DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA TELEMEDICINA EN LA IPS COLOMBIANA DE TRASPLANTES

JEFFERSON FABIAN BARBOSA SALINAS
DAVID ALEJANDRO GONZÁLEZ VARGAS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA, ESCUELA DE INGENIERÍAS TIC
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA TELEMEDICINA EN LA IPS COLOMBIANA DE TRASPLANTES

JEFFERSON FABIAN BARBOSA SALINAS
DAVID ALEJANDRO GONZÁLEZ VARGAS

Trabajo de grado para optar por el título de:
Especialista en seguridad informática

Asesora:
Lorena Ocampo Correa
Ingeniera de Sistemas Y Computación

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA, ESCUELA DE INGENIERÍAS TIC
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

Notas de aceptación:

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., 29 de junio de 2021

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

GLOSARIO

ACCIÓN CORRECTIVA: acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección[1].

ACTIVO: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización[2].

ALCANCE: ámbito de la organización que queda sometido al SGSI[3].

ALTA DIRECCIÓN: persona o grupo de personas que dirige y controla una organización. Al más alto nivel, la alta dirección tiene la facultad de delegar la autoridad y proporcionar recursos dentro de la organización[4].

AMENAZA: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[5].

ANÁLISIS DE RIESGOS: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos[6].

ATAQUE: intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo[7].

AUDITORÍA: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría[8].

BRECHA: indica que le hace falta a un control o requisito para cumplir frente a la norma ISO 27001:2013[9].

---

[1] ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html

[2] Ibíd.

[3] Ibíd.

[4] Ibíd.

[5] Ibíd.

[6] Ibíd.

[7] Ibíd.

[8] Ibíd.

CONFIDENCIALIDAD: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[10].

CONTROL: medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control[11].

DISPONIBILIDAD: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[12].

EVALUACIÓN DE RIESGOS: proceso global de identificación, análisis y estimación de riesgos[13].

EVENTO: ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente"[14].

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad[15].

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información[16].

---

[9] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información [en línea]. [Consulta 8 de abril de 2021]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf

[10] ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html

[11] Ibíd.

[12] Ibíd.

[13] Ibíd.

[14] Ibíd.

[15] Ibíd.

[16] Ibíd.

GESTIÓN DE RIESGOS: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos[17].

HISTORIA CLÍNICA: es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley[18].

HISTORIA CLÍNICA ELECTRONICA: es el registro integral y cronológico de las condiciones de salud del paciente, que se encuentra contenido en sistemas de información y aplicaciones de *software* con capacidad de comunicarse, intercambiar datos y brindar herramientas para la utilización de la información refrenada con firma digital del profesional tratante[19].

IMPACTO: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-[20].

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[21].

INDICADOR: medida que proporciona una estimación o evaluación[22].

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud[23].

OBJETIVO DE CONTROL: declaración que describe lo que se debe lograr como resultado de la implementación de los controles[24].

---

[17] ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html.

[18] COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución No. 1995 del 1999 [en línea]. (Consulta 8, Julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf, 1999. p. 1.

[19] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 2015 DE 2020 [en línea]. (Consulta 31 de enero de 2020). Por medio del cual se crea la Historia Clínica Electrónica interoperable y se dictan otras disposiciones. 51.213 de 31 de enero 2020. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_2015_2020.html, 2020.

[20] ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html

[21] Ibíd.

[22] Ibíd.

[23] Ibíd.

[24] Ibíd.

PLAN DE TRATAMIENTO DE RIESGOS: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma[25].

POLÍTICA: intenciones y dirección de una organización, expresada formalmente por su alta dirección[26].

PROBABILIDAD: posibilidad de que ocurra algo[27].

PROCESO: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas[28].

REQUISITO: necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria[29].

RIESGO: el riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización[30].

RIESGO RESIDUAL: el riesgo que permanece tras el tratamiento del riesgo[31].

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua[32].

SGSI: siglas de Sistema de Gestión de la Seguridad de la Información[33].

TRATAMIENTO DE RIESGOS: proceso para modificar el riesgo[34].

---

[25] ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html

[26] Ibíd.

[27] Ibíd.

[28] Ibíd.

[29] Ibíd.

[30] Ibíd.

[31] Ibíd.

[32] Ibíd.

[33] Ibíd.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas[35].

[34] Ibíd.

[35] ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html

INTRODUCCIÓN

Las empresas en los diferentes sectores tienden a potenciar la innovación tecnológica y la optimización de sus procesos, así como a adaptarse a los cambios, pero se debe tener en cuenta el cumplimiento de las leyes y los marcos regulatorios, así como la protección de sus activos más valiosos frente a todas las amenazas posibles; para esto, diferentes organizaciones desarrollan metodologías que se ajustan a las necesidades de las empresas como la de proteger la información y asegurar todos los procesos involucrados en su tratamiento. En el presente proyecto, se toma como referencia la norma ISO/IEC 27001:2013 con el objetivo de aplicar una metodología estandarizada y probada, donde a futuro, la empresa puede llegar a obtener una certificación. Esto no excluye ninguno de los requisitos de ley para tener en cuenta u otros marcos de referencia que apoyen el desarrollo del diseño.

La IPS Colombiana de Trasplantes es una empresa del sector salud, que tiene como propósito brindar una mejor calidad de vida a pacientes con problemas renales y hepáticos por medio del trasplante. En la actualidad, están adaptando su servicio con protocolos de atención virtual para garantizar el debido seguimiento y tratamiento de sus pacientes. Este tipo de atención está definido a nivel gobierno como telesalud y está reglamentado por el Ministerio de Salud y Protección Social mediante la resolución No. 2654 del 2019, en la que se establecen disposiciones para la telesalud y parámetros para la práctica de la telemedicina en el país, los cuales incluyen medidas para la protección de datos de los pacientes y lineamientos a seguir para la aplicación de procedimientos asociados al servicio.

Como fase inicial, para el servicio de telemedicina en la IPS Colombiana de Trasplantes, se diseñará la base para la gestión de la seguridad en los procesos que lo componen. Como punto de partida, el levantamiento de información será fundamental para un posterior análisis de los activos que arrojará los riesgos a los que el proceso se encuentra expuesto, ya que no se ha evaluado con anterioridad la exposición de la información privada de los pacientes en un entorno de telemedicina, donde al igual que en el proceso de consulta convencional, se manipulan datos confidenciales de los pacientes pero en diferentes medios de datos y en diferentes entornos de flujo de información que no se contemplan en la presencialidad, pero que deben cumplir con los parámetros dispuestos en la legislación para la protección de datos personales. Otro factor importante por determinar es el riesgo aceptable para la empresa; donde este permitirá evidenciar los riesgos que deben ser tratados y también permitirá sugerir un plan de tratamiento.

1. JUSTIFICACIÓN

La investigación nace de la necesidad de operación en la IPS Colombiana de Trasplantes durante la contingencia por la pandemia que se vive actualmente, donde se toma la decisión de cumplir con los lineamientos de la resolución 2654 de 2019 el Ministerio de Salud para la prestación de servicios en telemedicina, ya que de no cumplirse se vería expuesta a la intervención de los organismos de control y vigilancia, acarreando investigaciones que pueden conducir a sanciones o suspensión del servicio. Esto lleva a la compañía a concientizarse en lo importante de diseñar un sistema de gestión en seguridad de la información, en procura de proteger datos clínicos sensibles dentro de los procesos de la consulta virtual, y así, asegurar los niveles adecuados de protección en todo lo relacionado con la confidencialidad, integridad y disponibilidad de dicha información.

Actualmente, las amenazas han crecido considerablemente afectando las organizaciones al interior y exterior de todos los sistemas de información, por tal motivo, surge la necesidad de gestionar de manera eficiente todos los riesgos con el objetivo de minimizar el impacto que puedan tener dentro de la organización. Basándose en la norma ISO/IEC 27001:2013 se logrará establecer una base sólida para que la seguridad de la información apoye todos los objetivos estratégicos, garantizando una buena gestión administrativa y operativa.

Basados en lo anterior, es muy importante definir una política de seguridad que permita a futuro dar solución efectiva dentro de los controles sugeridos para el manejo de los posibles riesgos que se puedan presentar dentro de los procesos de la telemedicina, además de involucrar al personal que actúa dentro de dichos procesos en un programa de concientización con el objetivo que comprendan lo importante que son para que el sistema de seguridad de la información sea exitoso.

2. PROBLEMA DE INVESTIGACIÓN

2.1 PLANTEAMIENTO

Colombiana de Trasplantes es una IPS dedicada a prestar servicios de salud en Colombia, al prestar este tipo de servicios debe recolectar, manipular y tratar información reservada de sus pacientes. Esta información está protegida por la ley colombiana mediante la constitución política y la empresa como responsable de la misma debe dar cumplimiento a la legislación, garantizando la custodia, el uso adecuado y autorizado de toda la información personal.

Actualmente, la información de los pacientes en el proceso de telemedicina en Colombiana de Trasplantes está expuesta a riesgos de seguridad donde la información circula entre diferentes personas que participan en el proceso sin un control definido, dando pie a que pueda llegar a terceros que no deben tener acceso y que no cuentan con autorización expresa del titular. Adicionalmente, los canales de flujo de información son abiertos, sin control en los equipos personales y servicios de red públicos expuestos que, por su condición, permitirían la manipulación y modificación de los datos en algunos de los saltos que presenta la comunicación. Otro aspecto para tener en cuenta es la ausencia de una estrategia definida para garantizar la seguridad de la información en los componentes de infraestructura, tales como; las aplicaciones, servicios y equipos, que en caso de un evento que genere la pérdida o compromiso de la información personal de pacientes, empleados o terceros, no se puede llegar a restaurar el servicio de forma controlada. Los factores de riesgo descritos pueden conducir a la IPS a incumplir con los requisitos de ley, entrando en el campo de la responsabilidad jurídica al violar los derechos fundamentales consagrados en la legislación colombiana.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se pueden establecer los requerimientos en seguridad de la información íntima personal que se manipula en el proceso de Telemedicina en la IPS Colombiana de Trasplantes?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar el sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para telemedicina en la IPS Colombiana de Trasplantes.

3.2 OBJETIVOS ESPECÍFICOS

- Elaborar el análisis del estado actual para el proceso de Telemedicina con base a la norma ISO/ IEC 27001:2013 para seguridad de la información.
- Generar el inventario de activos de información para el proceso de Telemedicina.
- Realizar el análisis de riesgo para los activos del proceso de Telemedicina con base en la norma ISO/IEC 27005:2009 para la gestión de riesgos de la seguridad de la información.
- Plantear opciones de tratamiento para la gestión de los riesgos sobre el nivel de tolerancia para el proceso de Telemedicina con base en la norma ISO/ IEC 27001:2013.
- Formular las políticas de seguridad de la información en Colombiana de Trasplantes para el proceso de Telemedicina con base en la norma ISO/ IEC 27001:2013.
- Proponer un programa de capacitación y concientización en seguridad de la información para las partes que intervienen en el proceso de Telemedicina en Colombiana de Trasplantes.
- Presentar una propuesta de implementación para el proyecto de seguridad de la información en el proceso de Telemedicina en Colombiana de Trasplantes.

4. MARCO TEORICO

4.1 TELEMEDICINA

En el capítulo 3 de la resolución 2654 de 2019[36] se establecen todas las disposiciones para la telesalud y los parámetros para la práctica de la telemedicina, el cual tiene como objetivo facilitar acceso, oportunidad y resolutividad[37] en todo lo relacionado con la prestación de servicios de salud para cada una de las fases como lo son promoción, prevención, diagnóstico, tratamiento, rehabilitación y paliación. El servicio de telesalud puede ser ofrecido y utilizado por cualquier prestador, en cualquier zona geográfica siempre y cuando cumpla con la normatividad que regula la materia.
La telemedicina se compone por diferentes categorías las cuales se pueden combinar entre ellas y son las siguientes:

4.1.1 Telemedicina interactiva. Es la relación a distancia utilizando tecnologías de la información y comunicación, con herramientas que permiten realizar video llamadas en tiempo real, donde un profesional de la salud presta los servicios a un usuario en cualquiera de las fases. El profesional de la salud es el que asume la responsabilidad del diagnóstico, concepto, tratamiento e intervenciones que se ordenen, pero el prestador tendrá la autonomía de abstenerse o cancelar la atención con esta modalidad, fundamentando las razones de su decisión. Por último, el prestador deberá cumplir con todos los estándares y requisitos que se establecen en las normas que regulan la materia.

4.1.2 Telemedicina no interactiva. Esta relación entre profesional de la salud y el usuario se realiza por medio de una comunicación asincrónica ya que el servicio que se presta no requiere de una respuesta inmediata. Como en la anterior categoría, el profesional es el que asume la responsabilidad y puede abstenerse de la atención fundamentando sus razones. Por último, el prestador deberá cumplir con todos los estándares y requisitos que se establecen en las normas que regulan la materia.

---

[36] COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución No. 2654 del 2019 [en línea]. (Consulta 3 de octubre de 2019). Por la cual se establecen disipaciones para la telesalud y parámetros para la práctica de la telemedicina en el país. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%202654%20del%202019.pdf, 2019. p. 1.

[37] WWW.SCIELO.EDU.UY. Capacidad resolutiva del primer nivel de atención: experiencia de la Unidad Docente–Asistencial de Medicina Familiar y Comunitaria de Paysandú (2014) [en línea]. [Consulta 19 de mayo de 2021]. Disponible en internet: https://www.iso27000.es/glosario.htmlhttp://www.scielo.edu.uy/pdf/rmu/v32n3/v32n3a02.pdf.

4.1.3 Teleexperticia. Esta es la relación a distancia con métodos sincrónicos y asincrónicos para la provisión de los diferentes servicios de salud en cualquiera de sus fases.

Esta relación contará con dos profesionales de la salud: el primero atiende presencialmente y es el responsable del tratamiento y de las decisiones o recomendaciones que se le entregan al paciente. El segundo profesional, es quien atiende a distancia donde su responsabilidad radica en la opinión que entrega y este debe especificar las condiciones de dicha opinión. Estas opiniones deben quedar registradas en la historia clínica del paciente.

Contará también con personal de la salud no profesional: este comprende a un técnico, tecnólogo o auxiliar que atiende presencialmente al paciente y con un profesional de la salud de forma virtual o a distancia, donde este será responsable del tratamiento y de las recomendaciones que reciba el paciente y el personal no profesional será responsable de toda acción que esté dentro de su competencia.

4.1.4 Telemonitoreo. Esta relación se basa en una infraestructura tecnológica que permite la recopilación y trasmisión de datos clínicos con el objetivo de que el prestador pueda realizar un seguimiento y una revisión clínica que proporcione resultados con estos datos entregados.

4.1.5 Prescripción de medicamentos en telemedicina. Esta prescripción debe ser suministrada por el profesional autorizado y esta sólo podrá ser realizada en las categorías de telemedicina interactiva y teleexperticia sincrónica. Cada profesional será responsable de la prescripción que realice y también será autónomo de abstenerse de las mismas.

4.1.6 Autorizaciones de servicio. Cuando se requiera una solicitud de autorización de servicios por la modalidad de telemedicina que se expide por el profesional de la salud según su competencia, esta servirá como soporte para el trámite correspondiente según como lo regula la materia. Todo el personal que participe dentro de las anteriores categorías de la telemedicina realizará su trabajo de acuerdo con sus competencias y responsabilidades, donde para el desarrollo de estas acciones, se respetará la autonomía del profesional.

4.2 REQUISITOS LEGALES

4.2.1 Resolución Ministerio de Salud 2654 del 2019. El Ministerio de Salud mediante la resolución 2654 del 2019[38] establece disposiciones para la telesalud y parámetros para la práctica de la telemedicina en el país.

Entre los aspectos a resaltar se encuentran:

- Campo de aplicación.
- Consentimiento informado.
- Alcance telesalud.
- Alcance telemedicina.
- Calidad y seguridad de la información y los datos.
- Calidad y seguridad en la atención en salud.

4.2.2 Ley 1581 de 2012 protección de datos personales. La ley 1581 de 2012 de protección de datos personales[39] tiene como objetivo reconocer y proteger el derecho que tiene toda persona de conocer, actualizar, rectificar y revocar toda la información obtenida por bases de datos de entidades públicas o privadas.

Cuando se habla de datos personales hacemos referencia a toda la información que se asocia a una persona permitiendo su identificación, por ejemplo, número de cédula, fecha de nacimiento, lugar de nacimiento, edad, estado civil, etc. Igualmente existe información que es mucho más sensible como su historial clínico, características físicas o ideológicas, vida sexual, entre otros.

Estos datos se recolectan cuando las personas interactúan con empresas y/o entidades para que esta sea individualizada ante el resto de la sociedad, desarrollando flujos de información que ayudan al crecimiento económico y al mejoramiento de bienes y servicios, como por ejemplo, cuando hacemos una solicitud de crédito ante entidades financieras donde se requiere el diligenciamiento de formularios con información personal, o también, cuando se realiza una compra donde se genera la respectiva factura, y en esta, nos piden número de identificación, correo electrónico, dirección, teléfono,

[38] COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución No. 2654 del 2019 [en línea]. (Consulta 3 de octubre de 2019). Por la cual se establecen disipaciones para la telesalud y parámetros para la práctica de la telemedicina en el país. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%202654%20del%202019.pdf, 2019. p. 1.

[39] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 DE 2012 [en línea]. (Consulta 18 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html, 2012.

entre otros datos que nos identifican ante cualquier inconformidad o novedad que se presente ante la compra realizada.

¿Qué tipos de datos hay?

