de pleno conocimiento para proveedores, clientes y usuarios con el fin de realizar labores, transacciones y procesos claros para las partes involucradas.

3. OBJETIVOS

Proteger los sistemas de la información y los activos y recursos utilizados para el procesamiento de la información, salvaguardándola de amenazas internas o externas, y de

sucesos accidentales o deliberados, con el objetivo de cumplir con los principios de confidencialidad, integridad y disponibilidad de la información.

Describir los lineamientos y directrices para el buen desarrollo del sistema de seguridad de la información mejorando el desempeño y confiabilidad del personal que tiene contacto con la información de la empresa.

Implementar las políticas de seguridad de la información aquí establecidas teniendo en cuenta el presupuesto y los recursos correspondientes con el fin de asegurar los activos de la información que hacen parte del laboratorio clínico.

Orientar a los empleados, administrativos, clientes, proveedores, usuarios y particulares involucrados con el sistema de información del laboratorio clínico en la ejecución de sus actividades de forma segura tanto para la organización como para ellos mismos.

Establecer las políticas como normas estándares en la ejecución del trabajo y el manejo del sistema de seguridad de la información, actualizándolas frecuentemente con el fin de hacerlas valer y cumplir en la empresa.

4. RESPONSABILIDADES

Las políticas de seguridad de la información se aplican a los empleados, administrativos, proveedores, clientes y personas ajenas al laboratorio clínico que puedan tener acceso a los activos de la información de la empresa. Cada uno de ellos cumple una función muy importante en el cuidado y administración de la seguridad de la información lo que conlleva a que sea una responsabilidad para todos mantener un ambiente seguro.

La seguridad de la información debe ser constantemente monitoreada, esta labor es responsabilidad de la administración del laboratorio clínico y aunque es recomendable que la empresa establezca en su organización el área de seguridad de la información o un comité delegado, con el tiempo puede formalizarlo contando así con personal encargado de supervisar las funciones para que se dé cumplimiento a las políticas definidas en este documento, dentro de sus funciones están las de evaluar y plasmar los cambios requeridos en el manual y realizar las actualizaciones que sean necesarias para un efectivo cumplimiento de las políticas, logrando así generar el uso correcto de la información de la empresa para mantener la confidencialidad, integridad y disponibilidad que ella requiere.

5. POLITICA DE LA SEGURIDAD

5.1 POLITICA DE LA SEGURIDAD DE LA INFORMACION

Objetivo. Brindar apoyo y orientación a la dirección del laboratorio clínico CONFESALUD IPS LTDA referente a la seguridad de la información de acuerdo con los

requisitos de la entidad prestadora de salud, el reglamento interno de la organización y las leyes que rigen para su funcionamiento.

Controles.

5.1.1 La administración del laboratorio clínico debe estudiar, evaluar y aprobar el documento que orienta a los funcionarios de la empresa en sus labores y que será utilizado como manual de políticas de seguridad de la información con el fin de publicarlo y comunicarlo a todos los empleados y terceras partes que tengan acceso a la información de la organización.

5.1.2 La política establecida debe ser revisada de manera frecuente y en el periodo que estime la administración del laboratorio clínico, teniendo en cuenta que en cualquier momento se pueden presentar casos que ameriten un cambio en los parámetros establecidos o sea necesario anexar algún tipo de especificación que mejore las políticas, lo que garantiza dentro y fuera de la empresa un adecuado manejo de la información.

6. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION

6.1 ORGANIZACIÓN INTERNA

Objetivo. La dirección general del laboratorio clínico CONFESALUD IPS LTDA es la encargada de gestionar y dar cumplimiento a las políticas de seguridad de la información dentro de la empresa.

Controles.

6.1.1 La empresa junto con sus administrativos y funcionarios adquiere el compromiso de mantener la seguridad de la información dentro del laboratorio clínico, apoyando las directrices y procedimientos establecidos en el manual y divulgándolos al personal que hace parte de la empresa.

6.1.2 La administración del laboratorio clínico Asume la coordinación de la seguridad de la información, manteniendo un control de las actividades que se llevan a cabo en la empresa y de los roles y funciones del personal que tiene acceso a la información y a los procesos.

6.1.3 Es función de la administración asignar responsabilidades para mantener a salvo la información, definiendo de manera clara los compromisos, obligaciones y deberes del personal en el tratamiento de la información del laboratorio clínico.

6.1.4 La administración es la encargada de autorizar los procesos relacionados con la seguridad de la información, para ello es necesario identificarlos y evaluarlos para poder implementarlos.

6.1.5 La dirección del laboratorio realizará los acuerdos necesarios de confidencialidad o de no divulgación con el personal de la empresa definiendo las clausulas y requisitos necesarios para mantener protegida la información.

6.1.6 Será obligación de la administración realizar el control y revisión constantes de las políticas y procedimientos para la seguridad de la información del laboratorio con el fin de observar y evaluar los cambios en la implementación del sistema de gestión de seguridad de la información.

6.2 TERCEROS

Objetivo. El propósito es mantener segura la información a la que tienen acceso personal externo al laboratorio clínico, que pueda ser trasmitida, procesada o dirigida por terceros pero que tenga que ver con el funcionamiento de la organización.

Controles.

6.2.1 Se deberán identificar los riesgos relacionados con la información del laboratorio clínico que pueda ser manipulada por terceros. Para ello es necesario que la administración de la empresa implemente los siguientes controles apropiados antes de autorizar el acceso a terceros identificando:

a) El tipo de acceso, sea físico o lógico a los archivos de información del laboratorio.
b) Los motivos por los que se requiere o solicita el acceso a la información.
c) El valor de la información que se va a utilizar por terceros.
d) Los controles que el personal externo empleara en la seguridad de la información que la empresa le suministra.
e) La incidencia del caso en la seguridad de la información del laboratorio clínico.

