ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

MAESTRÍA EN GERENCIA DE SISTEMAS

DECIMO SEXTA PROMOCIÓN

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN GERENCIA DE SISTEMAS

TEMA "Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador**"**

AUTOR: TERÁN VALENZUELA, KARINA MARIBEL

DIRECTOR : RON EGAS, MARIO BERNABE

SANGOLQUI

2018

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACION, INNOVACION Y TRANSFERENCIA TECNOLOGICA

MAESTRÍA EN GERENCIA DE SISTEMAS

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador"***, realizado por la señora ***KARINA MARIBEL TERAN VALENZUELA***, ha sido revisado en su totalidad y analizado por el software anti – plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señora ***KARINA MARIBEL TERAN VALENZUELA*** para que lo sustente públicamente.

Sangolquí, 22 de diciembre de 2017

Ing. Mario Ron, MSc.
DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACION, INNOVACION Y TRANSFERENCIA TECNOLOGICA

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Yo, ***KARINA MARIBEL TERAN VALENZUELA***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador"***, cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 22 de diciembre de 2017

Ing. Karina Maribel Terán Valenzuela
C.C. 1712627114

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACION, INNOVACION Y TRANSFERENCIA TECNOLOGICA

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORÍA DE RESPONSABILIDAD

Yo, ***KARINA MARIBEL TERAN VALENZUELA***, con cédula de identidad N° 1712627114, declaro que este trabajo de titulación ***"Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador"***, ha sido desarrollado considerando los métodos de investigación existentes, así como también se han respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas. Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 22 de diciembre de 2017

Ing. Karina Maribel Terán Valenzuela
C.C. 1712627114

DEDICATORIA

El contenido de este trabajo y el esfuerzo realizado para concretar su efectiva culminación; va dedicado a mi amada familia, formada por mi esposo (Xavier) y mis dos hermosos hijos (Gabriel y Matías) por ser el centro de mi vida, a mis padres por su apoyo, a los familiares, amigos cercanos que de forma directa o indirecta me apoyaron.

Karina

AGRADECIMIENTO

Un enorme GRACIAS a Dios por permitirme alcanzar este objetivo. A todos los profesionales y docentes que conocí durante este proceso de aprendizaje. A mi esposo e hijos por ser el apoyo indiscutible y a mis compañeros de estudios y trabajo

Muy particular a mi tutor, Ing. Mario; por la confianza depositada en este proyecto, la cual fue vital y determinante.

Karina

INDICE DE CONTENIDOS

Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El presente trabajo desarrolla una Guía para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI), alineado a la norma técnica ecuatoriana NTE ISO/IEC 27000 con la finalidad de mejorar el nivel de seguridad de la información del Ministerio de Salud Pública del Ecuador (MSP). Según lo estipulado en el Art. 32 de la Constitución de la República del Ecuador, el MSP tiene como función garantizar el acceso permanente y oportuno derecho a la atención integral de salud. Para alcanzar estos objetivos existe el área denominada: Primer Nivel de Atención, la cual ofrece el servicio de agendamiento de citas, que proporciona a la población acceso a los servicios de salud a través de la línea gratuita 171 y una solución informática, para disminuir la problemática de obtención de citas y reducir la congestión del sistema. La información que maneja está clasificada como confidencial tanto por su tipo como por ser de propiedad de los usuarios y está conformada por los datos básicos de la persona como número de cedula, números de contacto, especialidad de su cita, enfermedad, antecedentes. A fin de poder realizar una propuesta para complementar la Norma ISO /IEC 27000 para configurar un proceso ágil, cercano a la realidad nacional. La guía permitirá implementar políticas, procedimientos y controles que garanticen la confidencialidad, integridad y disponibilidad de la información, del servicio de agendamiento de citas del Contact Center del MSP.

Palabras clave

- **NTE ISO 27000**
- **SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION**

ABSTRACT

The present work develops a Guide for the implementation of the Information Security Management System (ISMS), aligned with the Ecuadorian technical standard NTE ISO / IEC 27000 with the aim of improving the level of information security of the Ministry of Public Health of Ecuador (MSP).

As stipulated in Article 32 of the Constitution of the Republic of Ecuador, the MSP's function is to guarantee permanent and timely access to comprehensive health care. To reach these objectives there is the area called: First Level of Attention, which offers the appointment scheduling service, which provides the population with access to health services through the toll-free line 171 and a computer solution, to reduce problems obtaining appointments and reducing system congestion. The information handled is classified as confidential both by its type and by being owned by users and is made up of the basic data of the person such as id number, contacts, specialty of your appointment, illness, background. In order to make a proposal to complement the ISO / IEC 27000 standard to configure an agile process, close to the national reality. The guide will allow the implementation of policies, procedures and controls that guarantee the confidentiality, integrity and availability of the information, of the appointment scheduling service of the MSP Contact Center.

Palabras clave

- **NTE ISO 27000**
- **INFORMATION SECURITY MANAGEMENT SYSTEM**

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Introducción

Los avances en las Tecnologías de la Información y Comunicación (TIC), así como la necesidad de conservar la memoria institucional y cumplir con el mandato de acceso a la información pública, han logrado que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias instituciones y minimizar riesgos derivados de vulnerabilidades de la seguridad de la información.

La Secretaría Nacional de Administración Pública, emitió el Acuerdo Ministerial No 166 mediante el cual dispone el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000, para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), con el objetivo de que las entidades gubernamentales gestionen en forma eficiente y eficaz la seguridad de la información.

La norma internacional ISO/IEC 27000 ha sido elaborada para proporcionar las mejores prácticas de la seguridad de la información. Esta norma define el establecimiento, implementación, operación, seguimiento y revisión, mantenimiento y mejora de un sistema de un Sistema de Gestión de Seguridad de la información (SGSI), adoptando el modelo de procesos “Planificar-Hacer-Verificar-Actuar” aplicable a todo tipo de organización (Norma ISO/IEC 27001, 2013).

1.2. Formulación del problema

El Ministerio de Salud Pública del Ecuador (MSP) es una Institución de carácter público, que tiene como objetivo principal garantizar el derecho y acceso a la salud. Para este efecto ha implementado el servicio agendamiento de citas por medio del Contact Center, como puerta de acceso a los servicios de salud para la ciudadanía. La información que se maneja en este servicio, se encuentra clasificada como confidencial, tanto por su tipo, como por su propiedad y está conformada por los datos básicos de la persona, como número de cedula, números de contacto, especialidad de su cita, enfermedad, antecedentes y otros.

EL sistema de agendamiento de citas agilita el proceso de atención médica y evita largas filas para acceder al servicio de salud de usuarios a nivel nacional. Debe estar disponible las 24 horas los 365 días del año y brindar atención acorde a la asignación de la cita médica. Cabe recalcar que los casos de emergencia se atienden acorde a la prioridad determinada por el triaje médico. Caso contrario puede ser interpretado como negación del servicio a la atención médica al ciudadano e irse en contra de la misión y objetivos del MSP y del Plan Nacional del Buen Vivir.

En el MSP el servicio de agendamiento así como otras instituciones similares, se encuentra sometido a riesgos inherentes al procesamiento de la información como: robo de datos, denegación de servicios, acceso no autorizado, etc., que pueden ocasionar graves problemas como: dañar la imagen de la Institución, afectar su credibilidad por parte de los ciudadanos, pérdida de datos de las citas médicas, entre otros.

El servicio de agendamiento de citas no cuenta con un Sistema de Gestión de Seguridad de la Información y por tanto los controles que se

hayan implantado si el caso así fuere, se encuentran fuera de contexto y no brindan la confiabilidad necesaria en la protección de la información que es vital para respetar el derecho a la privacidad de los ciudadanos.

1.3. Justificación e importancia

La importancia de la Guía radica en la necesidad de contar con una herramienta para implantar en forma efectiva y eficiente el SGSI, que a su vez permitirá proteger la información personal y clínica que se maneja en el sistema de agendamiento de citas y que se obtiene al asignar una cita médica del ciudadano que utiliza la red de salud pública, como: datos básicos de la persona, especialidad de atención, enfermedad, síntomas, etc.

La información es clasificada como sensible porque pertenece a los usuarios del sistema de agendamiento y el MSP se convierte en custodio de ella, debe protegerla de los riesgos asociados y evitar el acceso no autorizado que puede generar desconfianza en la ciudadanía y comprometer la imagen dela Institución así como la violación al artículo 178 del Código Integral Penal COIP que establece que si no se cuenta con el consentimiento o la autorización legal y se “acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio”. Por lo que el acceso no autorizado viola el derecho a la intimidad de los pacientes, la información puede ser divulgada sin autorización o utilizarse con fines no éticos.

Es necesario contar con una guía para la implementación del SGSI que permita identificar los riesgos, determinar los controles a implementar para minimizarlos y evitar daños en los activos de la información. Además la guía debe contener la documentación de políticas y procedimientos para el manejo de la información y diseño de la campaña de concientización del

personal del MSP, siguiendo las mejores prácticas de la norma NTE ISO/IEC 27000. En este contexto se hace imprescindible desarrollar la guía en la que se describirá como establecer, implementar, operar, controlar, revisar, mantener y mejorar la seguridad de la información del servicio de agendamiento de citas del MSP garantizando su confidencialidad, integridad y disponibilidad.

1.4. Objetivos

1.4.1. Objetivo general

Elaborar una Guía para la implantación del Sistema de Gestión de la Seguridad de la Información SGSI del Servicio de Agendamiento de Citas Médicas del Ministerio de Salud Publica alineado a la norma NTE ISO/IEC 27000, con el fin de garantizar integridad, confidencialidad y disponibilidad de su información.

1.4.2 Objetivos específicos

- Evaluar la situación actual en el manejo de la confidencialidad, integridad y disponibilidad de la información en el Servicio de Agendamiento de Citas Médicas mediante la NTE ISO/IEC 27001.
- Elaborar la Guía para implementar el Sistema de Gestión de Seguridad de la Información en base de la NTE Norma ISO/IEC 27003 para el Servicio de Agendamiento de Citas Médicas del MSP.

CAPÍTULO II

MARCO TEORICO

2.1 Fundamentación teórica

2.1.1 Seguridad de Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger los activos de la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos por medio de análisis y valoración de riesgos. (Norma ISO/IEC 27001, 2013)

Hace varios años la información se registraba en papel y se almacenaba en sistemas de archivos que ocupaban grandes espacios físicos. Actualmente los sistemas de información computarizados, al digitalizar la información, reducen espacio físico y costos para las organizaciones, permiten procesamiento avanzado de los datos y se han convertido en uno de los activos más importantes de las organizaciones ya que en ellos se almacena datos de todo tipo (financiero, recursos humanos, comerciales, etc.).

El uso masivo de nuevas tecnologías y plataformas basadas, en el acceso a Internet hace que cada vez más empresas permitan a sus grupos de interés (clientes, proveedores, socios) acceso a sus sistemas de información.

El avance de la tecnología permite a los colaboradores y clientes de la organización, acceder a través de Internet a información de la institución desde cualquier lugar, incluso fuera de la empresa.

