DIRECCIONAMIENTO Y ESTRUCTURACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLÍNICA MONTSERRAT

María Victoria Alarcón Aponte

Duvan Felipe García Rodríguez

Carolina Isabel Pinzón Lesmes

UNIVERSIDAD SANTO TOMÁS - ICONTEC

FACULTAD DE INGENIERA MECÁNICA ESPECIALIZACIÓN EN DIRECCIÓN Y GESTIÓN DE LA CALIDAD

BOGOTÁ, D.C.

2022

DIRECCIONAMIENTO Y ESTRUCTURACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLÍNICA MONTSERRAT

María Victoria Alarcón Aponte

Carolina Isabel Pinzón Lesmes

Duvan Felipe García Rodríguez

Harold Wilson Hernández

Guillermo Peña Guarín

Director de proyecto de grado

UNIVERSIDAD SANTO TOMÁS - ICONTEC

FACULTAD DE INGENIERÍA MECÁNICA ESPECIALIZACIÓN EN DIRECCIÓN Y GESTIÓN DE LA CALIDAD

BOGOTÁ, D.C.

2022

Tabla de Contenido

Lista de Tablas

Lista de Figuras

1. Selección del tema y el contexto

El Instituto Colombiano Del Sistema Nervioso - Clínica Montserrat, en adelante (ICSN - CLÍNICA MONTSERRAT) es una institución privada sin ánimo de lucro, ubicada en la ciudad de Bogotá; nació hace 70 años, con el objetivo de brindar servicios de asistencia integral para pacientes y familias aquejados por enfermedades mentales.

Durante los primeros años de su funcionamiento construyó y se consolidó como una clínica innovadora y líder en el entendimiento de lo explícito e implícito de las problemáticas psiquiátricas; encabezando la atención psiquiátrica alejada del estigma y del modelo manicomial imperante en su momento.

En la última década, ha recorrido un camino que lo ha llevado a pasar de ser una clínica psiquiátrica, a una institución con tres grandes ejes misionales:

- Asistencia: mediante el cual se brindan servicios asistenciales de alta calidad, ampliando el campo de su actuar no solo a la psiquiatría sino a la salud mental
- Docencia: mediante el cual se forman profesionales médicos en el área de salud mental que replican el modelo montserratino a nivel nacional e internacional en diversos campos de acción.
- Investigación: mediante el cual se diseñan, desarrollan y publican estudios de investigación sobre problemáticas de salud mental.

El ICSN - Clínica Montserrat, trabaja con un enfoque psicodinámico que tiene en cuenta la autorreflexión constante sobre los procesos mentales y ambientales que determinan el funcionamiento humano y se basa en sólidos principios teóricos del funcionamiento mental. Integra diversos puntos de vista y adelantos científicos en los campos de la neurobiología y neuropsicofarmacología sobre dichos fenómenos, así como la importancia de un servicio humanizado que difunda y proteja los derechos y autonomía de nuestros pacientes y sus familias, a la vez que brinda una atención eficiente y segura.

Su modelo asistencial funciona tendiendo puentes a través del constante diálogo científico y humanizado entre los múltiples actores del sistema y sus visiones, por lo cual se ha consolidado como un sistema abierto, en el que la perspectiva de cada miembro del equipo enriquece de manera sinérgica la comprensión y atención. Busca transformar las dificultades, conflictivas y déficits del funcionamiento humano y familiar, en procesos creativos que mejoren la

sintomatología y brinden posibilidades de respuesta y recuperación sostenidas en el tiempo, con el fin de mejorar la calidad de vida y desarrollar el potencial del paciente, su familiar y el equipo.

Como parte del modelo asistencial, el ICSN - Clínica Montserrat, busca no solo hacer una clasificación nosológica de la sintomatología del paciente, sino comprender la personalidad de cada uno de ellos, utilizando las teorías psiquiátricas y psicodinámicas. (Clínica Montserrat, s. f.)

Dentro de su modelo, considera que la estructuración de cada ser humano determina la forma en que las situaciones, conflictos y déficits son vivenciados y expresados. Por eso el entender dicha estructura de personalidad y funcionamiento facilita:

- El análisis y presentación de la sintomatología, así como los factores precipitantes y su influencia.
- Ayuda en la formulación, integración y seguimiento individualizado de los planes de manejo para cada uno de los pacientes
- Permite adelantarse a las dificultades o puntos a favor del tratamiento.
- Determina el grupo terapéutico del cual se beneficiará el paciente en los ciclos de atención.
- Busca acompañar al paciente y su familia durante el ciclo de atención hospitalaria, el post egreso y los servicios ambulatorios orientados al mantenimiento y la reinserción social, laboral y académica.

Misión del instituto.

El ICSN - Clínica Montserrat, es una entidad privada, que presta servicios de atención en salud mental, centrados en las necesidades del paciente, basados en la evidencia científica y prácticas seguras, además de servicios docentes con énfasis psicodinámico. (Clínica Montserrat, s. f.)

Visión del instituto.

En el 2022 el ICSN - Clínica Montserrat, prestará servicios asistenciales, de investigación y de docencia, con calidad superior. Lo que nos permitirá ser un Hospital Universitario. (Clínica Montserrat, s. f.)

Tipificación ICSN - Clínica Montserrat.

- **Forma jurídica:** Utilidad común sin ánimo de lucro.
- **Tamaño:** Gran empresa; 265 colaboradores, 133 de planta, 15 prestación de servicios, 9 trabajadores temporales, 84 trabajadores de servicios tercerizados, 24 otros.

- **Sector:** Sector terciario.
- **Origen del capital:** Institución privada sin ánimo de lucro.
- **Interacción de sus miembros:** Empresa Formal.
- **Despliegue de operaciones:** El Instituto Colombiano Del Sistema Nervioso Clínica Montserrat, cuenta con una sede principal en la Calle 134 17 71, barrio contador de la localidad de Usaquén, donde se realiza la prestación de servicios asistenciales de consulta externa, hospitalización parcial y hospitalización intramural. Su segunda sede se encuentra ubicada en el Km 6 vía suba Cota, en la vereda Chorrillos de la localidad de Suba, donde se realiza la prestación de servicios de rehabilitación en la modalidad residencial.

El ICSN - Clínica Montserrat, entiende que la gestión de calidad, respaldada en su sistema de procesos, observación, reflexión y acción de mejora continua, guarda estrecha relación con la esencia de su funcionamiento; razón por la cual decidió acogerse a esta forma de funcionar, buscando el mejor servicio para todos los actores de su sistema. (M. A. Clínica Montserrat, 2021)

El sistema de gestión de calidad de la institución, se encuentra definido bajo la normatividad vigente para las instituciones prestadoras de servicios de salud IPS, donde se realiza la planeación, implementación y medición de los componentes del sistema obligatorio de garantía de calidad, dando cumplimiento a los requisitos normativos del sistema único de habilitación, el programa de auditoría para el mejoramiento de la calidad, el sistema de información para la calidad y el sistema único de acreditación, este último como proceso voluntario para el mejoramiento continuo. (Decreto 780, 2016)

Para el año 2010, el ICSN - Clínica Montserrat, obtuvo certificación en la norma NTC ISO 9001:2008, actualmente con certificación vigente por Bureau Veritas en la norma NTC ISO 9001:2015; este proceso que logró consolidar un sistema de gestión de calidad institucional, permitido contar con procesos organizados, implementar estrategias para identificar las necesidades de los clientes internos y externos; y fortaleciendo la planeación estratégica generando así mayor impacto en los proyectos Institucionales.

Su estructura se encuentra organizada por procesos, donde se han establecido los trazadores, estratégicos, misionales y de apoyo, permitiendo brindar atención a pacientes con necesidades en salud mental, desde tres pilares fundamentales que son: la asistencia, docencia e investigación. La estructuración de los procesos desde el sistema de gestión de calidad ha contribuido a que estos sean sistémicos

y sistemáticos y que sus actividades estén enfocadas a la consecución de la satisfacción de los usuarios.

El desarrollo del sistema de gestión de calidad se realiza a través de una herramienta de gestión integral denominada Almera; en este aplicativo se lleva el control documental de los procesos, el seguimiento y la gestión orientada al cumplimiento de cada uno de ellos.

A pesar de contar con el sistema de gestión de calidad bajo la norma NTC ISO 9001:2015 y tener un control adecuado para el manejo de la información, además de trabajar por la consecución de niveles superiores de calidad en salud; se identificó producto de la visita de otorgamiento de acreditación en salud realizada por ICONTEC en el mes de abril del año 2021, la necesidad de establecer lineamientos del dato clínico desde la captura, que asegure su validez, confiabilidad, y pertinencia, favoreciendo el desarrollo analítico para una adecuada toma de decisiones en los diferentes niveles, por medio de requisitos que permitan el aseguramiento de la información dentro del contexto de la organización, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de los resultados producto de la atención como lo es la historia clínica, siendo este un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. (Resolución 1995, 1999)

De acuerdo con los cambios en el contexto se encuentran los relacionados con la normatividad, para lo que el ICSN - Clínica Montserrat debe prepararse según los criterios contenidos en la Ley 2015 del 31 de enero de 2020, como se dispone en el capítulo IV disposiciones generales, Artículo 13, seguridad de la información y seguridad digital, (Ley 2015, 2020)

2. Formulación del problema

El ICSN - Clínica Montserrat, durante sus procesos de mejoramiento institucional, identifica la necesidad de establecer lineamientos del dato clínico desde la captura, que asegure su validez, confiabilidad, y pertinencia, favoreciendo el desarrollo analítico para una adecuada toma de decisiones en los diferentes niveles, por medio de requisitos que permitan el aseguramiento de la información dentro del contexto de la organización. Esto debido a que existe una inestabilidad en los datos que han generado impacto negativo en la ejecución de los procesos y la toma de decisiones basadas en la información para la

generación de oportunidades de mejora que fortalezcan el sistema de gestión de calidad.

Otro de los hallazgos identificados se encuentran relacionados con la historia clínica; como parte de la propiedad del cliente, el ICSN Clínica Montserrat debe preservar la confidencialidad, integridad y disponibilidad de los resultados producto de la atención, siendo este un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención.

Se identificó que existen riesgos de la no preservación de la integridad de la información. Durante el proceso de auditoría de historia clínica se evidenció que dos de los formatos de escalas de valoración de riesgos clínicos, no guardaban exactitud, debido a que los criterios de evaluación se encontraban inexactos, uno de los criterios de evaluación de riesgo nutricional estaba ubicado en la herramienta de evaluación de riesgo de evasión.

Durante el año 2021 se presenta incidente en el manejo de las redes sociales, en el que un grupo de personas no autorizadas accede a la información y obran en nombre de la clínica Montserrat.