6.2.2 La empresa deberá considerar los requisitos y controles de seguridad de la información antes de dar acceso a los proveedores o pacientes del laboratorio clínico a la información suministrada por la organización.

6.2.3 Se deben revisar previamente los acuerdos o contratos que realice el laboratorio clínico con terceras partes que implican el acceso, procesamiento, comunicación o gestión de la información por parte de ellos o la adición de productos o servicios a los procesos realizados por la empresa pertinentes a la seguridad de la información. Por tal motivo se revisaran cada uno de los factores con el fin de aplicar los siguientes controles:

a) Cumplir con las políticas de seguridad de la información del laboratorio clínico.

b) Proteger los activos que contienen la información del laboratorio clínico.
c) Restringir la copia y divulgación de la información.
d) Controlar la recuperación de la información y de los activos al finalizar el acuerdo o contrato.
e) Utilizar métodos de acceso, de control y uso de identificadores de usuarios y contraseñas de usuarios.
f) Autorizar al acceso a los usuarios de las cuentas o archivos que contienen la información del laboratorio clínico.

7. GESTION DE ACTIVOS

7.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

Objetivo. Mantener la protección adecuada de la información y de los activos del laboratorio clínico CONFESALUD IPS LTDA.

Controles.

7.1.1 La organización debe tener un inventario de todos los activos que posee el laboratorio clínico, en donde se puedan identificar claramente cuáles son los equipos que son propiedad de la empresa y la ubicación de los mismos.

7.1.2 La información y los activos que se utilizan para llevar a cabo los procesos, prestar el servicio de salud y de los cuales hace uso el laboratorio clínico, deben ser propiedad de la organización, para lo que es necesario su especificación e identificación, pues esto puede prevenir algún tipo de incidente o mal uso de los mismos.

7.1.1 Se deben identificar, documentar e implementar reglas para el uso correcto de los activos de la información que pertenecen al laboratorio clínico pues este debe ser aceptable ya que del cuidado que se le dé a la información y a los activos depende el buen funcionamiento de la organización.

a) Los equipos deben ser utilizados para las funciones inherentes a las labores del laboratorio clínico.
b) Los equipos deberán permanecer encendidos solamente en horas laborales.
c) Las conexiones eléctricas no deben estar a nivel del suelo y su estado debe ser bueno.
d) Se deben actualizar frecuentemente los antivirus para protección de los equipos.
e) Los equipos deben ubicarse en un lugar ventilado y fresco.
f) Los equipos, teclados y pantalla y mouse se deben mantener limpios para que el polvo no los deteriore.
g) Los equipos no deben ser manipulados con las manos sucias o mojadas, ni se deben consumir alimentos cerca de ellos.

h) Si se detentan daños en los equipos o alteraciones los empleados deberán reportarlos ante la administración del laboratorio clínico.
i) El empleado que haga uso del equipo será el responsable de darle el debido manejo tanto al activo como a la información, si es necesario utiliza contraseñas que autoricen el acceso a la información.
j) Se deben realizar periódicamente los mantenimientos requeridos por los equipos y estos deben hacerse por personal autorizado por la administración.

7.2 CLASIFICACION DE LA INFORMACIÓN

Objetivo. Asegurar que la información perteneciente al laboratorio clínico reciba el nivel de protección adecuado.

Controles.

7.2.1 El laboratorio clínico debe clasificar la información teniendo en cuenta; su valor, los requisitos legales, la sensibilidad y la importancia para el funcionamiento de la empresa. Para ello se tendrán en cuenta las tres características de la información en las que se basa la seguridad que son: la confidencialidad, la integridad y la disponibilidad.

7.2.2 La empresa deberá desarrollar e implementar los procedimientos adecuados para archivar, organizar y manejar la información de acuerdo a la clasificación que le dé el laboratorio clínico según el control anterior. Se manejara toda la información tanto en forma física como electrónica utilizando los siguientes procedimientos para procesar la información:

a) Copia.
b) Almacenamiento.
c) Trasmisión por fax o correo electrónico.
d) Trasmisión por teléfono o por correo de voz.

8 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

8.1 ANTES DEL EMPLEO

Objetivo. Asegurar que los empleados, contratistas y pacientes tengan claros sus deberes y responsabilidades antes de adquirir alguna relación con el laboratorio clínico y que estas son aplicadas teniendo en cuenta las actividades de cada uno y así reducir el riesgo de robo, fraude o uso inadecuado de la información.

Controles.

8.1.1 Los empleados, contratistas y pacientes deberán realizar sus labores teniendo en cuenta las responsabilidades asignadas por la administración de la empresa y según las funciones definidas para cada cargo, de acuerdo con la política de seguridad de la información del laboratorio clínico para proteger los activos, las actividades y los procesos.

8.1.2 Se llevaran a cabo controles para verificar los antecedentes del personal que es candidato a ocupar el puesto de trabajo y de los proveedores o contratistas dispuestos a crear vínculos laborales con el laboratorio clínico de a cuerdo con los códigos de ética y las normas legales, según lo que requiera la empresa teniendo en cuenta la clasificación de la información a la que se va a tener acceso y los posibles riesgos.

8.1.3 Los términos y condiciones de contratación se deben especificar antes de ocupar el puesto de trabajo, el empleado que ingresa deberá firmar un contrato donde adquiere el compromiso de confidencialidad o de no divulgación de la información a la que tenga acceso en el laboratorio clínico, dentro del contrato el empleado declara conocer y aceptar que sus actividades van a estar bajo supervisión y control de la empresa pero sin llegar a violar el derecho a la privacidad del empleado. La copia del contrato firmada por el empleado deberá ser guardada por la empresa de manera segura.

8.2 DURANTE EL EMPLEO

Objetivo. Asegurar que los empleados, proveedores y clientes estén conscientes de las amenazas respecto a la seguridad de la información, que conozcan sus responsabilidades y deberes y puedan servir como apoyo para el cumplimiento de la política de seguridad de la información del laboratorio clínico durante el tiempo que estén laborando en la empresa, igualmente tratar de reducir al máximo el riesgo de error humano en sus actividades laborales.