Bajo estas condiciones, ahora es más fácil acceder a la información, por lo que la información se encuentra expuesta a riesgos y amenazas como alteración, robo o mal uso que generan daño económico y afectan al prestigio para las instituciones. Para evitar estos riegos las organizaciones deben implementar procesos, procedimientos o técnicas que permita asegurar la integridad, confidencialidad y disponibilidad de la información.

La importancia de la seguridad de la información radica en que las organizaciones manejan información delicada de la misma organización y de sus clientes, estos últimos entregan información personal o reservada, imaginemos que pasaría si la información confidencial de millones de Ecuatorianos se divulgara libremente por una falla en la seguridad de la información, habría números de cedula, cuentas de correo, cuentas bancarias, contraseñas, historia laboral, historia clínica divulgadas libremente por internet.

Es evidente que el manejo de la seguridad de información es un problema grave y debe ser abordado eficientemente dependiendo de la actividad de cada institución o empresa. Las organizaciones deben ser responsables de la correcta administración de información interna y externa, protegiendo la información sensible de la organización y de sus clientes de riesgos y amenazas dentro y fuera de la institución.

Muchas organizaciones dejan en segundo plano la administración efectiva de la seguridad de información hasta que ocurre un evento que pone en riesgo la estabilidad de la propia organización y puede exponer a terceros la información de sus clientes, con graves consecuencias económicas, legales y de prestigio.

La decisión de desarrollar un SGSI se convierte en una iniciativa estratégica para el manejo de la seguridad de la información, permite determinar el riesgo para establecer las medidas para minimizarlo o

eliminarlo, logrando así mejorar el nivel de seguridad de la información existente.

El establecimiento y la implementación del sistema de gestión de seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos utilizados de la organización el tamaño y estructura de la organización. (INEN Servicio Ecuatoriano de Normalización, (2013)).

2.1.2. Sistema de Gestión de Seguridad de la Información

El SGSI son las siglas utilizadas para referirse al Sistema de Gestión de Seguridad de Información. El correcto manejo de la seguridad de información debe hacerse a través de un proceso debidamente documentado y sistemático, denominado SGSI, cuyo enfoque es metódico para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para conseguir los objetivos del negocio.

Se fundamenta en una evaluación del riesgo y de los niveles de aceptación del riesgo de la organización y está diseñado para tratarlos y gestionarlos riesgos de manera eficaz, analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizar su protección.

La metodología PDCA (Plan, Do, Check, Act) es una secuencia de acciones que permite implementar la mejora continua de un servicio, producto o proceso, para el caso de este trabajo, de un proceso como SGSI, como se describe en la Figura 1.

Este método fue ampliamente utilizado por el Dr. Edwards Deming, también llamado el padre del control de calidad total. El PDCA está basado en el principio científico de generar muchas interacciones que permitan confirmar o negar una posible afirmación o hipótesis. La constante repetición de la metodología acercará cada vez más al resultado correcto, permite además incrementar el conocimiento del proceso, servicio o producto, al implementar un mecanismo de mejora continua.

Figura 1 Etapas del ciclo Deming

Fuente: **(ALTRATRENCH360, 2016)**

Planificación (Plan): En esta etapa se define el problema o los elementos a ser mejorados, se establecen los objetivos a ser alanzados y las herramientas que se utilizarán para alcanzar dichos objetivos. También se definen los recursos que intervienen en el proceso de mejora, sean estos humanos, económicos, materiales u otros.

Ejecución (Do): En esta etapa se ejecutan las tareas planificadas de una forma controlada que permita verificar el estado de cada tarea. Es la etapa en la que se implementa la mejora que se ha planeado.

Evaluación (Check): Se analiza, comprueba y evalúa el resultado de la ejecución de la mejora tomando como referencia los objetivos y la planificación propuesta en las etapas anteriores. Es importante que previamente se haya definido el mecanismo de evaluación y los indicadores que se utilizará para comprobar si los objetivos fueron alcanzados.

Actuación (Act): Luego de analizar los resultados obtenidos, la etapa de actuación permite tomar medidas correctivas o preventivas que lleven a mejorar los resultados, en el caso de que los mismos no sean lo suficientemente satisfactorios. Los resultados obtenidos se convierten en el punto de partida de un nuevo proceso de mejora, dando inicio a un nuevo proceso.

La Norma ISO/IEC 27000 permite implementar eficientemente un SGSI, facilitando a las organizaciones tomar decisiones en cuanto a la seguridad de sus Sistemas de Información, es ineludible pensar que el método de Deming ayuda a la organización a implementar de mejor forma los controles necesarios que permiten cumplir con la normativa NTE ISO/IEC 27000, buscando continuamente mejorar sus controles, identificar riegos / amenazas y la forma de mitigarlos.

2.1.3. Norma ISO /IEC 27001:2013

Es un conjunto de normas emitidas por la Organización Internacional de Normalización (ISO), para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de información de todo tipo de

organización (empresas comerciales, agencias de gobierno, organizaciones sin fines de lucro, etc.). La primera versión de esta norma es publicada en el año 2005 tomando como referencia la norma BS7799-2. La norma 2013 es una mejora de la norma respecto a la versión 2005.

La ISO 27001 no establece controles a ser considerados dentro de seguridad de información, en su lugar muestra un conjunto de requisitos que deben ser implementados. Según la ISO/IEC 27001, la seguridad de información debe garantizar la confidencialidad, integridad y disponibilidad de la información, estos términos constituyen los cimientos de la seguridad de información. Al ser un estándar internacional, brinda directrices para implementar un SGSI, por lo que se la puede aplicar e implementar en todo tipo de organización. La norma ISO/IEC 27001 se encuentra elaborada para asegurar la selección de controles de seguridad adecuados que protejan los activos de información de las organizaciones, permite evaluar riesgos y aplicar controles necesarios para mitigarlos o eliminarlos, en base de los siguientes criterios:

- Confidencialidad: La información no puede exponerse, ni entregarse a personas o entidades no autorizadas
- Integridad: La información debe mantenerse completa y exacta todo el tiempo.
- Disponibilidad: Se debe garantizar el acceso a la información y los sistemas cuando sea requerido de acuerdo a la actividad de la organización.

La Norma fue diseñada en 7 capítulos principales que van del 4 al 10, que se describen brevemente a continuación:

- Capítulo 4 Determina el contexto interno y externo de la organización, las necesidades de los interesados, el alcance del SGSI
- Capítulo 5 Considera el liderazgo y compromiso de la alta gerencia, la política, roles y responsabilidades
- Capítulo 6 Considera la planificación, acciones en torno al riesgo, la necesidad de definir los objetivos de la seguridad de información

- Capítulo 7 El soporte donde se determina recursos, la competencia, comunicación y concienciación, la creación y control de información documentada
- Capítulo 8 Operación que requiere de la planificación y control operacional, apreciación de los riesgos y su tratamiento.
- Capítulo 9 El desempeño donde se requiere del monitoreo, medición, análisis y evaluación, la ejecución de la auditoria interna, compromiso y participación de la dirección
- Capítulo 10 Aquí se considera la aplicación de una mejora continua, las no conformidades y acciones correctivas

La Norma ISO 27001 se adecúa a diferentes usos y permite:

- La formulación de requerimientos y objetivos de seguridad.
- Asegurar que los riesgos de seguridad sean administrados de manera confiable.
- Asegurar el cumplimiento de las leyes y reglamentos.
- Mantener un marco de referencia para la implementación y administración de controles que permitan asegurar el cumplimiento de objetivos específicos de seguridad de la información.
- La definición de nuevos procesos de gestión de la seguridad de la información.
- La Identificación de los procesos existentes de gestión de la seguridad de la información.
- Determinar el estado de las actividades de gestión de la seguridad de la información.
- Una correcta determinación del grado de cumplimiento de las políticas, directivas y normas adoptadas en la organización, por parte de los auditores internos y externos.
- Definir el mecanismo para proporcionar información sobre políticas, directivas, normas y procedimientos de seguridad de la información a socios y grupos de interés con quienes se relacionan las organizaciones.

La última versión de la ISO/IEC 27001:2013, publicada en ese año, implementa mejoras respecto a su antecesora, las más importantes son:

- Se han validado y revisado muchos de los controles y requisitos.
- Muestra mayor tolerancia respecto al enfoque a procesos.
- Refuerza el análisis de riesgos.
- Se eliminan algunos documentos obligatorios en la norma 2005.
- El alcance del SGSI se define cuando se entienda las necesidades de los interesados, la organización y su entorno.
- Se compromete a la alta dirección de la organización con la gestión e importancia del SGSI.

Los objetivos de seguridad se convierten en requisito obligatorio.

La norma ISO/IEC 27001:2013 hace posible que las organizaciones obtengan la certificación ISO 27001 a través de una institución de certificación independiente, que corrobora que la organización ha logrado implementar y cumplir las normas de seguridad de información descritas en ella.

2.1.4. Norma ISO / IEC 27002:2013

Es una guía con las mejores prácticas para la gestión de la seguridad de información, para ello define objetivos y recomendaciones para la gestión de la seguridad de información, adicionalmente expone las preocupaciones de las organizaciones en materia de seguridad de información, nace en el año 2007 como parte de las normas ISO 27000, en 2013 se publica la segunda edición. La norma ayuda a las organizaciones que buscan:

- Seleccionar controles durante el proceso de implementación de un SGSI basado en la norma ISO 27001.
- Aplicar controles.

- Desarrollar directrices propias para la gestión de la seguridad de información.

En su estructura contiene 14 capítulos de controles de 35 categorías y 114 controles, los puntos más importantes en los que se enfocan son:

- Capítulo 5.- Política de seguridad: Políticas claramente definidas que regulen las actividades entorno a la seguridad de información.
- Capítulo 6.- Organización de la seguridad de la información dentro de la organización y con terceros requisito de definir roles y responsabilidades acorde a sus funciones, comunicación con autoridades, gestión de proyectos de S.I., dispositivos móviles y teletrabajo.
- Capítulo 7.- considera la seguridad de los Recursos humanos: Detalla la necesidad de los procesos antes, durante y después de la contratación, la formación, concienciación y responsabilidad en cuanto al manejo y acceso de la información en S.I.
- Capítulo 8.- Gestión de activos: Claramente identificado, propietarios, inventario y manejo de los activos su uso, aceptación, clasificación de la documentación, gestión de medios extraíbles
- Capítulo 9.- Control de acceso: Un control adecuado del acceso a la información, sistemas, aplicaciones mediante políticas garantizando que solo personas autorizadas y debidamente autenticadas accedan a la información pública como secreta
- Capítulo 10.- Gestión para la aplicación y control criptográfico
- Capítulo 11.- considera toda la gestión para seguridad física y del entorno
- Capítulo 12.- Asegurar la seguridad de las operaciones, mediante procedimientos, gestión de cambios en sus ambientes, protección contra todo tipo de amenazas, gestión de vulnerabilidades, controles de la auditoria de sistemas de información
- Capítulo 13.- Seguridad en las comunicaciones, política y procedimientos de transferencia de información, acuerdos de confidencialidad

- Capítulo 14.- Adquisición, desarrollo y mantenimiento de los sistemas de información para asegurar los servicios
- Capítulo 15.- Asegurar mantener la seguridad de la información en relación con proveedores, gestión de la provisión de servicios
- Capítulo 16.- Gestión de incidentes: Registro adecuado de los incidentes de seguridad de información, garantizando un seguimiento correcto a fin de evitar recurrencias.
- Capítulo 17.- Continuidad del negocio: Contar con planes de contingencia documentados, actualizados que hagan frente a incidentes que pongan riesgo la continuidad del negocio y la operación de la organización.
- Capítulo 18.- Requisitos Legales: Asegurar el cumplimiento en propiedad intelectual y leyes en general. (INEN Norma Tècnica Ecuatoriana ISO/IEC 27001:2013, 2017)

2.1.5. ISO/IEC 27003:2017

Esta norma provee a las organizaciones de una guía para el desarrollo del plan de implementación del SGSI, contiene una descripción del proceso de delimitación del SGSI, además del diseño y ejecución de los planes para una correcta certificación del SGSI.