Las disposiciones sobre protección de datos establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación:

- Dato público: Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.
- Dato semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.
- Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.
- Dato sensible: Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

¿A qué datos personales no se aplica la ley?

- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- Las que tengan por finalidad la seguridad y defensa nacional, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- Las que tengan como fin y contengan información de inteligencia y contrainteligencia.
- Las que contengan información periodística y otros contenidos editoriales
- Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

Los derechos serán vulnerados cuando el uso de las tecnologías de la información y las telecomunicaciones permitan en muchas ocasiones que la información obtenida se utilice para fines diferentes al que inicialmente fue requerido, afectando la privacidad de las personas y lesionando en algunos casos, otros derechos y libertades. También, cuando la información no es actualizada o no se toman medidas necesarias para garantizar la seguridad de este. Por último, que la entidad entregue datos a terceros sin previa autorización del titular.

Es importante aclarar que el tratamiento de los datos no está prohibido siempre y cuando se cumplan plenamente con las disposiciones de la ley para el uso, recolección, circulación o supresión de los datos personales, todo con autorización del dueño de los datos.

4.2.3 Ley 2015 de 2020 Historia Clínica Electrónica – IHCE. El congreso de la república decreta la ley 2015 de 2020 para regular la interoperabilidad de la historia clínica electrónica en Colombia, estableciendo las pautas para el intercambio de información efectivo y seguro que garantice los derechos de las personas titulares de la información.

Entre los aspectos a resaltar se encuentran:

- Derechos de titularidad sobre la información de la historia clínica y obligaciones de consentimiento a terceros para el acceso.
- Lineamientos sobre el contenido y el seguimiento de modificaciones.
- Acceso gratuito a los pacientes por medios electrónicos.
- Definición de tiempos de retención y custodia.
- Requerimientos de estrategia en seguridad de la información y seguridad digital por los actores que traten la información.

4.2.4 Resolución Ministerio de Salud 1995 del 1999. El Ministerio de Salud mediante la resolución 1995 de 1999 establece definición, disposiciones generales, diligenciamiento, organización y manejo de archivo de las historias clínicas en Colombia, para ser aplicada en todas las entidades y partes que intervienen en el sistema general de seguridad social y salud.

Entre los aspectos a resaltar se encuentran:

- Resolución de obligatorio cumplimiento para todos los prestadores de servicios de salud, además de personas naturales y jurídicas que intervienen.
- Definición de características de las historias clínicas.
- Obligatoriedad del registro de observaciones conceptos decisiones y resultados.
- Apertura e identificación de la historia clínica.
- Numeración consecutiva de la historia clínica.
- Identificación del usuario.
- Registros específicos.
- Obligatoriedad del archivo.
- Custodia de la historia clínica.
- Acceso a la historia clínica.
- Retención y tiempo de conservación.
- Seguridad del archivo de historias clínicas.
- Condiciones físicas de conservación de las historias clínicas, y los medios técnicos de conservación.
- Comité de historias clínicas y sus funciones.

4.2.5 Resolución Ministerio de Salud 839 del 2017. El Ministerio de Salud mediante la resolución 839 de 2017 modifica la resolución 1995 de 1999 y establece nuevas disposiciones para los lineamientos en el manejo de la historia clínica, custodia, tiempo de retención, conservación y disposición final, además del consentimiento informado y los anexos correspondientes.

Entre los aspectos a resaltar se encuentran:

- Retención y tiempos de conservación documental del expediente de la historia clínica.
- Disposición final del expediente de historia clínica.
- Procedimiento de eliminación de historias clínicas.
- Protección de datos personales.

4.3 NORMA INTERNACIONAL ISO/IEC 27001:2013

Los estándares internacionales proporcionan un punto de referencia para implementar modelos funcionales probados y aprobados por expertos en diferentes materias según corresponda, esto permite a las empresas alinear sus procesos a prácticas sólidas teniendo en cuenta el proceso de madurés que experimentan constantemente.

La Organización Internacional de Estandarización (ISO por sus siglas en inglés) crea normativa para diferentes estándares, aunque no es la única organización con este fin, sí se puede considerar la más grande y difundida. Para administrar la gestión de la seguridad en la empresa la ISO desarrolló la norma ISO/IEC 27001, que es una norma actualmente certificable por diferentes empresas que actúan como ente certificador avalado; basándose en esta norma una empresa puede estandarizar procesos dentro del marco de la seguridad de la información sin importar su naturaleza o tamaño; al ser una norma ISO debe cumplir el ciclo de mejora continua.

Dentro de la familia de normas ISO/IEC 27000 se pueden encontrar diferentes estándares que ayudan a implementar un sistema de gestión para seguridad de la información, pero la norma ISO/IEC 27001 es la única certificable, también se debe tener en cuenta que más allá de la familia de normas ISO/IEC 27000, las normas ISO en general comparten características de fondo entre sus normativas certificables que van desde los aspectos generales de estructura, el ciclo de mejora continua y “debes” generales entre otros, lo que facilita en las empresas tener sistemas de gestión integrados teniendo como referencia estándares ya implementados.

La norma ISO/IEC 27001:2013 no es el único marco de referencia aplicable al sector salud ya que existen diversos marcos de referencia generales que aplican para todo tipo de empresas sin importar naturaleza o tamaño, como ya se mencionó, otros marcos van desde lo general hasta lo específico; muchos de estos toman como base normativas de ley

de otros países como la Ley HIPPA de Estados Unidos, o para Colombia, las regulaciones locales impartidas por el gobierno y los entes de control como el Instituto Nacional de Salud, el Ministerio de Salud o el Ministerio de las Tecnologías, entre otros; pero como parte del cumplimiento de la norma ISO/IEC 27001:2013 se debe contemplar principalmente el cumplimiento de las regulaciones de ley aplicables como un requisito obligatorio.

Entre los diferenciales de la norma ISO/IEC 27001 se encuentran los dominios para los objetivos de control del Anexo A de la norma descritos a continuación:

- A. 5 Políticas de seguridad de la información.
- A. 6 Organización de la seguridad de la información.
- A. 7 Seguridad de los recursos humanos.
- A. 8 Gestión de activos.
- A. 9 Controles de acceso.
- A.10 Criptografía – Cifrado y gestión de claves.
- A.11 Seguridad física y ambiental.
- A.12 Seguridad operacional.
- A.13 Seguridad de las comunicaciones.
- A.14 Adquisición, desarrollo y mantenimiento del sistema.
- A.16 Gestión de incidentes de seguridad de la información.
- A.18 Cumplimiento.

En total la norma ISO/IEC 27001:2013 tiene 114 controles, contenidos en 35 objetivos de control que a su vez están contenidos en 14 dominios.

4.4 NORMA INTERNACIONAL ISO/IEC 27005:2009

La norma internacional ISO/IEC 27005:2009 es un estándar internacional que proporciona directrices para la gestión del riesgo en la seguridad de la información, facilitando la implementación de un sistema de gestión basado en la gestión de riesgo para el cumplimiento de requisitos de la norma ISO/IEC 27001.

Esta norma está concebida para aplicar en cualquier tipo de empresa u organización, ya sea pública o privada, donde se necesiten lineamientos para la gestión del riesgo, pero sin imponer una metodología específica, dando cabida al uso de diferentes metodologías según se disponga durante el diseño del sistema.

La norma plantea las siguientes actividades específicas para el proceso de gestión del riesgo en la seguridad de la información:

- Numeral 7. Establecimiento del contexto.

- Numeral 8. Valoración del riesgo.
- Numeral 9. Tratamiento del riesgo.
- Numeral 10. Aceptación del riesgo.
- Numeral 11. Comunicación del riesgo.
- Numeral 12. Monitoreo y revisión del riesgo.

Adicionalmente, la norma presenta en sus anexos información de apoyo pertinente para el desarrollo de las actividades:

- Anexo A. Definición del alcance y los límites del proceso de gestión del riesgo en la seguridad de la información.
- Anexo B. Identificación y valoración de los activos y valoración del impacto.
- Anexo C. Ejemplos de amenazas comunes.
- Anexo D. Vulnerabilidades y métodos para la valoración de vulnerabilidades.
- Anexo E. Enfoques para la valoración del riesgo de la seguridad de la información.
- Anexo F. Restricciones para la reducción de riesgos.

4.5 PUBLICACIÓN ESPECIAL NIST 800-50

La publicación especial NIST 800-50 contiene los lineamientos proporcionados por el Instituto Nacional de Estándares y Tecnología perteneciente al departamento de comercio de los Estados Unidos de América, para la creación de un programa de capacitación y concientización sobre seguridad en tecnologías de la información.

El NIST, por sus siglas en ingles de *National Institute Of Standards And Technology,* propone tres componentes principales para tener en cuenta para construir un plan de capacitación y concientización, que son: concienciación, capacitación y educacion. La finalidad de la concienciación es cambiar los comportamientos de los usuarios orientándolos a buenas prácticas de seguridad, donde por medio de la presentación de temáticas que le lleguen al usuario, este se sensibilice sobre los aspectos más relevantes en seguridad. Con las capacitaciones se pretende generar en los participantes habilidades y competencias en seguridad para ser aplicadas en su cotidianidad, por último, con la educacion se integran diferentes habilidades, competencias y especialidades para generar profesionales con un conocimiento especializado en seguridad, además que tengan la capacidad de analizar y responder.

El programa de concienciación y capacitación contempla principalmente:

- Realización de una evaluación de necesidades.
- Desarrollar una estrategia para el plan de sensibilización y formación.
- Estableciendo prioridades.
- Financiamiento del programa de capacitación y concientización sobre seguridad.

- Desarrollo de material de sensibilización y formación
- Desarrollo de material de concienciación.
- Selección de temas de sensibilización.
- Fuentes de material de sensibilización.
- Desarrollo de material de formación.
- Implementación del programa de sensibilización y formación.
- Comunicando el plan.
- Técnicas para transmitir material de sensibilización.
- Técnicas para entregar material de capacitación.
- Post-implementación.
- Supervisión del cumplimiento.
- Evaluación y retroalimentación.
- Cambio de gerencia.
- Mejora continua.
- Indicadores de éxito del programa.

4.6 CONTEXTO GENERAL DE LA ORGANIZACIÓN

Colombiana de Trasplantes dedicada al servicio de la salud y líder en Trasplante Renal en Colombia. Con sedes en Bogotá, Medellín, Armenia y Barranquilla; cuentan con un equipo altamente calificado de cirujanos, especialistas en salud mental, científicos en el área de investigación y desarrollo y el equipo de enfermería las cuales han permitido la realización de 1.400 trasplantes en Colombia con un alto porcentaje de éxito en los pacientes.

Colombiana De Trasplantes S.A.S. es una Sociedad Comercial con domicilio principal en la Ciudad de Bogotá D. C. constituida mediante Escritura Pública No.804 otorgada por la Notaría 48 del Círculo de Bogotá. D. C. del 28 de abril de 2003 bajo el nombre de COLOMBIANA DE TRASPLANTES S.A. Su objeto principal es el desarrollo social en la prestación de servicios de salud, en particular trasplante renal, hígado, combinado, o cualquier órgano del cuerpo humano, ya sea en pacientes nacionales o extranjeros. En reunión extraordinaria de la asamblea general de accionistas celebrada el 18 de diciembre de 2013, se presentó a los accionistas de Colombiana de Trasplantes S.A., las ventajas de transformar la sociedad al tipo de Sociedad por Acciones Simplificada (S.A.S.) de conformidad con la Ley 1258 de 2008 por parte del presidente de la compañía.

4.6.1 Historia. Colombiana de Trasplantes fundada en marzo 08 de 2003 ya lleva en el servicio de la salud más 15 años, conformada por un equipo de médicos especialistas en el campo de trasplantes los Doctores Úrsula Betancourth, Sergio Salcedo Herrera, Fernando Girón Luque, Alejandro Niño Murcia y Jorge Rodríguez Rozo quienes decidieron brindar sus experiencias al beneficio de la Salud a los aliados estratégicos que son: Pacientes, Clientes, Proveedores y al Estado de Colombia. La historia se sigue escribiendo y debemos ser parte activa en la misma, todos podemos aportar una letra en la historia del trasplante.

El primer trasplante fue de riñón se realizó el mes de junio del mismo año, para completar un total de tres trasplantes exitosos durante 2003.

4.6.2 Misión. En Colombiana de Trasplantes SAS brindamos nuestra experiencia para el beneficio de la salud pública en Colombia y el mundo, a través de la prestación de servicios de salud en trasplantes, satisfaciendo a nuestros empleados y aliados estratégicos, como son: pacientes, clientes, proveedores y el estado colombiano.

4.6.3 Visión. Colombiana de Trasplantes SAS será la principal empresa nacional dedicada a mejorar los estándares de vida de los pacientes con patologías agudas o crónicas, susceptibles de tratamiento con trasplante.

4.6.4 Contexto de negocio. Colombiana de Trasplantes SAS, se enfoca en un modelo de atención integral, aportando su experiencia en la prestación de servicios de salud a aquellos usuarios que requieren trasplante de órganos, fundamentalmente renal, hepático y combinado (renal – hepático).

Teniendo en cuenta lo anterior, su principal enfoque es brindar una mejor calidad de vida al paciente, basados principalmente en un entorno de respeto, excelencia y hospitalidad.
A continuación, se describen las tres líneas de negocio de la IPS Colombiana de Trasplantes, las cuales a su vez están clasificadas por tipo de producto.

4.6.4.1 Servicio renal. Servicio dirigido a pacientes diagnosticados con insuficiencia renal crónica, se divide en tres actividades, en la primera se identifica si el paciente es apto o no para el trasplante. Se genera el proceso quirúrgico donde se realiza la sustitución del órgano que no cumple con sus funciones, por uno en buen estado, posterior a esto se realizan los controles post-trasplante.

- Fase 1: Proceso de valoración psicológica y procedimientos prequirúrgicos, que se realizan a los pacientes diagnosticados con patología renal, para determinar si son aptos para trasplante de riñón.
- Fase 2: Procedimiento quirúrgico en el cual se implanta un riñón sano, obtenido de donante vivo o donante cadavérico, a pacientes con insuficiencia renal crónica que han pasado el proceso de fase 1.
- Fase 3: Corresponde a los controles mensuales de monitoreo y seguimiento post-trasplante.

4.6.4.2 Servicio hepático. Servicio dirigido a pacientes diagnosticados con insuficiencia hepática crónica, dividida en tres etapas, en la primera se identifica si el paciente es apto o no para el trasplante. Se genera el proceso quirúrgico, donde se realiza la sustitución del órgano malo por uno en buen estado, posterior a esto se encuentran los controles post-trasplante.

- Etapa A: Proceso de valoración psicológica y procedimientos prequirúrgicos, que se realizan a los pacientes diagnosticados con patología hepática, para determinar si son aptos para trasplante de hígado.
- Etapa B: Procedimiento quirúrgico en el cual se implanta un hígado sano, obtenido de donante vivo o donante cadavérico, a pacientes con patología hepática aptos para el trasplante.
- Etapa C: Corresponde a los controles mensuales de monitoreo y seguimiento post-trasplante.

4.6.4.3 Servicio combinado. Servicio especializado para pacientes diagnosticados con insuficiencia renal y hepática en estado crónico, el cual se divide en tres ciclos, primero se realizan estudios clínicos para identificar si el paciente es apto o no para el trasplante. Una vez salen positivos los análisis, se realiza el proceso quirúrgico donde se genera la sustitución del órgano a reemplazar por uno en buen estado, posterior a esto se encuentran los controles post-trasplante.

- Ciclo 1: Procedimientos prequirúrgicos que se realizan a los pacientes diagnosticados con patología hepática y renal, para determinar si son aptos para trasplante.
- Ciclo 2: Procedimiento quirúrgico en el cual se implanta a un receptor, un hígado o un riñón sano obtenido de donante vivo o donante cadavérico.
- Ciclo 3: Corresponde a los controles mensuales de monitoreo y seguimiento post-trasplante.

4.6.5 Estructura Organizacional. Colombiana de Trasplantes divide su estructura organizacional en los grupos estratégico, táctico y operativo, cargos que soportan los procesos misionales, de apoyo y estratégicos.