Controles.

8.2.1 La administración del laboratorio clínico deberá exigir a los empleados el cumplimiento de sus responsabilidades, aplicando las políticas y los respectivos procedimientos establecidos por la organización con el fin de cuidar la información de la empresa.

8.2.2 Los empleados del laboratorio clínico deberán recibir la orientación para crear conciencia, la formación y capacitación en la seguridad de la información, igualmente los proveedores y clientes deberán recibir la orientación en el momento en que sea necesario, teniendo en cuenta las funciones laborales de cada uno.

8.2.3 El laboratorio clínico deberá interponen el proceso disciplinario respectivo de manera formal cuando alguno de los empleados haya cometido alguna violación a la seguridad de la información de la empresa o incumpla las políticas y normas establecidas.

8.3 CESE DEL EMPLEO O CAMBIO DE PUESTO DE TRABAJO

Objetivo. Asegurar que los empleados, proveedores y clientes del laboratorio clínico que salen de la empresa o que cambian de puesto o de contrato laboral, lo hagan de manera ordenada y clara para evitar cualquier tipo de anomalía que afecte el sistema de información.

Controles.

8.3.1 Las pautas y procedimientos que se aplicaran inmediatamente se termine la contratación ya sea con el personal o con terceros, o si se realiza algún cambio de contrato o de asignación laboral deberán proteger la información custodiada por la empresa.

a) La información que era utilizada por terceros debe ser devuelta a la empresa en su totalidad.
b) Si el empleado utilizaba contraseñas para acceder a la información debe entregarlas a la administración de la empresa.
c) La empresa debe cambiar los usuarios y contraseñas una vez tenga acceso de nuevo a la información que manipulaban terceros.
d) Los equipos que eran utilizados por terceros deben ser entregados a la empresa si estos son de propiedad de la organización y si no deben comprometerse a eliminar toda la información que posean del laboratorio clínico.

8.3.2 Cualquier activo de la información o dato ya sea usuario o contraseña de acceso o la información como tal debe ser entregada completamente por el personal a la empresa a penas se dé por terminado el contrato laboral o el acuerdo hecho con terceras partes.

8.3.3 Se deben retirar todos los derechos de acceso a la información por parte de los empleados o terceros con quienes se dé por terminado el contrato o acuerdo laboral o si hay algún cambio en el puesto deben ser ajustados a las nuevas funciones.

9 SEGURIDAD FISICA Y DEL ENTORNO

9.1 ÁREAS SEGURAS

Objetivo. Evitar el acceso físico no autorizado a las instalaciones del laboratorio clínico de personal mal intencionado o amenazas que puedan causar cualquier tipo de daño e interferencia en los activos y en la información de la empresa.

Controles.

9.1.1 Se debe proteger la información utilizando medidas de control físicas en los perímetros de las instalaciones del laboratorio clínico para mantener la seguridad y proteger el procesamiento de la información tales como paredes, puertas de acceso controladas o una recepción donde se encuentre personal atento al cuidado de las instalaciones, activos y la información de la empresa.

9.1.2 Las áreas donde se encuentra guardada la información de la empresa deben estar protegidas con controles de acceso que puedan asegurar que solo se permite el acceso a personal autorizado.

9.1.3 Se establecerán controles para la protección física para las oficinas, consultorios, e instalaciones que hacen parte del laboratorio clínico.

9.1.4 Se deben seleccionar las áreas del laboratorio clínico que sean vulnerables a algún daño como incendios, inundaciones, explosiones, terremotos, manifestaciones sociales o algún tipo de desastre natural o incidente provocado por humanos teniendo en cuenta las disposiciones en materia de sanidad y seguridad, y considerando todas las amenazas a la seguridad que representan las edificaciones y zonas cercanas al laboratorio.

9.1.5 Para hacer efectiva la seguridad de los empleados se establecerán lineamientos adicionales que incluyan controles para la protección física del personal y de las áreas seguras del laboratorio clínico.

a) Los empleados deberán ser previamente capacitados y adiestrados para ocupar el puesto de trabajo y para utilizar los equipos.
b) Se deberán mantener limpias y despejadas las áreas de trabajo.
c) Los empleados deberán portar sus implementos de trabajo de forma correcta y limpia.
d) Los empleados no podrán tener acceso a los equipos si muestran síntomas de trasnocho o si se encuentran ebrios.
e) Señalizar las zonas de riesgo o áreas restringidas del laboratorio clínico para que el personal las identifique claramente.

9.1.6 Con el fin de impedir el acceso no autorizado de personal ajenos a la empresa se supervisara el ingreso a las instalaciones del laboratorio clínico en especial a las áreas de acceso público, estas deben estar controladas para conocer el ingreso de personal a las instalaciones de la empresa y evitar el acceso en áreas restringidas o donde se encuentran ubicados los servicios de procesamiento de la información que maneja la empresa.

9.2 SEGURIDAD DE LOS EQUIPOS

Objetivo. Evitar la pérdida, el daño, el robo o la posibilidad de poner en peligro los activos de la empresa o situaciones que puedan interrumpir las actividades normales del laboratorio clínico.

Controles.

9.2.1 Los equipos que contienen la información del laboratorio clínico estarán ubicados y protegidos de los peligros del entornos de manera tal que se reduzcan al máximo los riesgos, amenazas, peligros ambientales y los posibles accesos no autorizados por terceros a la información de la empresa.

9.2.2 Los equipos de la empresa deben estar protegidos contra posibles fallas de energía u otras anomalías en el suministro de energía, se deben tener en cuenta las especificaciones de los fabricantes y proveedores de cada equipo.

9.2.1 El cableado de energía eléctrica y de telecomunicaciones que trasporta datos o suministra apoyo a los servicios de información deben estar protegidos contra interceptaciones o daños.