El estándar fue publicado en el año 2010, enfocado en cómo planificar los proyectos de implementación del SGSI. En abril del año 2017 se publica la nueva versión de la norma, con cambios importantes adaptados a la estructura de la norma ISO/IEC 27001: 2013 para facilitar su uso conjunto, cancela y reemplaza la edición del 2010. La edición anterior tenía un enfoque de proyecto con una secuencia de actividades, esta edición

proporciona orientación sobre los requisitos independientemente del orden en que se implementan.

La norma ISO/IEC 27003: 2017 es una guía para implementar los requisitos de un SGSI, como se especifica en ISO / IEC 27001 y proporciona recomendaciones ('debería'), posibilidades ('puede') y permisos ('puede') en relación con ellos. No es la intención de esta norma orientar en forma general sobre todos los aspectos de la seguridad de la información.

Esta norma explica la implementación del SGSI mediante cinco fases representada en clausulas y son:

- Cláusula 5.- Iniciación, obtención de aprobación de la Dirección a partir de su alcance y con una prioridad establecida
- Cláusula 6.- Definir el alcance del SGSI, desarrollar la política y las delimitaciones de las tecnológicas, comunicaciones
- Cláusula 7.- Realizar la identificación y análisis de los requerimientos de seguridad de la información, identificar los activos del alcance
- Cláusula 8.- Evaluación y tratamiento del riesgo, selección de controles a ser aplicados autorización para implementar un SGSI.
- Cláusula 9.- Diseño del SGSI, diseño de un marco referencial normas y procedimientos de la seguridad de la información, programas de capacitación y concientización sobre la seguridad

Es un documento genérico y puede ser aplicable a todas las organizaciones, independientemente de su naturaleza o tamaño. La organización debe identificar qué parte de esta guía se aplica a ella de acuerdo con su contexto organizacional. Las organizaciones no están obligadas a cumplir con las recomendaciones de esta norma, cuando se someten a la certificación de un SGSI (EESTI STANDARDIKESKUS, 2017)

2.1.6. Auditoría del SGSI

La Auditoría es un proceso ordenado, metódico, independiente y documentado para obtener evidencia, que servirá para evaluar de forma objetiva si se cumplen con los criterios establecidos previamente, debe estar basada en hechos que sirven para establecer los puntos fuertes y débiles del sistema u organización auditada. Su objetivo es brindar consejo, recomendaciones para prepararse para la certificación.

El resultado de una auditoría se verá reflejado en controles apropiados, enmarcados en el contexto de la organización. En las auditorias del SGSI se aplican los mismos principios y técnicas de una auditoria de gestión, conforme lo establece la Norma ISO 19011: Directrices para la auditoría de Sistemas de Gestión. Las auditorías pueden ser internas o externas.

Auditoría interna o auditoria de primera parte.- se caracteriza por ser independiente y objetiva que mejora las operaciones y contribuye a la creación de valor agregado lo que garantiza el nivel de control.

Auditoria externa o de tercera parte.- es realizada con un propósito específico y puede ejecutarse por organizaciones externas e independientes que otorgan la certificación de conformidad del Sistema de Gestión. (PECB Professional Evaluation and Certiification Bord, 2005)

2.1.7. Norma ISO 19011

Esta Norma Internacional inserta la definición de riesgo en la auditoría del Sistema de Gestión, relaciona el riesgo de que un proceso de auditoría

no logre sus objetivos y el hecho de que la auditoría obstaculice las actividades y procesos a ser auditados.

La auditoría combinada es aplicada en los casos en que requiera auditar más de un sistema de gestión de diferentes disciplinas.

La norma está compuesta de 7 capítulos y un anexo.

- Capítulo 3.- Contiene términos y definiciones usadas en esta norma.
- Capítulo 4.- Se basa en principios que ayudan a comprender la razón de ser de la auditoria
- Capítulo 5.- Proporciona directrices para establecer y manejar el programa de auditoria, desde sus objetivos hasta las actividades a ejecutar.
- Capítulo 6.- Es una guía de la planeación y ejecución de la auditoría a un sistema de gestión.
- Capítulo 7.- Proporciona los lineamientos para la competencia y evaluación de auditores y equipos de auditoria.

2.2. Estado del arte

La organización internacional de estandarización ISO establece que de un total de 1.519.952 certificados ISO 27001, que se han emitido a nivel mundial de las diferentes normas internacionales en el año 2015, ha existido un incremento del 3%. En el caso de Ecuador esto se puede observar en la tabla 1, la cantidad de certificados ISO 27001 emitidos en los 3 últimos años son: (EESTI STANDARDIKESKUS, 2017)

Tabla 1
Certificados ISO 27001 en Ecuador

ISO / IEC 27001 - Certificados en el Ecuador		
2013 año	2014 año	2015 año
5	7	6

Fuente: https://www.iso.org/the-iso-survey.html

En el sector de la salud y trabajo social, la ISO establece que en la norma ISO 27001, en el año 2015, se han certificado 231 instituciones de un total de 9094, lo que representa el 2,54%.

La Asociación Española de Normalización y Certificación (AENOR) hace conocer que a nivel mundial, se han certificado 1500 organizaciones del sector salud, con la intención de mejorar la salud de la población, acercar el sistema sanitario a la sociedad, mejorar la gestión e incrementar la eficiencia del sector (AENOR).

Hasta el momento las empresas más significativas que cuentan con certificaciones ISO 27001 en el territorio ecuatoriano, entre otras son:

- TELCONET.- obtuvo la certificación ISO/IEC 27001:2005 en el año 2008. Tiene como objetivo brindar servicios de telecomunicaciones a través de NGN (Net Generación Netoworking), su misión está enfocada en proveer servicios de voz, video y datos.
- Corporación Nacional de Telecomunicaciones (CNT).- su visión es ser la primera empresa de telecomunicaciones del Ecuador, para lo cual ofrece un portafolio de productos entre los que se encuentra la telefónica fija y móvil, internet fijo y móvil y televisión. CNT es la única empresa pública en el Ecuador que posee una certificación en seguridad en la información ISO/IEC 27001: 2007 obtenida el año 2012, que además de buscar calidad cuida de la seguridad en la información que maneja.

CAPÍTULO III

FUNDAMENTACIÓN METODOLÓGICA DE LA PROPUESTA

3.1. Descripción de la Organización

3.1.1. Ministerio de Salud Pública (MSP)

Misión: “Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la Salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la Salud” (Ministerio de Salud Publica, 2017).

Visión: “El Ministerio de Salud Pública, ejercerá plenamente la gobernanza del Sistema Nacional de Salud, con un modelo referencial en Latinoamérica que priorice la promoción de la salud y la prevención de enfermedades, con altos niveles de atención de calidad, con calidez, garantizando la salud integral de la población y el acceso universal a una red de servicios, con la participación coordinada de organizaciones públicas, privadas y de la comunidad” (Ministerio de Salud Publica, 2017).

Valores:

- “Respeto.- Entendemos que todas las personas son iguales y merecen el mejor servicio, por lo que nos comprometemos a respetar su

dignidad y a atender sus necesidades teniendo en cuenta, en todo momento, sus derechos.

- Inclusión.- Reconocemos que los grupos sociales son distintos y valoramos sus diferencias.
- Vocación de servicio.- Nuestra labor diaria lo hacemos con pasión.
- Compromiso.- Nos comprometemos a que nuestras capacidades cumplan con todo aquello que se nos ha confiado.
- Integridad.- Tenemos la capacidad para decidir responsablemente sobre nuestro comportamiento.
- Justicia.- Creemos que todas las personas tienen las mismas oportunidades y trabajamos para ello.
- Lealtad.- Confianza y defensa de los valores, principios y objetivos de la entidad, garantizando los derechos individuales y colectivos". (Ministerio de Salud Publica, 2017)

Estructura Orgánica: La figura 2 ilustra la estructura organizacional del Ministerio de Salud Pública que se ha establecido para el cumplimiento de su misión y responsabilidades.

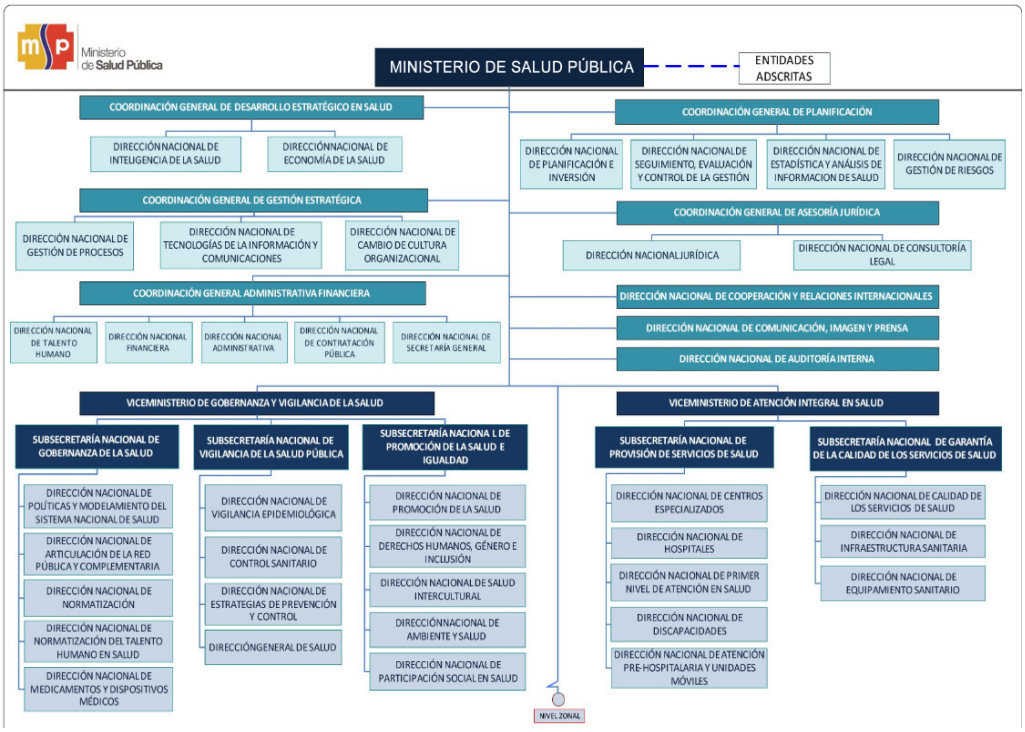

Figura 2 Organigrama estructural del MSP.