Se consideran estas, afectaciones en la seguridad de la información, que ponen en riesgo a los procesos y a la institución, consiguiendo generar desconfianza a las partes interesadas en relación con la prestación de los servicios y la gestión de los riesgos. (M. A. Clínica Montserrat, 2021)

Contar con un sistema de gestión de calidad en el ICSN - Clínica Montserrat, es considerada una ventaja, ya que favorece a la integración de otros sistemas de gestión debido a los avances en la transformación cultural del mejoramiento continuo organizacional, siendo un logro para que los procesos sean sistémicos y sistemáticos, favorecido la toma de conciencia organizacional.

Contar con un sistema de gestión de calidad implementado en el ICSN - Clínica Montserrat, es considerado una ventaja que favorece y permite la integración de otros sistemas de gestión, debido a los avances en la transformación cultural del mejoramiento continuo organizacional y que a su vez permite que los procesos sean sistémicos, sistemáticos y que apoyan a la toma de conciencia organizacional.

Integrar a futuro la norma NTC ISO 27001:2013 al sistema de gestión de calidad existente permitirá asegurar la confidencialidad, la integridad y la disponibilidad además de preservar los datos, con el objetivo de mitigar los riesgos de vulnerabilidad de la información.

3. Marco Conceptual

El ICSN - Clínica Montserrat requiere establecer buenas prácticas que aseguren e integren de manera confiable toda la información de la institución y así dar cumplimiento a los requisitos legales, de los clientes y los propios de la organización; evitando la materialización de riesgos asociados a la pérdida de información y proporcionando un modelo consistente que permita establecer, implementar, monitorear y revisar su desempeño mediante el sistema de gestión de seguridad de la información.

Al contar con un sistema de gestión de calidad implementado y certificado bajo la norma técnica colombiana NTC ISO 9001:2015 y siendo este un aspecto fundamental para la estructuración de la norma técnica colombiana NTC ISO 27001:2013, en este caso, se requiere revisar las actividades que se realizan en función de los requisitos de esta norma y su aplicación.

Los sistemas de gestión desde la definición del contexto externo e interno de la institución, utiliza un marco de recursos para alcanzar sus objetivos, incluyendo la estructura organizacional, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, recursos y la interacción de las actividades de los procesos con el objetivo de transformar las entradas en salidas. (Andrés & Gómez, 2009)

La seguridad de la información implica, la aplicación y la gestión de los controles apropiados que involucran la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información (Instituto Colombiano de Normas Técnicas y Certificación ICONTEC, 2013)

La historia clínica como propiedad de los clientes, es un documento privado, obligatorio y sometido a reserva, en el que se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley. (Resolución 1995, 1999)

Como garantes de la historia clínica debemos cumplir con las características básicas descritas en la Resolución 1995 de 1999, por la cual se establecen normas para el manejo de la historia clínica.

Integralidad: La historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordando como un todo en sus aspectos biológico, psicológico y social, e interrelacionado con sus dimensiones personal, familiar y comunitaria. (Resolución 1995, 1999)

Secuencialidad: Los registros de la prestación de los servicios en salud deben consignarse en la secuencia cronológica en que ocurrió la atención. Desde el punto de vista archivístico la historia clínica es un expediente que de manera cronológica debe acumular documentos relativos a la prestación de servicios de salud brindados al usuario. (Resolución 1995, 1999)

Racionalidad científica: Para los efectos de la presente resolución, es la aplicación de criterios científicos en el diligenciamiento y registro de las acciones en salud brindadas a un usuario, de modo que evidencie en forma lógica, clara y completa, el procedimiento que se realizó en la investigación de las condiciones de salud del paciente, diagnóstico y plan de manejo. (Resolución 1995, 1999)

Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley. (Resolución 1995, 1999)

Seguridad de la información y seguridad digital: Los actores que traten información en el marco del presente título deberán establecer un plan de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, para lo cual establecerán una estrategia a través de la cual deberán realizar periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deberán contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo mediante la adopción de los lineamientos para la administración de la seguridad de la información y la seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones o quien haga sus veces. Lo anterior, incluyendo lo señalado por la Ley 1581 de 2012 de Hábeas Data y Ley 527 de 1999 de Comercio Electrónico, o las normas que las modifiquen, sustituyan o complementen.(Ley 2015, 2020)

Oportunidad: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio. (Resolución 1995, 1999)

Comprendiendo la información como un activo importante para el Instituto, esta necesita ser debidamente protegida, validada y verificada mediante procedimientos de confirmación y verificación que permitan aportar la evidencia objetiva de que se han cumplido los requisitos para su uso o aplicación, además de garantizar la seguridad de los datos requeridos para el seguimiento de las mediciones de indicadores institucionales.

Como parte de la mejora continua, se establecen mecanismos de control a través de la gestión de los riesgos, realizando seguimiento a los procesos y actividades con el objetivo de disminuir la probabilidad de materialización de estos.

4. Justificación

El ICSN - Clínica Montserrat como institución prestadora de servicios de salud para pacientes con enfermedad mental, docencia e investigación busca mejorar sus procesos, atención y la experiencia de los usuarios, con el fin de garantizar el cumplimiento de los requisitos que permitan la alta calidad durante la prestación del servicio; a través del fortalecimiento de los procesos organizacionales y mediante la estructuración del sistema de gestión de la seguridad de la información. Incrementando así el nivel de seguridad en la información con la que se cuenta y evaluar los riesgos con el objetivo de mitigar la materialización de estos.

La seguridad de la información implica la aplicación y la gestión de los controles apropiados donde se evalúan las amenazas, con el objetivo de asegurar el éxito institucional de manera sostenida, así como su continuidad, minimizando las consecuencias de los incidentes de la seguridad de la información.(Instituto Colombiano de Normas Técnicas y Certificación ICONTEC, 2013)

La estructuración del sistema de seguridad de la información permitirá establecer, implementar, monitorear, verificar y gestionar la seguridad de la información para el contexto interno y externo de la organización, generando confianza a las partes interesadas y demás procesos que requieren de la seguridad en la información.

Adicionalmente favorecerá en el cumplimiento de los requerimientos normativos evitando afectaciones a los recursos financieros por sanciones asociadas con la pérdida de información y vulneración de los datos, además asegurará que los

datos clínicos y registros de la atención cuenten con validez, sean confiables y pertinentes, favoreciendo el dato analítico para una adecuada toma de decisiones en los diferentes niveles de la organización, contribuyendo a la imagen corporativa y la reputación institucional.

El direccionamiento y la estructuración del sistema de seguridad de la información, favorecerá el aumento de la calidad y la eficiencia de los servicios de salud en las modalidades de atención ofertadas por el instituto mejorando la atención de los pacientes, garantizando la protección de los derechos a la privacidad y confidencialidad de su información, así como la seguridad, el control en el acceso y el uso de los datos clínicos, que permiten mantener la seguridad del paciente mediante la actualización de los métodos de custodia de información. (Antomás & Huarte del Barrio, 2011)

Identificar riesgos y oportunidades para los proveedores que intervienen en el sistema de seguridad de la información, permitiendo las mejoras contractuales (renovación de contratos, prórrogas de contrato).

Asegurar a través del plan de educación, sensibilización y concientización sobre la utilización de las tecnologías de la información como herramienta para el tratamiento adecuado de los datos, permitiendo así garantizar su confidencialidad, salvaguarda y el análisis confiable para la atención del paciente.

5. Formulación de objetivo general y objetivos específicos

5.1. Objetivo general.

Direccionar y estructurar un sistema de gestión basado en los requisitos de la norma técnica colombiana NTC ISO 27001:2013, articulado con el sistema de gestión de la calidad actual, que permita establecer, implementar, monitorear, verificar y gestionar la mejora continua de los sistemas de información, asegurando la confidencialidad e integridad de los datos para los procesos de la organización.

5.2. Objetivos específicos.

1. Determinar las vulnerabilidades del sistema de información bajo los requisitos de la norma técnica colombiana NTC ISO 27001:2013, a través del diagnóstico e identificación de las brechas que no permiten garantizar la seguridad de la información.
2. Proponer la planificación del SGSI con base en las vulnerabilidades y capacidades de la organización a partir de los resultados obtenidos en la aplicación de la evaluación diagnóstica.
3. Determinar acciones de verificación para las actividades propuestas.

4.

6. Alcance

Direccionar y estructurar el sistema de gestión de seguridad de la información basado en la norma técnica colombiana NTC ISO 27001:2013, permitirá brindar un diagnóstico de vulnerabilidades a la institución y así poder documentar la estructura general, recursos, procesos, procedimientos y las herramientas para implementar el sistema de seguridad de la información como parte de los proyectos de gestión futuros.

Esto permitirá contribuir en el mantenimiento y mejora de la prestación de servicios asistenciales, de docencia e investigación, garantizando el cumplimiento de la ley de protección de datos, el manejo de la historia clínica y lo relacionado con el control, seguimiento y vigilancia de medicamentos monopolio del estado.

El alcance de este proyecto de investigación, se encuentra enfocado bajo la norma técnica colombiana NTC ISO 27001:2013, hacia las partes interesadas de la institución como entes de control, clientes externos y clientes internos; además está definido para todos los procesos de la sede principal ubicada en la CL 134 17 71, en la localidad de Usaquén y para la sede integrada en red que se encuentra en el Km 6 vía suba Cota vereda chorrillos. Su ejecución corresponde a diez meses, comprendidos entre el mes de octubre del año 2021 y el mes de junio del año 2022.

7. Metodologías y acciones

Tabla 1 *Metodologías y acciones*

OBJETIVO ESPECÍFICO	ESTRATEGIA METODOLÓGICA	ACCIONES	OBSERVACIONES /ENTREGABLES
Determinar a través de un diagnóstico las vulnerabilidades del sistema de información bajo los requisitos de la norma técnica colombiana NTC ISO 27001:2013, para identificar las brechas que no permiten garantizar la seguridad de la información.	- Aplicación del cuestionario de diagnóstico, mediante una encuesta.	- Adecuación del instrumento diagnóstico. - Seleccionar el recurso humano para aplicación del instrumento. - Aplicación de la herramienta de diagnóstico para evaluación de brechas 27001:2013, para evaluar los requisitos e identificar los recursos necesarios para la estructuración del SGSI. - Elaboración del informe de los resultados de la aplicación de la encuesta.	Informe con el análisis de los resultados.
Proponer la planificación del SGSI con base en las vulnerabilidades y capacidades de la organización a partir de los resultados obtenidos en la aplicación de la evaluación diagnóstica.	- Mediante entrevistas y mesas de trabajo. - Mesas de Trabajo - Grupos focales - Talleres (lluvia de ideas)	- Plantear el tema, desarrollo de la reunión y generar conclusiones.	- Caracterización del Procesos - Política de seguridad de la información - Manual de seguridad de la información - Normograma - Matriz de Riesgos - Mapa de procesos con integración de TIC´S

Determinar acciones de verificación para las actividades propuestas.	- Encuestas	- Comparación de los resultados de aplicación de herramientas diagnósticas. - Informe de hallazgos identificados después de los resultados obtenidos en la aplicación del instrumento.	- Comparación de los resultados e Informe final.