9.2.2 Se realizaran mantenimientos periódicos a los equipos para asegurar que se encuentren en buen estado y disponibles teniendo en cuenta:

a) Realizar el mantenimiento preventivo a los equipos del laboratorio de acuerdo con las especificaciones dadas por los proveedores.
b) Solo personal autorizado por la empresa puede realizar tales mantenimientos y llevar a cabo reparaciones en los equipos.
c) Se debe llevar el registro de las fallas y del mantenimiento preventivo o correctivo realizado a los equipos de la empresa.
d) Se debe autorizar el retiro del equipo de las instalaciones del laboratorio clínico si fuese necesario.
e) Realizar las copias de seguridad necesarias antes de efectuar cualquier tipo de arreglo o mantenimiento y eliminar la información confidencial que contengan los equipos de la empresa.

9.2.3 Si fuese necesario utilizar algún equipo fuera de las instalaciones del laboratorio clínico se debe retirar de la empresa con previa autorización de la administración y si el equipo contiene información importante de la empresa debe ser estudiada y evaluada la posibilidad de ser utilizado fuera de la empresa teniendo en cuenta los riesgos a los que se expone fuera de la organización.

9.2.4 Los medios de almacenamiento o equipos que contienen material importante de la empresa serán físicamente destruidos o sobrescritos de forma segura en lugar de utilizar métodos como borrado estándar de la información, según corresponda cada caso.

9.2.5 Ningún equipo, información de la empresa ni software o documento de la empresa de deben retirar sin autorización previa.

10 GESTION DE COMUNICACIONES Y OPERACIONES

10.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN

Objetivo. Asegurar la operación correcta de los servicios de procesamiento de información del laboratorio clínico.

Controles.

10.1.1 Los procesos, exámenes y servicios que presta el laboratorio clínico deben estar disponibles para todos los usuarios que lo necesiten.

10.1.2 Cuando se realice algún cambio en el sistema de información utilizado por el laboratorio clínico, debe ser controlado de tal manera que no afecte los servicios prestados por la empresa.

10.1.3 Las tareas y funciones deben estar distribuidas según las responsabilidades para reducir la manipulación de información, el uso no autorizado e inadecuado de los activos de la información que hace parte del laboratorio clínico.

10.1.4 Las instalaciones donde se desarrollan los procesos de toma de muestras y procesamiento de resultados incluyendo el almacenamiento de la información deben estar separadas del resto de áreas de la empresa con el fin de reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

10.2 GESTION DE LA PROVISION DE SERVICIOS POR TERCEROS

Objetivo. Mantener la seguridad de la información y de la prestación del servicio cuando se realizan acuerdos de prestación de servicios por terceras partes.

Controles.

10.2.1 Cuando el laboratorio clínico realice contratos con terceros se debe definir la clase de servicio que se requiere y las obligaciones de los mismos, tratando de que sean implementados, mantenidos y operados por las terceras partes.

10.2.2 Los servicios suministrados por terceros al laboratorio clínico deberán ser controlados y revisados con regularidad según lo estime la empresa en intervalos de tiempo y teniendo en cuenta la duración del acuerdo o del contrato pactado.

10.2.3 Si fuese necesario realizar cambios en el acuerdo pactado con terceros se hace necesario revisar las políticas de seguridad de la información de la empresa para que no afecte las funciones y los procesos del laboratorio que puedan ocasionar riesgos en el sistema.

10.3 PLANIFICACION Y ACEPTACION DEL SISTEMA

Objetivo. Minimizar el riesgo de fallas en los sistemas de información utilizados por el laboratorio clínico.

Controles.

10.3.1 El uso de los activos y del sistema debe estar supervisado por la administración del laboratorio clínico para prevenir cualquier falla futura o falta de capacidad del sistema utilizado para almacenar la información de la organización.

10.3.2 Los programas y redes utilizados para llevar a cabo los procesos de información del laboratorio clínico deben ser constantemente actualizados y se debe comprobar que las versiones utilizadas sean las adecuadas para que no exista falla en el sistema.

10.4 PROTECCION CONTRA CODIGOS MALICIOSOS Y DESCARGABLE

Objetivo. Proteger la integridad del software utilizado para procesar la información del laboratorio clínico.

Control.

10.4.1 Los equipos que procesan la información del laboratorio clínico deberán utilizar, actualizar y realizar un constante mantenimiento al antivirus de defensa al sistema con el propósito de protegerlos contra códigos maliciosos que puedan deteriorar o afectar los datos y el sistema de información de la empresa.

10.5 COPIAS DE SEGURIDAD

Objetivo. Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de la información del laboratorio clínico.

Controles.

10.5.1 Para asegurar la información que posee el laboratorio clínico se deben realizar copias de respaldo de la información y del software constantemente, según lo requiera y lo apruebe la administración de la empresa.

10.6 GESTION DE LA SEGURIDAD DE LAS REDES

Objetivo. Asegurar la protección de la información de las redes y la protección de la infraestructura de soporte del sistema de información del laboratorio clínico.

Controles.

10.6.1 El laboratorio debe mantener seguras las redes de información que utiliza aplicando el control adecuado de la configuración y uso de la misma para protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que se utilizan de la red, incluyendo la información que sale y que ingresa a la empresa.

10.6.2 Cuando la empresa realice algún acuerdo sobre los servicios de la red, es necesario identificar y utilizar las características de seguridad, los niveles del servicio que se adquiere y los requisitos de gestión de todos los servicios de la red.

10.7 MANIPULACION DE LOS SOPORTES

Objetivo. Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada y la interrupción en las actividades del laboratorio clínico.

Controles.

10.7.1 El manejo y almacenamiento de la información en dispositivos o soportes ajenos a los equipos debe llevarse a cabo estableciendo cuidados y procedimientos que lo protejan contra divulgación no autorizada o uso inadecuado.