El grupo estratégico lo componen:

- Asamblea de accionistas
- Junta directiva
- Presidente
- Director de calidad y auditoría
- Vicepresidente científico
- Director fase 1, director fase 2, director fase 3
- Vicepresidente de gestión
- Director de cultura y liderazgo
- Director comercial noroccidente
- Director comercial centro oriente

El grupo táctico lo componen:

- Coordinador salud mental,
- Coordinador enfermería,
- Coordinador de investigación
- Químico farmacéutico
- Coordinador de sistemas
- Jefe de logística
- Coordinador financiero

El grupo operativo lo componen:

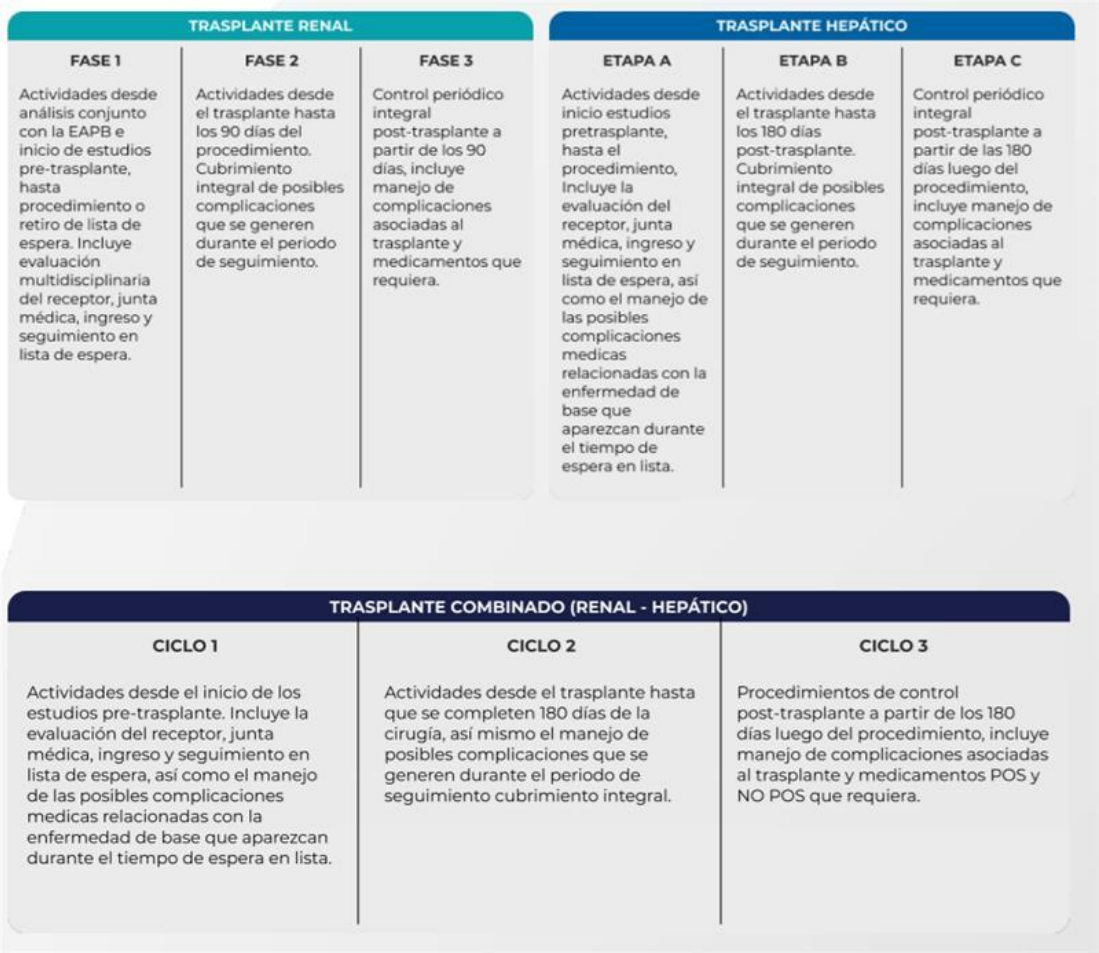
- Psiquiatra
- Psicólogo
- Enfermero profesional
- Auxiliar de enfermería
- Auxiliar administrativo
- Médico de investigación
- Auxiliar administrativa de investigación
- Trabajador social
- Cirujano de trasplantes
- Cirujano general
- Anestesiólogo
- Nutricionista
- Regente de farmacia
- Auxiliar de farmacia
- Ingeniero de TI

- Técnico de TI
- Aprendiz de TI
- Administradora de sede
- Profesional de logística
- Auxiliar de logística
- Auxiliar front line
- Ayudante de logística
- Mensajero conductor
- Aprendiz logística
- Tesorero
- Analista financiera
- Analista de facturación
- Analista de costos
- Auxiliar contable
- Auxiliar contable
- Aprendiz financiera
- Analista de cultura y liderazgo
- Aprendiz de cultura y liderazgo
- Ejecutivo de cuenta norte
- Ejecutivo de cuenta occidente sur
- Ejecutivo de cuenta centro
- Ejecutivo de cuenta oriente
- Sector de servicio al cliente

4.6.6 Mapa de procesos. Colombiana de Trasplantes en su mapa de procesos contempla los misionales, los estratégicos y los de apoyo.

En la figura 1, se describen los procesos misionales de Colombiana de Trasplantes, donde se encuentran los servicios asistenciales, que a su vez se dividen en fases para los trasplantes renales, etapas para los trasplantes hepáticos y ciclos para los trasplantes combinados.

Figura 1. Procesos misionales



Fuente: Colombiana de Trasplantes.

Adicionalmente, encontramos los procesos de apoyo:

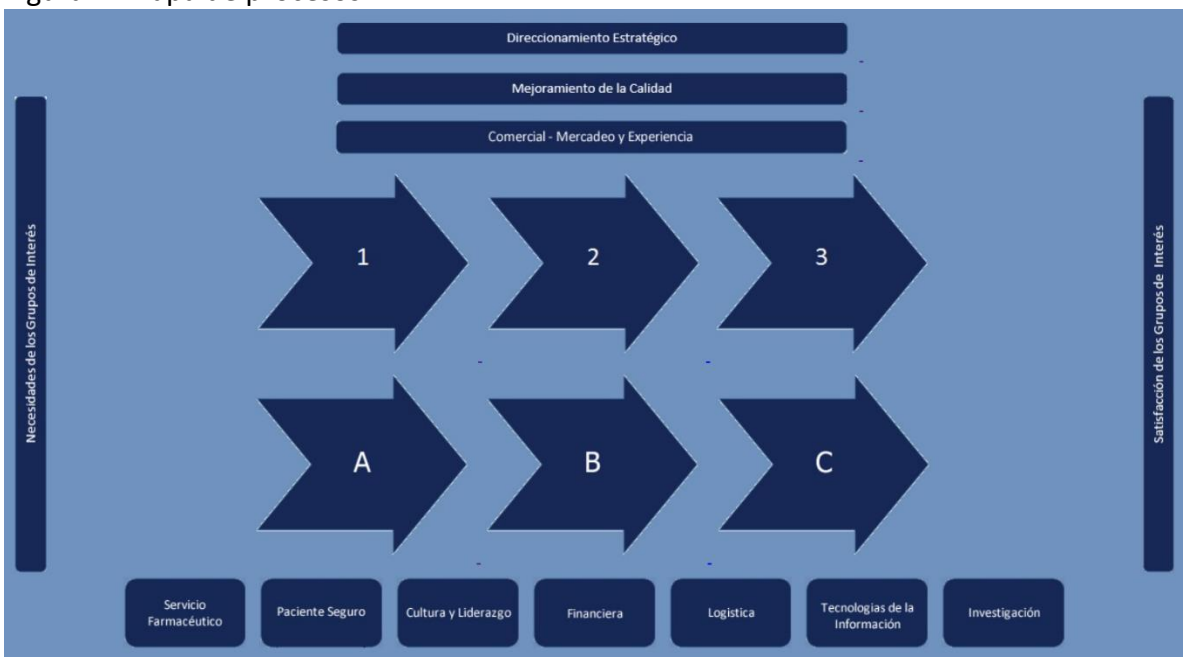
- Servicios famaceuticos.
- Paciente seguro.
- Cultura y liderazgo.
- Financiera.
- Logística.
- Tecnologías de la información.
- Investigación.

Los procesos estratégicos:

- Direccionamiento estratégico.
- Mejoramiento de la calidad.
- Comercial – Mercadeo y experticia.

En la figura 2, se presenta el mapa de procesos definido por Colombiana de Trasplantes, donde se muestran los procesos misionales con las fases representadas con los números del uno al tres y las etapas representadas con las letras A, B y C. Tambien están presentes los procesos estratégicos y de apoyo.

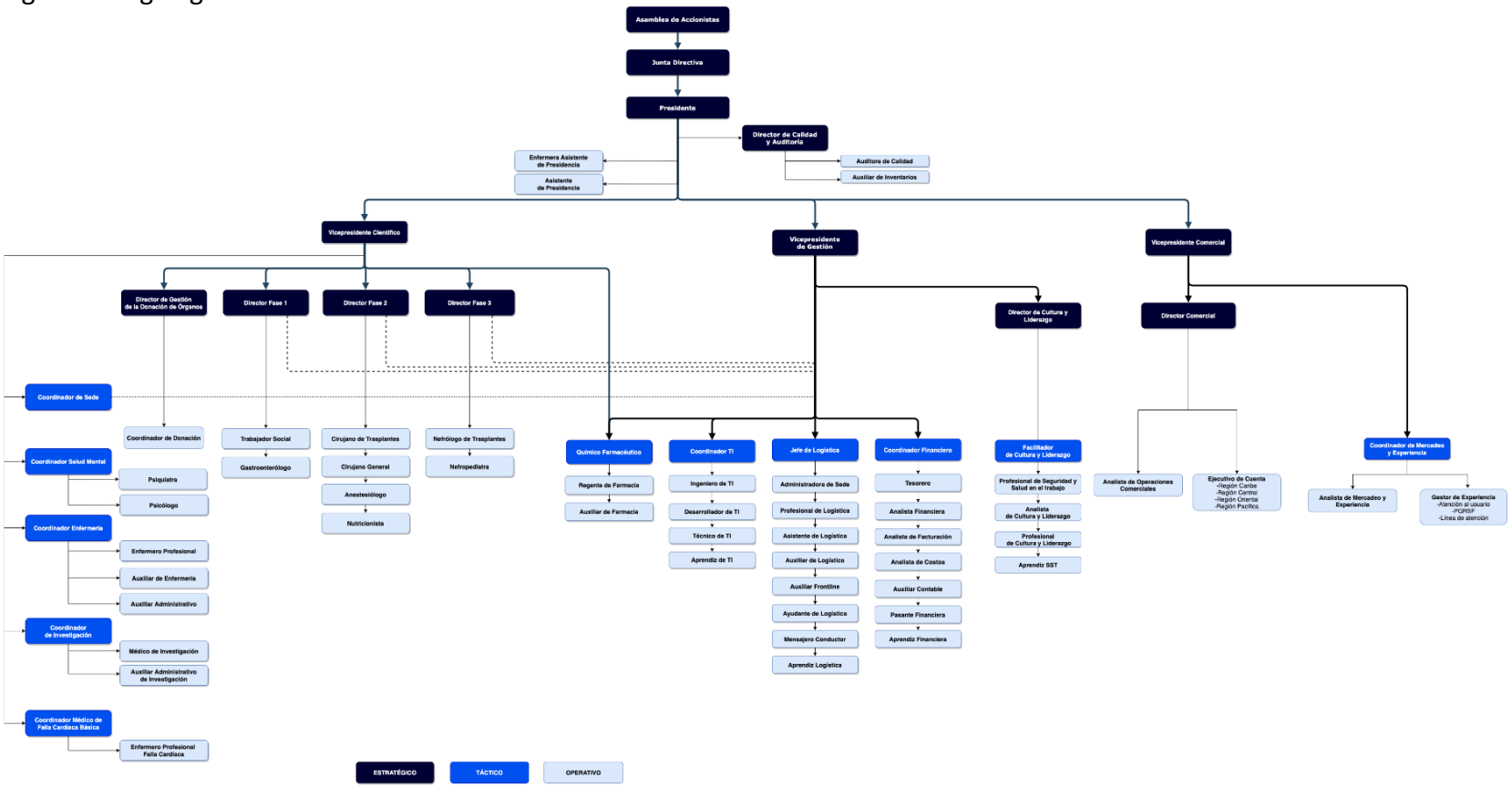
Figura 2. Mapa de procesos



Fuente: Colombiana de Trasplantes.

4.6.7 Organigrama Colombiana de Trasplantes. En la figura 3, se presenta el organigrama que soporta la estructura organizacional de Colombiana de Trasplantes. Se puede identificar claramente los cargos gerenciales, así como la subdivisión de las dependencias de la vicepresidencia científica, la vicepresidencia de gestión y la vicepresidencia comercial.

Figura 3. Organigrama



Fuente: Colombiana de Trasplantes.

4.7 DESCRIPCIÓN DEL PROCESO DE TELEMEDICINA EN COLOMBIANA DE TRASPLANTES

En Colombiana de Trasplantes S.A.S. se tiene definido diferentes actividades en el proceso de Telemedicina para prestarle el servicio a los pacientes que así lo requieren, todo inicia con la evaluación de viabilidad de los pacientes candidatos por parte del auxiliar de investigación donde revisa que se cumplan con criterios médicos y tecnológicos requeridos para ser aceptados en el programa. Cuando un candidato resulta viable, se programa una cita en la agenda comercial y se presenta el candidato para la revisión médica al Coordinador de Investigación, Médico de Investigación y a la Vicepresidencia Científica. Para esta presentación, se obtienen los datos médicos del paciente de la plataforma *ImedicalCloud*, en este punto es la Vicepresidencia Científica quien aprueba el candidato para continuar con el proceso.

Los candidatos aprobados hasta el momento continúan con una verificación técnica por parte del trabajador social que comprueba que los pacientes cumplan con las condiciones tecnológicas establecidas para participar en el programa de telemedicina y da la aprobación final. Todos los candidatos que participan en el proceso de selección son registrados en la base de datos del programa de telemedicina, esto incluye aprobados, no aprobados, retirados y no adherentes.

Cuando un candidato es aprobado se notifica a enfermería mediante un grupo de mensajería electrónica en *WhatsApp* y se programan en la plataforma de *Bookings*. Por otra parte, el auxiliar de investigación contacta telefónicamente al paciente aprobado y le comparte la documentación de consentimiento y autorización de tratamiento de información, donde el paciente tendrá que firmar digitalmente los documentos mediante el servicio de firma electrónica *DocuSing*.

Posteriormente, se realiza seguimiento semanal al paciente, se programan y confirman sus citas, así como sus exámenes de laboratorio, para finalmente realizar la valoración por parte del especialista en una tele consulta.

De ser necesario se coordinará con el área de farmacia y logística el envío de medicamentos y/o dispositivos médicos.

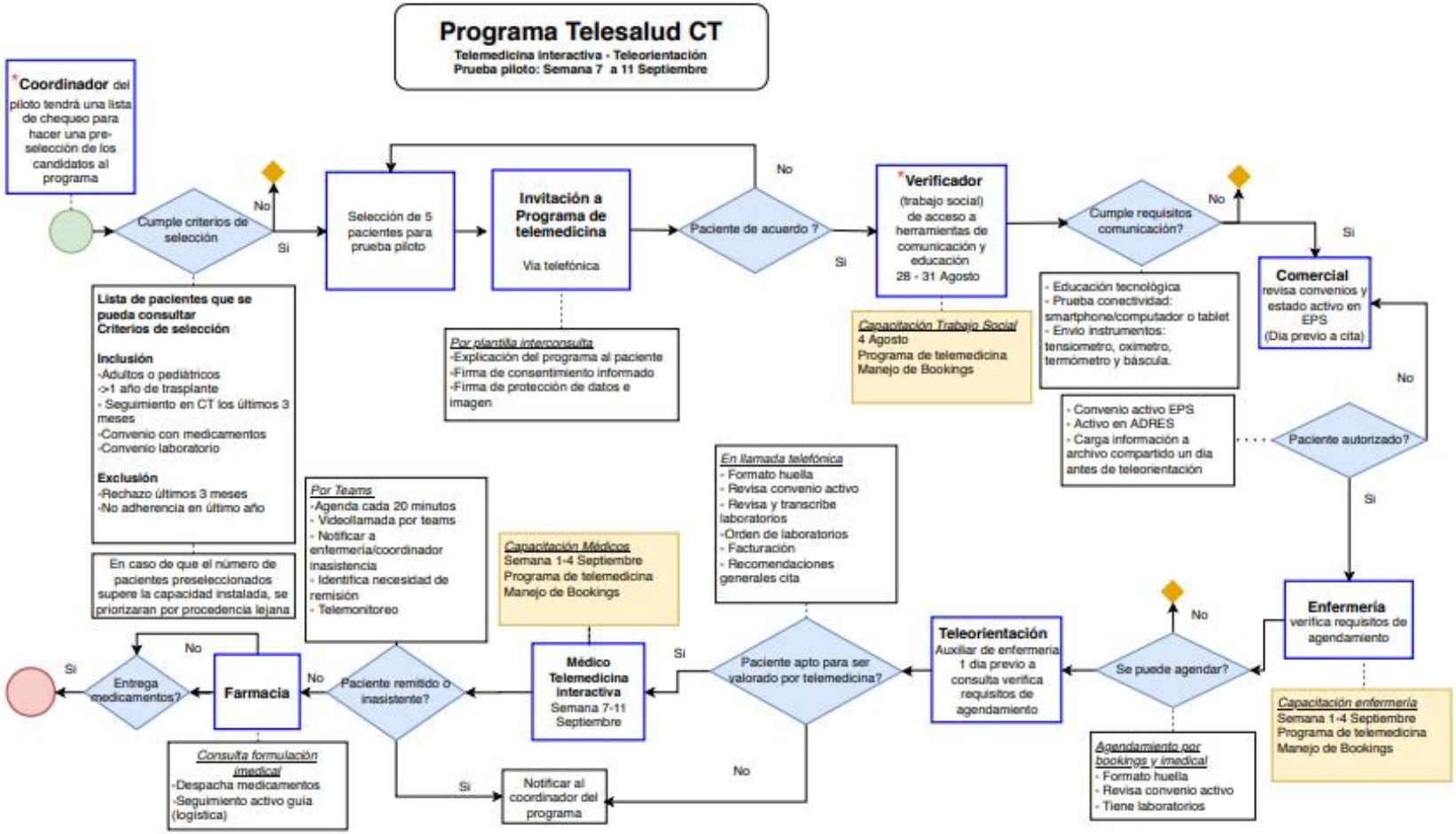
En la figura 4, se presentan las diferentes etapas del flujo de actividades para la atención de pacientes involucrados en el proceso de telemedicina en Colombiana de Trasplantes.

Figura 4. Etapas proceso telemedicina

Fuente: Grupo de investigación Colombiana de Trasplantes.

4.7.1 Flujograma proceso telemedicina. En la figura 5, se presenta el flujograma en detalle del proceso de telemedicina en Colombiana de Trasplantes, donde están plasmadas cada una de las actividades y sus responsables.