Fuente: Ministerio de Salud, 2016

3.1.2. Dirección Nacional de Primer Nivel de atención

Misión: “Planificar y garantizar la prestación que brinda el Ministerio de Salud Pública con respecto a los servicios de salud del primer nivel de atención, con calidad y calidez; de forma articulada a todos los niveles de atención que conforman el Sistema Nacional de Salud, conforme a las políticas sectoriales, en el marco del derecho y equidad social.” (Ministerio de Salud Publica, 2017)

Atribuciones y responsabilidades:

- “Asesorar a las máximas autoridades sobre los servicios de salud del primer nivel de atención del Ministerio de Salud Pública
  b. Conducir y coordinar la formulación de insumos para los proyectos de ley, reglamentos, políticas públicas y otros instrumentos legales relacionados los servicios de salud del primer nivel de atención.
- Conducir y coordinar la elaboración de modelos de gestión, planes, proyectos y demás herramientas para los servicios de salud de primer nivel de atención del Ministerio de Salud Pública, en base a las políticas y lineamientos estratégicos establecidos, y en coordinación con la Dirección Nacional de Articulación de la Red Pública y Complementaria para su articulación con los niveles de atención que conforman el Sistema Nacional de Salud.
- Coordinar y controlar la implementación de modelos de gestión, planes, proyectos y demás herramientas establecidas para los servicios de salud de primer nivel de atención del Ministerio de Salud Pública.
- Coordinar y controlar la implementación de los principios, normas y modelos que regulan las relaciones de establecimientos de primer nivel de atención en salud del Ministerio de Salud Pública con otros establecimientos de la red pública y complementaria para la referencia y contra referencia, en base a los lineamientos estratégicos establecidos y

en coordinación con la Dirección Nacional de Articulación de la Red Pública y Complementaria.

- Desarrollar y controlar la implementación de las estrategias y guías de operativización para la organización y direccionamiento de los establecimientos de salud de primer nivel de atención del Ministerio de Salud Pública a través de la gestión desconcentrada, en base a los lineamientos estratégicos y normas establecidas desde el Viceministerio de Gobernanza y Vigilancia, y en coordinación con la Dirección Nacional de Gestión de Procesos.
- Desarrollar planes y estrategias para implementar el modelo de atención primaria, cartera de servicios intra y extramurales, y capacidad resolutiva de los establecimientos de primer nivel de atención en salud del MSP.
- Proveer a la Dirección Nacional de Tecnologías de la Información y Comunicaciones y a la Dirección Nacional de Gestión de Procesos, lineamientos e insumos para el diseño de sistemas que permitan el monitoreo y evaluación de la aplicación de las políticas, ejecución de planes y proyectos relacionados al ámbito de su competencia.
  i. Proveer a la Dirección Nacional de Estadística y Análisis de Información de Salud, lineamientos e insumos técnicos, para la recolección de información de gestión de los servicios y para la adscripción de población a cargo de los establecimientos del primer nivel de atención del Ministerio de Salud Pública.
- Coordinar y desarrollar estrategias para la detección de las necesidades de salud de la población, en base a los lineamientos estratégicos establecidos.
- Proveer a la Dirección Nacional de Políticas y Modelamiento del Sistema Nacional de Salud, insumos para el establecimiento de lineamientos de prioridades de investigación sobre la atención de los establecimientos de salud del primer nivel de atención del Ministerio de Salud Pública.
- Aprobar las prioridades de investigación operativa para la atención de los establecimientos de salud del primer nivel de atención del Ministerio de Salud Pública.

- Proveer a la Dirección Nacional de Políticas y Modelamiento del Sistema Nacional de Salud, la Dirección Nacional de Normatización y la Dirección Nacional de Normatización del Talento Humano en Salud, insumos para el desarrollo de modelos, normativas, planes y otras herramientas técnico-legales, sobre los servicios de salud de primer nivel de atención del Ministerio de Salud Pública, el fortalecimiento de su talento humano y su capacitación continua.
- Proveer a la Dirección Nacional de Normalización, insumos para la actualización de guías clínicas, protocolos terapéuticos y procedimientos para la atención de los establecimientos del primer nivel de atención del Ministerio de Salud Pública.
- Proveer a la Dirección Nacional de Infraestructura Sanitaria y a las demás instancias involucradas, insumos técnicos para definir la pertinencia de adecuación y/o construcción de establecimientos de salud de primer nivel de atención del Ministerio de Salud Pública.
- Coordinar con la Dirección de Nacional de Talento Humano, los requerimientos de profesionales y necesidades de capacitación dentro del ámbito de su competencia.
- Proveer insumos y verificar el cumplimiento de la distribución de cupos de salud rural y pregrado para el primer nivel de atención del Ministerio de Salud Pública, en base a los lineamientos establecidos y en coordinación con la Dirección Nacional de Normatización del Talento Humano en Salud y la Dirección Nacional de Talento Humano.
- Coordinar y controlar la aplicación e implementación de las normas médicas, técnicas, administrativas y financieras, con la finalidad de mantener control sobre la gestión y racionalizar los recursos de los establecimientos de primer nivel de atención en salud del Ministerio de Salud Pública.
- Asesorar técnicamente a los niveles desconcentrados del Ministerio de Salud Pública, en la definición e implementación de sistemas gerenciales y mecanismos de control de la gestión de los establecimientos de primer nivel de atención.

- Planificar, dirigir, aprobar y evaluar la gestión de la Dirección a su cargo, y asegurar la adecuada coordinación con las demás instancias del Ministerio.
- Generar y monitorear el cumplimiento de objetivos, metas e indicadores para la gestión y atención de los servicios de salud de primer nivel de atención del Ministerio de Salud Pública, alineados a los estándares y lineamientos estratégicos establecidos.
- Generar y monitorear el cumplimiento de indicadores de gestión de la Dirección a su cargo.
- Participar de ser requerido y de acuerdo al ámbito de su competencia, en la sala situacional del Ministerio de Salud Pública.
- Ejercer las funciones, representaciones y delegaciones que le asigne el Subsecretario/a Nacional de Provisión de Servicios de Salud.” (Ministerio de Salud Publica, 2017)

3.1.3. Gerencia de Contact Center

Funciones asignadas:

- Desarrollar y establecer planes de implementación del servicio de agendamiento de citas por Contact Center en los establecimientos de salud de primer nivel, que permitan supervisar y evaluar la gestión de los establecimientos en los cuales se ha implementado el servicio de agendamiento por Contact Center, en conjunto con la Dirección Nacional de Primer Nivel de Atención en Salud.
- Emitir directrices para establecer la parametrización de agendas de cada establecimiento de salud con Contact Center, y así revisar las matrices de capacidad instalada, la cual es elaborada por el nivel desconcentrado previo a ser puesta en operación.
- Asesorar técnicamente a los niveles desconcentrados en el manejo y desempeño del agendamiento de citas por Contact Center; así como

desarrollar estrategias de mejora y evaluar la calidad del servicio implementado en los establecimientos de salud del primer nivel de atención.

- Elaborar, revisar y gestionar la aprobación de insumos para los procesos de contratación del servicio de agendamiento por Contact Center; así como administrar, ejecutar y supervisar el cumplimiento de los procesos contractuales que se deriven de la contratación del mismo.
- Dirigir la Articulación del servicio de Contact Center con los requerimientos de otras instancias del MSP, distintas a la Dirección Nacional de Primer Nivel de Atención en Salud.

3.2. Descripción del Servicio de Agendamiento de Citas del Contact Center

El servicio de agendamiento de citas médicas desarrolla un proceso sistemático en el que intervienen varios actores: pacientes, proveedores, médicos y personal administrativo. Tiene como objetivos: la asignación de citas médicas, la administración de la capacidad de los establecimientos de salud y la provisión de la información requerida para los procesos de historia clínica y sistema estadísticos del MSP.

3.2.1. Descripción del Proceso de Agendamiento de Citas Médicas del MSP.

El ingreso al servicio de salud en el país, se hace a través los establecimientos de salud del primer nivel de atención que comprende los centros de salud y unidades médicas de diferentes capacidades e involucra

al equipo funcional y gerencial del MSP, entidades gubernamentales, proveedores, Contact Center e infraestructura tecnológica.

El proceso de agendamiento es soportado por el sistema informático denominado Phuyu Salud, que permite el manejo de la agenda por cada consultorio, especialidad y establecimiento de salud; administra los perfiles y roles de usuarios, valida los datos de pacientes, entrega citas médicas y realiza manejo de agendas. Actualmente el sistema fue contratado por régimen especial.

Con fecha 23 de mayo 2017 se renovó el contrato del Servicio de Contact Center con la Corporación Nacional de Telecomunicaciones (CNT EP) por el lapso de un año, para contar con el sistema de agendamiento y seguimiento de citas médicas Phuyu Salud, con el objeto de mejorar la atención y optimizar la accesibilidad a los servicios que el MSP proporciona al usuario.

La arquitectura de equipamiento y conectividad provee la plataforma de Cloud de CNT y cuenta con un sistema de alta redundancia con opciones de escalabilidad de recursos. El sistema es utilizado por 750 establecimientos de salud de primer nivel para la atención, a un promedio de atención de 800.000 pacientes por mes.

El flujograma del proceso del servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador se presenta en la Figura 3.