8. Cronograma

El cronograma de actividades establecidas para el desarrollo del proyecto se ejecutó entre el mes de octubre del año 2021 y el mes de junio del año 2022.

Las actividades y documentos entregables determinados se desarrollaron y alinearon a lo definido en las cuatro (4) fases para la implementación del SGSI (planificación, direccionamiento, aplicación, evaluación y mejora), no obstante, las fases de aplicación, evaluación y mejora no fueron aplicadas atendiendo que el alcance del proyecto de investigación se encuentra establecido para el direccionamiento y estructuración del sistema de gestión de seguridad de la información bajo el conocimiento de la NTC ISO 27001:2013.

Tabla 2 *Cronograma actividades segundo semestre 2021*

CRONOGRAMA ACTIVIDADES SEGUNDO SEMESTRE 2021																
ETAPA	**ACTIVIDADES**	**RESPONSABLE**	**RESULTADO/ ENTREGABLE**	**oct-21**				**nov-21**				**dic-21**				
				1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**5**
PLANIFICACIÓN DEL PROYECTO	Adecuación de la herramienta de diagnóstico para evaluación de brechas bajo norma NTC ISO 27001:2013, para evaluar los requisitos e identificar los recursos necesarios para la estructuración del SGSI.	María Victoria Alarcón Aponte Duvan Felipe García Rodríguez Carolina Isabel Pinzón Lesmes	Herramienta diagnóstica del Sistema de Gestión de la Seguridad de la Información con Base en el Modelo NTC ISO 27001:2013.		X	X										
	Aplicación de la herramienta de diagnóstico por medio de entrevistas a personas de la institución.		Herramienta diagnóstica diligenciada con información obtenida de encuestas aplicadas.				X									
	Tabulación de las encuestas aplicadas.		Herramienta diagnóstica con Información tabulada.					X								
	Análisis del diagnóstico de brechas.		Análisis de los resultados del diagnóstico aplicado del sistema de gestión.					X								
FASE DE DIRECCIONAMIENTO	Aplicación y análisis de matriz DOFA	María Victoria Alarcón Aponte Duvan Felipe García Rodríguez Carolina Isabel Pinzón Lesmes	Matriz DOFA.				X									
	Revisión y Análisis Documental.		Mapa de Procesos							X						
			Políticas de la calidad, seguridad de la información y objetivos de la seguridad de la información.				X									
FASE DE ESTRUCTURACIÓN	Definición de la estructura del proceso.	María Victoria Alarcón Aponte Duvan Felipe García Rodríguez Carolina Isabel Pinzón Lesmes	Caracterización del proceso de Tecnología de información y comunicaciones.									X				

Tabla 3 *Cronograma actividades primer semestre 2022*

CRONOGRAMA ACTIVIDADES PRIMER SEMESTRE 2022																										
ETAPA	ACTIVIDADES	RESPONSABLE	RESULTADO/ ENTREGABLE	feb-22				mar-22				abr-22					may-22				jun-22				
				1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	5
FASE ESTRUCTURACIÓN	Desarrollo de la fase documental para la gestión del proceso.	María Victoria Alarcón Aponte Duvan Felipe García Rodríguez Carolina Isabel Pinzón Lesmes	Manual de la gerencia de la información		X																				
	Evaluación cualitativa de vulnerabilidades y amenazas. .		Matriz de Riesgos, con evaluación de probabilidad e impacto y definición de controles. .		X																				
FASE APLICACIÓN	Aplicación de la herramienta de diagnóstico para evaluación de brechas bajo norma NTC ISO 27001:2013 después del desarrollo de la fase de Direccionamiento y Estructuración.	María Victoria Alarcón Aponte Duvan Felipe García Rodríguez Carolina Isabel Pinzón Lesmes	Herramienta diagnóstica diligenciada con tabulación de los datos contenidos.																X						
	Divulgación de los resultados del diagnóstico de brechas a la alta dirección.		Presentación de resultados del análisis de brechas mediante herramienta diagnóstica posterior a propuestas realizadas.																	X		X			

Como parte de los productos generados en los espacios académicos, específicamente para la fase de direccionamiento, se presenta la propuesta para la evaluación del contexto organizacional, la identificación de stakeholders, la actualización de la política de la calidad, los objetivos de calidad y el mapa de procesos que permiten proporcionar un alcance al sistema de gestión seguridad de la información.

Se evidencia que en la fase de aplicación se desarrollaron cambios en cuanto a la actividad final puesto que inicialmente se mencionaba realizar mesas de trabajo y aplicar un taller para definir la apropiación de la información dejando documentado el resultado actividades que se cambiaron por la aplicación nuevamente del diagnóstico del sistema de gestión de la información con base en el modelo NTC ISO 27001:2013 y la socialización del mismo a el instituto.

En relación con el desarrollo y completitud de las actividades relacionadas en el cronograma se puede evidenciar la ejecución de 10 de las 11 definidas, quedando pendiente por socializar los resultados del diagnóstico de brechas a la alta dirección. Esta actividad ha sido aplazada debido a la atención de compromisos adquiridos y programados con anterioridad en el Instituto, sin embargo, se cuenta con un nuevo agendamiento para la segunda semana del mes de junio de 2022.

A la fecha de entrega del proyecto de investigación el porcentaje global de ejecución de las actividades corresponde al 90%.

9. Resultados

Fase de Direccionamiento.

Comprensión de la organización, su contexto y su estado actual

El ICSN - Clínica Montserrat es una institución privada sin ánimo de lucro, fundada hace 70 años; dedicada a la prestación de servicios de atención en salud mental y psiquiatría, con enfoque de docencia e investigación. Cuenta con siete proyectos estratégicos direccionados al cumplimiento de la visión institucional.

Análisis del contexto

El análisis del contexto se realizó a través de la evaluación de los factores internos y externos a la organización mediante la aplicación de la matriz DOFA, identificando como fortalezas que contribuyen a la estructuración del sistema de seguridad de la información los procesos que se encuentran definidos, estructurados, implementados, medidos y mejorados, que se cuenta con un proceso de gestión del riesgo, en el marco del sistema de gestión de la calidad, bajo la certificación con la norma técnica colombiana NTC ISO 9001:2015, lo que permite tener una estructura organizada, garantizando el control de los procesos y la identificación de la mejora continua.

En cuanto al recurso humano se encontró que cuenta con un equipo de trabajo idóneo, con competencias formativas, que permiten dar respuesta a las necesidades de los procesos, además con estabilidad laboral que se representa en la baja rotación del personal.

En relación con la infraestructura, se cuenta con herramientas para el manejo de la información y la documentación que permiten tener un acceso controlado a ellas; además se identifican recursos como un data center para salvaguardar la información.

Desde el sistema de gestión documental se cuenta con la política de gestión de la tecnología, los manuales de gerencia de la información, políticas web, interno de políticas y procedimientos de tratamiento de datos, interno de políticas de seguridad de base de datos, protocolo de seguridad de historias clínicas electrónicas y protocolo de atención, además del mecanismo para asegurar que se acepta el tratamiento de datos en los procesos clínicos derivados de la atención médica.

Desde el aspecto financiero se considera una institución con solidez económica, con un presupuesto definido para cada uno de los procesos, lo que permite cumplir de una manera adecuada con las metas anuales propuestas.

Se identificaron como debilidades en el análisis que, en el mapa de procesos vigente para el año 2021, se encontraban las actividades de tecnología y telecomunicaciones como un subproceso, no permitiendo su identificación de manera transversal para el apoyo de las actividades de las demás áreas, a falta de autonomía incurriendo en fallos de seguridad de la información, errores en el desarrollo y/o la configuración de los formatos para el registro de los datos en cada una de las actividades y no contando con lineamientos del dato clínico desde la captura, que asegure su validez, confiabilidad, y pertinencia, lo que no permite una adecuada toma de decisiones en los diferentes niveles de la organización.

Existen fallas en la integridad y disponibilidad en la historia clínica, que puede repercutir en la continuidad del tratamiento y se evidenciaron debilidades en la seguridad para el acceso a las redes sociales, esto relacionado con incidente de seguridad de la información presentado en el año 2021.

Como oportunidades se encuentran a nivel tecnológico, la necesidad de adquirir una infraestructura tecnológica para el registro de datos de una manera precisa que permitan la disponibilidad e integridad de la información consultada; así como la posibilidad de fortalecer y mejorar los servicios habilitados como lo es la telemedicina, donde se requiere de avances en el sistema de información de la institución.

Los hallazgos identificados como amenazas se relacionan con los cambios en disposiciones legales para la prestación del servicio en el sector salud que requieran de modificación y mejoras en el proceso de seguridad de la información; así como en lo económico en cuanto al crecimiento en competencia directa de los servicios prestados y los cambios en las condiciones del mercado.

Desde el aspecto social, la situación actual de salud pública relacionada con la declaración de la emergencia sanitaria, hace que la institución avance en la implementación de herramientas tecnológicas para la continuidad de la operación

y aseguren que los procesos cuente con niveles de seguridad y accesos para prevenir los riesgos asociados a la prestación del servicio como por ejemplo, la falsificación de soportes de historia clínica (incapacidades), el robo de información a través de ataques cibernéticos, la ausencia de análisis de riesgos y vulnerabilidades bajo el sistema de seguridad de la información que predisponen a la materialización de los mismos.

Para las disposiciones legales existe la probabilidad de que se materialicen sanciones de tipo económicas y/o reputacionales por el incumplimiento de requisitos legales que afecten la prestación del servicio, de igual manera se pueden presentar afectaciones a nivel financiero al incurrir en pagos por omisión o inexactitud de la nómina, seguridad social o ser requeridos por la UGPP (Unidad de gestión pensional y parafiscales).

Contar con un diagnóstico del contexto permite identificar los aspectos claves a intervenir, además de integrarlos con el resultado de la matriz de diagnóstico para así poder abordar los aspectos relevantes y estructurar el sistema de seguridad de la información para la organización.