Figura 5. Flujograma proceso telemedicina



Fuente: Grupo de investigacion Colombiana de Trasplantes.

5. DISEÑO METODOLÓGICO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La elaboración del diseño del sistema de gestión de seguridad de la información para telemedicina en la IPS Colombiana de Trasplantes contempló el desarrollo gradual de actividades que permitieron recolectar la información general de la IPS, para organizarla y finalmente analizarla con base a las necesidades del proyecto.

Las actividades desarrolladas consistieron en:

- Análisis del estado actual de seguridad de la información en base a la norma ISO/IEC 27001:2013. Esta actividad se realizó mediante el levantamiento de información y entrevistas a los responsables de procesos.
- Levantamiento de información del inventario de activos de información para el proceso de telemedicina. Para esta actividad se analizó el proceso de telemedicina y se identificaron los activos que lo componen.
- Elaboración del análisis de riesgos para los activos de información identificados tomando como referencia la norma ISO/IEC 27005.
- Planteamiento de opciones de tratamiento de los riesgos encontrados para los activos del proceso de telemedicina, que se encontraron fuera del nivel de tolerancia para la empresa.
- Formulación del conjunto de políticas para la seguridad de la información para el proceso de telemedicina con base en la norma ISO/ IEC 27001:2013 anexo A y el código de prácticas GTC-ISO/IEC 27002.
- Desarrollo de una propuesta para el plan de capacitación y concienciación del sistema de seguridad de la información para las partes que intervienen en el proceso de telemedicina.
- Desarrollo de un plan para presentar a la alta dirección una propuesta de la implementación del sistema de seguridad de la información en el proceso de telemedicina. El plan presenta recursos, actividades, opciones de controles, inversión y tiempos de implementación.

5.1 ANÁLISIS DEL ESTADO ACTUAL DE COLOMBIANA DE TRASPLANTES CON BASE A LA NORMA ISO/ IEC 27001:2013

Con el objetivo de tener un punto de partida de cómo se encuentra la IPS Colombiana de Trasplantes S.A.S. frente a la norma ISO 27001:2013 se desarrolló un análisis que permite identificar el estado actual de cumplimiento de la norma en la empresa para el proceso de telemedicina.

En el cuadro 1, se presenta la agenda de entrevistas con el representante de la alta dirección y los responsables de los procesos involucrados en telemedicina en Colombiana de Trasplantes, donde se realizó el levantamiento de información inicial para el diseño del proyecto.

Cuadro 1. Agendamiento entrevistas con responsables de procesos

Cargo	Nombre	Fecha de entrevista
Representante Alta Dirección – vicepresidente de gestión	Pablo Tejerina	12 mayo 2020
Coordinador de Logística	Yamile Mora	9 febrero 2021
Director de Cultura y Liderazgo	Katherine Varón	21 enero 2021
Coordinador de Investigación	Andrea García	29 mayo 2020, 4 junio 2020, 18 enero 2020, 20 abril 2021
Coordinador de TI	Sergio Riveros	12 febrero 2021
Coordinador Financiera	Leidy Guarnizo	20 mayo 2021
Fuente: elaboración propia.		

El 12 de mayo del 2020 se desarrolló la reunión con el vicepresidente de gestión, el señor Pablo Tejerina en representación de la alta dirección de Colombiana de Trasplantes, a quien se le presentó la propuesta para el desarrollo del proyecto “DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA TELEMEDICINA EN LA IPS COLOMBIANA DE TRASPLANTES”, quien aprobó por parte de la alta dirección de Colombiana de Trasplantes su desarrollo.

En el cuadro 2, se plasman los criterios para determinar el estado de cumplimiento de cada control tomando como referencia el instrumento de Evaluación MSPI divulgado por El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, donde está definida una escala de evaluación basada en criterios de implementación y que presenta una calificación en cada nivel. Como en otros sistemas de gestión, un sistema de gestión de seguridad de la información busca la mejora continua, mejora que se ve reflejada mediante la madurez progresiva de los controles, entendiendo que para lograrlo se deben evaluar periódicamente aspectos como efectividad, cambios organizacionales, cambios tecnológicos, entre otros.

Cuadro 2. Escala de valoración del estado de controles ISO 27001:2013 ANEXO A

Escala de valoración de controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Falta total de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, biblioteca de seguridad, Instructivo instrumento Evaluación MSPI.		

En el cuadro 3, se muestra el total acumulado que se presenta al terminar cada evaluación de los dominios de control, correspondiente a la suma total del porcentaje de implementación dividido en el número de controles evaluados, hasta ese punto.

Cuadro 3. Análisis estado actual SGSI

Análisis controles ISO/IEC 27001/2013				
Código	**Objetivo de control**	**Control**	**Porcentaje**	**Estado**
A.5	**Políticas de seguridad de la información**			
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**			
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y las partes externas pertinentes.	40%	Repetible
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	0%	Inexistente
Total del dominio: 20%				
Total acumulado: 20%				
A.6	**Organización de la seguridad de la información**			
A.6.1	**Organización interna**			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	0%	Inexistente
A.6.1.3	Contacto con las autoridades	Se deben tener contactos apropiados con las autoridades pertinentes	0%	Inexistente
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	0%	Inexistente
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	0%	Inexistente
A.6.2	**Dispositivos móviles y teletrabajo**			
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	80%	Gestionado
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	40%	Repetible
Total del dominio: 17%				
Total acumulado: 17,78%				

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.7	**Seguridad de los recursos humanos**			
A.7.1	**Antes de asumir el empleo**			
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	80%	Gestionado
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	80%	Gestionado
A.7.2	**Durante la ejecución del empleo**			
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	0%	Inexistente
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, así como los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	40%	Repetible
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	80%	Gestionado

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.7.3	**Terminación y cambio de empleo**			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	80%	Gestionado
Total del dominio: 60,00%				
Total acumulado: 34,67%				
A.8	**Gestión de activos**			
A.8.1	**Responsabilidad por los activos**			
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	0%	Inexistente
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	0%	Inexistente
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	0%	Inexistente
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se entregan a su cargo, al terminar su empleo, contrato o acuerdo.	0%	Inexistente
A.8.2	**Clasificación de la información**			
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización.	0%	Inexistente
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.	0%	Inexistente
A.8.3	**Manejo de medios**			
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.	0%	Inexistente
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	0%	Inexistente
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	20%	Inicial
Total del dominio: 2%				
Total acumulado: 21,60%				
A.9	**Control de accesos**			
A.9.1	**Requisitos del negocio para control de accesos**			
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	60%	Efectivo
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.9.2	**Gestión de acceso de usuarios**			
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	80%	Gestionado
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	80%	Gestionado
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	0%	Inexistente
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	80%	Gestionado
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	60%	Efectivo
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	80%	Gestionado
A.9.3	**Responsabilidades de los usuarios**			
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	80%	Gestionado

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.9.4	**Control de acceso a sistemas y aplicaciones**			
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	0%	Inexistente
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	0%	Inexistente
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	80%	Gestionado
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	0%	Inexistente
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe registrar el acceso a los códigos fuente de los programas.	0%	Inexistente
Total del dominio: 43%				
Total acumulado: 29,23%				
A.10	**Criptografía**			
A.10.1	**Controles criptográficos**			
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	0%	Inexistente
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante su ciclo de vida.	0%	Inexistente
Total del dominio: 0,00%				
Total acumulado: 27,80%				

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.11	**Seguridad física y del entorno**			
A.11.1	**Áreas seguras**			
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	60%	Efectivo
A.11.1.2	Control de accesos físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite acceso a personal autorizado.	60%	Efectivo
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	80%	Gestionado
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	80%	Gestionado
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	80%	Gestionado
A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	80%	Gestionado
A.11.2	**Equipos**			
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	0%	Inexistente
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	80%	Gestionado
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	80%	Gestionado
A.11.2.5	Retiro de activos	Los equipos, información o *software* no se deben retirar de su sitio sin autorización previa.	0%	Inexistente
A.11.2.6	Seguridad de activos y equipos fuera de la oficina	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	0%	Inexistente
A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o *software* licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	0%	Inexistente
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	80%	Gestionado
A.11.2.9	Políticas de escritorio y pantalla limpios	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	0%	Inexistente
Total del dominio: 45,33%				
Total acumulado: 32,50%				

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.12	**Seguridad de las operaciones**			
A.12.1	**Procedimientos operacionales y responsabilidades**			
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	80%	Gestionado
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	0%	Inexistente
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	0%	Inexistente
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	0%	Inexistente
A.12.2	**Protección contra códigos maliciosos**			
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos.	80%	Gestionado
A.12.3	**Proteger contra la pérdida de datos**			
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de información, *software* e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	40%	Repetible

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.12.4	**Registro y seguimiento**			
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros a cerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	80%	Gestionado
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	80%	Gestionado
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	80%	Gestionado
A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	80%	Gestionado
A.12.5	**Control de *software* operacional**			
A.12.5.1	Instalación de *software* en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de *software* en sistemas operativos.	80%	Gestionado
A.12.6	**Gestión de la vulnerabilidad técnica**			
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	0%	Inexistente
A.12.6.2	Restricciones sobre la instalación de *software*	Se debe establecer e implementar las reglas para la instalación de *software* por parte de los usuarios.	80%	Gestionado

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.12.7	**Consideraciones sobre auditorías de sistemas de información**			
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	0%	Inexistente
Total del dominio: 49%				
Total acumulado: 35,71%				
A.13	**Seguridad de las comunicaciones**			
A.13.1	**Gestión de la seguridad de las redes**			
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	60%	Efectivo
A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	40%	Repetible
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	80%	Gestionado
A.13.2	**Transferencia de información**			
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	40%	Repetible
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	20%	Inicial

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	60%	Efectivo
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	80%	Gestionado
Total del dominio: 54%				
Total acumulado: 37,40%				
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A.14.1	**Requisitos de seguridad de los sistemas de información**			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	0%	Inexistente
A.14.1.2	Seguridad de servicio de las aplicaciones en redes publicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	0%	Inexistente
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado la alteración no autorizada de mensajes, la divulgación no autorizada y la divulgación o reproducción de mensajes no autorizados.	80%	Gestionado

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.14.2	**Seguridad en los procesos de desarrollo y soporte**			
A.14.2.1	Políticas de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de *software* y de sistemas, a los desarrollos dentro de la organización.	0%	Inexistente
A.14.2.2	Procedimiento de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	0%	Inexistente
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	0%	Inexistente
A.14.2.4	Restricción en los cambios a los paquetes de *software*	Se deben desalentar las modificaciones a los paquetes de *software*, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	0%	Inexistente
A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	0%	Inexistente
A.14.2.6	Ambiente seguro de desarrollo	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.14.2.7	Desarrollo externamente contratado	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	0%	Inexistente
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	0%	Inexistente
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	0%	Inexistente
A.14.3	**Datos de pruebas**			
A.14.3.1	Protección de datos de pruebas	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	0%	Inexistente
Total del dominio: 6%				
Total acumulado: 32,89%				
A.15	**Relaciones con los proveedores**			
A.15.1	**Seguridad de la información en las relaciones con los proveedores**			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	0%	Inexistente
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	0%	Inexistente
A.15.2	**Gestión de la prestación de servicios de proveedores**			
A.15.2.1	Seguimiento y revisión a los servicios proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	20%	Inicial
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	20%	Inicial
Total del dominio: 8%				
Total acumulado: 31,58%				
A.16	**Gestión de incidentes de seguridad de la información**			
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**			
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	0%	Inexistente
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	0%	Inexistente
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decir si se van a clasificar como incidentes de seguridad de la información.	0%	Inexistente
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	0%	Inexistente
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	0%	Inexistente
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que puede servir como evidencia.	0%	Inexistente
Total del dominio: 0%				
Total acumulado: 29,41%				
A.17	**Aspectos de seguridad de la información de la gestión de continuidad del negocio**			
A.17.1	**Continuidad de seguridad de la información**			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	0%	Inexistente
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	0%	Inexistente
A.17.2	**Redundancia**			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	0%	Inexistente
Total del dominio: 0%				
Total acumulado: 28,30%				
A.18	**Cumplimiento**			
A.18.1	**Cumplimiento de requisitos legales y contractuales**			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	80%	Gestionado

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de *software* patentados.	60%	Efectivo
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	80%	Gestionado
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	60%	Efectivo
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	0%	Inexistente
A.18.2	**Revisiones de seguridad de la información**			
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	0%	Inexistente
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	0%	Inexistente

Cuadro 3. (Continuación)

Código	Objetivo de control	Control	Porcentaje	Estado
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	0%	Inexistente
Total del dominio: 35%				
Total acumulado: 28,77%				
Fuente: elaboración propia, con base en la Norma ISO/IEC 27001:2013 Anexo A.				

En el cuadro 4, se presentan el número de controles por cada dominio de control y su respectivo porcentaje de cumplimiento, así como el cumplimiento deseado. Se encontró que de los 114 controles contemplados en la norma ISOIEC 27001:2013 se tiene un acumulado de implementación que representa un porcentaje del 28,77% de los controles totales.

Cuadro 4. Estado de cumplimiento de controles ISO/IEC 27001:2013 Anexo A

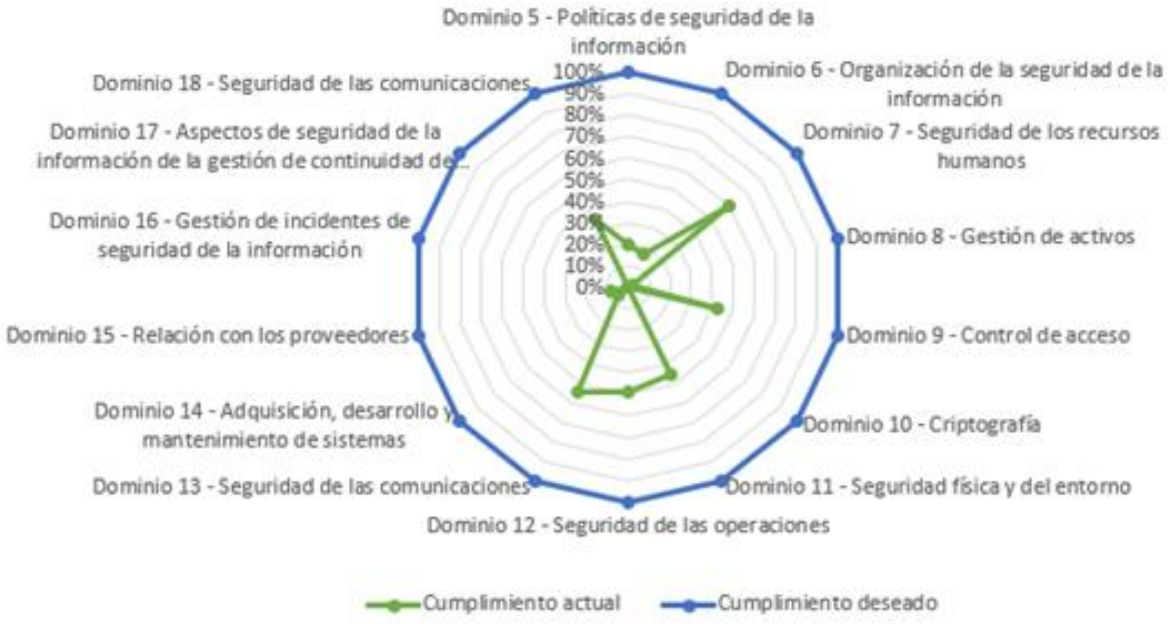
Nombre dominio de control	Controles que aplican	Cumplimiento actual	Cumplimiento deseado
Dominio 5 - Políticas de seguridad de la información	2	20%	100%
Dominio 6 - Organización de la seguridad de la información	7	17%	100%
Dominio 7 - Seguridad de los recursos humanos	6	60%	100%
Dominio 8 - Gestión de activos	10	2%	100%
Dominio 9 - Control de acceso	14	43%	100%
Dominio 10 – Criptografía	2	0%	100%
Dominio 11 - Seguridad física y del entorno	15	45,33%	100%
Dominio 12 - Seguridad de las operaciones	14	49%	100%

Cuadro 4. (Continuación)

Nombre dominio de control	Controles que aplican	Cumplimiento actual	Cumplimiento deseado
Dominio 13 - Seguridad de las comunicaciones	7	54%	100%
Dominio 14 - Adquisición, desarrollo y mantenimiento de sistemas	13	6%	100%
Dominio 15 - Relación con los proveedores	5	8%	100%
Dominio 16 - Gestión de incidentes de seguridad de la información	7	0%	100%
Dominio 17 - Aspectos de seguridad de la información de la gestión de continuidad de negocio	4	0%	100%
Dominio 18 - Seguridad de las comunicaciones	8	35%	100%
Fuente: elaboración propia.			

En la figura 6, se muestra una gráfica tipo radial con una representación visual del estado de cumplimento de los controles ISO/IEC 27000:2013 en Colombiana de Trasplantes.

Figura 6. Gráfica Estado de cumplimento controles ISO/IEC 27000:2013



Fuente: elaboración propia.

5.1 ACTIVOS DE INFORMACIÓN PARA EL PROCESO DE TELEMEDICINA

Dentro del dominio de control A.8 del anexo A de la norma ISO/ IEC 27001 se establece la necesidad de gestionar los activos de información y definir las responsabilidades de protección apropiadas.

5.2.1 Inventarios de activos. En Colombiana de Trasplantes no se tiene un inventario de activos consolidado y actualizado, por lo que se realiza la identificación de los activos de información inicial para el proceso de telemedicina, mediante el levantamiento de información con los responsables de los procesos involucrados, esto, teniendo en cuenta que el inventario de activos es un prerrequisito fundamental para el análisis de riesgos con base en la norma ISO/IEC 27005.