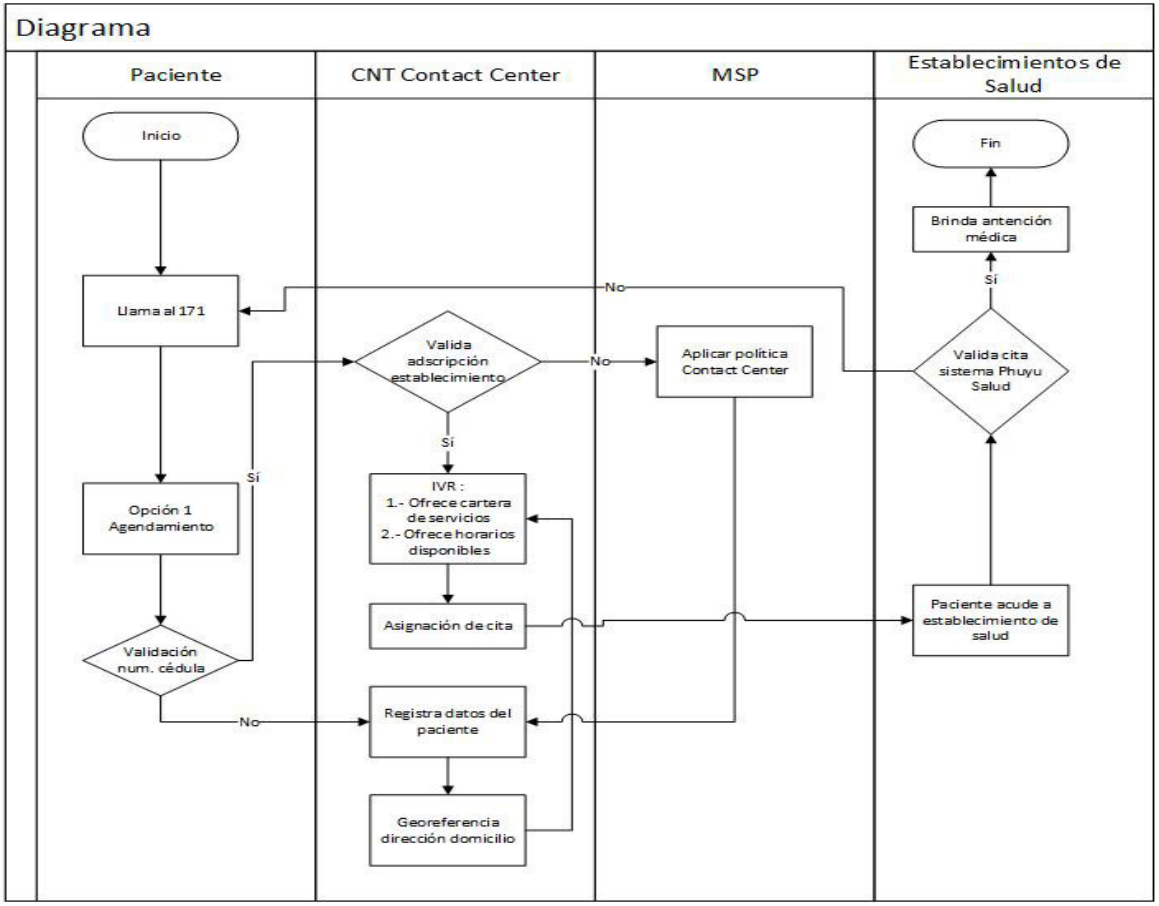

Figura 3 Flujograma Proceso de Agendamiento.

3.3. Evaluación de la Situación Actual.

3.3.1. Aplicación de la metodología de Investigación de campo.

Considerando que se pretende en el futuro implantar la Norma ISO/IEC INEN 27001:2013, el método empleado para esta investigación, es el de una Auditoría-Evaluación de Cumplimiento, en la que se tiene como Criterio de Evaluación los requisitos de la norma mencionada y como procedimientos los que establece la Norma ISO 19011. El objetivo de la evaluación es determinar el estado de cumplimiento de la Norma ISO/IEC INEN 27001 en el SGSI, cuyo alcance es el Proceso de Citas Médicas del MSP.

Para proceder con la Investigación de campo se elabora el Plan de Investigación de Campo (PIC) (Anexo “1” Plan de Investigación de Campo), que consiste en un cuadro descriptivo de los instrumentos de investigación, que se utilizan para obtener la información relacionada con los requisitos de la norma ISO 27001

3.3.2. Resultados de la Investigación de campo.

Tabla 2
Resultados de la Investigación de campo

PREGUNTA BÁSICA	Wendy Barreno	Stalin Peña	Cristian Ortiz	Diego Betancourt	Observaciones	NO	SI	NO CONOCE
1	no	no	no	no	S.A. Se tiene como disposición incluir en temas de contratación	4		
2	no	no	no	no		4		
3	si	si	si	si	No existe evidencia		4	
4	si	no	no	si	Instructivo de la seguridad de la información MSP 2016	2	2	
5	no	no	no	no		4		
6	no	no	no	no		4		
7	no	si	si	no	C.O. No existe evidencia	2	2	
8	no	no	no	no		4		
9	si	no	no	si		2	2	
10	no	no	no	no		4		
11	no	no	no	no		4		
12	no	no	no	no		4		
13	no	no	si	no	D.B. El Instructivo lo considera C.O. No existe evidencia	3	1	
14	no	no	no	no		4		
15	no	no conoce	si	no	C.O. No existe evidencia	2	1	1
16	no	no	no	no	D.B. Hay una POLITICA interna pero no incluye a terceros		4	
17	si	si	no	si	D.B. Instructivo de la seguridad de la información MSP 2016	1	3	
18	si	si	no	si	D.B. Instructivo de la seguridad de la información MSP 2016	1	3	
19	si	si	no conoce	si	D.B. Instructivo de la seguridad de la información MSP 2016		3	1
20	no	no	No	no		4		
21	si	no	no	si	D.B. Memorando Nro. MSP-SDM-10-2014-0389-M	2	2	

22	si	no	no	si	D.B. Memorando Nro. MSP-SDM-10-2014-0389-M	2	2	
23	no	no	no	no		4		
24	no	no	si	no	C...O. No existe evidencia	3	1	
25	si	no	no	si	D.B. Instructivo de la seguridad de la información MSP 2016 considera el riesgo en áreas restringidas, riesgo nacional en uso de software, riesgo institucional	2	2	
26	no	no	no	no	D.B. No existe evidencia de auditorías que considera mejoras	4		
27	no	no	no	no		4		
28	no	no	no	no		4		
29	no	no	no	no		4		
30	no	no	no	no		4		
31	no	no	no	no		4		
32	no	no	no	no		4		
33	no	no	no	no		4		
34	no	no	no	no		4		
35	no	no	si	no	No existe evidencia	3	1	
36	no	no	no	no		4		
37	no	no	no	no		4		
38	no	no	no	no		4		
39	no	no	no	no		4		
40	no	no	no	no		4		
41	no	no conoce	no conoce	no		2		2
42	no	no	no conoce	no		3		1
43	no conoce	no conoce	no	no conoce		1		3
44	si	no	si	si	D.B. En la vinculación de un empleado se da una capacitación en temas de seguridad de información C.O. No existe evidencia	1	3	
45	si	si	no	si	D.B. Instructivo de la seguridad de la información MSP 2016 considera el riesgo en áreas restringidas, riesgo nacional en uso de software, riesgo institucional	1	3	

46	no	no	no	no		4		
47	no conoce	no	no	no conoce		2		2
48	no	no conoce	no	no		3		1
49	no	no	no	no	D.B. Instructivo de la seguridad de la información MSP 2016 considera el riesgo en áreas restringidas, riesgo nacional en uso de software, riesgo institucional	4		
50	No	no	No	no conoce		3		1

3.3.2.1 Instrumentos de medición

La entrevista consiste en 50 preguntas formuladas a 4 funcionarios en el periodo de septiembre a octubre del 2017, los resultados de la tabulación de datos están agrupados por cada uno de los requisitos de la norma nacional y se detalla a continuación:

En relación al requisito 4 de la norma ISO 27001, Contexto de la Organización, se realizaron 8 preguntas orientadas a los funcionarios. La fig. 4 ilustra sus resultados.

NO: 16 (75%) **SI: 4 (25%)**

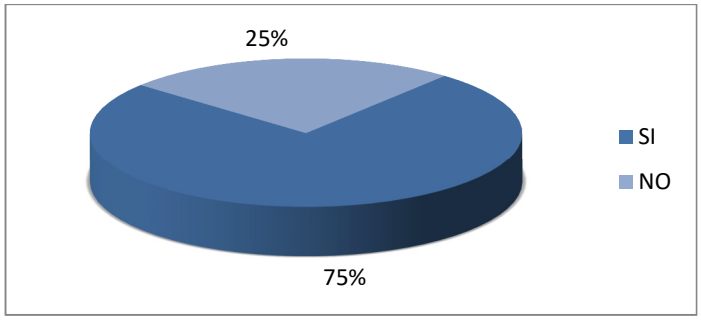

Figura 4 Preguntas del requisito 4

RESULTADO: De los resultados, se tiene que gran parte de los encuestados, no considera que la organización determine a la seguridad de la información parte del plan estratégico, no está definido un alcance para el SGSI, tampoco considera interfaces y dependencias entre las actividades realizadas por la organización y las que son realizadas por otras organizaciones

En relación al requisito 5 de la norma ISO 27001, Liderazgo, se realizaron 14 preguntas orientadas a los funcionarios. La fig. 5 ilustra sus resultados

NO: 34 (60.71%) **SI: 18 (32.14%)** **NO CONOCE : 4 (7.14)**

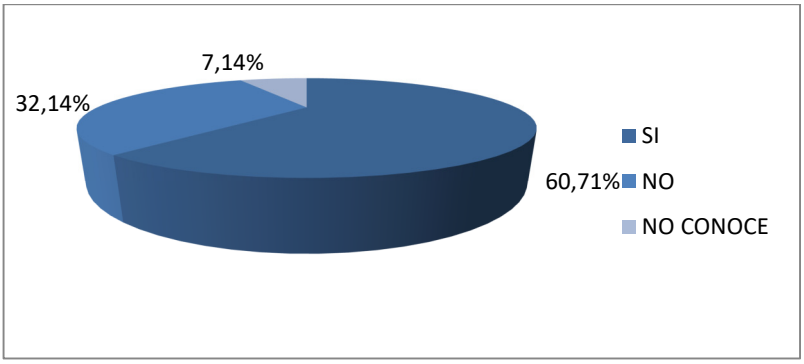

Figura 5 Preguntas del requisito 5

RESULTADO: De los resultados, se tiene que gran parte de los encuestados, considera que no existe un compromiso de la alta dirección no se encuentran integrado los requisitos del SGSI en la organización, la Política no incluye un compromiso de mejora continua del SGSI

En relación al requisito 6 de la norma ISO 27001 Planificación, se realizaron 20 preguntas orientadas a los funcionarios. La fig. 6. Ilustra sus resultaos

NO: 73 (91.25%) **SI: 4 (5%)** **NO CONOCE: 3 (3.75%)**

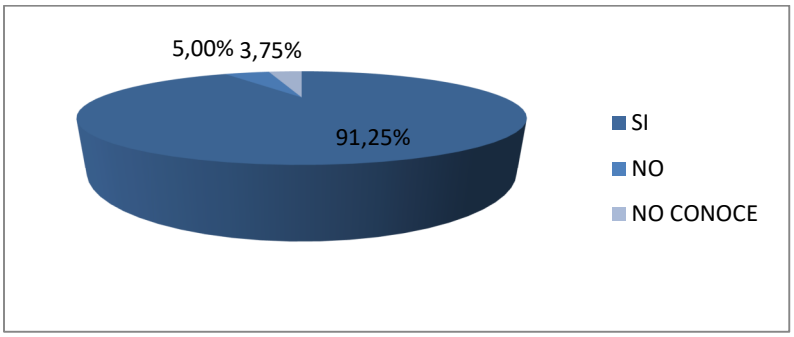

Figura 6 Preguntas del requisito 6

RESULTADO: De los resultados, se tiene que gran parte de los encuestados, indica que no se ha realizado un análisis de los riesgos, no se ha tratado la prevención de riesgos ni su tratamiento