Tabla 4 *DOFA*

AL INTERIOR

FORTALEZAS	DEBILIDADES
Procesos ● Los procesos se encuentran definidos, estructurados, implementados, medidos y mejorados y cuentan con proceso de gestión de riesgo. ● Se tiene un sistema de gestión de calidad, con proceso de certificación que permite tener una estructura organizada, que garantiza el control de los procesos y la identificación de mejora continua. **Personas** ● Cuenta con recurso humano idóneo, con competencias formativas, que permiten dar respuesta a las necesidades en los procesos. ● Estabilidad laboral que se representa en la baja rotación de personal. **Infraestructura** ● Se cuenta con herramientas para el manejo de la información y la documentación que permiten un acceso controlado a ellas. ● La institución cuenta con un data center para salvaguardar la información. **Métodos** ● Se cuenta con programas, manuales, protocolos, procedimientos, instructivos, donde se define el funcionamiento de los procesos para la prestación de los servicios. **Financiero** ● Se considera una institución con solidez financiera. ● El plan financiero definido en la institución permite cumplir de una manera adecuada con las metas propuestas en el presupuesto anual.	**Procesos** ● En el mapa de procesos actual, se encuentran las actividades de tecnología y telecomunicaciones como un subproceso, no permitiendo su identificación de manera transversal para el apoyo de las actividades de las demás áreas. **Seguridad de la información** ● Errores en el desarrollo y/o la configuración de los formatos para el registro de los datos en cada una de las actividades. ● No se cuentan con lineamientos del dato clínico desde la captura, que asegure su validez, confiabilidad, y pertinencia, favoreciendo el desarrollo analítico para una adecuada toma de decisiones en los diferentes niveles de la organización. ● Existen fallas en la integridad y disponibilidad en la historia clínica, que puede repercutir en la continuidad del tratamiento. ● Se encuentran debilidades en la seguridad para el acceso a las redes sociales.

AL EXTERIOR	
OPORTUNIDADES	**AMENAZAS**
Político ● No se encuentran contempladas dentro de las estrategias financieras de la institución. **Tecnológico** ● Adquirir infraestructura tecnológica para el registro de datos de una manera precisa que permitan la disponibilidad e integridad de la información consultada. **Legal** ● Nuevos servicios bajo resolución de habilitación.	**Político** ● Cambios en disposiciones legales para la prestación del servicio en el sector salud. **Económico** ● Crecimiento en competencia directa de los servicios prestados. ● Cambios en las condiciones del mercado. **Social** ● Situación actual de salud pública, relacionada con emergencia sanitaria. **Tecnológico** ● Falsificación de soportes de historia clínica (incapacidades). ● Robo de información a través de ataques cibernéticos. ● Ausencia de análisis de riesgos y vulnerabilidades bajo sistema de seguridad de la información **Legal** ● Sanciones económicas y reputacionales por incumplimiento requisitos legales y afectación del servicio. ● Incurrir en pagos por omisión o inexactitud de la nómina y seguridad social o ser requeridos por UGPP.

Diagnóstico - análisis situacional.

Instrumento de evaluación diagnóstica

Con el objetivo de realizar la evaluación diagnóstica del sistema de seguridad de la información se adaptó la herramienta diagnóstica del sistema de gestión de calidad ISO 9001:2015 aportada por la institución de educación superior Universidad Santo Tomás, con los criterios de la NTC ISO 27001:2013, lo que permitió realizar una evaluación organizada y objetiva de cada uno de los requisitos para generar el diagnóstico del sistema de información.

Diagnóstico del sistema de gestión de la información

La verificación del sistema de gestión de la información se realizó por medio de la aplicación de la herramienta diagnóstica que contiene los criterios de evaluación de la NTC ISO 27001:2013, un total de 107 criterios a evaluar. Este instrumento fue resuelto por cuatro (4) funcionarios de la institución, vinculados a los procesos de subdirección docente asistencial, subdirección administrativa y financiera, gestión de calidad y tecnologías de la información y comunicaciones. Después de contar con los diagnósticos diligenciados se procede a la tabulación y el análisis de los datos obtenidos y como resultado se puede identificar que el nivel de madurez de la organización se encuentra clasificado en la categoría C: 41% al 60%, definida en la herramienta diagnostica, que a su vez indica que los resultados son consistentes y evidenciables. El promedio global de cumplimiento es del 55,51%.

Las brechas presentadas se han relacionado según se presentan en cada uno de los criterios de la norma evaluados y de acuerdo con el componente al que pertenece. Si bien el ICSN Clínica Montserrat cuenta con la implementación del sistema de gestión de calidad, se encontraron aspectos trazadores que al momento que se requiera estructurar el sistema de seguridad de la información a futuro, lo puede apalancar.

A continuación, se relacionan los resultados obtenidos para cada una de las preguntas dispuestas en el instrumento diagnóstico y que se basan en los criterios de evaluación de la norma NTC ISO 27001:2013, se ha definido un nivel de calificación que se describe así:

(1) No hay aproximación formal: Los resultados son impredecibles. Solo declaraciones informales.

(2) Aproximación reactiva: Basada en necesidades puntuales, problemas presentados o ejemplos.

(3) Sistema formal definido: Existe planificación, pero poca aplicación o resultados; hay documentación.

(4) Sistema formal estable: Procesos sistemáticos; se cumplen los objetivos. Hay realimentación.

(5) Mejora continua: Hay datos válidos de mejora; tendencias conocidas. Dominio de los procesos.

NS/NA: No sabe o no aplica.

Cada uno de los entrevistados calificaba el criterio de acuerdo con su conocimiento en el sistema de gestión de calidad actual y considerando que estos pueden dar alcance al sistema de seguridad de la información, ninguna de las preguntas contó con una calificación de NS/NA. Para el análisis de brechas se realiza mayor énfasis

El componente estratégico está definido por 41 criterios de la norma NTC 27001:2013 y obtuvo un porcentaje de cumplimiento global del 48,53%. Se encontraron brechas en los numerales 4.3. Determinación del alcance del sistema de gestión de seguridad de la información; 5.1. Liderazgo y compromiso; 5.2. Política; 6.2. Objetivos de la seguridad de la información y planes para lograrlos; 7.1. Recursos; 8.2. Valoración de riesgos de la seguridad de la información y 9.3. Revisión por la dirección.

Finalmente, para el componente humano se evaluaron los 14 criterios relacionados con la norma NTC 27001:2013 que lo conforman, arrojando como resultado un porcentaje de cumplimiento global del 68,57%. Las brechas de este componente se asocian a los numerales 5.3. Roles, responsabilidades y autoridades en la organización; 7.2. Competencias; 7.3. Toma de conciencia y 7.4. Comunicación.

Del componente humano se evaluaron los 14 criterios relacionados con la norma NTC 27001:2013 y arrojó como resultado un porcentaje de cumplimiento global del 68,57%. Las brechas de este componente se asocian a los numerales 5.3. Roles, responsabilidades y autoridades en la organización; 7.2. Competencias; 7.3. Toma de conciencia y 7.4. Comunicación.

Se identifica que no existe aproximación formal o en algunos casos la aproximación es reactiva en los aspectos relacionados al cumplimiento de los numerales normativos por no contar con un sistema de gestión de seguridad de la información.

Con base a las propuestas derivadas de la fase de direccionamiento y de estructuración desarrolladas en el proyecto de investigación, se realiza una nueva aplicación del diagnóstico para evaluar la disminución o cierre de las brechas que de identificaron en la evaluación inicial. El segundo del diagnóstico fue calificado por el equipo investigador, por lo que la muestra corresponde a uno (1), teniendo en cuenta los productos generados y como se relacionan directamente al sistema de gestión de seguridad de la información; los criterios similares con la norma NTC ISO 9001:2015 pueden ser homologados y se califica entre los niveles tres, cuatro y cinco. Los resultados de la segunda aplicación son los siguientes:

Componente estratégico, 41 criterios de la norma NTC 27001:2013 evaluados, cuyo porcentaje de cumplimiento es del 65,85%, se evidencia una mejora del 17,32% en comparación al resultado del primer diagnóstico, este se logra al definir las propuestas para el alcance, la definición del sistema de gestión de la seguridad de la información, política y objetivos de seguridad de la información y asignación de recursos. Las brechas identificadas en los numerales 8.2. Valoración de riesgo de la seguridad de la información y 9.3. Revisión por la dirección, se deben atender en fases posteriores.

Para el componente operativo, se evidencia un porcentaje de cumplimiento del 59,61%, encontrando un aumento porcentual del 2,11%, debido a que las brechas identificadas para los numerales 6.1.3 Tratamiento de riesgos y determinación de controles, 7.5.2 fueron tratadas por medio de la actualización documental del proceso al realizar la caracterización, matriz de riesgos, el manual de la seguridad de la información, matriz de comunicaciones dando cumplimiento a los requisitos de la NTC ISO 27001. Para el caso del numeral 7.5.3 a los documentos actualizados y creados se les asigna el código y numerales de acuerdo con el sistema de gestión documental establecido en la institución; en relación con el numeral 9.2. Auditoría interna, se actualizó el programa de auditorías internas donde se incluyó la auditoría que permitió la aplicación del análisis de brechas. Los numerales 10. Mejora y 10.1. No conformidades y acciones correctivas requieren de gestión en un nuevo ciclo. (véase Anexo D. Programa de Auditorias - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat)

Del componente humano se obtuvo un porcentaje de cumplimiento del 75,71%, por lo que los resultados son consistentes y sistémicos gracias a las estrategias implementadas en el instituto con el sistema de gestión actual, la actualización del mapa de procesos en el que se define el proceso Tecnologías de Información y comunicaciones permiten dar respuesta al numeral 7.2. Competencias, ya que se actualiza el perfil de cargo del jefe de TICS para incluir las competencias que permitan el manejo del sistema de seguridad de la información. En relación con el numeral 7.4. Comunicación, se actualizó la matriz de comunicaciones con la inclusión de temas relacionados con la seguridad de la información. (Véase Anexo E. Matriz de Comunicaciones - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat)

Como conclusión del comparativo de los análisis y con base a las propuestas realizadas, se encuentra una disminución de las brechas presentadas en cada uno de los componentes, lo que conlleva a un resultado global de cumplimiento del 65,04% y a la clasificación del instituto en la categoría D: Mejora continua demostrable.

El cierre total de las brechas puede darse al implementarse el sistema de seguridad de la información, dar cumplimiento a todos los requisitos normativos y desarrollar las fases de aplicación, evaluación y mejora, esta información se socializará con la alta dirección. (Véase Anexo F. Diagnóstico del Sistema de Gestión de la Información con Base en el Modelo ISO 270012013 - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat)

Determinación de tipos de clientes y requisitos CLIO.

La determinación de los clientes y los requisitos CLIO, se realizó mediante el conocimiento de los procesos institucionales para la definición de los stakeholders por cada uno de estos de la siguiente manera:

Tabla 5 *Identificación partes interesadas*

Partes interesadas	Proceso que identifica las necesidades y expectativas
Pacientes y familias.	• Servicios ambulatorios • Hospitalización • Seguridad del paciente • Sede integrada en red (Campoalegre)
Proveedores y Contratistas	• Subdirección administrativa y financiera • Apoyo logístico
Junta y Asamblea (Miembros)	• Gestión estratégica
Médicos Tratantes	• Subdirección docente asistencial
Colaboradores	• Talento humano • TICS • Gestión de calidad
Entes de control	• Gestión de calidad
Comunidad científica y Asociaciones	• Investigación
Comunidad	• Atención al usuario
Sector farmacéutico	• Servicio farmacéutico
Docentes, Universidades (Convenios docentes) Estudiantes	• Docencia

Se realizó una evaluación de los aspectos relevantes que se esperan de los servicios y/o de la organización por medio de la comparación de los atributos de calidad, los requisitos del cliente, legales, los inherentes a la organización y a los dispuesto en la norma técnica colombiana NTC ISO 27001:2013.