En el cuadro 5, se presentan los tipos de activos con base en el anexo B de la norma ISO/IEC 27005 donde se encuentran descritos y con ejemplos.

Cuadro 5. Tipos de Activos

Tipo de activos	Descripción/Ejemplos
Información	Activo primario, Información vital para el proceso, información personal, información estratégica, etc.
Hardware	Elementos físicos que dan soporte a los procesos, equipos, periféricos, medios electrónicos, etc.
Software	Todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos, sistema operativo, *software* de servicio, aplicaciones de negocio, etc.
Redes	Dispositivos de telecomunicaciones utilizados para interconectar varios equipos remotos físicamente o los elementos de un sistema de información, equipos de comunicación, interfases de comunicación, etc.
Personal	Personas involucradas en el sistema de información, personas a cargo de la toma de decisiones, usuarios, personal de operación y mantenimiento, etc.
Fuente: norma ISO/IEC 27005:2009 Anexo B.	

En el cuadro 6, se presentan los activos relacionados con el proceso de telemedicina descritos con base al cuadro 5 y se define la nomenclatura del identificador del activo para cada tipo: Tipo información con la nomenclatura iniciando con INF, tipo *hardware* iniciando con HW, tipo *software* iniciando con SW, tipo red iniciando con RD y tipo personal iniciando con RH; de esta forma los activos serán referenciados de forma individual en los siguientes apartados del diseño.

Cuadro 6. Inventario de activos

Código	Activo	Tipo de activo	Descripción	Cantidad
INF1	Información de contacto	Información	Información personal del paciente para contacto: Nombres, apellidos, edad, números telefónicos, información de acompañante, dirección física, barrio, ciudad, dirección de correo electrónico, número de cedula y EPS.	24
INF2	Historia clínica	Información	Registro cronológico de las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud.	24
INF3	Reporte telemedicina	Información	Informe mensual de atención en telemedicina.	1
HW1	Equipo portátil ingeniero TI	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, DD 150Gb SSD/ 1Tb HDD.	1
HW2	Equipo portátil tecnólogo TI	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	1
HW3	Equipo portátil Auxiliar de Investigación	*Hardware*	Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	1
HW4	Equipo portátil Coordinador de Investigación	*Hardware*	Equipo marca Lenovo, Core i5, RAM 8Gb, DD 256Gb SSD, Tarjeta gráfica invidia.	1
HW5	Equipo portátil médico de investigación	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	1
HW6	Equipo portátil agente comercial – *Call Center*	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	4
HW7	Equipo Portátil Verificador	*Hardware*	Equipo marca Lenovo, Core i5, 8 RAM DD 256 SSD.	1
HW8	Equipo portátil coordinador de enfermería	*Hardware*	Equipo marca MacBook, Air 13”, 128 SSD, 8 RAM	1
HW9	Equipo portátil médico telemedicina interactiva	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	7
HW10	Equipo escritorio médico telemedicina interactiva	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	10
HW11	Equipo Portátil farmacia	*Hardware*	Equipo marca Lenovo, Core I7, RAM 8Gb, 1Tb HDD.	1
HW12	UPS, sistema de alimentación eléctrica ininterrumpida	*Hardware*	Equipo de respaldo de energía marca *Libert* trifásica *OnLine*, capacidad 30 KVA.	1
SW1	Solución Ofimática	*Software*	Licencia Microsoft Office 365, Outlook, word, excel y power point.	29
SW2	Solución de mensajería y comunicaciones	*Software*	Licencia Microsoft *Teams*, herramienta para la realización de las teleconsultas y conferencias.	29
SW3	Solución de gestión documental	*Software*	Licencia Microsoft SharePoint y OneDrive, herramienta para almacenar y compartir información del proceso.	29
SW4	Solución para programar y administrar citas medicas	*Software*	Licencia Microsoft *Bookings*, herramienta para agendamiento de citas médicas y actividades de pacientes.	2
SW5	Sistema operativo Windows	*Software*	Licencia Microsoft Windows 10 profesional	28

Cuadro 6. (Continuación)

Código	Activo	Tipo de activo	Descripción	Cantidad
SW6	Sistema operativo Mac OS X	*Software*	Licencia Apple macOS 10.13 High Sierra	1
SW6	Sistema operativo Mac OS X	*Software*	Licencia Apple macOS 10.13 High Sierra	1
SW7	Solución de telefonía	*Software*	Licencia como servicio *Wolkvoz*	4
SW8	Solución de gestión de historias clínicas	*Software*	Servicio en nube *Imedical Cloud* para la administración de historias clínicas, agendamientos, exámenes de laboratorio, inventario de medicamentos, etc.	1
SW9	Solución de firma digital	*Software*	Servició en nube *DocuSign*, para el manejo de firmas digitales de consentimientos informados de paciente y documentos en general.	1
SW10	Herramienta Administración base de datos	*Software*	Microsoft SQL *Server Management Studio Express*, permite la conexión a la base de datos del servicio *ImedicalCloud* en nube para la ejecución del script SQL que genera los datos del informe mensual de telemedicina.	2
RD1	Firewall	Red	*Firewall* marca Cisco referencia Meraky MX84, para los permisos de conexión y filtrado de contenido.	1
RD2	*Switch Core*	Red	*Switch* marca Cisco referencia Meraky MS250-24, 24 puertos.	1
RD3	*Switch* acceso	Red	*Switch* marca Cisco referencia Meraky MS120-24P, 24 puertos.	4
RD4	Punto de acceso inalámbrico 1	Red	*Access Point* marca Cisco referencia Meraky MR42.	1
RD5	Punto de acceso inalámbrico 2	Red	*Access Point* marca Cisco referencia Meraky MR33.	4
RD6	Canal internet 1	Red	Canal de internet, proveedor ETB, capacidad 100 Mb.	1
RD7	Canal internet 2	Red	Canal de internet, proveedor Claro, capacidad 150 Mb.	1
RD8	Cableado de red	Red	Conexiones físicas internas, medio de cobre, categoría 6.	1
RH1	Ingeniero TI	Personal	Ingeniero de Sistemas y Desarrollo, responsable de la generación del informe mensual de telemedicina y las consultas relacionadas con las historias clínicas. Apoyo casos de soporte con el proveedor del servicio *Imedical Cloud.*	1
RH2	Tecnólogo TI	Personal	Tecnólogo en sistemas, responsable de apoyar la generación de informes mensuales de telemedicina y consultas relacionadas. Apoyo casos de soporte con el proveedor del servicio *Imedical Cloud.*	1

Cuadro 6. (Continuación)

Código	Activo	Tipo de activo	Descripción	Cantidad
RH3	Auxiliar de investigación	Personal	Enfermera profesional en el área de la salud, responsable de la preselección de pacientes nuevos, el registro de la agenda, apoyo en la presentación de candidatos, registro de pacientes en la base de datos, confirmación de pacientes, bienvenida de pacientes, envíos de documentos de autorización para el tratamiento de datos para firma de los pacientes, seguimiento de actividades y apoyo en él envió de dispositivos médicos.	1
RH4	Coordinador de investigación	Personal	Médico especialista en epidemiologia, responsable del programa de investigación en Colombiana de Trasplantes y encargada de la implementación y seguimiento del programa de telemedicina.	1
RH5	Médico de investigación	Personal	Médico especialista en investigación molecular o afines, responsable de la preselección de pacientes nuevos, el registro de la agenda, apoyo en la presentación de candidatos, registro de pacientes en la base de datos, confirmación de pacientes, bienvenida de pacientes, envíos de documentos de autorización para el tratamiento de datos para firma de los pacientes, seguimiento de actividades y apoyo en él envió de dispositivos médicos.	1
RH6	Verificador	Personal	Trabajador Social en el área de la salud, responsable de la verificación tecnológica de los requisitos por parte de los candidatos al servicio de telemedicina.	1
RH7	Coordinador de enfermería	Personal	Enfermera profesional en el área de la salud, responsable del acompañamiento semanal de los pacientes programados en el servicio de telemedicina para los servicios de laboratorio, preconsulta y valoración.	1
RH8	Médico telemedicina Interactiva	Personal	Médico Especialista en nefrología responsable de la valoración del paciente en fase 3.	7
RH9	Responsable Farmacia	Personal	Químico farmacéutico responsable de la preparación y logística para el envío de medicamentos a los pacientes.	1
RH10	Agente comercial – *Call Center*	Personal	Profesional, técnico o tecnólogo responsable del contacto con los pacientes del programa para la asignación de citas o brindar información general.	4

Fuente: elaboración propia.

5.2.2 Valoración de activos. Para la valoración de activos la norma ISO/IEC27005 plantea definir la escala a utilizar y los criterios para ubicar los activos en esta, las escalas pueden ser cuantitativas, cualitativas o ambas, para los cálculos del ejercicio se utiliza principalmente escalas cuantitativas.

Los criterios utilizados para la valoración de los activos de información están basados en: la pérdida de confidencialidad plasmada en el cuadro 7, la pérdida de integridad en el cuadro 8 y la pérdida de disponibilidad en el cuadro 9, donde la escala de cada uno está dividida en alto, medio y bajo; con sus respectivos valores cuantitativos.

Cuadro 7. Criterio de valoración de confidencialidad

Confidencialidad		
Valor cuantitativo	**Valor cualitativo**	**Descripción**
3	Alto	Información disponible exclusivamente para el personal autorizado dentro del proceso de telemedicina, en caso de ser divulgada sin autorización a terceros o externos del proceso puede incurrir en consecuencias negativas de carácter reputacional, disciplinario, legal y/o económico.
2	Medio	Información disponible en general para todos los empleados y procesos de Colombiana de Trasplantes, pero no puede ser divulgada sin autorización a terceros o externos, porque puede incurrir en consecuencias negativas de carácter reputacional, disciplinario, legal y/o económico.
1	Bajo	Información disponible en general para todos los empleados, procesos y usuarios de Colombiana de Trasplantes, que puede ser divulgada fuera de la entidad sin incurrir en consecuencias negativas.
Fuente: elaboración propia.		

Cuadro 8. Criterio de valoración de integridad

Integridad		
Valor cuantitativo	**Valor cualitativo**	**Descripción**
3	Alto	Información que al perder sus atributos de exactitud y completitud puede incurrir en consecuencias severas, de carácter operativo, reputacional, legal y/o económico; con una tolerancia máxima para restauración de 1 hora.
2	Medio	Información que al perder sus atributos de exactitud y completitud puede incurrir en consecuencias negativas de carácter operativo, reputacional, legal y/o económico; con una tolerancia máxima para restauración de 24 horas.
1	Bajo	Información que al perder sus atributos de exactitud y completitud no representa consecuencias significativas; con una tolerancia máxima para restauración de 8 días.
Fuente: elaboración propia.		

Cuadro 9. Criterio de valoración de disponibilidad

Disponibilidad		
Valor cuantitativo	**Valor cualitativo**	**Descripción**
3	Alto	La no disponibilidad del activo de información por más de 30 minutos genera una detención total del proceso con un impacto severo en la operación, ocasionando pérdidas económicas y de imagen.
2	Medio	La no disponibilidad del activo de información por más de 24 horas genera una detención parcial del proceso con un impacto negativo en la operación, ocasionando pérdidas económicas.
1	Bajo	El activo de información puede tener una indisponibilidad máxima de cuatro días, sin que esta represente impacto en la continuidad del proceso.
Fuente: elaboración propia.		

Se define la escala en tres niveles para la valoración independiente de cada uno de los atributos de seguridad, donde tres (3) es el nivel más alto, dos (2) el nivel medio y uno (1) el nivel bajo, para la valoración general de los activos de información se define igualmente una escala con tres niveles donde el valor total corresponde a la sumatoria de los parciales de cada uno de los atributos analizados.

En el cuadro 10, se presenta la sumatoria de los criterios de valoración, donde entre tres y cuatro corresponde al nivel bajo, entre cinco y siete al nivel medio, y finalmente entre ocho y nueve el nivel alto.

Cuadro 10. Criterio de valoración general de activos

Valor cuantitativo	**Nivel**
9	Alto
8	
7	Medio
6	
5	
4	Bajo
3	
Fuente: elaboración propia.	

Con base en los atributos de los activos, su valoración particular y la definición de niveles de valoración general se construye el cuadro 11, con la información consolidada de los activos de información, valoración general y responsables.

Cuadro 11. Valoración de activos

Código	Activo	Responsable	Confidencialidad	Integridad	Disponibilidad	Valoración
INF1	Información de contacto	Telemedicina	3	3	3	9
INF2	Historia clínica	Telemedicina	3	3	3	9
INF3	Reporte telemedicina	Telemedicina	3	3	1	7
HW1	Equipo portátil ingeniero TI	Tecnología	3	2	1	6
HW2	Equipo portátil tecnólogo TI	Tecnología	3	2	1	6
HW3	Equipo portátil Auxiliar de Investigación	Tecnología	3	2	1	6
HW4	Equipo portátil coordinador de Investigación	Tecnología	3	2	1	6
HW5	Equipo portátil médico de investigación	Tecnología	3	2	1	6
HW6	Equipo portátil agente comercial – *Call Center*	Tecnología	2	2	1	5
HW7	Equipo Portátil Verificador	Tecnología	3	2	2	7
HW8	Equipo portátil coordinador de enfermería	Tecnología	3	3	2	8
HW9	Equipo portátil médico telemedicina interactiva	Tecnología	3	2	1	6
HW10	Equipo escritorio médico telemedicina interactiva	Tecnología	2	1	1	4
HW11	Equipo Portátil farmacia	Tecnología	3	3	2	8
HW12	UPS, sistema de alimentación eléctrica	Tecnología	1	1	3	5
SW1	Solución Ofimática	Tecnología	1	1	2	4
SW2	Solución de mensajería y comunicaciones	Tecnología	3	2	3	8
SW3	Solución de gestión documental	Tecnología	3	3	2	9
SW4	Solución para programar y administrar citas medicas	Tecnología	2	2	2	6
SW5	Sistema operativo Windows	Tecnología	1	1	1	3
SW6	Sistema operativo Mac OS X	Tecnología	1	1	1	3
SW7	Solución de telefonía	Tecnología	2	2	2	6
SW8	Solución de gestión de historias clínicas	Tecnología	3	3	3	9
SW9	Solución de firma digital	Tecnología	2	3	2	7
SW10	Herramienta Administración base de datos	Tecnología	1	1	2	5
RD1	Firewall	Tecnología	3	2	3	8
RD2	*Switch Core*	Tecnología	3	2	3	8
RD3	*Switch* acceso	Tecnología	3	2	2	7
RD4	Punto de acceso inalámbrico	Tecnología	3	2	2	7
RD5	Punto de acceso inalámbrico	Tecnología	3	2	2	7

Cuadro 11. (Continuación)

Código	Activo	Responsable	Confidencialidad	Integridad	Disponibilidad	Valoración
RD6	Canal internet 1	Tecnología	3	2	2	7
RD7	Canal internet 2	Tecnología	3	2	2	7
RD8	Cableado de red	Tecnología	1	2	1	4
RH1	Ingeniero TI	Tecnología	3	2	2	7
RH2	Tecnólogo TI	Tecnología	3	2	2	7
RH3	Auxiliar de investigación	Investigación	3	3	1	7
RH4	Coordinador de Investigación	Investigación	3	2	1	6
RH5	Médico de investigación	Investigación	3	3	1	7
RH6	Verificador	Trabajo Social	3	3	2	8
RH7	Coordinador de enfermería	Asistencial	3	3	2	8
RH8	Médico telemedicina Interactiva	Asistencial	3	3	1	7
RH9	Responsable Farmacia	Asistencial	3	3	2	8
RH10	Agente comercial – *Call Center* Personal	Comercial	3	2	1	6

Fuente: elaboración propia.

5.3 ANÁLISIS DE RIESGOS

Parte fundamental del diseño del sistema de seguridad de la información en el proceso de telemedicina en Colombiana de Trasplantes, es realizar la valoración de los riesgos como lo indica el numeral 8.2 de la norma ISO/IEC 27001:2013, actividad que se debe desarrollar periódicamente o cuando el proceso tenga un cambio importante; todas las evidencias deben quedar documentadas. Posterior a la identificación de los activos se identifican las amenazas y vulnerabilidades relacionadas, adicionalmente se tiene en cuenta los controles existentes, pero al no existir análisis de riesgos previos en consecuencia no se disponen de planes de tratamiento definidos por Colombiana de Trasplantes para tener en cuenta en el análisis.

5.3.1 Identificación de Amenazas. En el cuadro 12, se presentan las amenazas tomando como referencia el catálogo tipos de amenazas de la norma ISO/IEC 27005 anexo C y se les asigna un código que inicia con la letra A para su manejo en los siguientes apartados del diseño. Para el análisis de las amenazas se tiene en cuenta las vulnerabilidades y las consecuencias que generarían la pérdida de alguno de los atributos de la información.