10.7.2 La documentación e información contenida en soportes debe estar protegida contra al acceso no autorizado.

10.8 INTERCAMBIO DE INFORMACIÓN

Objetivo. Mantener segura la información que se intercambie dentro del laboratorio clínico o con cualquier entidad externa.

Controles.

10.8.1 Cuando se intercambie información se deben aplicar los procedimientos establecidos para mantener el control de la seguridad de la información del laboratorio clínico.

- **a)** La información intercambiada debe ser previamente autorizada por la administración del laboratorio clínico.
- **b)** Las entidades externas deberán firmar un convenio de confidencialidad con el fin de salvaguardar la información de la empresa.
- **c)** Los funcionarios y contratistas deberán comprometerse a no dar uso diferente al que se pacta previamente en el convenio.
- **d)** Las entidades se comprometerán a proteger la confidencialidad de los documentos e información recibida.
- **e)** La información debe ser entregada nuevamente a la empresa o eliminada por las entidades externas una vez se dé por terminado el convenio.

10.8.2 Se deberán establecer acuerdos bilaterales para el intercambio de la información, teniendo en cuenta la seguridad de la información y las políticas de funcionamiento de cada una de las partes involucradas.

10.8.3 Los medios que contienen información deben protegerse contra accesos no autorizados, el uso inadecuado o la corrupción.

10.8.4 Los correos y mensajes electrónicos se deberán proteger por medio de usuarios y contraseñas seguras.

10.9 SERVICIO DE COMERCIO ELECTRONICO

Objetivo. Garantizar la seguridad de los servicios adquiridos a partir del comercio electrónico, dándole el uso debido por parte de la organización.

Controles.

10.9.1 La información que sea trasmitida por vía electrónica para realizar algún tipo de comercio debe estar protegida contra actividades fraudulentas y divulgación o modificación no autorizada.

10.9.2 La información utilizada para realizar transacciones en línea debe estar protegida para evitar transmisión incompleta, alteraciones, divulgaciones o duplicaciones no autorizadas del mensaje.

10.9.3 La información que está expuesta en la web para que el público tenga acceso a ella debe estar protegida para que no pueda ser modificada de ninguna manera.

10.10 SUPERVICIÓN

Objetivo. El laboratorio clínico deberá detectar actividades de procesamiento de información no autorizadas.

Controles.

10.10.1 El laboratorio clínico debe supervisar el uso del sistema y de los procesos de la información con regularidad, evaluando los resultados de las actividades que se realizan en la organización.

10.10.2 Sera restringido el acceso a los registros de las actividades que procesa la empresa para proteger la información de manipulaciones inadecuadas.

10.10.3 Las actividades realizadas por el personal del laboratorio clínico que involucren el buen estado del sistema de información deberán estar registrados para conocer el historial de uso y así evitar posibles riesgos.

10.10.4 Cualquier falla en el sistema debe estar debidamente registrada para ser analizada y tomar las decisiones y las acciones pertinentes a su mejora.

11 CONTROL DE ACCESO

11.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO

Objetivo. Controlar el acceso a la información perteneciente y procesada por el laboratorio clínico.

Control.

11.1.1 Los controles para tener acceso a la información procesada, deberán establecerse teniendo en cuenta los requisitos de funcionamiento del laboratorio clínico y la seguridad que este requiera.

11.2 GESTION DE ACCESO DE USUARIO

Objetivo. Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información del laboratorio clínico.

Controles.

11.2.1 El laboratorio clínico deberá implementar un procedimiento formal para el registro y cancelación del usuario, que otorgue y bloquee el acceso al sistema, a las bases de datos y a la información de la empresa.

11.2.2 El sistema de información utilizado por el laboratorio clínico requiere protección contra accesos no autorizados para ellos se debe prever la asignación de privilegios controlada mediante el proceso de autorización formal ante la administración de la empresa.

11.2.3 Para asignar las contraseñas y usuarios se deberá llevar a cabo un proceso de administración formal controlado por la dirección del Laboratorio clínico.

11.2.4 Con el fin de mantener el control del acceso a la información, la dirección del laboratorio clínico deberá realizar una revisión periódica de los derechos de acceso de los usuarios.

11.3 RESPONSABILIDAD DEL USUARIO

Objetivo. Evitar el acceso de usuarios no autorizados que ponga la información en riesgo de sufrir robo, o en algún peligro que pueda alterar el funcionamiento normal del laboratorio clínico.

Controles.

11.3.1 Los empleados del laboratorio clínico que accedan a la información de la empresa, deben hacer uso de contraseñas pues estas constituyen un medio de validación y de autenticación de la identidad de un usuario y en consecuencia es un medio que sirve para establecer el derecho de acceso al sistema de información.

11.3.2 La administración del laboratorio clínico debe cerciorarse que los equipos de la empresa que se encuentren en áreas no restringidas estén protegidos contra accesos no autorizados y en especial si estos equipos se encuentran desatendidos. Es importante crear conciencia en los empleados para que estos apliquen los procedimientos de seguridad adecuados y realicen sus funciones en relación a la implementación de la protección de la información

11.4 CONTROL DE ACCESO A LAS REDES

Objetivo. La administración del laboratorio clínico deberá evitar el acceso no autorizado a servicios en red.

Controles.

11.4.1 Los empleados del laboratorio clínico solo cuentan con la autorización de la empresa para tener acceso a los servicios en red que estén dentro de sus funciones.

11.4.2 La administración del laboratorio clínico deberá emplear los métodos más apropiados para el control de acceso y de usuarios a las redes a conexiones externas.

11.4.3 Se debe considerar la identificación automática de los equipos como un medio para autenticar las conexiones, utilizando como medio una computadora que registre las conexiones y que de aviso de accesos no autorizados, de esto se encargara la administración del laboratorio clínico.

11.4.4 Los puertos de configuración y de diagnóstico deben estar controlados ya que representan un medio de acceso no autorizado, por esta razón será indispensable aplicar mecanismos de protección para la información que procesa el laboratorio clínico.