Tabla 6 *Tipos de clientes y condiciones o requisitos del servicio*

Clientes y/o partes interesadas	**Aspecto relevante que esperan del servicio y/o de la organización**	**Atributo/requisito**
Pacientes y familias	Acceder a los servicios de atención en salud mental, durante la prestación de estos recibir información relacionada con el tratamiento, manejo de las patologías y uso de medicamentos.	• Tratamiento oportuno. • Continuidad para el tratamiento. • Oportunidad en la prestación del servicio. • Pertinencia al recibir el tratamiento adecuado según patología. • Accesibilidad, permitir el uso de los servicios. • Seguridad para el paciente, minimizar los riesgos en la prestación del servicio. • Confidencialidad de la información. • Seguridad de sus datos.
Prestadores de servicios, proveedores y contratistas (Personas jurídicas)	Mantener relación contractual con el Instituto, recibiendo garantías de pago de los productos y servicios contratados.	• Continuidad, oportunidad, recibir garantía del producto o servicio contratado.
Universidades, Convenios docentes	Mantener relación docencia servicio con el instituto, a través de escenarios de práctica para desarrollar competencias	• Garantizar capacidad instalada para los escenarios de práctica convenidos. • Recibir gestión del

	en salud mental, investigación y procesos administrativos en salud, mediante la gestión de conocimiento.	conocimiento para los estudiantes de los programas de formación por recurso humano capacitado y con experiencia en el campo de salud mental y psiquiatría, así como en otras áreas de la salud y administrativas.
Entes regulatorios y aseguradores	Cumplimiento de la normatividad vigente para el sector; prestación de servicios del portafolio bajo los atributos de calidad en salud, generando bienestar a los usuarios, demostrar eficacia en los tratamientos, cumplimiento de la relación contractual, manejar menores costos.	• Vigilar, controlar, regular la prestación de los servicios en salud, de forma oportuna, de calidad.
Junta y Asamblea (Miembros)	Conseguir reconocimiento y estatus institucional en los campos de desarrollo, logrando ser una institución perdurable y cumplir la promesa de valor. Contar con infraestructura segura y acorde a las necesidades de la prestación del servicio.	• Mantener una institución con solidez financiera.
Tratantes	Servicios oportunos para sus pacientes, que se definan lineamientos	• Oportunidad y eficacia en los tratamientos instaurados a pacientes

	flexibles para su manejo, contar con un equipo humano idóneo que apoye sus labores terapéuticas.	con enfermedad mental.
Colaboradores	Estabilidad laboral, pago oportuno, contratación legal, cumplimiento de condiciones laborales, capacitación, remuneración y buen clima laboral.	• Recibir bienestar como empleados. • Seguridad durante la realización de sus funciones. • Continuidad en la relación laboral.
Estudiantes	Recibir gestión del conocimiento actualizado que les permita adquirir competencias para su formación profesional como proyecto personal, mediante asesoría y supervisión de prácticas; además de explorar el campo de la investigación.	• Oportunidad en la formación. • Seguridad durante la realización de prácticas formativas. • Continuidad en la realización de supervisión y asesorías.
Comunidad científica y asociaciones	A través del conocimiento, generar aportes e información a la comunidad para la atención en salud mental como parte de la responsabilidad social.	• Generar aportes a la comunidad científica para el abordaje y atención en salud mental y psiquiatría.
Comunidad	Recibir psicoeducación para aprender herramientas para el manejo de la enfermedad y conocer estrategias de identificación de crisis y cómo acceder a los servicios de salud.	• Accesibilidad a los servicios de salud mental y psiquiatría. • Recibir información pertinente para el manejo de la enfermedad mental.

Docentes	Que se garantice formación para adquirir competencias como docentes, generar oportunidad de investigación. Que se mantengan las relaciones docencia y servicio con el objetivo de formar nuevos profesionales en el área de la salud mental.	• Mantener convenios de docencia y servicio con las instituciones de educación superior. • Garantizar competencias en docencia

Gestión del cambio, comprensión de la Cultura de la organización.

La gestión del cambio se encuentra definido como proceso en el ICSN - Clínica Montserrat, este se realiza a través de la identificación de necesidades que puedan afectar la integridad del SGC como la eliminación y/o inclusión de nuevos procesos, nuevos productos, nuevos servicios, ampliación o disminución de mercado, cambio en la infraestructura (técnica, equipos), cambios en las plataformas tecnológicas, nuevos requisitos legales, etc. Cambios de contratistas, proveedores críticos, cambios que impacten en el SGC de las necesidades y expectativas de las partes interesadas; cambios en los manejos presupuestales ya establecidos, metodologías de control de cambio, definición de nuevas fuentes de ingreso; cambios de la estructura organizacional (organigrama) en las líneas de responsabilidad y autoridad, ascensos, reubicaciones de personal clave de la organización, así como los respectivos respaldos a esos cargos.(P. del C. Clínica Montserrat, 2018)

Este proceso de gestión del cambio organizacional ha tenido adherencia en el sistema de gestión de calidad en el instituto como resultado de la transformación cultural, proceso con avances significativos debido a la definición de competencias organizacionales y comportamientos esperados determinados según los niveles de responsabilidad en la estructura organizacional, utilizando estrategias de comunicación que permiten la apropiación de los conceptos y la adherencia en los procesos del sistema de gestión.

Sensibilización con principios de la gestión de la calidad.

La sensibilización en el sistema de gestión de calidad del ICSN - Clínica Montserrat, es un proceso que está asociado a las estrategias de comunicación definidas desde el Plan Estratégico de Comunicaciones Organizacionales en Salud (PECOS), que corresponde a la metodología de comunicaciones institucional establecida de acuerdo con las necesidades y expectativas de las partes interesadas identificadas en el marco de la planeación estratégica que realizan con frecuencia anual. Las actividades documentadas están enfocadas a los procesos de aprendizaje y apropiación de la información, a través de mecanismos lúdicos dirigidos con enfoque al cliente.

Otro de los mecanismos implementados corresponde a las actividades de mejoramiento institucional, donde se resalta el proceso de comunicación efectiva que incluye mecanismos de comunicación de doble vía en el instituto en busca del desarrollo y el fortalecimiento del liderazgo por parte de los líderes de proceso, donde se promueve su colaboración y el empoderamiento desde las unidades funcionales.

Desde estos niveles de mejoramiento institucional también se realiza la evaluación de los resultados de la interrelación entre los procesos, con el fin de lograr la consecución de los objetivos organizacionales permitiendo así generar la mejora como premisa fundamental para el instituto, promoviendo la toma de decisiones basadas en el análisis de los resultados.

Finalmente se han mejorado los espacios de relación con las demás partes interesadas, lo que ha permitido la integración para la construcción y aportes en el mejoramiento continuo de los procesos organizacionales.

Estrategia Organizacional precisar y alinear el SIG: alcance - política – objetivos - mapa de procesos - despliegue de objetivos a procesos. BSC (Indicadores clave)

Política de la calidad.

La revisión de la política de la calidad se realizó con base al direccionamiento estratégico de la institución, identificando que está enfocada al sistema de gestión bajo la norma NTC ISO 9001:2015, actualmente certificado; siendo esta una limitante para la implementación de otros sistemas de gestión, como lo es el objetivo de la propuesta del presente proyecto de investigación desde el direccionamiento y estructuración del sistema de gestión de la seguridad de la información según la norma NTC ISO 27001:2013.

Se define como propuesta la siguiente política de la calidad:

El INSTITUTO COLOMBIANO DEL SISTEMA NERVIOSO - CLÍNICA MONTSERRAT, se compromete a trabajar basado en la evidencia científica con las prácticas más seguras y sostenibles que garanticen el trato humanizado, la calidad de vida de sus usuarios, el cumplimiento de la normatividad en la prestación de sus servicios de salud mental, docencia e investigación; para lo cual, cuenta con recursos tecnológicos, científicos y humanos idóneos, que actúan para la mejora continua de su sistema integrado de gestión.

Así mismo, al realizar la evaluación de la plataforma estratégica y las necesidades y expectativas de las partes interesadas, se propone la política de seguridad de la información, donde se incluyen los objetivos de la seguridad de la información, los compromisos para el cumplimiento de requisitos aplicables y de mejoramiento continuo de este sistema.

Como propuesta de la política de seguridad de la información, se define lo siguiente:

El ICSN - CLÍNICA MONTSERRAT, se compromete a garantizar el cumplimiento de la normatividad en la prestación de sus servicios de salud mental, docencia e investigación, a través de la gestión de los niveles adecuados para la integridad, confidencialidad y disponibilidad de la información, preservando los derechos de las partes interesadas en la custodia y salvaguarda de la misma; para lo cual, cuenta con recursos tecnológicos, científicos y humanos idóneos, que actúan para la mejora continua de su sistema integrado de gestión.

Objetivos de la política de seguridad de la información.

Posterior a la revisión de la política de la calidad, y la propuesta de la política de la seguridad de la información, se realizó la redacción de los objetivos de donde se incluye la integración de los sistemas de gestión y que permitan evaluar su cumplimiento:

- Mantener el cumplimiento de los requisitos aplicables a la organización.
- Lograr que, a través de la metodología de administración integral del riesgo, se identifiquen todos los controles para abordar los asociados a la seguridad de la información.
- Lograr la integridad, confidencialidad y disponibilidad a través de la implementación de la norma NTC-ISO 27001:2013.
- Aumentar la competencia del personal requerido para la estructuración del sistema de seguridad de la información.
- Mantener los recursos necesarios para la gestión, administración, prestación y mantenimiento del sistema de seguridad de la información.