En relación al requisito 7 de la norma ISO 27001 Soporte, se realizaron 3 preguntas orientadas a los funcionarios. La fig. 7. Ilustra sus resultaos

NO: 3 (25%) **SI: 6 (50%)** **NO CONOCE: 3 (25%)**

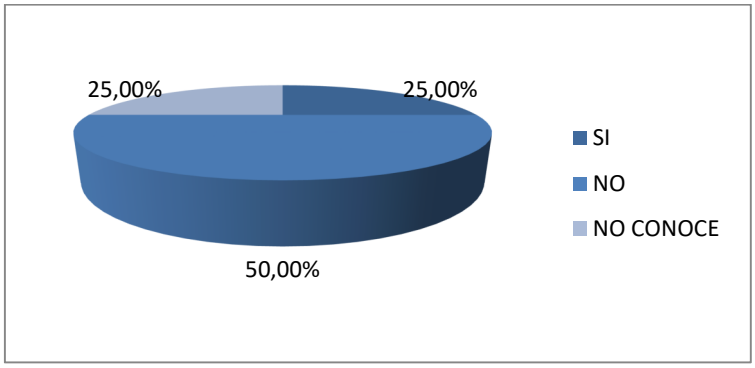

Figura 7 Preguntas del requisito 7

RESULTADO: De los resultados, se obtiene que si cuentan con recursos capacitados pero no se tiene la seguridad que la organización este comprometida en la implementación del SGSI

En relación al requisito 8 de la norma ISO 27001 Operación, se realizó 1 pregunta orientada a los funcionarios. La fig. 8. Ilustra sus resultaos

NO: 1 (100%) **SI: 0 (0%)** **NO CONOCE: 0 (0%)**

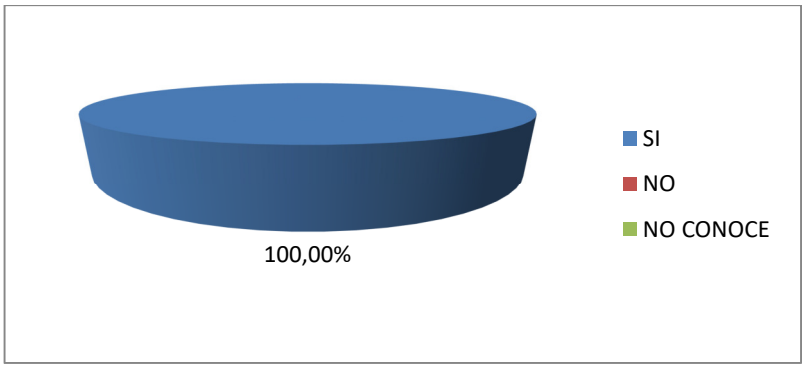

Figura 8 Preguntas del requisito 8

RESULTADO: De los resultados, de esta pregunta fue aún más desalentador, pero al mismo tiempo esperado; ya que en el resultado del requisito 6 se indicó que no existe el análisis de riesgos por tanto no hay una revisión periódica de los criterios de apreciación de los riesgos

En relación al requisito 9 de la norma ISO 27001 Evaluación de desempeño, se realizó 1 pregunta orientada a los funcionarios. La fig. 9. Ilustra sus resultaos

NO: 9 (75%) **SI: 0 (0%)** **NO CONOCE: 3 (25%)**

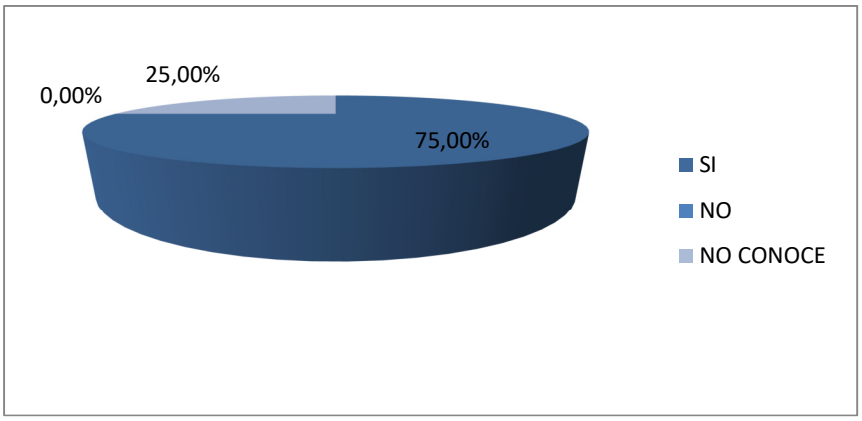

Figura 9 Preguntas del requisito 9

RESULTADO: De los resultados, de esta pregunta denota que no se mide la eficacia de la seguridad de la información, los encuestados desconocen si se realizan auditorias y con qué frecuencia

En relación al requisito 10 de la norma ISO 27001 Mejora, se realizó 1 pregunta orientada a los funcionarios. La fig. 10 Ilustra sus resultaos

NO: 3 (750%) **SI: 0 (0%)** **NO CONOCE: 1 (25%)**

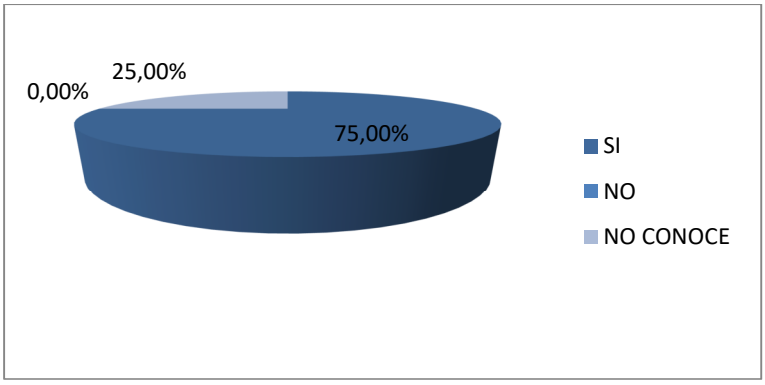

Figura 10 Preguntas del requisito 10

RESULTADO: De los resultados, de esta pregunta los encuestados no conocen si existe un documento formalmente aprobado en el cual como resultado de la revisión al SGSI se ha tenido no conformidades, se ha analizado sus causas y tomado acciones correctivas

3.3.3. Análisis, conclusiones y recomendaciones de la Investigación de campo.

Análisis.

De las encuestas y entrevistas personales realizadas a los funcionarios del Ministerio de Salud, se puede observar lo siguiente:

- El 75% de los entrevistados, indican que no está determinado el alcance del SGSI, la organización tiene establecido un EGSI pero no se realiza mantenimiento ni mejoras en el sistema de gestión de seguridad de la información.
- En cuanto al liderazgo y compromiso, los resultados señalan que el 32,14% coincide en que la alta dirección ha considerado establecer la política de seguridad de la información, sin embargo, no se tiene informes que evidencie sobre el desempeño del EGSI.
- Respecto del riesgo y oportunidades, el 91,25% de los entrevistados coinciden en que los riesgos no han sido identificados ni tratados y no se cuenta con un plan de tratamiento de riesgos de seguridad de la información.
- Acerca del requisito Recursos, el 50% confirma que existen recursos competentes para mantenimiento del EGSI y el 25% señala que no conoce de procesos de capacitación sobre seguridad de la información.
- En la evaluación de desempeño, el 75% indica que no existen evidencias del monitoreo, análisis y evaluación al EGSI, al mismo tiempo el 25% no conocen si se realizan auditorias o si se hace revisión por la dirección.
- Para el requisito de la mejora, el 75% de los entrevistados indican que no se tiene no conformidades, ya que ellas se desprenden de las auditorias y éstas no se han realizado, por lo que no se toman acciones de control ni mejora.

Conclusiones preliminares:

- Pese a estar identificadas las partes interesadas, no se ha determinado el alcance del SGSI para el proceso de agendamiento.
- No se tiene conocimiento ni comunicación oficial de la alta Dirección del desempeño del cumplimiento de la política ni controles. No se verifica el cumplimiento de la norma ISO 27000 ni EGSI en los contratos con terceros.
- Hace falta gestionar los riesgos y plan de tratamiento para mitigarlos así como la sociabilización a los funcionarios para que sean conscientes de ellos.
- Pese a contar con personal capacitado técnicamente, encargado de la seguridad de la información no se cuenta con un plan de capacitación, en la MSP tampoco existe un plan o programa de charlas de concientización a los funcionarios, por lo que están expuestos a ser víctimas de ingeniería social, entre otros tipos de ataques cibernéticos.
- Hace falta el compromiso de las autoridades del MSP para implementar, mantener y mejorar el EGSI y la norma ISO 27001.

Recomendaciones:

- Implementar adecuadamente el SGSI en base a una guía práctica basada en normas y estándares reconocidos que asegure un proceso sistemático confiable.

3.4. Análisis metodológico para la configuración de la propuesta. Norma ISO 27003:2017.

Como elementos esenciales de la norma ISO 27003:2017, que pueden ser considerados para la aplicación en el presente trabajo, se tienen los siguientes:

- Cláusula 5.- La obtención de aprobación de la Dirección para iniciar un proyecto de SGSI mediante un caso de negocio y el plan del proyecto, tiene como objetivos establecer la importancia de un SGSI, así como designar de roles y responsabilidades de seguridad de la información.
- Cláusula 6.- Tiene por objetivo definir el alcance, límites del SGSI, el plan inicial, desarrollar la política, la aceptación y el respaldo de la Dirección para una implementación de éxito.
- Cláusula 7.- Realizar la identificación y análisis de los requerimientos de seguridad de la información, identificar los activos de información que será parte del alcance al momento de implementar el SGSI.
- Cláusula 8.- Define la metodología de evaluación y tratamiento planificado de riesgos relevantes, selección de controles a ser aplicados y autorización para implementar un SGSI.
- Cláusula 9.- Diseño del SGSI, aquí se contempla el diseño a detalle del proyecto SGSI, cuyo plan final será único y podrá tener un impacto en los procesos del negocio, los componentes del SGSI se integran con acuerdos de gestión e infraestructura ya existente, una vez que se encuentre implementado el proyecto SGSI ingresa al ciclo PHVA.

CAPÍTULO IV

PROPUESTA: GUÍA PARA LA IMPLANTACIÓN DEL SGSI PARA EL SERVICIO DE AGENDAMIENTO DE CITAS DEL CONTACT CENTER DEL MSP

4.1. Desarrollo de la Propuesta

4.1.1. Introducción

Un sistema de gestión de seguridad de la información tiene por objetivo proteger la integridad, confidencialidad y disponibilidad de la información, para ello se debe contar con el establecimiento del proyecto, objetivos, alcance, estructura de seguridad de la información, políticas, procedimientos y su programa de difusión entre otros.