Cuadro 12. Definición de Amenazas

Código	Amenaza	Tipo de amenaza	Vulnerabilidad
A1	Fuego	Daño físico	Ausencia de controles adecuados y exposición a conexiones eléctricas defectuosas.
A2	Daño por agua o líquidos	Daño físico	Ausencia a condiciones de uso inadecuadas y exposición a líquidos.
A3	Destrucción de equipos o medios	Daño físico	Manipulación indebida de equipos y medios. Falta de entrenamiento al personal en manipulación y disposición de equipos. Ausencia de un plan de reposición de equipos y medios por deterioro.
A4	Fenómenos naturales (terremoto, inundaciones, pandemias, climáticos)	Eventos naturales	Ausencia de un plan de continuidad.
A5	Pérdida en el suministro de energía	Pérdida de servicios esenciales	Ausencia de respaldo de energía fuera de las instalaciones.
A6	Falla en equipo de telecomunicaciones	Compromiso de la información	Ausencia de conexión a internet.
A7	Espionaje remoto	Compromiso de la información	Arquitectura insegura de red. Ausencia de controles sobre *software* de acceso remoto.
A8	Hurto de medios y documentos	Compromiso de la información	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad. Insuficiencia de política sobre uso de medios y documentos. Ausencia de política de escritorio y pantalla limpios.
A9	Hurto equipos	Compromiso de la información	Ausencia de procedimientos definidos para el tratamiento de incidentes de seguridad de la información. Ausencia de política forma sobre la utilización de computadores portátiles y medios. Insuficiencia en el control de activos fuera de las instalaciones.
A10	Recuperación de información sobre equipos reciclados y rentados	Compromiso de la información	Ausencia de procedimiento de borrado seguro para equipos que salen de operación.
A11	Divulgación	Compromiso de la información	Ausencia de mecanismos de monitoreo sobre el flujo de información personal de pacientes no autorizada.
A12	Manipulación con *software*	Compromiso de la información	Ausencia en el seguimiento de la ejecución de copias de respaldo en los equipos. Descarga y uso no controlado de *software.* Intrusiones por explotación de brechas y vulnerabilidades.
A13	Códigos maliciosos	Compromiso de la información	Ausencia de controles de navegación y uso de medios de almacenamiento extraíbles. Descarga y uso no controlado de s*oftwar*e. Ataques de código desconocido.
A14	Falla de equipo	Fallas técnicas	Ausencia de planes de continuidad. Ausencia de un plan de reposición de equipos y medios por deterioro.
A15	Mal funcionamiento de equipo	Fallas técnicas	Ausencia de un plan de mantenimiento de equipos.
A16	Mal funcionamiento del *software*	Fallas técnicas	Ausencia de plan de instalación de parches y actualizaciones de *software*.

Cuadro 12. (Continuación)

Código	Amenaza	Tipo de amenaza	Vulnerabilidad
A17	Incumplimiento en el mantenimiento del sistema de información	Fallas técnicas	Ausencia de un plan de mantenimiento de equipos.
A18	Uso no autorizado de equipo	Acciones no autorizadas	Insuficiencia en la política de uso autorizado de equipo, medios de telecomunicaciones y mensajería.
A19	Uso no autorizado de *software*	Acciones no autorizadas	Insuficiencia en controles y en la política de uso autorizado de *software.*
A20	Corrupción de datos	Acciones no autorizadas	Ausencia de control para la calidad de datos de las historias clínicas de los pacientes.
A21	Error de uso	Compromiso de funciones	Entrenamiento insuficiente en seguridad. Falta de conciencia acerca de la seguridad. Uso incorrecto de s*oftware* y *hardware*.
A22	Abuso de derechos	Compromiso de funciones	Ausencia de control para el bloqueo de la sesión de trabajo en equipos desatendidos. Asignación herrada de derechos de acceso. Ausencia de auditorías regulares.
A23	Falsificación de derechos	Compromiso de funciones	Gestión deficiente de contraseñas para sistemas operativos de usuarios finales.
A24	Incumplimientos en la disponibilidad del personal	Compromiso de funciones	Ausencia de personal.

Fuente: elaboración propia con base en la Norma ISO/IEC 27005:2009 Anexo C/D.

5.3.2 Valoración de impacto. En el cuadro 13, se describe la escala para la valoración del impacto teniendo en cuenta las pérdidas en cada uno de los niveles, el impacto se genera cuando se materializa un evento o un incidente de seguridad de la información, teniendo en cuenta que como lo indica la norma el impacto puede tener un costo diferente al valor del activo, así como puede ser directo relacionado con la operación o indirecto asociado a costos futuros.

Adicionalmente, el valor del impacto cambia gradualmente con la implementación del plan de tratamiento y los controles definidos, también cambia en relación con los cambios propios del proceso de telemedicina, así como en las modificaciones que sufren los requerimientos del negocio y de regulación.

Cuadro 13. Criterio de valoración de impacto

Impacto		
Valor	**Criterio**	**Descripción**
0	Muy bajo	Sin pérdidas de activos, sin daños reputacionales o incumplimientos de los objetivos de la organización.
1	Bajo	Pérdidas menores de activos, afectación mínima de la seguridad. Pérdidas financieras inferiores a $3.000.000 millones de pesos.
2	Medio	Pérdidas de activos, lesiones menores, daños de reputación e incumplimiento parcial de los objetivos de la organización. Pérdidas financieras entre $3.000.001 millones de pesos y 30.000.000 millones de pesos.
3	Alto	Pérdidas elevadas de activos, lesiones severas, daños graves de reputación e incumplimiento total de los objetivos de la organización. Pérdidas financieras entre $30.000.001 millones de pesos y 130.000.000 millones de pesos.
4	Muy Alto	Pérdidas elevadas de activos, lesiones severas, daños graves de reputación e incumplimiento total de los objetivos de la organización que conduzca a la liquidación de la empresa. Pérdidas financieras superiores a $ 130.000.001 millones de pesos.
Fuente: elaboración propia.		

5.3.3 Valoración de probabilidad. En el cuadro 14, se describe la escala para la valoración de la probabilidad de ocurrencia de la materialización de una amenaza teniendo en cuenta los antecedentes del número de ocurrencias presentadas en cada uno de los niveles para Colombiana de Trasplantes.

Cuadro 14. Criterio de valoración de probabilidad

Probabilidad			
Valor	**Criterio**	**Descripción**	**Frecuencia**
0	Muy baja	Se espera que nunca ocurra.	Cinco años sin ocurrencia.
1	Baja	Puede suceder en ocasiones remotas.	Una vez en los últimos cinco años.
2	Media	Sucede eventualmente.	Una vez en los últimos dos años.
3	Alta	Sucede regularmente una vez al año.	Una vez en el último año.
4	Muy Alta	Se espera que el evento ocurra en cualquier momento.	Una o más veces en los últimos seis meses.
Fuente: elaboración propia.			

5.3.4 Método de Valoración del riesgo. Para la valoración de riesgo se tienen en cuenta los criterios definidos en cuanto a la valoración de la probabilidad de ocurrencia de un incidente, más la valoración del impacto que el incidente pueda generar para el proceso y para Colombiana de Trasplantes.

En el cuadro 15, se presentan los valores de referencia para la definición de nivel de riesgo basados en la probabilidad por el impacto.

Cuadro 15. Matriz de valoración del riesgo

Matriz de valoración del riesgo						
		Probabilidad				
		Muy baja (0)	Baja (1)	Media (2)	Alta (3)	Muy Alta (4)
Impacto	Muy Bajo (0)	0	1	2	3	4
	Bajo (1)	1	2	3	4	5
	Medio (2)	2	3	4	5	6
	Alto (3)	3	4	5	6	7
	Muy Alto (4)	4	5	6	7	8

Fuente: elaboración propia con base en la Norma ISO/IEC 27005:2009 Anexo E.

5.3.5 Escala de valoración de riesgos y riesgo aceptable. En el cuadro 16, se presentan los criterios de valoración para cada uno de los niveles de riesgo definidos en una escala de cero a ocho. Para Colombiana de Trasplantes, los riesgos medios y altos no son aceptables en el proceso de telemedicina, por lo que se deben mitigar mediante acciones de tratamiento que permitan llevarlos a un nivel bajo.

Cuadro 16. Criterio de valoración de niveles de riesgo

Niveles de riesgo			
Nivel	**Escala**	**Descripción**	**Aceptable**
Alto	6-8	El riesgo se debe trata de forma inmediata porque impactan significativamente los objetivos de la organización y el proceso de telemedicina.	No
Medio	3-5	El riesgo se debe tartar oportunamente para mantenerlo controlado y evitar un mayor impacto en los objetivos de la organización y el proceso de telemedicina.	No
Bajo	0-2	El riesgo no afecta significativamente los objetivos de la organización o el proceso de telemedicina, por lo que no se hace obligatorio su tratamiento y pueden ser aceptados.	Si

Fuente: elaboración propia.

5.3.6 Valoración del riesgo. Con los criterios que se definieron para la valoración de la probabilidad de ocurrencia y el impacto, en el cuadro 17, se define el riesgo inherente sumando los dos valores para cada una de las amenazas identificadas en cada activo de información del proceso de telemedicina.

Cuadro 17. Valoración de riesgo

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
INF1	Información de contacto	A7	Espionaje remoto	3	3	6	R1
INF1	Información de contacto	A8	Hurto de medios y documentos	3	3	6	R2
INF1	Información de contacto	A11	Divulgación	3	1	4	R3
INF1	Información de contacto	A20	Corrupción de datos	3	1	4	R4
INF1	Información de contacto	A22	Abuso de derechos	3	2	5	R5
INF2	Historia clínica	A7	Espionaje remoto	4	4	8	R6
INF2	Historia clínica	A8	Hurto de medios y documentos	4	4	8	R7
INF2	Historia clínica	A11	Divulgación	4	4	8	R8
INF2	Historia clínica	A20	Corrupción de datos	4	3	7	R9
INF2	Historia clínica	A22	Abuso de derechos	4	4	8	R10
INF3	Reporte telemedicina	A7	Espionaje remoto	4	0	4	R11
INF3	Reporte telemedicina	A8	Hurto de medios y documentos	4	0	4	R12
INF3	Reporte telemedicina	A11	Divulgación	4	0	4	R13
INF3	Reporte telemedicina	A20	Corrupción de datos	4	0	4	R14
HW1	Equipo portátil ingeniero TI	A2	Daño por agua o líquidos	1	0	1	R15
HW1	Equipo portátil ingeniero TI	A3	Destrucción de equipos o medios	1	0	1	R16
HW1	Equipo portátil ingeniero TI	A9	Hurto equipos	4	0	4	R17
HW1	Equipo portátil ingeniero TI	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R18
HW1	Equipo portátil ingeniero TI	A14	Falla de equipo	1	1	2	R19
HW1	Equipo portátil ingeniero TI	A15	Mal funcionamiento de equipo	1	3	4	R20
HW1	Equipo portátil ingeniero TI	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R21
HW1	Equipo portátil ingeniero TI	A18	Uso no autorizado de equipo	2	0	2	R22

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
HW2	Equipo portátil tecnólogo TI	A2	Daño por agua o líquidos	1	0	1	R23
HW2	Equipo portátil tecnólogo TI	A3	Destrucción de equipos o medios	1	0	1	R24
HW2	Equipo portátil tecnólogo TI	A9	Hurto equipos	4	0	4	R25
HW2	Equipo portátil tecnólogo TI	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R26
HW2	Equipo portátil tecnólogo TI	A14	Falla de equipo	1	1	2	R27
HW2	Equipo portátil tecnólogo TI	A15	Mal funcionamiento de equipo	1	2	3	R28
HW2	Equipo portátil tecnólogo TI	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R29
HW2	Equipo portátil tecnólogo TI	A18	Uso no autorizado de equipo	2	0	2	R30
HW3	Equipo portátil Auxiliar de Investigación	A2	Daño por agua o líquidos	1	0	1	R31
HW3	Equipo portátil Auxiliar de Investigación	A3	Destrucción de equipos o medios	1	0	1	R32
HW3	Equipo portátil Auxiliar de Investigación	A9	Hurto equipos	4	0	4	R33
HW3	Equipo portátil Auxiliar de Investigación	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R34
HW3	Equipo portátil Auxiliar de Investigación	A14	Falla de equipo	1	0	1	R35
HW3	Equipo portátil Auxiliar de Investigación	A15	Mal funcionamiento de equipo	1	0	1	R36
HW3	Equipo portátil Auxiliar de Investigación	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R37
HW3	Equipo portátil Auxiliar de Investigación	A18	Uso no autorizado de equipo	3	0	3	R38
HW4	Equipo portátil coordinador de Investigación	A2	Daño por agua o líquidos	1	0	1	R39

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
HW4	Equipo portátil coordinador de Investigación	A3	Destrucción de equipos o medios	1	0	1	R40
HW4	Equipo portátil coordinador de Investigación	A9	Hurto equipos	4	0	4	R41
HW4	Equipo portátil coordinador de Investigación	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R42
HW4	Equipo portátil coordinador de Investigación	A14	Falla de equipo	1	3	4	R43
HW4	Equipo portátil coordinador de Investigación	A15	Mal funcionamiento de equipo	1	3	4	R44
HW4	Equipo portátil coordinador de Investigación	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R45
HW4	Equipo portátil coordinador de Investigación	A18	Uso no autorizado de equipo	3	0	3	R46
HW5	Equipo portátil médico de investigación	A2	Daño por agua o líquidos	1	0	1	R47
HW5	Equipo portátil médico de investigación	A3	Destrucción de equipos o medios	1	0	1	R48
HW5	Equipo portátil médico de investigación	A9	Hurto equipos	4	0	4	R49
HW5	Equipo portátil médico de investigación	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R50
HW5	Equipo portátil médico de investigación	A14	Falla de equipo	1	0	1	R51
HW5	Equipo portátil médico de investigación	A15	Mal funcionamiento de equipo	1	4	5	R52
HW5	Equipo portátil médico de investigación	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R53
HW5	Equipo portátil médico de investigación	A18	Uso no autorizado de equipo	3	0	3	R54

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
HW6	Equipo portátil agente comercial – *Call Center*	A2	Daño por agua o líquidos	1	1	2	R55
HW6	Equipo portátil agente comercial – *Call Center*	A3	Destrucción de equipos o medios	1	1	2	R56
HW6	Equipo portátil agente comercial – *Call Center*	A9	Hurto equipos	4	0	4	R57
HW6	Equipo portátil agente comercial – *Call Center*	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R58
HW6	Equipo portátil agente comercial – *Call Center*	A14	Falla de equipo	1	3	4	R59
HW6	Equipo portátil agente comercial – *Call Center*	A15	Mal funcionamiento de equipo	1	3	4	R60
HW6	Equipo portátil agente comercial – *Call Center*	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R61
HW6	Equipo portátil agente comercial – *Call Center*	A18	Uso no autorizado de equipo	2	1	3	R62
HW7	Equipo Portátil Verificador	A2	Daño por agua o líquidos	1	0	1	R63
HW7	Equipo Portátil Verificador	A3	Destrucción de equipos o medios	1	0	1	R64
HW7	Equipo Portátil Verificador	A9	Hurto equipos	4	0	4	R65
HW7	Equipo Portátil Verificador	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R66
HW7	Equipo Portátil Verificador	A14	Falla de equipo	1	0	1	R67
HW7	Equipo Portátil Verificador	A15	Mal funcionamiento de equipo	1	3	4	R68
HW7	Equipo Portátil Verificador	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R69
HW7	Equipo Portátil Verificador	A18	Uso no autorizado de equipo	2	1	3	R70
HW8	Equipo portátil coordinador de enfermería	A2	Daño por agua o líquidos	1	0	1	R71

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
HW8	Equipo portátil coordinador de enfermería	A3	Destrucción de equipos o medios	1	0	1	R72
HW8	Equipo portátil coordinador de enfermería	A9	Hurto equipos	4	0	4	R73
HW8	Equipo portátil coordinador de enfermería	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R74
HW8	Equipo portátil coordinador de enfermería	A14	Falla de equipo	1	0	1	R75
HW8	Equipo portátil coordinador de enfermería	A15	Mal funcionamiento de equipo	1	3	4	R76
HW8	Equipo portátil coordinador de enfermería	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R77
HW8	Equipo portátil coordinador de enfermería	A18	Uso no autorizado de equipo	2	1	3	R78
HW9	Equipo portátil médico telemedicina interactiva	A2	Daño por agua o líquidos	1	3	4	R79
HW9	Equipo portátil médico telemedicina interactiva	A3	Destrucción de equipos o medios	1	2	3	R80
HW9	Equipo portátil médico telemedicina interactiva	A9	Hurto equipos	4	2	6	R81
HW9	Equipo portátil médico telemedicina interactiva	A10	Recuperación de información sobre equipos reciclados y rentados	4	4	8	R82
HW9	Equipo portátil médico telemedicina interactiva	A14	Falla de equipo	1	3	4	R83
HW9	Equipo portátil médico telemedicina interactiva	A15	Mal funcionamiento de equipo	1	4	5	R84
HW9	Equipo portátil médico telemedicina interactiva	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R85

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
HW9	Equipo portátil médico telemedicina interactiva	A18	Uso no autorizado de equipo	2	2	4	R86
HW10	Equipo escritorio médico telemedicina interactiva	A2	Daño por agua o líquidos	1	0	1	R87
HW10	Equipo escritorio médico telemedicina interactiva	A3	Destrucción de equipos o medios	1	0	1	R88
HW10	Equipo escritorio médico telemedicina interactiva	A9	Hurto equipos	1	0	1	R89
HW10	Equipo escritorio médico telemedicina interactiva	A10	Recuperación de información sobre equipos reciclados y rentados	1	1	2	R90
HW10	Equipo escritorio médico telemedicina interactiva	A14	Falla de equipo	1	0	1	R91
HW10	Equipo escritorio médico telemedicina interactiva	A15	Mal funcionamiento de equipo	1	3	4	R92
HW10	Equipo escritorio médico telemedicina interactiva	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R93
HW10	Equipo escritorio médico telemedicina interactiva	A18	Uso no autorizado de equipo	1	2	3	R94
HW11	Equipo Portátil farmacia	A2	Daño por agua o líquidos	1	0	1	R95
HW11	Equipo Portátil farmacia	A3	Destrucción de equipos o medios	1	0	1	R96
HW11	Equipo Portátil farmacia	A9	Hurto equipos	4	2	6	R97
HW11	Equipo Portátil farmacia	A10	Recuperación de información sobre equipos reciclados y rentados	4	1	5	R98
HW11	Equipo Portátil farmacia	A14	Falla de equipo	1	0	1	R99
HW11	Equipo Portátil farmacia	A15	Mal funcionamiento de equipo	1	3	4	R100