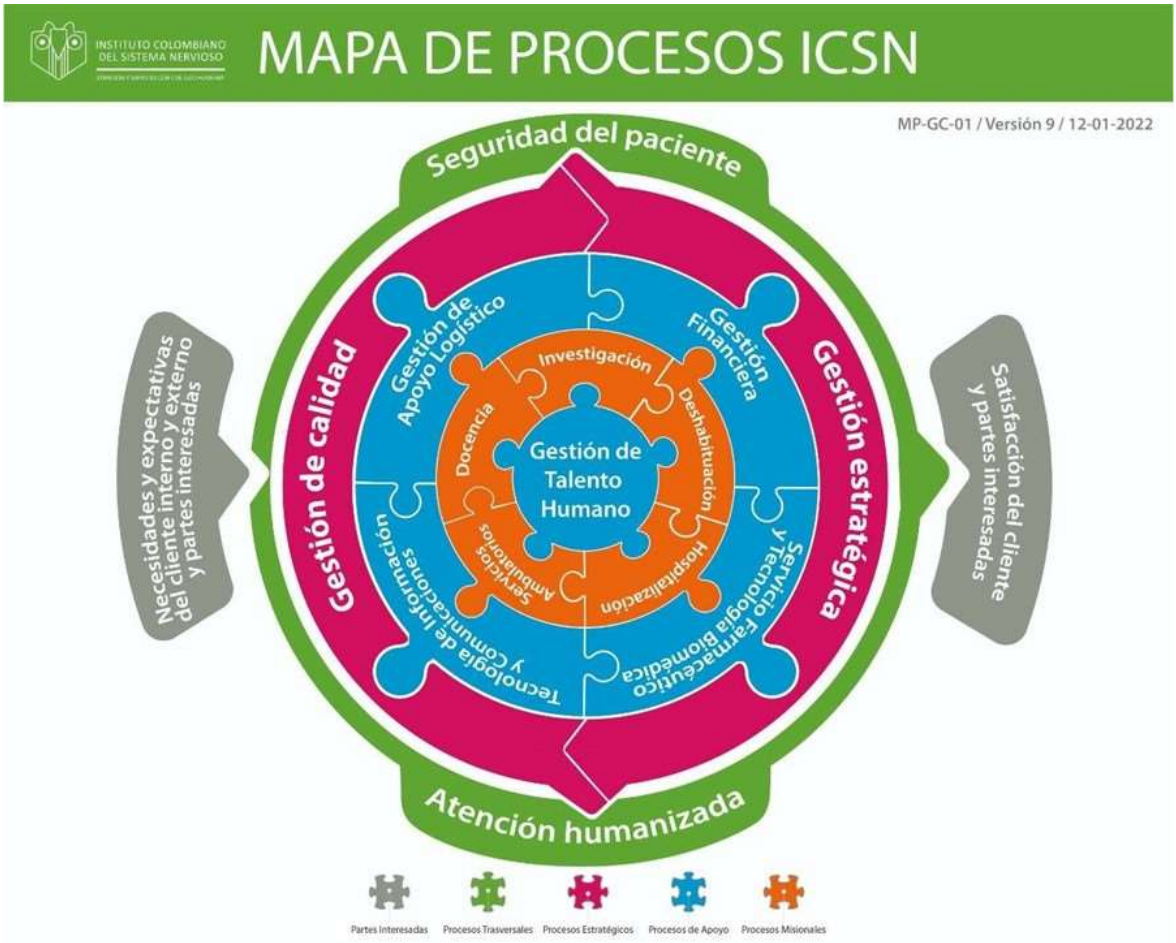
- Lograr el mejoramiento continuo del sistema integrado de gestión de la Institución.

Mapa de procesos.

Se realizó revisión del mapa de procesos, en donde se encontraban definidos doce procesos organizados así: **Procesos estratégicos:** Gestión estratégica y Gestión de calidad; **Procesos Misionales:** Hospitalización, Deshabituación, Consulta, Docencia, Investigación, Seguridad del paciente; **Procesos de apoyo:** Gestión del talento humano, Gestión Financiera, Apoyo logístico, Servicio farmacéutico, sin contar con el proceso de tecnologías de la información, ya que se encontraba como un subproceso de gestión estratégica.

Posterior a la revisión y al ejercicio de referenciación virtual, en consonancia con el modelo de acreditación en salud en el que se enfoca el Instituto, se propuso un modelado de procesos de tipo colaborativo que permite su interrelación, definiendo dentro de los procesos de apoyo el proceso de Tecnologías de información y comunicaciones, con el objetivo de generar impacto como cadena de valor en la prestación de servicios, además de poder orientar el sistema de seguridad de la información el en Instituto.

Figura 1 *Mapa de procesos, Versión 9 12/01/2022.*



Las propuestas realizadas como resultado del desarrollo de los espacios académicos del primer semestre de la especialización de dirección y gerencia de la calidad, fueron presentadas a la alta gerencia del ICSN-Clínica Montserrat en el mes de diciembre del año 2021, siendo tenidos en cuenta durante el desarrollo de la planeación estratégica institucional en enero de 2022; a la fecha las propuestas presentadas, fueron aprobadas e implementadas, permitiendo que los productos generados durante la especialización, favorecieron en la gestión de la innovación empresarial como resultado del programa académico

Indicadores del BSC.

Dentro de los indicadores del balance scorecard del instituto se propone incluir dos, relacionados con el proceso de tecnologías de información que se encuentran enfocados a la seguridad de la información; estos corresponden a *cobertura de la historia clínica electrónica en servicios* y *plan de contingencia por caídas del sistema de información*.

La cobertura de la historia clínica electrónica en servicios, permitirá realizar la medición del número de registros encaminados a la búsqueda de la integridad, disponibilidad y confidencialidad de la información, con el objetivo de asegurar procesos electrónicos que disminuyan el uso de registros físicos en los que se tengan procesos manuales que vayan en contravía de los pilares de la seguridad de la información, además esto con el objetivo de utilizar de forma óptima la herramienta de historia clínica electrónica con la que cuenta la institución.

El plan de contingencia por caídas del sistema de información, corresponde a otro de los indicadores propuestos para la inclusión en el BSC, esto con el fin de evaluar la oportunidad de respuesta a las situaciones en las que se ponga en riesgo la disponibilidad de la información por fallos o afectaciones como ataques cibernéticos al sistema electrónico de historia clínica, permitiendo identificar factores de riesgo que se puedan mitigar para futuras ocasiones en las que se pueda materializar el riesgo de caídas del sistema de información y así definir las acciones para abordar los riesgos.

Identificar y valorar los riesgos del SGI

Matriz de riesgos.

El Instituto Colombiano Del Sistema Nervioso Clínica Montserrat cuenta con un manual de gestión de riesgo código MN-SO-02, donde se encuentra definida la metodología de análisis y evaluación de los riesgos que se describe a continuación:

Análisis de riesgos.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados: Probabilidad e Impacto.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

Tabla 7 *Análisis de Probabilidad*

PROBABILIDAD

Improbable	Es casi imposible que ocurra. Puede ocurrir en circunstancias excepcionales.
Remota	Baja probabilidad de ocurrencia. Es poco probable que ocurra, pero es posible.
Ocasional	Mediana probabilidad de ocurrencia. Es probable que ocurra algunas veces
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias
Altamente Probable	Se espera que el evento ocurra en la Mayoría de las circunstancias

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Tabla 8 *Análisis de Impacto*

IMPACTO	
Insignificante	Insignificante: Requiere de intervención, pero no afecta el proceso ni el cumplimiento del objetivo.
Menor	Menor: Se dificulta o retrasa el cumplimiento del objetivo, aunque es posible ejecutar el proceso como estaba diseñado.
Moderada	Moderado: Se dificulta o retrasa el cumplimiento del objetivo, aunque es posible ejecutar el proceso como estaba diseñado.
Mayor	Mayor: Se afecta el cumplimiento del objetivo (aunque se logra), requiriendo un cambio o modificación en el proceso.
Catastrófica	Catastrófico: No es posible cumplir con el objetivo definido.

Evaluación del riesgo.

De acuerdo con la calificación que se le otorga al riesgo según su probabilidad por impacto este riesgo se clasifica en una matriz de calor calificándolo según la

escala de Aceptable, Tolerable, Inaceptable o Inadmisible, siendo estos inadmisibles los riegos que por decisión estratégica deberán contar con controles sin que esto exima de asignar controles a los demás riesgos de la matriz.

Si se presenta alguna acción de mejora identificada como corrección y el riesgo no ha sido identificado, la matriz del proceso debe ser actualizada, al igual que si se presenta una acción correctiva o de mejora este debe ser actualizado de la misma forma.

Figura 2 *Evaluación de Probabilidad e Impacto.*

Fuente: Manual de gestión del riesgo MN-SO-02 10-09-2021 versión vigente número 3.

- Teniendo en cuenta la metodología de análisis y evaluación de los riesgos en el ICSN Clínica Montserrat y como parte del proyecto de investigación, se propusieron dieciséis riesgos para el proceso de tecnología de información y comunicaciones - TICS, de los cuales quince se encuentran enfocados específicamente a los pilares de seguridad de la información definidos en la NTC 27001:2013; de acuerdo a la evaluación del riesgo, cinco de estos fueron calificados como inadmisibles, ocho inaceptables y dos tolerables; generando adicionalmente controles para cada uno de estos riesgos. (Véase Anexo G. Matriz de Riesgos de TIC - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat).

Descripción de los controles.

Con base a los 16 riesgos identificados y propuestos para el proceso de TIC, se establecen diferentes controles que puedan ayudar al ICSN - Clínica Montserrat a eliminar, prevenir o mitigar los riesgos, a continuación, se describen las actividades descritas en los controles:

- Definir proveedores críticos y no críticos para la operación del instituto: con este control se busca definir los proveedores que tiene gran impacto para el proceso de TIC, garantizando la disponibilidad, custodia y salvaguarda de la documentación, también se debe realizar una evaluación y reevaluación para todos los proveedores de la institución.
- Gestionar conocimiento sobre el uso adecuado de las plataformas tecnológicas: para el ICSN - Clínica Montserrat es importante divulgar y dar a conocer el uso de sus herramientas tecnológicas en los diferentes niveles organizacionales, por lo cual se debe trabajar en los instructivos que permitan documentar el uso de estas para cada una de las actividades de los procesos.
- El instituto debe contar con procedimientos que estén enfocados en la confidencialidad y salvaguarda de la documentación en los diferentes niveles organizacionales, garantizando la integridad y administración de estos, además debe divulgar su matriz de comunicaciones para dar a conocer el proceso a seguir en caso de solicitudes o requerimientos entre procesos o clientes internos o externos.
- Asegurar el mantenimiento preventivo de los equipos, el soporte de redes y la realización de las copias de seguridad correspondientes, evitando fallas operativas en los recursos tecnológicos del instituto.
- Se debe implementar política y procesos que favorezcan la preservación, confidencialidad e integridad de la información dentro del instituto, la cual debe ser divulgada a las partes interesadas.
- Se debe mejorar los canales de comunicación actual garantizando la respuesta eficiente a las solicitudes de los clientes internos y externos, logrando medir la oportunidad de respuesta para la mejora continua.

Lograr el compromiso de la alta dirección, beneficios/costos.

La alta dirección se encuentra comprometida con el sistema de gestión de calidad y con el mejoramiento continuo institucional, ya que ha encontrado resultados de gestión para el instituto, así como los procesos enfocados a la asistencia, docencia e investigación, lo que ha generado impacto en los procesos de atención brindando beneficios a sus clientes internos y externos.

Además de estos beneficios, como parte de los procesos de mejoramiento ha generado estrategias de disminución de costos y control de gastos, lo que ha

permitido en el último año tener un excedente del 78% en comparación al año 2021, valor histórico reconocido en el proceso de acreditación en salud como fortaleza, dinero que se dispone para reinversión de los proyectos institucionales.