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC), ha convertido los medios tecnológicos en pilares fundamentales de las organizaciones, este beneficio requiere la implementación de las mejores prácticas para minimizar el riesgo inherente al uso y protección de la información.

El presente trabajo busca ofrecer una guía práctica para la implementación tomando como referencia la norma NTE INEN-ISO/IEC 27001 que se enfoca en aspectos críticos que son requeridos en la etapa de diseño e implementación y el trabajo publicado por el Ing. Mario Ron y otros; Practical Guide To Implement An Academic Computing Security Incident Response Team (Academic CSIRT). También se incluye recomendaciones basadas en experiencias propias del tutor y del maestrante como aporte a la presente tesis.

4.2. Consideraciones generales

La implementación de un SGSI se gestiona de forma general como un proyecto basado en configuración, organización, procesos y gestión. El proyecto para la implementación del SGSI debe incluir un diseño eficiente y efectivo, a continuación algunas consideraciones que debe incluir el proyecto del Servicio de Agendamiento por Contact Center:

- Los recursos económicos en la Gerencia del Contact Center son limitados, por tanto es importante la eficiencia.
- Las normas se encuentran en revisión y sujetas a mejoras por parte de los comités técnicos de ISO e IEC
- La implementación de un SGSI debe basarse en metodologías estandarizadas de proyectos y mejores prácticas.
- El acuerdo ministerial Nro. 166, la Secretaría Nacional de la Administración Pública, dispone la implementación del EGSI (Esquema Gubernamental de Seguridad de la Información) y se constituye como un instrumento base para todas las entidades públicas.
- El diseño de la organización debe ser escalable y evolutiva.
- El proyecto debe planificarse para que sea autosustentable y permita mejoras continuas mediante auditorías internas.

4.3. Procedimiento

A continuación se describe las actividades a seguir para la implementación del SGSI.

Conformar la comisión del Proyecto.- Se conforma una comisión que será la encargada de coordinar todas las acciones referentes a seguridad de la información en la institución y se designa al patrocinador del proyecto de

implementación del SGSI, esta dignidad recae sobre un funcionario de la alta dirección. Adicionalmente se designará a los directivos y personas que son afectadas por el SGSI, el número de personas no debe ser excesivo.

Desarrollo del caso de negocio.- El caso de negocio sirve como base para el proyecto de implementación del SGSI y justifica su factibilidad. En el caso de negocio, se desarrolla el perfil del proyecto donde se establece antecedentes, metas, objetivos generales y específicos, beneficios roles y responsabilidades de los interesados, recursos necesarios, cronograma de actividades, hitos, base financiera u otra base en caso de existir, factores críticos.

Desarrollar el Plan inicial de trabajo.- El plan de trabajo debe describir el proceso a seguir en las etapas de inicio, planificación, seguimiento, control y finalización. Es de gran importancia realizar una evaluación de la situación actual, el problema que se desea resolver, actividades apegadas a una estructura de trabajo y su financiamiento que debe quedar formalizado. El caso de negocio y plan inicial de trabajo se debe presentar a la dirección para su aprobación y apoyo en la preparación del proyecto formal del SGSI

Abrir un registro.- Se recomienda abrir un registro de las actividades que se realicen durante la implementación del SGSI, el responsable de esta actividad deberá ser designado por el equipo del proyecto, adicionalmente se definirá el mecanismo de comunicación entre los interesados del proyecto.

Definir el apoyo de la Dirección.- Para el desarrollo e implementación del proyecto se debe asegurar el compromiso de la Dirección, así como la aprobación y designación del recurso humano, material y económico a utilizarse durante el desarrollo del proyecto. La Dirección será quien apruebe el proyecto y el plan de trabajo para obtener el compromiso de toda la organización e iniciar su ejecución.

Análisis de la organización y su contexto.- Para conseguir resultados satisfactorios en la implementación del SGSI, la organización debe considerar los aspectos internos y externos más relevantes. Se debe considerar las leyes y normativas que disponen medidas de seguridad de la

información, entre ellas el acuerdo Nro. 166 de la Secretaria Nacional de Administración Pública para implementar el Esquema Gubernamental de Seguridad de Información (EGSI), donde se establece un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información e inicia un proceso de mejora continua. Con esta base, el MSP desarrollo un instructivo de Seguridad de Información para formalizar el EGSI y dotar de una herramienta para su implementación.

Análisis de las necesidades y expectativas de las partes interesadas.- El proyecto de implementación del SGSI debe identificar a los interesados, se debe conocer sus requerimientos funcionales, técnicos, económicos y estratégicos, por tanto es necesario mantener un acercamiento con todos y levantar formalmente sus necesidades y expectativas con el objeto de contemplarlos en el alcance y desarrollo del proyecto.

Análisis del Alcance del SGSI.- El alcance del SGSI y sus límites se realiza posterior al planteamiento del problema definido en el plan inicial. Es importante que el alcance sea lo más detallado posible, con lo cual, se debe considerar la eficacia del sistema para identificar, valorar y proteger los activos de información más valiosos de la institución.

El alcance puede contemplar a toda la organización, a una parte, un proceso o servicio definido. Para ello se deberá ejecutar las siguientes actividades:

- Definición del alcance y límites organizacionales.
- Definición del alcance y límites de las Tecnologías de la Información.
- Definición del alcance y límites físicos.

Los alcances individuales deberán integrarse a fin de conseguir los límites estructurados del SGSI.

Elaborar los objetivos de seguridad de la información.- Los objetivos de seguridad de la información deben establecerse para mejorar y coadyuvar las condiciones de seguridad de la información en la organización, deben estar alineados con los objetivos estratégicos de la organización.

Los objetivos deben ser:

- Medibles (procurar que sean)
- Acorde a la política de seguridad de la información.
- Aplicables y considerar los criterios de riesgos y su tratamiento.
- Sociabilizados.
- Actualizados según se requiera

Comunicar la importancia de SGSI.- La alta Dirección debe conocer que un SGSI contribuye con los objetivos del negocio, porque garantiza la confidencialidad, integridad y disponibilidad de la información y debe apoyar el proceso de comunicación a todo el personal para que conozca y concientice la importancia de tener un Sistema de Gestión de Seguridad de la Información. La organización debe comunicar frecuentemente las actividades que se realiza para garantizar la seguridad de la información.

Definir la Política de Seguridad de Información.- La política de seguridad debe plasmar hacia dónde quiere llegar la organización respecto de la seguridad de la información en base a sus objetivos, regulaciones y reglamentos. La política también sirve de marco para la elaboración de procedimientos específicos de seguridad y considera el cumplimiento de terceros. La base para la elaboración de la política es la información relevante de la organización y su giro de negocio, previamente analizada por la Dirección, la política es actualizada de forma periódica, debe ser redactada de forma clara, concisa, en leguaje sencillo, de tal modo que todo el personal puede entender su propósito. Un elemento a incluir es su validez legal.

Definir los roles organizacionales, responsabilidades y autoridades.- El SGSI debe garantizar a través de la alta Dirección el apoyo para la conformación de un equipo de trabajo que cumpla con las funciones necesarias que les permita poner en marcha el SGSI en la organización. Parte de las responsabilidades del equipo de trabajo es comunicar el resultado de la evaluación de los objetivos del SGSI.

Definir la metodología de análisis, tratamiento y responsabilidades en la gestión de riesgos.- Es importante definir una metodología de análisis de

riesgo, partiendo de la identificación de vulnerabilidades, amenazas y las consecuencias de la pérdida de confidencialidad, integridad, disponibilidad de la información. Para ello se debe considerar el alcance, objetivos y parámetros de evaluación de riesgo.

Para conseguir una adecuada evaluación de riesgos, se debe considerar los siguientes aspectos: probabilidad, impacto, vulnerabilidad, aceptación del riesgo.

La valoración del riesgo puede ser analizado en base a la identificación, estimación y evaluación del riesgo.

El tratamiento del riesgo contempla, tomar acciones necesarias para eliminar o mitigar su impacto. Los riegos deben ser priorizados en base a la criticidad que será determinada tras una categorización acompañada por criterio de impacto a la organización (alto, medio, bajo).

La responsabilidad de la gestión de riesgos recae en los propietarios de la información y el Comité de Seguridad, este último se encarga del monitoreo y control de los riesgos identificados. Estará atento a las amenazas que pongan el riesgo los recursos de información de la organización.

Formular un plan de tratamiento de riesgos de seguridad de la información.- Al hablar de tratamiento de riesgos se debe considerar que el riesgo se puede reducir, evitar, mantener y transferir en base de una valoración, por ello se requiere de un plan de tratamiento de riesgos como elemento clave en la implementación del SGSI. El Plan debe contemplar los riesgos priorizados, los aceptables, los controles para reducir, transferir o prevenir los riesgos, los requisitos legales, la regulación a cumplir y el costo de implementación de los controles.

Como parte de los riesgos aceptables se aplica los criterios de aceptación, es decir, los criterios bajo los cuales el riesgo es aceptable. Adicionalmente se debe analizar si los riesgos residuales cumplen con los criterios de aceptación.

Determinar todos los controles que sean necesarios para implementar la gestión de riesgos.- Una vez definido el tratamiento de riesgos a ser aplicado con el objeto de eliminarlos o mitigarlos levándolos a límites aceptados dentro de los umbrales definidos por la seguridad de la información en la fase de diseño del SGSI. Es necesario realizar un plan de tratamiento de riesgos y aplicar controles que deberá contener un listado con el detalle que relaciona el riesgo con el tratamiento del riesgo.

En el anexo A de la Norma INEN ISO/IEC 27001 se listan objetivos de control y controles específicos aplicables a cualquier institución, sin embargo en caso de no existir un control apropiado se debe definir y aplicar según la necesidad de la organización.

La información que resulta de aplicar un control puede ser delicada, en estos casos se debe implementar las medidas de seguridad para su correcto manejo, interno y externo.

El resultado de los controles a implementar y propuesta de evaluación se debe reflejar en un informe que contenga recomendaciones para su correcta implementación.

Elaborar la Declaración de Aplicabilidad que contenga los controles necesarios.- La declaración de aplicabilidad contiene el alcance, la política y la norma ISO/IEC que se tomara como referencia. Este documento es muy importante porque describe los controles que se van a implementar acorde a la necesidad de cada tratamiento de riesgo. Los puntos más importantes de este informe son: descripción del control, objetivo del control, requerimiento, definición de aplicabilidad (es aplicable o no) y razones para su selección.- si aplica se deberá indicar el documento que referencia en el SGSI, caso contrario se deberá justificar su exclusión.

Elaborar y diseñar un plan de comunicación y concienciación.- Esta actividad es parte de la implementación de un SGSI y es parte de un programa que deberá ser diseñado y comunicado de forma periódica. El plan de comunicación consiste en capacitar de forma sencilla y accesible a empleados y terceras partes para crear conciencia y promover la formación

en políticas y procedimientos relacionados a seguridad de la información y el SGSI. Se deberá capacitar las actualizaciones a políticas, procedimientos y normas cuando así lo amerite. Existen varios métodos de comunicación que se pueden utilizar para llegar con la concientización, entre ellos están las campañas, educación virtual, comunicación presencial, entre otros.