11.4.5 Las redes que utiliza el laboratorio clínico deben estar separadas en grupos; red de servicio de información, red de usuarios y red de sistemas de información.

11.4.6 Si el laboratorio clínico mantiene redes compartidas, especialmente aquellas que son externas a la empresa, se deben restringir las capacidades de los usuarios para conectarse a la red, de acuerdo con el control de acceso que se requiera para el sistema de información que utiliza el laboratorio clínico.

11.4.7 Se deben controlar las redes utilizadas por el sistema de información del laboratorio clínico con el fin de asegurar las conexiones entre equipos y la información que se trasmite entre ellos para que solo exista acceso a las aplicaciones de la empresa.

11.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO

Objetivo. Evitar el acceso no autorizado al sistema operativo utilizado por el laboratorio clínico.

Controles.

11.5.1 Se deben utilizar procedimientos seguros para la autenticación al ingresar a los sistemas operativos y de informaciones utilizadas por el laboratorio clínico, tales como claves seguras en el procedimiento de inicio de sesión.

11.5.2 Todos los empleados del laboratorio clínico que tiene acceso al sistema operativo deberán disponer de un identificador único para su uso personal y exclusivo es decir un Usuario (ID) y se debe implementar una técnica de autenticación adecuada que compruebe la identidad del usuario del sistema.

11.5.3 El laboratorio clínico deberá utilizar un sistema de gestión de contraseñas que garanticen la seguridad y calidad:

- **a)** El uso de contraseñas debe ser individual, casa usuario tiene responsabilidad sobre la información.
- **b)** Se permite que los empleados selecciones y cambien las contraseñas personales.
- **c)** La administración podrá imponer cambios en las contraseñas en aquellos casos que lo amerite la empresa.
- **d)** Mantener un registro de las últimas contraseñas utilizadas por los usuarios y evitar la reutilización de las mismas.
- **e)** Evitar mostrar las contraseñas en la pantalla cuando se realiza el ingreso.
- **f)** Garantizar que el medio utilizado para ingresar al sistema de información no tenga acceso a información temporal o en tránsito de forma no protegida.
- **g)** Modificar las contraseñas predeterminadas por el proveedor, después de ser instalado el software y el hardware.

11.5.4 Se debe controlar el uso de programas de utilidad del sistema que puedan eludir los controles de las aplicaciones y afecten la seguridad del sistema de información del laboratorio clínico.

11.5.5 Las secciones se deben desconectar después del tiempo estimado por el laboratorio clínico de uso y de ingreso al sistema de información de la empresa.

11.5.6 Se estimara un tiempo de conexión determinado por la administración, para brindar seguridad a las aplicaciones de alto riesgo utilizadas por el laboratorio clínico.

11.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN

Objetivo. Evitar el acceso no autorizado a la información contenida en los sistemas de información del laboratorio clínico.

Controles.

11.6.1 El personal del laboratorio clínico que tiene acceso a las aplicaciones, podrán tendrá acceso a la información y a las funciones del sistema de aplicación.

11.6.2 Los sistemas que son sensibles deben estar ubicados en un ambiente aislado, pues la sensibilidad puede requerir el uso de un equipo restringido que no comparta recursos con los sistemas que pueden generar amenazas.

12 ADQUISICION DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

12.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Objetivo. Garantizar que la seguridad es parte integral de los sistemas de información del laboratorio clínico.

Controles.

12.1.1 Se deben analizar los requisitos para la seguridad del sistema de información del laboratorio clínico, sea de carácter propio o con terceros realizando mejoras y actualizaciones con los que la empresa pueda incorporar controles que apoyen a la gestión del sistema.

12.2 TRATAMIENTO CORRECTO DE LAS APLICACIONES

Objetivo. Evitar errores, pérdidas, modificaciones o uso inadecuado o no autorizado de la información del laboratorio clínico.

Controles.

12.2.1 Los datos para ingresar al sistema y tener acceso a las aplicaciones deben ser validados para asegurar que estos son correctos y apropiados.

12.2.2 Se deberá verificar la validación en las aplicaciones para reconocer cualquier acto de corrupción que afecte directamente el sistema de información del laboratorio clínico ya sean errores deliberados o de procesamiento.

12.2.3 La administración del laboratorio clínico deberá asegurar la autenticidad y proteger la integridad de los mensajes que salen y de las aplicaciones que utilizan en el procesamiento y uso del sistema de la información.

12.2.4 Se deben establecer procedimientos que validen la salida de los datos y mensajes de la empresa tales como:

a) Comprobar que la razón de la salida de los datos es necesaria.
b) Controlar las cuentas para asegurar el procesamiento de los datos.
c) Tener la información suficiente para determinar la clasificación de la información.
d) Determinar el procedimiento adecuado para realizar las pruebas necesarias y validar la salida de la información.
e) Definir las responsabilidades del personal que hacen parte del proceso de salida de datos.

12.3 CONTROLES CRIPTOGRAFICOS

Objetivo. Proteger la confidencialidad, autenticidad e integridad de la información del laboratorio clínico utilizando medios criptográficos.

Controles.

12.3.1 Sera necesaria la utilización de los medios criptográficos en los casos tales como:

a) Proteger las claves de acceso al sistema, a los datos o a los servicios del laboratorio clínico.
b) Trasmitir información clasificada fuera del laboratorio clínico.
c) Proteger la información de los riesgos identificados en el análisis y la evaluación que se realice del sistema de gestión de la información de la empresa.

12.3.2 Si la administración del laboratorio lo decide se implementara un sistema para la protección de claves para los medios criptógrafos. Las claves deberán protegerse contra cambios, copias o destrucción no autorizada utilizando un método efectivo que almacene, archive y proteja las claves.

12.4 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

Objetivo. Organizar la seguridad de los archivos del sistema de información controlando el acceso a los registros del laboratorio clínico.

Controles.

12.4.1 La administración del laboratorio clínico deberá controlar las instalaciones del software en el sistema operativo utilizado en los equipos que procesan la información del laboratorio clínico.