Para el caso del direccionamiento y estructuración de la norma NTC ISO 20071:2013, se ha contado con el apoyo de la alta dirección en el desarrollo de cada una de las fases, comprendiendo esta mejora como un avance en la gestión del sistema que permitirá fortalecer los procesos y mitigar los riesgos a los que se ve expuesto el instituto al no cumplir con los requisitos básicos de la seguridad de la información.

Definir equipos de trabajo y elaborar el plan de implementación operacional

Desde la estructura organizacional se cuenta con un equipo de trabajo, de personas que conforman el área de tecnología de información y comunicaciones, liderado por un Ingeniero de sistemas que ocupa la Jefatura de TICS y dos personas como recurso humano operativo del proceso. Al realizar la propuesta de la estructuración del área como un proceso de apoyo, no se requiere realizar ninguna modificación en el recurso humano ya que desde el organigrama se encuentra definido este personal.

Existen manuales de funciones claros y estructurados, donde se visualizan las responsabilidades con los sistemas de información institucional y para el caso del proyecto de investigación con la seguridad de la información.

Fase de Estructuración.

Análisis y modelación de los procesos y de sus interacciones

Caracterización del proceso

Teniendo definido Tecnologías de Información y Comunicaciones - TICS desde el mapa de procesos como un proceso de apoyo, se realizó actualización de la caracterización donde se definen las entradas, las actividades y las salidas del proceso, siendo esta una herramienta que facilita la descripción del proceso y los elementos que permitirán la gestión y control en la confidencialidad, integridad y disponibilidad continua de la información. (Véase Anexo H. Caracterización del Proceso de TIC - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat)

Identificar requisitos de los procesos: productos, aspectos legales, identificar riesgos de los procesos

Realizada la evaluación del contexto institucional, se identificaron oportunidades enfocadas al sistema de seguridad de la información como lo son aquellas relacionadas con la infraestructura de tecnologías de información y comunicación que cumplen con las necesidades para el acceso a los servicios y el incremento en la demanda de servicios de salud mental.

Dentro de las amenazas se identificaron los cambios normativos y los equipos informáticos actualizados y estrategias de transformación digital en salud que no se encuentran inmersas en los proyectos institucionales.

Uno de los mecanismos contemplados para abordar los riesgos, se trata del proyecto de investigación orientado al direccionamiento y estructuración del sistema de gestión de la seguridad de la información, lo que permitirá tener una aproximación al cumplimiento normativo y un análisis diagnóstico para una futura integración al sistema de gestión institucional.

Definir y controlar la información documentada requerida por los procesos con criterios de riesgos y conocimiento.

La gestión documental se realiza desde el sistema de gestión integral Almera, con la parametrización de los documentos del sistema de gestión, donde se han generado códigos para identificar los, programas, manuales, protocolos, procedimientos, instructivos, las caracterizaciones de los procesos, indicadores y formatos de cada uno de los procesos, mecanismo transversal para la gestión documental.

El proceso de tecnologías de información se encuentra en la línea de los procesos de apoyo de la institución, los demás documentos que se creen para el proceso contarán con la siguiente codificación y se asignará número consecutivo: **Manual** MN-TI-XX, **Programa** PG-TI-XX, **Protocolo** PT-TI-XX, **Procedimiento** PR-TI-XX, **Instructivo** IN-TI-XX, **Caracterización** CR-TI-XX, **Indicador** ID-TI-XX, siguiendo los criterios de gestión documental del sistema de gestión del ICSN - Clínica Montserrat.

Se documentó una propuesta de manual de la información con el objetivo de lograr la integración de la información clínica y administrativa para su uso en la toma de decisiones en cualquier nivel de la organización, además de integrar estrategias y mecanismos para garantizar la seguridad, confidencialidad y disponibilidad de la información, su mejoramiento y su ubicación centralizada. (Véase Anexo I. Manual de la Gerencia de la Información - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat)

Control operacional, Indicadores de gestión de los procesos ¿cuáles datos recopilar?

Desde la definición de la caracterización del proceso de tecnología de información y comunicaciones, se determinaron los requisitos, los recursos y los mecanismos de control operacional aplicables durante su ejecución, con el objetivo de lograr conformidad en el proceso.

Como indicadores de gestión del proceso de TICS orientados al control de proceso relacionados con el sistema de seguridad de la información, se proponen los siguientes:

- Cobertura de la Historia Clínica electrónica en registros
- Cumplimiento de Cronograma Mantenimiento Preventivo - Equipos de cómputo
- Eventos relacionados con violación de la confidencialidad en la información
- Horas de parada Equipos de cómputo
- Número de horas de no disponibilidad en los sistemas de información
- Porcentaje de cumplimiento de mantenimientos correctivos
- Quejas relacionadas con la Confidencialidad
- Proporción de Backups Funcionales
- Recuperación de información

(Véase Anexo J. Fichas técnicas Indicadores - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat)

Asignar los recursos para implementar el SIG y para aumentar la satisfacción de los clientes

Se realizó entrevista a la subdirectora administrativa y financiera del ICSN - Clínica Montserrat, quien nos permitió conocer el mecanismo para la designación de recursos encontrando que, anualmente se realiza una revisión de las cifras relevantes tanto internas como externas que puedan afectar el desempeño económico del instituto, como lo son las siguientes:

Cifras internas:

• Estados Financieros del año en curso y del año anterior.

• Ejecución presupuestal del año en curso y del anterior.

• Proyectos planeados y recomendados por dirección y junta directiva a corto y mediano plazo.

• Recomendaciones descritas en la revisión por la dirección y aquellas del comité económico del instituto.

Cifras externas:

• Indicadores macroeconómicos

• IPC generales y del sector.

• Tendencias del mercado y del sector salud en lo relacionado a salud mental.

• Oportunidades del mercado en nuevos productos y servicios.

Entre los meses de octubre y noviembre se elaboran los primeros borradores de presupuesto en los que se incluyen las diferentes variables que los pueden afectar en el año siguiente, labor que se realiza desde el área financiera con los soportes e informes de ejecuciones del año y demás datos contables.

Este primer borrador de presupuesto es presentado por la subdirección administrativa y financiera a la dirección, donde se genera un espacio de análisis y debate sobre las cifras globales (ingresos y egresos totales, excedentes totales) lo que permite llegar a la definición de una cifra general para aprobación del director.

La cifra aprobada por la dirección general es debatida y socializada por las áreas quienes pueden argumentar cambios internos, es decir, en valores que componen la cifra global, pero sin modificar esta. Es importante resaltar que los presupuestos deben tener en cuenta la participación de los líderes de proceso, pero es la dirección y la junta directiva quienes toman las decisiones de las cifras y montos asignados, esta labor de socialización ocurre en el mes de noviembre, quedando lista para la primera semana de diciembre.

La dirección general verifica las cifras y analiza las últimas ejecuciones para presentar en junta directiva quien aprueba el presupuesto a ejecutar y controlar en el siguiente año.

Teniendo en cuenta que como parte del sistema de gestión de calidad implementado bajo la norma NTC ISO 9001:2015, cómo se define en el numeral 4.4 Sistema de gestión de calidad y sus procesos; 4.4.1 literal d, y el numeral 5. Liderazgo, 5.1.; se identifica que se determinan los recursos necesarios para el sistema de gestión de calidad y se aseguran de su disponibilidad, durante el proceso de entrevista se pudo evidenciar que para el sistema de gestión de calidad existe un rubro presupuestado para el año 2022 de $106.900.000 millones de pesos.

Como parte de las propuestas del proyecto de investigación se encuentra la ampliación del alcance del sistema de gestión de calidad a un sistema integral de

gestión, con el objetivo de implementar el sistema de seguridad de la información si así lo decidiera el instituto, se considera que el presupuesto asignado para este año al sistema de gestión de calidad permite la implementación del direccionamiento y estructuración del SGSI en caso de ser aprobado.

El proceso de tecnología de la información, como se describe en el artículo **(How to Budget an ISO 27001 Implementation Project)**, cuenta con asignación de presupuesto para el año 2022 con un rubro de $162.200.000, lo que permite dar cobertura en parte al cumplimiento de los pilares de seguridad de la información, esto como fortaleza asociada a los avances por la implementación del sistema de gestión de calidad bajo la norma NTC ISO 9001:2015; este valor se encuentra presupuestado para los sistemas de información y las licencias de seguridad con el proveedor SilverIT, sin embargo para la implementación del sistema de seguridad de la información se requiere re realizar un costeo más detallado de acuerdo a los requerimientos del sistema. (27001 Academy, 2016)

Costos de personal: Costos relacionados con el trabajo de las personas internas involucradas con el proyecto (a tiempo completo u ocasionalmente), considerando el número de horas de trabajo requeridas y las tarifas por hora. (27001 Academy, 2016)

Los costos de materiales: Costos relacionados con equipos, herramientas, instalaciones, documentos, software y similares necesarios para realizar el trabajo, considerando condiciones de arrendamiento, alquiler, compra y precio del artículo. (27001 Academy, 2016)

Costos del proveedor: Costos relacionados con los contratistas regulares de la organización (p. ej., proveedores de equipos de TI, servicios de transporte y otros que ya trabajan con la organización antes de que comience el proyecto) que estarán involucrados en el proyecto, considerando el número de horas de trabajo requeridas y la situación contractual. (27001 Academy, 2016)

Costos del servicio: Costos relacionados con capacitaciones externas, consultoría y servicios de certificación necesarios para respaldar el proyecto, considerando los beneficios de obtener asistencia externa, el precio del servicio y la frecuencia de uso. Tenga en cuenta que algunos de estos costos pueden volverse permanentes (p. ej., servicios de certificación y capacitaciones específicas sobre gestión de riesgos y asuntos legales). (27001 Academy, 2016)