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
HW11	Equipo Portátil farmacia	A17	Incumplimiento en el mantenimiento del sistema de información	1	2	3	R101
HW11	Equipo Portátil farmacia	A18	Uso no autorizado de equipo	1	2	3	R102
HW12	UPS, sistema de alimentación eléctrica ininterrumpida	A1	Fuego	3	0	3	R103
HW12	UPS, sistema de alimentación eléctrica ininterrumpida	A3	Destrucción de equipos o medios	3	0	3	R104
HW12	UPS, sistema de alimentación eléctrica ininterrumpida	A4	Fenómenos naturales	3	0	3	R105
HW12	UPS, sistema de alimentación eléctrica ininterrumpida	A14	Falla de equipo	2	1	3	R106
HW12	UPS, sistema de alimentación eléctrica ininterrumpida	A15	Mal funcionamiento de equipo	2	1	3	R107
SW1	Solución Ofimática	A16	Mal funcionamiento del *software*	1	1	2	R108
SW2	Solución Ofimática	A19	Uso no autorizado de *Software*	1	1	2	R109
SW3	Solución Ofimática	A20	Error de Uso	1	2	3	R110
SW2	Solución de mensajería y comunicaciones	A16	Mal funcionamiento del *software*	2	4	6	R111
SW2	Solución de mensajería y comunicaciones	A19	Uso no autorizado de *Software*	1	1	2	R112
SW2	Solución de mensajería y comunicaciones	A20	Error de Uso	1	2	3	R113
SW3	Solución de gestión documental	A11	Divulgación	4	1	5	R114
SW4	Solución de gestión documental	A16	Mal funcionamiento del *software*	4	1	5	R115
SW5	Solución de gestión documental	A19	Uso no autorizado de *Software*	4	1	5	R116

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
SW6	Solución de gestión documental	A20	Error de Uso	3	2	5	R117
SW4	Solución para programar y administrar citas medicas	A16	Mal funcionamiento del *software*	2	0	2	R118
SW4	Solución para programar y administrar citas medicas	A20	Error de Uso	2	1	3	R119
SW5	Sistema operativo Windows	A12	Manipulación con *software*	2	2	4	R120
SW5	Sistema operativo Windows	A13	Códigos maliciosos	3	1	4	R121
SW5	Sistema operativo Windows	A16	Mal funcionamiento del *software*	2	2	4	R122
SW5	Sistema operativo Windows	A17	Incumplimiento en el mantenimiento del sistema de información	2	2	4	R123
SW5	Sistema operativo Windows	A19	Uso no autorizado de *Software*	1	3	4	R124
SW5	Sistema operativo Windows	A22	Abuso de derechos	3	1	4	R125
SW5	Sistema operativo Windows	A23	Falsificación de derechos	3	1	4	R126
SW6	Sistema operativo Mac OS X	A12	Manipulación con *software*	2	0	2	R127
SW6	Sistema operativo Mac OS X	A13	Códigos maliciosos	3	0	3	R128
SW6	Sistema operativo Mac OS X	A16	Mal funcionamiento del *software*	2	0	2	R129
SW6	Sistema operativo Mac OS X	A17	Incumplimiento en el mantenimiento del sistema de información	2	2	4	R130
SW6	Sistema operativo Mac OS X	A19	Uso no autorizado de *Software*	1	0	1	R131
SW6	Sistema operativo Mac OS X	A22	Abuso de derechos	3	1	4	R132
SW6	Sistema operativo Mac OS X	A23	Falsificación de derechos	3	1	4	R133
SW7	Solución de telefonía	A16	Mal funcionamiento del *software*	1	0	1	R134
SW7	Solución de telefonía	A19	Uso no autorizado de *Software*	1	0	1	R135
SW7	Solución de telefonía	A21	Error de Uso	1	1	2	R136

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
SW8	Solución de gestión de historias clínicas	A13	Códigos maliciosos	4	0	4	R137
SW8	Solución de gestión de historias clínicas	A16	Mal funcionamiento del *software*	3	3	6	R138
SW8	Solución de gestión de historias clínicas	A21	Error de Uso	3	4	7	R139
SW9	Solución de firma digital	A16	Mal funcionamiento del *software*	2	0	2	R140
SW9	Solución de firma digital	A20	Error de Uso	1	1	2	R141
SW10	Herramienta Administración base de datos	A16	Mal funcionamiento del *software*	1	0	1	R142
SW10	Herramienta Administración base de datos	A20	Error de Uso	1	0	1	R143
RD1	Firewall	A3	Destrucción de equipos o medios	2	0	2	R144
RD1	Firewall	A13	Códigos maliciosos	2	1	3	R145
RD1	Firewall	A14	Falla de equipo	2	0	2	R146
RD1	Firewall	A15	Mal funcionamiento de equipo	1	1	2	R147
RD1	Firewall	A21	Error de uso	2	0	2	R148
RD2	*Switch Core*	A3	Destrucción de equipos o medios	2	0	2	R149
RD2	*Switch Core*	A14	Falla de equipo	2	1	3	R150
RD2	*Switch Core*	A15	Mal funcionamiento de equipo	1	1	2	R151
RD2	*Switch Core*	A21	Error de uso	1	0	1	R152
RD3	*Switch* acceso	A3	Destrucción de equipos o medios	1	0	1	R153
RD3	*Switch* acceso	A14	Falla de equipo	1	1	2	R154
RD3	*Switch* acceso	A15	Mal funcionamiento de equipo	0	1	1	R155
RD3	*Switch* acceso	A21	Error de uso	0	0	0	R156
RD4	Punto de acceso inalámbrico 1	A3	Destrucción de equipos o medios	1	1	2	R157
RD4	Punto de acceso inalámbrico 1	A14	Falla de equipo	1	1	2	R158
RD4	Punto de acceso inalámbrico 1	A15	Mal funcionamiento de equipo	0	1	1	R159
RD4	Punto de acceso inalámbrico 1	A21	Error de uso	0	1	1	R160
RD5	Punto de acceso inalámbrico 2	A3	Destrucción de equipos o medios	1	1	2	R161

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
RD5	Punto de acceso inalámbrico 2	A14	Falla de equipo	1	1	2	R162
RD5	Punto de acceso inalámbrico 2	A15	Mal funcionamiento de equipo	0	1	1	R163
RD5	Punto de acceso inalámbrico 2	A21	Error de uso	0	1	1	R164
RD6	Canal internet 1	A3	Destrucción de equipos o medios	1	0	1	R165
RD6	Canal internet 1	A5	Pérdida en el suministro de energía	1	0	1	R166
RD6	Canal internet 1	A6	Falla en equipo de telecomunicaciones	1	1	2	R167
RD7	Canal internet 2	A3	Destrucción de equipos o medios	1	0	1	R168
RD7	Canal internet 2	A5	Pérdida en el suministro de energía	1	0	1	R169
RD7	Canal internet 2	A6	Falla en equipo de telecomunicaciones	1	1	2	R170
RD8	Cableado estructurado	A3	Destrucción de equipos o medios	1	2	3	R171
RD8	Cableado estructurado	A2	Daño por agua o líquidos	1	3	4	R172
RH1	Ingeniero TI	A4	Fenómenos naturales	1	4	5	R173
RH1	Ingeniero TI	A11	Divulgación	4	3	7	R174
RH1	Ingeniero TI	A21	Error de Uso	1	1	2	R175
RH1	Ingeniero TI	A24	Incumplimientos en la disponibilidad del personal	1	4	5	R176
RH2	Tecnólogo TI	A4	Fenómenos naturales	1	0	1	R177
RH2	Tecnólogo TI	A11	Divulgación	4	3	7	R178
RH2	Tecnólogo TI	A21	Error de Uso	1	1	2	R179
RH2	Tecnólogo TI	A24	Incumplimientos en la disponibilidad del personal	1	2	3	R180
RH3	Auxiliar de investigación	A4	Fenómenos naturales	1	0	1	R181
RH3	Auxiliar de investigación	A11	Divulgación	4	3	7	R182
RH3	Auxiliar de investigación	A21	Error de Uso	1	1	2	R183
RH3	Auxiliar de investigación	A24	Incumplimientos en la disponibilidad del personal	1	1	2	R184

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
RH4	Coordinador programa telemedicina	A4	Fenómenos naturales	1	0	1	R185
RH4	Coordinador programa telemedicina	A11	Divulgación	4	3	7	R186
RH4	Coordinador programa telemedicina	A21	Error de Uso	1	1	2	R187
RH4	Coordinador programa telemedicina	A24	Incumplimientos en la disponibilidad del personal	1	2	3	R188
RH5	Médico de investigación	A4	Fenómenos naturales	1	0	1	R189
RH5	Médico de investigación	A11	Divulgación	4	3	7	R190
RH5	Médico de investigación	A21	Error de Uso	1	1	2	R191
RH5	Médico de investigación	A24	Incumplimientos en la disponibilidad del personal	1	1	2	R192
RH6	Verificador	A4	Fenómenos naturales	1	0	1	R193
RH6	Verificador	A11	Divulgación	2	3	5	R194
RH6	Verificador	A21	Error de Uso	1	1	2	R195
RH6	Verificador	A24	Incumplimientos en la disponibilidad del personal	1	2	3	R196
RH7	Coordinador de enfermería	A4	Fenómenos naturales	1	0	1	R197
RH7	Coordinador de enfermería	A11	Divulgación	4	3	4	R198
RH7	Coordinador de enfermería	A21	Error de Uso	1	1	2	R199
RH7	Coordinador de enfermería	A24	Incumplimientos en la disponibilidad del personal	2	1	3	R200
RH8	Médico telemedicina Interactiva	A4	Fenómenos naturales	1	4	5	R201
RH8	Médico telemedicina Interactiva	A11	Divulgación	4	3	7	R202
RH8	Médico telemedicina Interactiva	A21	Error de Uso	1	1	2	R203
RH8	Médico telemedicina Interactiva	A24	Incumplimientos en la disponibilidad del personal	1	4	5	R204
RH9	Responsable Farmacia	A4	Fenómenos naturales	1	0	1	R205

Cuadro 17. (Continuación)

Código activo	Activo	Código amenaza	Amenaza	Impacto	Probabilidad	Riesgo inherente	Código riesgo
RH9	Responsable Farmacia	A11	Divulgación	4	3	7	R206
RH9	Responsable Farmacia	A21	Error de Uso	1	1	2	R207
RH9	Responsable Farmacia	A24	Incumplimientos en la disponibilidad del personal	2	1	3	R208
RH10	Agente comercial – *Call Center*	A4	Fenómenos naturales	1	0	1	R209
RH10	Agente comercial – *Call Center*	A11	Divulgación	4	3	7	R210
RH10	Agente comercial – *Call Center*	A21	Error de Uso	1	1	2	R211
RH10	Agente comercial – *Call Center*	A24	Incumplimientos en la disponibilidad del personal	1	1	2	R212

Fuente: elaboración propia.

5.3.7 Mapa de calor del riesgo inherente. El cuadro 18, muestra la ubicación de cada uno de los riesgos en su respectivo cuadrante del mapa de calor, encontrando un total de 92 riesgos bajos, identificables visualmente de color verde que son aceptables para Colombiana de Trasplantes en el proceso de telemedicina, así como 97 riesgos medios identificables visualmente de color amarillo y 23 riesgos altos identificables visualmente de color rojo. Los riesgos con un valor cuantitativo de cinco o superior deben ser tratados según definió Colombiana de Trasplantes para un total de 120 riesgos a contemplar en el plan de tratamiento.

Para la disposición del cuadro 18, del mapa de calor se tomó como referencia la tabla E.1 b) del anexo e de la norma ISO/IEC 27005:2009 donde la probabilidad se incrementa de izquierda a derecha y el impacto incrementa de arriba hacia abajo, de igual forma se maneja una escala de cero a cuatro en los valores cuantitativos y con su respectiva equivalencia cualitativa para referencia.

Cuadro 18. Mapa de calor del riesgo inherente

Matriz de valoración del riesgo						
		Probabilidad				
		Muy baja (0)	Baja (1)	Media (2)	Alta (3)	Muy Alta (4)
Impacto	Muy Bajo (0)	R156	R155 R159 R160 R163 R164	–	–	–
	Bajo (1)	R15 R16 R23 R24 R31 R32 R35 R36 R39 R40 R47 R48 R51 R63 R64 R67 R71 R72 R75 R87 R88 R89 R91 R95 R96 R99 R131 R134 R135 R142 R143 R152 R153 R165 R166 R168 R169 R177 R181 R185 R189 R193 R197 R205 R209	R19 R27 R55 R56 R90 R108 R109 R112 R136 R141 R147 R151 R154 R157 R158 R161 R162 R167 R170 R175 R179 R183 R184 R187 R191 R192 R195 R199 R203 R207 R211	R21 R28 R29 R37 R45 R53 R61 R69 R77 R80 R85 R93 R94 R101 R102 R110 R113 R171 R180 R188 R196 R212	R20 R43 R44 R59 R60 R68 R76 R79 R83 R92 R100 R124 R172	R52 R84 R173 R176 R201 R204
	Medio (2)	R22 R30 R118 R127 R129 R140 R144 R146 R148 R149	R62 R70 R78 R106 R107 R119 R145 R150 R200 R208	R86 R120 R122 R123 R130	R194	R111
	Alto (3)	R38 R46 R54 R103 R104 R105 R128	R3 R4 R121 R125 R126 R132 R133	R5 R117	R1 R2 R138	R139
	Muy Alto (4)	R11 R12 R13 R14 R17 R25 R33 R41 R49 R57 R65 R73 R137	R18 R26 R34 R42 R50 R58 R66 R74 R98 R115 R116	R81 R97	R9 R174 R178 R182 R186 R190 R198 R202 R206 R210	R6 R7 R8 R10 R114 R82

Fuente: elaboración propia.

5.3.8 Plan de tratamiento de riesgos y riesgo residual esperado. En el plan de tratamiento se identifican los controles con respecto a la norma ISO/ IEC 27001:2013 que permitirán mitigar los riesgos inaceptables para la organización dentro del proceso de telemedicina, adicionalmente se define la estrategia de implementación para cada control. Los controles están diseñados para disminuir los riesgos al nivel aceptable para Colombiana de Trasplantes, se definen controles preventivos para reducir la probabilidad de materialización del riesgo y controles correctivos orientados a disminuir el impacto de la materialización del riesgo. Dada la naturaleza del proyecto donde el alcance no contempla la implementación de los controles no es posible medir la efectividad real que vendría de una evaluación posterior a la implementación de los controles propuestos, por lo que se estima la efectividad esperada en la reducción del impacto y la probabilidad según corresponda. En el cuadro 19, se detallan los riesgos con su respectivo control, estrategia, estimación de reducción de impacto, estimación de reducción de probabilidad y cálculo resultante del nivel de riesgo residual esperado.