12.4.2 Las pruebas al sistema se efectuaran una vez se instale con éxito el software que decida la empresa utilizar para el manejo de la información de la empresa.

12.4.3 La administración del laboratorio clínico deberá tener el control sobre el cuidado y manejo de los programas fuente, utilizados en las funciones de la empresa.

12.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Objetivo. La administración del laboratorio clínico deberá mantener la seguridad del software y de la información del sistema de aplicaciones.

Controles.

12.5.1 Se deben cumplir los procedimientos formales para controlar los cambios que se realicen en el sistema.

12.5.2 La administración deberá revisar y probar las aplicaciones y los programas cuando sea necesario realizar cambios en el sistema operativo con el fin de evitar errores que afecten el funcionamiento normal del laboratorio clínico.

12.5.3 Cuando se realice un cambio del software o programa utilizado por el sistema de información del laboratorio clínico, se debe realizar un control estricto de este cambio.

12.5.4 Se deben evitar y prevenir los posibles riesgos de una fuga de información perteneciente al laboratorio clínico.

13. GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INORMACIÓN

13.1 NOTIFICACION DE EVENTOS Y PUNTOS DEBILES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo. Certificar que los eventos y las debilidades de la seguridad de la información asociados con el sistema de información del laboratorio clínico se comunican de forma tal que permiten a la empresa tomar las acciones correctivas oportunamente.

Controles.

13.1.1 Si se llegase a presentar alguna situación que ponga en riesgo la seguridad de la información se debe informar mediante un reporte o informe formal a la administración del laboratorio clínico, para que estos a su vez realicen los procedimientos pertinentes y tomen las decisiones apropiadas en el tiempo requerido antes de presentarse un incidente mayor.

13.1.2 Los empleados, proveedores y usuarios del laboratorio clínico tendrán la responsabilidad de reportar a la administración de la empresa cualquier anomalía o sospecha detectada en el sistema de información.

13.2 GESTION DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo. Revisar que se apliquen los controles para la gestión de incidentes de la seguridad de la información.

Controles.

13.2.1 La responsabilidad de llevar a cabo los procedimientos adecuados de la gestión en caso de presentarse algún incidente es de la dirección del laboratorio clínico para que se tomen las decisiones prudenciales de manera rápida, eficaz y ordenada.

13.2.2 Cuando se presente algún incidente que tenga implicaciones legales ya sean civiles o penales para la empresa o para terceros, la evidencia deberá ser recolectada, retenida y presentada ante los organismos pertinentes para cumplir con las leyes y normas establecidas.

14. GESTION DE LA CONTINUIDAD DEL NEGOCIO

14.1 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO

Objetivo. Proteger los procesos de la empresa que puedan afrontar efectos negativos como fallas en el sistema de información o desastres naturales y asegurar la pronta recuperación del laboratorio clínico a estos daños.

Controles.

14.1.1 La administración del laboratorio clínico será la responsable de la coordinación para el desarrollo de los procesos de seguridad que garanticen la continuidad del negocio.

14.1.2 Se hace necesario que el laboratorio clínico cuente con un plan de continuidad de los procesos y actividades que realiza el laboratorio clínico en donde se identifiquen las amenazas que puedan causar interrupciones en los procesos de la empresa, evaluar los riesgos para determinar el impacto e identificar los controles para prevenir la situación.

14.1.3 La administración del laboratorio clínico deberá elaborar, desarrollar e implementar planes de contingencia con el propósito de garantizar la disponibilidad de la información para la continuidad de las actividades de la empresa.

14.1.4 Mantener un esquema único de plan de contingencia para garantizar la continuidad del negocio y que sea consistente en el tratamiento de los riesgos cumpliendo con los requisitos del sistema de seguridad de la información y que aporte a identificar las prioridades de prueba y de mantenimiento. El plan de contingencia deberá especificar:

a) Las condiciones para ser implementado.
b) Las personas requeridas para ejecutar los componentes del plan.
c) La identificación de los requerimientos y la modificación de los procedimientos de emergencia.

14.1.5 La administración del laboratorio clínico deberá establecer un cronograma de pruebas periódicas según lo estimen necesario, realizando el mantenimiento y reevaluación de los planes de contingencia para garantizar su actualización y eficacia.

15. CUMPLIMIENTO

15.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES

Objetivo. Cumplir las leyes, normas y reglas que orienten a la seguridad de la información del laboratorio clínico.

Controles.

15.1.1 Se deberán cumplir con todos los requisitos normativos y contractuales pertinentes a la protección del sistema de información del laboratorio clínico, igualmente se tendrán en cuenta los controles aplicados y las responsabilidades de los administrativos, empleados y terceras partes para cumplir con dichos requisitos.

15.1.2 Se implementaran los procedimientos necesarios para la protección de la propiedad intelectual según las normas existentes y teniendo en cuenta las siguientes pautas:

a) Definir las normas para cumplir con los derechos de propiedad intelectual, que definan el uso legal de la información.
b) Divulgar las políticas de adquisición de programas teniendo en cuenta las disposiciones legales de propiedad intelectual.
c) Tomar las decisiones y acciones disciplinarias pertinentes en caso de infringir las normas propuestas.

d) Mantener el registro adecuado de los activos del laboratorio clínico.
e) Conservar las evidencias como licencias y manuales.
f) Implementar los controles requeridos para evitar el exceso de usuarios permitidos.
g) Verificar que los productos instalados en los equipos cumplan con las licencias y estén autorizados legalmente.
h) Realizar los procedimientos de mantenimiento adecuados con respecto a las licencias de uso.
i) Realizar los procedimientos pertinentes a la eliminación o transferencia a terceros de los programas de información.
j) Realizar auditorías.
k) Cumplir con los términos y condiciones establecidos para obtener los programas y la información en redes públicas.