La gestión de la seguridad de la información debe ser comunicada de forma interna y externa y su planificación debe considerar, qué comunicar, cuándo, a quién y el medio el medio de comunicación apropiado.

Planificar los procesos necesarios para cumplir los requisitos de seguridad de la información.- Considerando la importancia y función de los procesos críticos dentro de la organización, se debe planificar el análisis y afectación de dichos procesos considerando para ello los requisitos de seguridad de la información que son un insumo del SGSI, estos requisitos deben ser definidos y analizados de la siguiente forma:

- Identificar y recolectar los activos de la información que deben ser respaldados.
- Analizar y definir la criticidad de los proceso de la organización para especificar el nivel de protección a resguardar.
- Identificación factores que podrían afectar la seguridad de la información como funciones, lugar físicos, redes de comunicaciones etc.
- Levantar el inventario de aplicaciones y sistemas asociados a los procesos.

Otro factor importante es el análisis de la afectación de los incidentes de seguridad en los procesos. En caso de existir factores que no consten en el alcance en este inventario se los deberá incluir.

Definir la metodología para controlar los cambios.- Todo cambio debe ser rigurosamente planificado y controlado, para ello se debe seguir una metodología que incluya los siguientes puntos: registrar formalmente los cambios y su detalle, establecer los niveles de aprobación, pruebas a aplicarse, el impacto, las consecuencias no previstas y las acciones para

mitigar cambios no previstos. Esta metodología también aplica para contratos externos.

Determinar los procesos para evaluar el desempeño de seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.- Es preciso determinar los procesos de la organización que se considere fundamentales y analizar cómo interactúan con el resto de procesos, para ello se puede apoyar en flujogramas y técnicas como entrevistas o encuestas para conocer el estado actual de la organización, así como nivel de madurez, requerimientos de seguridad y controles vigentes. Todo esto debe quedar documentado y formalizado.

A continuación se debe evaluar y medir el desempeño para ello se puede comparar normas, políticas, plan estratégico, objetivos de control, controles propuestos y conocer la reacción frente a incidentes de seguridad. Todo para verificar que las medias son las correctas y conocer el desempeño del SGSI. Las mejores prácticas recomiendan realizar monitoreo regular y auditorias periódicas.

Para evaluar el desempeño de la seguridad de información se deberá considerar a recursos internos y externos. Los recursos internos deben tener un alto conocimientos técnico a más de conocimiento de la situación actual de la seguridad de la información. Los recursos externos deben actuar de forma objetiva e imparcial evaluando y determinando el nivel de madurez de la seguridad de la información en la organización.

Si los resultados no son los esperados se debe revisar los controles aplicados en la seguridad de la información así como a la organización, con el objeto de mejorar y asegurar la eficacia de los controles y procesos, es de gran importancia involucrar a todos los interesados del proyecto.

Elaborar el programa de auditoría internas del SGSI.- El objetivo de la auditoria interna es recomendar mejoras y modificaciones de ser el caso, se basa en mediciones del SGSI y tiene por característica ser independiente y objetiva.

Es necesario planificar un programa de auditorías internas del SGSI considerando los siguientes puntos:

- Ser ejecutado de forma periódica, por lo general cada año o podrá ser solicitado por la Dirección en casos de cambios importantes que afecten al SGSI
- Que considere su alcance
- Considerar criterios de auditoria y clasificación de hallazgos
- Motivada por el Oficial de Seguridad de la Información
- Los auditores seleccionados no podrán cumplir con actividades del proceso o área a ser auditada.
- Autorizada por la Dirección para contar con la cooperación de todo el personal en la organización.

Los resultados y evidencias deben ser documentados en un informe y ser comunicados a la Dirección a fin de implementar mejoras al SGSI.

Como referencia existen 3 normas a considerar en procesos de auditoria: ISO 19011:2011, ISO/IEC 27007:2011 e ISO/IEC TR-27008.

Elaborar el Plan de Revisión por la dirección.- El informe preliminar de auditoria para la dirección deberá contener: la lista de hallazgos, observaciones, no conformidades, mejoras, clasificación de las acciones correctivas, conclusiones y recomendaciones; las no conformidades deben estar descritas acorde a la evaluación de los hallazgos, con su respectiva evidencia, esta última reconocida por el área auditad y las oportunidades de mejora que son el valor agregado de la auditoría. Son recomendaciones que de no ser tratadas, a futuro podrán convertirse en no conformidades.

El informe de auditoría deberá ser aprobado y sociabilizado con cada representante del área auditada, se recomendara que las no conformidades se las trate con acciones correctivas con el objeto de generar planes de acción. A continuación el informe final y los planes de acción deben ser puestos a consideración de la Dirección.

Elaborar el procedimiento para la determinación de no conformidades y acciones correctivas.- La organización debe desarrollar un procedimiento en el cual se clasifique y defina las no conformidades mayores y menores. En él se definen si las no conformidades serán tratadas como acciones correctivas o preventivas. La categorización (preventiva / correctiva) se definirá tomando en cuenta el impacto causado. Las acciones correctivas se definen para solucionar las no conformidades detectadas. Las acciones preventivas son establecidas para evitar no conformidades.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La implementación de un sistema de seguridad de la información constituye un objetivo estratégico en las organizaciones, a través de éste, se consigue una ventaja competitiva, y beneficios como la mejora de la imagen corporativa y el cumplimiento del marco regulatorio y legal.
- El Ministerio de Salud es un organismo gubernamental que debe implementar un EGSI por disposición del gobierno además cuenta con estructura orgánica lo que conlleva a que si será factible poner en práctica esta guía propuesta en la implementación del SGSI
- La guía propuesta complementa la Norma ISO /IEC 27001 y pasa a constituirse en una guía práctica para nuevos implementadores.
- Los controles implementados en un SGSI y la madurez de la seguridad de información en una organización, son indicadores del nivel de vulnerabilidad y riesgo sobre la información de la organización. Estos indicadores son susceptibles de cambios y deben ser gestionados con dinamismo para mejorar o mantener su efectividad.
- Luego del análisis de la situación actual, es importante, no sólo para evidenciar la necesidad de la implementación de un SGSI, sino también para concienciar a las autoridades que toman la decisión y los empleados o funcionarios que lo van a implementar.

- Se ha considerado la norma ISO 27003, con las que se ha conseguido establecer un conjunto de actividades que configuren un proceso ágil, cercano a la realidad nacional, tomando como ejemplo una entidad pública y un sistema informático de alta demanda e importancia como es el Sistema de agendamiento de citas médicas del MSP.
- El adoptar un SGSI en una organización implica un cambio de cultura organizacional, servicios de calidad, control interno, monitoreo así como el compromiso en las actividades diarias del personal. Todo esto, genera valor a la organización.

5.2. Recomendaciones

- Es importante que en toda institución se considere la implementación de un sistema de seguridad de la información, como parte de su Plan Estratégico Institucional, el Plan Operativo y el Presupuesto Anual.
- Utilizar la guía propuesta para complementar la Norma ISO /IEC 27003, en la implantación del SGSI del Sistema de Agendamiento de Citas Médicas del MSP.
- Tomar en cuenta el análisis de la situación actual realizado en el presente trabajo, para la implantación del SGSI del MSP.
- Considerar el mejoramiento de la guía propuesta en base a las implementaciones que se realicen y comparar esos resultados con lo que propone la norma ISO 27003 y otros trabajos considerados en este estudio.
- Considerar un fuerte trabajo en concienciación, porque el adoptar un SGSI en una organización implica un cambio de cultura organizacional.
- Para la implementación de la guía propuesta se recomienda designar un líder del proyecto que tenga las debidas competencias y

atribuciones sobre el proyecto. Esto le permitirá proponer iniciativas que permitan llegar al resultado esperado, el líder también debe poseer el conocimiento de las normas internacionales ISO 27000, así como una capacidad de investigación y búsqueda de oportunidades de mejora.

- En la implementación del SGSI, la Dirección debe estar comprometida y empoderada del proyecto. Debe transmitir los beneficios para la organización, la importancia de los activos de la información y su protección, así como transparentar la brecha de seguridad existente en la organización.

BIBLIOGRAFIA

Aceituno, V. (2008). *Seguridad de la información.* Mexico: Limusa Noriega Editores.

AENOR. (s.f.). *www.aenor.es*. Obtenido de http://www.aenor.es/aenor/certificacion/sectores/sanidad.asp#.WScQ65I1_IU

Alexander, A. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información- Óptica ISO 27001:2005.* Alfaomega.

Bertolín, J. (2008). *Seguridad de la información,redes, informàtica y sistemas de informaciòn.* España, Madrid : Cengage Learning, Paraninfo S.A.

BSI. (2013). *Sistema de gestión ISO/IEC 27001 de Seguridad de la Información*. Recuperado el 2017, de https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/.

EESTI STANDARDIKESKUS. (2017). *https://www.evs.ee*. Obtenido de https://www.evs.ee/products/iso-iec-27003-2017

El portal de ISO 27001 en Español. (s.f.). *http://www.iso27000.es.* Recuperado el 03 de 2017, de http://www.iso27000.es

El portal de ISO 27001 en Español. ISO27000. ES. ((2006)). *Anexo A ISO 27001.* Obtenido de http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

El portal de ISO 27001 en Español. ISO27000. ES. ((2001)). *Sistema de Gestión de Seguridad de la Información.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

El portal de ISO 27001 en Español. ISO27000. ES. (2006). *ISO-27001: LOS CONTROLES Parte II.* Obtenido de http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf

El portal de ISO 27001 en Español. ISO27000. ES. (2011). *Normas ISO y estándares referentes .* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

INEN NORMA TECNICA ECUATORIANA ISO/IEC 27001:2013. (2017). Tecnicas de seguridad - Codigo de practica para la aplicacion de controles .

INEN Servicio Ecuatoriano de Normalización. ((2013)). *NTE INEN-ISO /IEC 27001.*

Instituto Ecuatoriano de Normalización . (2012). *Norma Técnica Ecuatoriana INEN ISO/EC 27001:2010 Tecnologías de Información .Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información.*

INTECO Instituto Nacional de Tecnologías de la Comunicación. (2013). *Implantación de un SGSI en la empresa.* España.

ISO 27003:2012. (2012). *Tecnología de información Técnicas de Seguridad Guía de implementación del Sistema de Gestión de la Seguridad de la Información.*

Ministerio de Salud Publica. (2017). *Ministerio de Salud Publica*. Obtenido de http://www.salud.gob.ec/valores-mision-vision/

Norma ISO/IEC 27001. ((2013)). *Técnicas de Seguridad - Sistema de Gestión de la Seguridad de Información requisitos.*

PECB. (2005). Auditor Lider Certificado en la norma ISO/IEC 27001.

PECB Professional Evaluation and Certiification Bord. (2005). Auditor Lider Certificado en la Norma ISO/IEC27001. *Capacitacion en Seguridad de Informacion*.