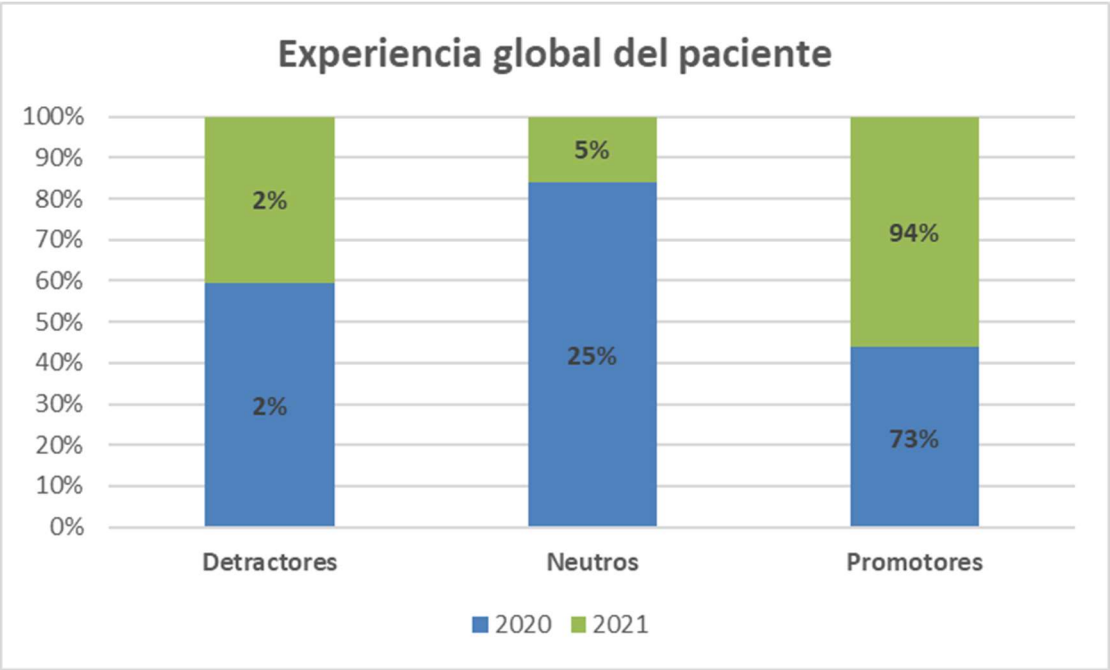
Costes de riesgos: Costos relacionados con la implementación de controles para prevenir o minimizar las pérdidas del proyecto con respecto a la realización de riesgos, como que un miembro del equipo del proyecto abandone el proyecto u organización, la pérdida de una computadora portátil, la repetición del trabajo en un entregable, retrasos en las actividades, etc. (27001 Academy, 2016)

La asignación de recursos para el sistema de gestión de calidad a lo largo de los años en el instituto ha permitido generar mejores resultados en los procesos de atención a los pacientes como lo reflejan los indicadores de gestión clínica con los que cuentan en el tablero único de control de indicadores, además del porcentaje de satisfacción de los usuarios que durante los últimos cinco años ha superado el 90%.

Figura 3 *Indicador porcentaje de satisfacción global de los usuarios en la IPS B2.*

Este resultado hizo que se tuviera una transformación en la medición de satisfacción, pasando a realizar la evaluación de experiencia del paciente y la identificación del nivel de la lealtad de los usuarios con los servicios del instituto, a través de la herramienta NPS Net Promoter Score; encontrando un incremento del 21% en los promotores de los servicios entre el año 2020 y 2021.

Figura 4 *Resultado Indicador experiencia global del paciente ID-AU-44.*



Estos resultados reflejan la efectividad del sistema de gestión de calidad implementado y el impacto en la mejora de los procesos institucionales, lo que fortalece el compromiso de la alta dirección en el mantenimiento del sistema y se considera se pueden mantener para atender el SGSI.

Formación a todos los involucrados.

Durante la ejecución de las fases de direccionamiento y estructuración del proyecto de investigación, se realizó la presentación a la alta gerencia del conocimiento de la norma NTC ISO 27001:2013 y el despliegue de los objetivos planteados como parte del problema de investigación identificado; además de las propuestas realizadas de acuerdo con la aplicación de herramienta diagnóstica que permitió generar el análisis de brechas enfocado a la seguridad de la información en el ICSN - Clínica Montserrat.

De las propuestas y documentos entregables, producto de los espacios académicos de la Especialización de Dirección y Gestión de Calidad, fueron presentados a la alta gerencia y se aprobaron aquéllos que permiten fortalecer los procesos de gestión de la calidad institucional siendo una herramienta de innovación empresarial.

Estos espacios de divulgación han permitido la formación a los integrantes de la alta dirección y la construcción de la toma de conciencia sobre la importancia y los

beneficios de la implementación a futuro del sistema de gestión de gestión de seguridad de la información.

Construir conciencia

La construcción de conciencia (numeral 7.3. de la norma NTC ISO 9001:2015), se ha conceptualizado como proceso fundamental en el instituto para la implementación y mantenimiento del sistema de gestión de calidad y los demás procesos de mejoramiento continuo institucional, esta se encuentra alineada al desarrollo del modelo de competencias organizacionales, que se asocia a los comportamientos esperados de los colaboradores, su evaluación se realiza a través del cumplimiento del desempeño del sistema de gestión de calidad.

El fortalecimiento de los procesos de comunicación ha sido una estrategia fundamental en la toma de conciencia que ha generado impacto positivo en la eficacia del sistema de gestión de calidad, permitiendo el entendimiento y comprensión por parte de los colaboradores sobre los beneficios y las implicaciones que se pueden llegar a tener en caso de incumplimiento de los requisitos normativos.

Se considera que esta fortaleza que se identifica en el instituto hace parte de la transformación cultural y que permitiría la construcción de conciencia de una forma más fácil ante la integración de nuevos sistemas de gestión.

10. Conclusiones

Tras el análisis de brechas, se puede demostrar que al contar con un sistema de gestión de la calidad implementado en el ICSN - Clínica Montserrat, se identifican bases sólidas que le permiten dar cumplimiento a algunos de los requisitos de la norma NTC-ISO 27001:2013, de una manera más rápida, se respalda esta afirmación con la valoración obtenida en la primera aplicación de la herramienta diagnóstico del sistema de gestión de la información con base en el modelo ISO 27001:2013, atendida por 4 funcionarios de la clínica, cuyo resultado ubicó al instituto organización en un rango de valoración del 41% al 60% de cumplimiento y el cual indica que la información y demás aspectos relacionados son consistentes y evidenciables. Las brechas identificadas se abordaron desde la generación de propuestas documentales enfocadas al cumplimiento de los numerales 4.3. Determinación del alcance del sistema de gestión de seguridad de la información, 5.1. Liderazgo y compromiso, 5.2. Política, 5.3. Roles, responsabilidades y autoridades en la organización, 6.1.3. Tratamiento de riesgos de la seguridad de la información, 6.2. Objetivos de seguridad de la información y planes para lograrlos, 7.1. Recursos, 7.5.1 Información documentada - Generalidades.

El desarrollo de las propuestas generadas como parte de las fases de direccionamiento y estructuración del SGSI, permitió contar con datos para establecer la propuesta de planificación del sistema de gestión bajo la norma NTC 27001:2013 a la alta gerencia de la institución, siendo este un mecanismo de fortalecimiento para los procesos de mejora que contribuyen con la consecución de niveles de calidad en salud.

El seguimiento a las actividades definidas en el cronograma de trabajo para el proyecto de investigación, fueron verificadas en espacios de asesoría en el marco del programa académico. Por parte del instituto fueron socializados durante reuniones con la alta gerencia; el cumplimiento al cronograma de actividades no solo tuvo como objetivo generar resultados para la especialización, sino que además hace parte de los compromisos adquiridos de una de las estudiantes en quien el instituto promovió la gestión del conocimiento mediante el fortalecimiento de competencias desde el plan carrera institucional.

A través de la aplicación del diagnóstico por segunda vez, se disminuyeron brechas del componente estratégico como resultado de las propuestas y entregables de los espacios académicos generados en el marco del proyecto de investigación; el resultado global obtenido corresponde a la clasificación D: Mejora continua demostrable con un porcentaje global de cumplimiento del 65,04%.

Para resolver el problema de investigación identificado, se encuentra necesario la ejecución de las etapas de aplicación, evaluación y mejora para lograr así la implementación del sistema de seguridad de la información en el instituto y dar cumplimiento a los requisitos faltantes que en porcentaje corresponde al 34.96%.

11. Recomendaciones

Como recomendaciones resultado del direccionamiento y estructuración del SGSI para el ICSN - Clínica Montserrat, desarrollado durante el proceso de formación en la especialización de dirección y gestión de calidad de la Universidad Santo Tomás en convenio con el ICONTEC, se plantean las siguientes:

- Contar con un SGSI favorecerá el aumento de la calidad y la eficiencia de los servicios de salud en las modalidades de atención ofertadas por el instituto, mejorando la atención de los pacientes; además, permitirá prevenir y mitigar la materialización de riesgos financieros, legales y reputacionales que puedan afectar a la institución; por lo que se sugiere implementar los entregables de este proyecto de investigación que generan avances en los procesos de la institución y en la posibilidad de implementar a futuro el sistema de seguridad de la información.
- La implementación del SGSI garantiza la protección de los derechos a la privacidad y confidencialidad de su información, así como la seguridad, el control en el acceso y el uso de los datos clínicos, siendo la información el recurso con mayor sensibilidad en el tratamiento, como propiedad del cliente.
- El desarrollo de las fases de aplicación, evaluación y mejora pueden ser resultado del ejercicio académico de la especialización de dirección y gestión de calidad y/o de la maestría en calidad y gestión integral de la Universidad Santo Tomás en convenio con el ICONTEC, disminuyendo costos en la realización de actividades operativas relacionadas con la documentación e implementación de algunos de los numerales de la norma NTC ISO 27001:2013.

12. Bibliografía

- 27001 Academy. (2016). *How to Budget an ISO 27001 Implementation Project*. https://infomania-services.fr/controle/file/181221025813000000_9878907642_1545404293.pdf
- Andrés, A., & Gómez, L. (2009). *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. AENOR.
- Antomás, J., & Huarte del Barrio, S. (2011). Confidencialidad e historia clínica: Consideraciones ético-legales. *Anales del Sistema Sanitario de Navarra*, *34*(1), 73-82.
- Clínica Montserrat. (s. f.). *Clínica Montserrat*. Clínica Montserrat. Recuperado 15 de octubre de 2021, de https://clinicamontserrat.com.co/clinicamontserrat/
- Clínica Montserrat, M. A. (2021). *Modelo Asistencial Clínica Montserrat*.
- Clínica Montserrat, P. del C. (2018). *Clínica Montserrat Instructivo: PLANIFICACIÓN DEL CAMBIO*.
- Decreto 780. (2016). *DECRETO NÚMERO 780 DE 2016*. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/decreto-780-unico-modificado-2016.pdf
- Instituto Colombiano de Normas Técnicas y Certificación ICONTEC, T. de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información. requisitos. (2013). *Norma Técnica NTC-ISO-IEC Colombiana 27001*. Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
- Ley 2015, 2020. (2020). *LEY 2015 DEL 31 DE ENERO DE 2020*.
- Resolución 1995. (1999). *Resolución 1995*.

13. Anexos

1. Anexo A. Carta de Presentación - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
2. Anexo B. Carta de Aceptación - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
3. Anexo C. Bitácora - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
4. Anexo D. Programa de Auditorias - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
5. Anexo E. Matriz de Comunicaciones - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
6. Anexo F. Diagnóstico del Sistema de Gestión de la Información con Base en el Modelo ISO 27001:2013 - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
7. Anexo G. Matriz de Riesgos de TIC - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
8. Anexo H. Caracterización del Proceso de TIC - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
9. Anexo I. Manual de la Gerencia de la Información - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
10. Anexo J. Fichas técnicas Indicadores - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat
11. Anexo K. Normograma - Instituto Colombiano del Sistema Nervioso - Clínica Montserrat