15.1.3 Los documentos, datos y registros importantes se deben proteger de pérdida, destrucción y falsificación para que la gestión del laboratorio clínico y el sistema de información de la empresa funcionen normalmente.

15.1.4 Se deberá garantizar la protección de la información y de los datos privados del personal que tiene acceso al sistema de información del laboratorio clínico.

15.1.5 Toda utilización de los recursos de procesamientos de información con propósitos no autorizados debe ser considerado como uso indebido, Los empleados del laboratorio clínico deberán conocer el alcance del uso adecuado de los recursos de la información y deben respetarlos.

15.1.6 Si se utilizan firmas digitales o electrónicas debe considerarse el marco legal donde se establezcan las condiciones en las que las firmas digitales son legalmente válidas.

15.2 CUMPLIMIENTO DE LAS POLITICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TECNICO

Objetivo. Asegurar que el sistema de información cumpla con las normas y políticas de seguridad del laboratorio clínico

Controles.

15.2.1 La dirección del laboratorio clínico debe velar por el cumplimiento de las normas y procedimientos de seguridad establecidos dentro de las responsabilidades de la empresa para garantizar el cumplimiento de las normas y políticas de la información, algunas de las áreas a supervisar son: Sistemas de información, proveedores de sistemas, usuarios y propietarios de la información.

15.2.2 Se debe verificar constantemente que los sistemas de información utilizados por la empresa cumplan con las políticas establecidas para realizar los procedimientos de seguridad; revisando los sistemas, implementando los controles y garantizando que los procesos se hayas implementado correctamente.

15.3 CONSIDERACIONES SOBRA LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACION

Objetivo. Aumentar la eficacia en los procesos de auditoría realizados en el sistema de información utilizado en el laboratorio clínico.

Controles.

15.3.1 Cuando sea necesario realizar auditorías para verificar los sistemas de información del laboratorio clínico se tomaran en cuenta los resultados para minimizar los riesgos y evitar las interrupciones en las operaciones normales de la empresa.

15.3.2 Se protegerá el acceso a las herramientas de auditoría al sistema de información para evitar el uso inadecuado de los datos o ponerlas en peligro de perdida, daño o robo.

ANEXO D. Controles de la seguridad de la información.

CONTROLES DE LA SEGURIDAD DE LA INFORMACION
POLÍTICA DE SEGURIDAD. **5.1 Política de seguridad de la información.** 5.1.1 Documento de política de seguridad de la información. 5.1.2 Revisión de la política de seguridad de la información. **6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.** **6.1 Organización interna.** 6.1.1 Compromiso de la Dirección con la seguridad de la información. 6.1.2 Coordinación de la seguridad de la información. 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información. 6.1.4 Proceso de autorización de recursos para el tratamiento de la información. 6.1.5 Acuerdos de confidencialidad. 6.1.6 Contacto con las autoridades. 6.1.7 Contacto con grupos de especial interés. 6.1.8 Revisión independiente de la seguridad de la información. **6.2 Terceros.** 6.2.1 Identificación de los riesgos derivados del acceso de terceros. 6.2.2 Tratamiento de la seguridad en la relación con los clientes. 6.2.3 Tratamiento de la seguridad en contratos con terceros. **7. GESTIÓN DE ACTIVOS.** **7.1 Responsabilidad sobre los activos.** 7.1.1 Inventario de activos. 7.1.2 Propiedad de los activos. 7.1.3 Uso aceptable de los activos. **7.2 Clasificación de la información.** 7.2.1 Directrices de clasificación. 7.2.2 Etiquetado y manipulado de la información. **8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** **8.1 Antes del empleo.** 8.1.1 Funciones y responsabilidades. 8.1.2 Investigación de antecedentes. 8.1.3 Términos y condiciones de contratación. **8.2 Durante el empleo.** 8.2.1 Responsabilidades de la Dirección. 8.2.2 Concienciación, formación y capacitación en seguridad de la información. 8.2.3 Proceso disciplinario. **8.3 Cese del empleo o cambio de puesto de trabajo.**

8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
9.1 Áreas seguras.
9.1.1 Perímetro de seguridad física.
9.1.2 Controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos e instalaciones.
9.1.4 Protección contra las amenazas externas y de origen ambiental.
9.1.5 Trabajo en áreas seguras.
9.1.6 Áreas de acceso público y de carga y descarga.
9.2 Seguridad de los equipos.
9.2.1 Emplazamiento y protección de equipos.
9.2.2 Instalaciones de suministro.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de los equipos.
9.2.5 Seguridad de los equipos fuera de las instalaciones.
9.2.6 Reutilización o retirada segura de equipos.
9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
10.1 Responsabilidades y procedimientos de operación.
10.1.1 Documentación de los procedimientos de operación.
10.1.2 Gestión de cambios.
10.1.3 Segregación de tareas.
10.1.4 Separación de los recursos de desarrollo, prueba y operación.
10.2 Gestión de la provisión de servicios por terceros.
10.2.1. Provisión de servicios.
10.2.2 Supervisión y revisión de los servicios prestados por terceros.
10.2.3 Gestión del cambio en los servicios prestados por terceros.
10.3 Planificación y aceptación del sistema.
10.3.1 Gestión de capacidades.
10.3.2 Aceptación del sistema.
10.4 Protección contra el código malicioso y descargable.
10.4.1 Controles contra el código malicioso.
10.4.2 Controles contra el código descargado en el cliente.
10.5 Copias de seguridad.
10.5.1 Copias de seguridad de la información.
10.6 Gestión de la seguridad de las redes.
10.6.1 Controles de red.
10.6.2 Seguridad de los servicios de red.
10.7 Manipulación de los soportes.
10.7.1 Gestión de soportes extraíbles.

10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.
10.8 Intercambio de información.
10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.
10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.

11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.
12.1.1 Análisis y especificación de los requisitos de seguridad.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.
12.4 Seguridad de los archivos de sistema.
12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.
13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sistemas de información.

Fuente. NTC/IEC ISO 27002