Cuadro 19. Plan de tratamiento

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R1	INF1	6	A.9.1.2 Acceso a redes y a servicios de red	Se debe garantizar que solo accedan a la red los usuarios autorizados y específicamente a los permisos otorgados en la red.	1	1	2
R1	INF1		A.12.6.1 Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de todos los sistemas de información que se use; evaluar la exposición de la organización de estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.			
R1	INF1		A.12.6.2 Restricciones sobre la instalación de *software*	Se debe establecer e implementar las reglas para la instalación de *softwar*e por parte de los usuarios.			
R2	INF1	6	A. 12.3.1 Respaldo de la información	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.	1	1	2
R2	INF1		A. 9.3.1 Uso de información de autenticación secreta	Se debe exigir a los empleados hacer buen uso de la información secreta de autenticación evitando divulgarla, dejarla expuesta u omitir los controles de autenticación establecidos.			
R2	INF1		A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen .			
R3	INF1	4	A. 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Se debe definir e implementar plan de concientización a los empleados y contratistas sobre aspectos generales en seguridad de la información y sus restricciones sobre el tratamiento de esta. De igual forma se debe definir un cronograma de reentrenamiento anual.	1	1	2
R3	INF1		A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.			
R3	INF1		A. 8.3.1 Gestión de medios removibles	Se deben restringir el uso de medios removibles mediante el bloqueo de puertos.			
R3	INF1		A. 13.2.1 Políticas y procedimientos para la transferencia de información.	Se debe crear una política y sus procedimientos para definir los parámetros aceptables y las condiciones apropiadas de transferencia de información en general.			
R3	INF1		A.13.2.4 Acuerdos de confidencialidad o de no divulgación.	Incluir en toda contratación los acuerdos de confidencialidad y no divulgación garantizando el compromiso por parte del personal.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R4	INF1	4	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	0	1	1
R4	INF1		A. 12.2.1 Controles contra códigos maliciosos	Se deben implementar controles para la detección, bloqueo de código maliciosos, que afecten el correcto funcionamiento de los sistemas de información locales o como servicio.			
R4	INF1		A. 12.4.1 Registro de eventos	Se deben recolectar y almacenar la información de eventos relacionados con los activos de información por medio de herramientas que permitan la retención y acceso necesarios definidos por el negocio para posteriores consultas y análisis.			
R4	INF1		A. 16.1.4 Evaluación de eventos de seguridad de la información y decisión sobre ellos	Se debe analizar los eventos de seguridad de la información para detectar la causa raíz y definir planes de acción para que no se repita.			
R4	INF1		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R5	INF1	5	A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.	1	1	2
R5	INF1		A. 9.1.1 Política de control de acceso	Se debe definir, documentar y divulgar una política de control de acceso basada en otorgar el mínimo acceso que los usuarios necesitan a los activos de información.			
R5	INF1		A. 18.1.4 Privacidad y protección de información de datos personales	Se deben cumplir todas las disposiciones de ley para el manejo y tratamiento de datos personales en el proceso de Telemedicina.			
R6	INF2	8	A.9.1.2 Acceso a redes y a servicios de red	Se debe garantizar que solo accedan a la red los usuarios autorizados y específicamente a los permisos otorgados en la red.	1	1	2
R6	INF2		A.12.6.1 Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de todos los sistemas de información que se use; evaluar la exposición de la organización de estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.			
R6	INF2		A.12.6.2 Restricciones sobre la instalación de s*oftware*	Se debe establecer e implementar las reglas para la instalación de *software* por parte de los usuarios.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R7	INF2	8	A. 12.3.1 Respaldo de la información	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.	1	1	2
R7	INF2		A. 9.3.1 Uso de información de autenticación secreta	Se debe exigir a los empleados hacer buen uso de la información secreta de autenticación evitando divulgarla, dejarla expuesta u omitir los controles de autenticación establecidos.			
R7	INF2		A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.			
R8	INF2	8	A. 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Se debe definir e implementar plan de concientización a los empleados y contratistas sobre aspectos generales en seguridad de la información y sus restricciones sobre el tratamiento de esta. De igual forma se debe definir un cronograma de reentrenamiento anual.	1	1	2
R8	INF2		A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.			
R8	INF2		A. 8.3.1 Gestión de medios removibles	Se deben restringir el uso de medios removibles mediante el bloqueo de puertos.			
R8	INF2		A. 13.2.1 Políticas y procedimientos para la transferencia de información.	Se debe crear una política y sus procedimientos para definir los parámetros aceptables y las condiciones apropiadas de transferencia de información en general.			
R8	INF2		A.13.2.4 Acuerdos de confidencialidad o de no divulgación.	Incluir en toda contratación los acuerdos de confidencialidad y no divulgación garantizando el compromiso por parte del personal.			
R9	INF2	7	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	1	2
R9	INF2		A. 12.2.1 Controles contra códigos maliciosos	Se deben implementar controles para la detección, bloqueo de código maliciosos, que afecten el correcto funcionamiento de los sistemas de información locales o como servicio.			
R9	INF2		A. 12.4.1 Registro de eventos	Se deben recolectar y almacenar la información de eventos relacionados con los activos de información por medio de herramientas que permitan la retención y acceso necesarios definidos por el negocio para posteriores consultas y análisis.			
R9	INF2		A. 16.1.4 Evaluación de eventos de seguridad de la información y decisión sobre ellos	Se debe analizar los eventos de seguridad de la información para detectar la causa raíz y definir planes de acción para que no se repita.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R9	INF2		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R10	INF2	8	A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.	1	1	2
R10	INF2		A. 9.1.1 Política de control de acceso	Se debe definir, documentar y divulgar una política de control de acceso basada en otorgar el mínimo acceso que los usuarios necesitan a los activos de información.			
R10	INF2		A. 9.2.5 Revisión de los derechos de acceso de los usuarios	Se debe definir actividades periódicas cada seis meses donde los propietarios de los activos revisen los permisos de acceso de los usuarios basados en el rol que el usuario desarrolle en el proceso, estos roles y sus permisos de acceso deben estar documentados.			
R10	INF2		A. 9.2.6 Retiro o ajuste de los derechos de acceso	Se deben retirar o modificar los derechos de acceso cuando el responsable de un activo identifique que el rol de un usuario no corresponde con los privilegios asignados sobre el activo.			
R10	INF2		A. 18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Se deben realizar revisiones periódicas y estar ajustando el proceso a las nuevas disposiciones de ley que afecten el proceso de Telemedicina.			
R10	INF2		A. 18.1.4 Privacidad y protección de información de datos personales	Se deben cumplir todas las disposiciones de ley para el manejo y tratamiento de datos personales en el proceso de Telemedicina.			
R11	INF3	4	A.9.1.2 Acceso a redes y a servicios de red	Se debe garantizar que solo accedan a la red los usuarios autorizados y específicamente a los permisos otorgados en la red.	1	0	1
R11	INF3		A.12.6.1 Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de todos los sistemas de información que se use; evaluar la exposición de la organización de estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.			
R11	INF3		A.12.6.2 Restricciones sobre la instalación de *software*	Se debe establecer e implementar las reglas para la instalación de *software* por parte de los usuarios.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R12	INF3	4	A. 12.3.1 Respaldo de la información	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.	1	0	1
R12	INF3		A. 9.3.1 Uso de información de autenticación secreta	Se debe exigir a los empleados hacer buen uso de la información secreta de autenticación evitando divulgarla, dejarla expuesta u omitir los controles de autenticación establecidos.			
R12	INF3		A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.			
R13	INF3	4	A. 7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	Se debe definir e implementar plan de concientización a los empleados y contratistas sobre aspectos generales en seguridad de la información y sus restricciones sobre el tratamiento de la misma. De igual forma se debe definir un cronograma de reentrenamiento anual.	2	0	2
R13	INF3		A. 8.1.3 Uso aceptable de los activos	Se deben identificar los vectores de fuga de información e implementar controles que detecten estos movimientos de información reservada y los bloqueen.			
R13	INF3		A. 8.3.1 Gestión de medios removibles	Se deben restringir el uso de medios removibles mediante el bloqueo de puertos.			
R13	INF3		A.13.2.4 Acuerdos de confidencialidad o de no divulgación.	Incluir en toda contratación los acuerdos de confidencialidad y no divulgación garantizando el compromiso por parte del personal.			
R13	INF3		A. 13.2.1 Políticas y procedimientos para la transferencia de información.	Se debe crear una política y sus procedimientos para definir los parámetros aceptables y las condiciones apropiadas de transferencia de información en general.			
R14	INF3	4	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	0	1
R14	INF3		A. 12.2.1 Controles contra códigos maliciosos	Se deben implementar controles para la detección, bloqueo de código maliciosos, que afecten el correcto funcionamiento de los sistemas de información locales o como servicio.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R14	INF3		A. 12.4.1 Registro de eventos	Se deben recolectar y almacenar la información de eventos relacionados con los activos de información por medio de herramientas que permitan la retención y acceso necesarios definidos por el negocio para posteriores consultas y análisis.			
R14	INF3		A. 16.1.4 Evaluación de eventos de seguridad de la información y decisión sobre ellos	Se debe analizar los eventos de seguridad de la información para detectar la causa raíz y definir planes de acción para que no se repita.			
R14	INF3		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R17	HW1	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R17	HW1		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R17	HW1		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R17	HW1		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R17	HW1		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R18	HW1	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	0	1
R18	HW1		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R18	HW1		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R20	HW1	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	0	0
R20	HW1		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R20	HW1		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R21	HW1	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R21	HW1		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R25	HW2	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R25	HW2		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R25	HW2		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R25	HW2		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R25	HW2		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R26	HW2	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	1	2
R26	HW2		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R26	HW2		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R28	HW2	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R28	HW2		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R28	HW2		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R29	HW2	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	1	0	1
R29	HW2		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R33	HW3	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R33	HW3		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R33	HW3		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R33	HW3		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R33	HW3		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R34	HW3	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	0	1
R34	HW3		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R34	HW3		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R37	HW3	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	1	0	1
R37	HW3		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R38	HW3	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	0	1
R38	HW3		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R38	HW3		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R41	HW4	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R41	HW4		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R41	HW4		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R41	HW4		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R41	HW4		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R42	HW4	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	0	1
R42	HW4		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R42	HW4		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R43	HW4	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R43	HW4		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R43	HW4		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R44	HW4	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	1	1	2
R44	HW4		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R44	HW4		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R45	HW4	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R45	HW4		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R46	HW4	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	0	1

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R46	HW4		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R46	HW4		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R49	HW5	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R49	HW5		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R49	HW5		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R49	HW5		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R49	HW5		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R50	HW5	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	0	1	1
R50	HW5		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R50	HW5		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R52	HW5	5	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	1	1	2
R52	HW5		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R52	HW5		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R53	HW5	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R53	HW5		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R54	HW5	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	0	1
R54	HW5		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R54	HW5		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R57	HW6	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R57	HW6		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R57	HW6		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R57	HW6		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R57	HW6		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R58	HW6	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	0	1
R58	HW6		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R58	HW6		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R59	HW6	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R59	HW6		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R59	HW6		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R60	HW6	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R60	HW6		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R60	HW6		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R61	HW6	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R61	HW6		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R62	HW6	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	1	2

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R62	HW6		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R62	HW6		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R65	HW7	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R65	HW7		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R65	HW7		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R65	HW7		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R65	HW7		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R66	HW7	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	1	2

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R66	HW7		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R66	HW7		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R68	HW7	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	1	1	2
R68	HW7		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R68	HW7		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R69	HW7	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R69	HW7		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R70	HW7	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	1	2

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R70	HW7		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R70	HW7		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R73	HW8	4	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	0	1
R73	HW8		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R73	HW8		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R73	HW8		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R73	HW8		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R74	HW8	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	1	2

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R74	HW8		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R74	HW8		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R76	HW8	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R76	HW8		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R76	HW8		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R77	HW8	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R77	HW8		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R78	HW8	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	1	2

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R78	HW8		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R78	HW8		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R79	HW9	4	A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.	0	1	1
R79	HW9		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R79	HW9		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad o daños físicos.			
R80	HW9	3	A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.	0	1	1
R80	HW9		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R80	HW9		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R81	HW9	6	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	1	2
R81	HW9		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R81	HW9		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R81	HW9		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R81	HW9		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R82	HW9	8	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	1	2
R82	HW9		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R82	HW9		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R83	HW9	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R83	HW9		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R83	HW9		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R84	HW9	5	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R84	HW9		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R84	HW9		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R85	HW9	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R85	HW9		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R85	HW9		A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R86	HW9	4	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	0	1
R86	HW9		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R86	HW9		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R92	HW10	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R92	HW10		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R92	HW10		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R93	HW10	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R93	HW10		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R93	HW10		A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.			
R94	HW10	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	1	1	2
R94	HW10		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R94	HW10		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R97	HW11	6	A. 10.1.1 Política sobre el uso de controles criptográficos	Se deben definir e implementar controles criptográficos para el cifrado de medios de almacenamiento y el acceso a activos que protejan contra el acceso no autorizado.	1	1	2
R97	HW11		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R97	HW11		A. 11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Se deben definir e implementar medidas para los equipos que están fuera de las instalaciones de la organización tales como seguros y copias de seguridad.			
R97	HW11		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R97	HW11		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R98	HW11	5	A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.	1	1	2
R98	HW11		A.11.2.7 Disposición segura de activos	Definir un procedimiento adecuado de borrado seguro para el manejo de equipos con unidades de almacenamiento de información.			
R98	HW11		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R100	HW11	4	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R100	HW11		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			
R100	HW11		A. 17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe implementar y probar el plan de continuidad para el proceso en caso de un evento de seguridad.			
R101	HW11	3	A. 11.2.4 Mantenimiento de equipos	Se debe definir e implementar un plan de mantenimiento preventivo de equipos, que se ejecute cada 6 meses, donde se documente la actividad.	0	1	1
R101	HW11		A. 12.3.1 Respaldo de la información	Se deben establecer actividades de creación de copias de respaldo de información y/o configuración, adicionalmente las copias se deben poner a prueba de forma regular para garantizar su correcto funcionamiento dejando el registro de pruebas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R101	HW11		A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.			
R102	HW11	3	A. 8.1.3 Uso aceptable de los activos	Se deben definir las condiciones de uso aceptable para los activos de información y las restricciones de uso de estos, de igual forma se deben divulgar con los usuarios internos y externos.	0	1	1
R102	HW11		A. 11.2.1 Ubicación y protección de los equipos	Se deben definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R102	HW11		A. 11.2.8 Equipos de usuario desatendidos	Se debe exigir a los empleados que los equipos no deben quedar desbloqueados con sesiones abiertas sin la presencia del usuario responsable.			
R103	HW12	3	A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.	2	0	2
R103	HW12		A.11.1.4 Protección contra amenazas externas y ambientales	Se debe implementar seguridad física contra ataques, accidentes, eventos o acciones amenazantes.			
R103	HW12		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R103	HW12		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R104	HW12	3	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	2	0	2
R104	HW12		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			
R104	HW12		A.11.2.1 Ubicación y protección de los equipos	Se debe definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R105	HW12	3	A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.	2	0	2
R105	HW12		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R105	HW12		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R106	HW12	3	A.11.2.4 Mantenimiento de equipos	Se debe planificar y ejecutar un plan de mantenimiento preventivo para equipos, así como una estrategia de mantenimientos correctivos.	1	0	1
R106	HW12		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R106	HW12		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R107	HW12	3	A.11.2.4 Mantenimiento de equipos	Se debe planificar y ejecutar un plan de mantenimiento preventivo para equipos, así como una estrategia de mantenimientos correctivos.	1	0	1
R107	HW12		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R107	HW12		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R110	SW3	3	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	0	1	1
R110	SW3		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			
R110	SW3		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R111	SW2	6	A.12.1.2 Gestión de cambios	Se debe definir un procedimiento de control de cambios donde se evalúen antes de su implementación, considerando el impacto que pueda tener sobre la operación y donde deben aprobar por las partes interesadas.	1	1	2
R111	SW2		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R111	SW2		A.12.5.1 Instalación de *software* en sistemas operativos	Se deben definir las directrices para controlar los camios en el *software* operacional en sistemas operativos que garantice mediante pruebas el correcto funcionamiento de los cambios y la estrategia de mitigación en caso de problemas con las nuevas versiones.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R113	SW2	3	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	1	1	2
R113	SW2		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			
R113	SW2		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R113	SW2		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R114	SW3	8	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R114	SW3		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R114	SW3		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R114	SW3		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R114	SW3		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R115	SW4	5	A.12.1.2 Gestión de cambios	Se debe definir un procedimiento de control de cambios donde se evalúen antes de su implementación, considerando el impacto que pueda tener sobre la operación y donde deben aprobar por las partes interesadas.	1	1	2
R115	SW4		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R115	SW4		A.12.5.1 Instalación de *software* en sistemas operativos	Se deben definir las directrices para controlar los camios en el *software* operacional en sistemas operativos que garantice mediante pruebas el correcto funcionamiento de los cambios y la estrategia de mitigación en caso de problemas con las nuevas versiones.			
R116	SW5	5	A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.	2	0	2
R116	SW5		A.18.1.2 Derechos de propiedad intelectual	Se debe implementar procedimientos eficientes para el cumplimento legal y contractual del uso de productos de *software* y propiedad intelectual.			
R117	SW6	5	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	1	1	2
R117	SW6		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			
R117	SW6		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R117	SW6		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R119	SW4	3	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	0	1	1
R119	SW4		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			
R119	SW4		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R119	SW4		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R120	SW5	4	A.9.4.4 Uso de programas utilitarios privilegiados	Se debe controlar el uso de programas que tenga la capacidad de anular el sistema y los controles sobre los equipos.	1	0	1
R120	SW5		A.12.6.1 Gestión de vulnerabilidades técnicas	Se debe desarrollar un plan de detección y mitigación de vulnerabilidades técnicas para los activos de información.			
R121	SW5	4	A.9.4.1 Restricción de acceso a la información	Se debe implementar controles técnicos y procedimentales para restringir el acceso a sistemas de acuerdo con una política.	1	1	2
R121	SW5		A.12.2.1 Controles contra códigos maliciosos	Se debe evaluar periódicamente la efectividad de los controles y ajustarlos para cumplir los requerimientos de seguridad de la información.			
R121	SW5		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R121	SW5		A.12.6.1 Gestión de vulnerabilidades técnicas	Se debe desarrollar un plan de detección y mitigación de vulnerabilidades técnicas para los activos de información.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R122	SW5	4	A.12.1.2 Gestión de cambios	Se debe definir un procedimiento de control de cambios donde se evalúen antes de su implementación, considerando el impacto que pueda tener sobre la operación y donde deben aprobar por las partes interesadas.	1	1	2
R122	SW5		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R122	SW5		A.12.5.1 Instalación de *software* en sistemas operativos	Se deben definir las directrices para controlar los camios en el *software* operacional en sistemas operativos que garantice mediante pruebas el correcto funcionamiento de los cambios y la estrategia de mitigación en caso de problemas con las nuevas versiones.			
R123	SW5	4	A.11.2.4 Mantenimiento de equipos	Se debe planificar y ejecutar un plan de mantenimiento preventivo para equipos, así como una estrategia de mantenimientos correctivos.	0	1	1
R123	SW5		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R124	SW5	4	A.12.5.1 Instalación de *software* en sistemas operativos	Se deben definir las directrices para controlar los camios en el s*oftware* operacional en sistemas operativos que garantice mediante pruebas el correcto funcionamiento de los cambios y la estrategia de mitigación en caso de problemas con las nuevas versiones.	0	2	2
R124	SW5		A.12.6.2 Restricciones sobre la instalación de s*oftware*	Se debe definir, implementar y divulgar directrices para la instalación y uso de *software* por parte de los usuarios.			
R124	SW5		A.18.1.2 Derechos de propiedad intelectual	Se debe implementar procedimientos eficientes para el cumplimento legal y contractual del uso de productos de *software*.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R125	SW5	4	A.9.2.2 Suministro de acceso de usuarios	Se debe desarrollar e implementar un proceso formal para asignar y revocar el acceso a usuarios para todos los sistemas de información y servicios.	0	1	1
R125	SW5		A.9.2.5 Revisión de los derechos de acceso de los usuarios	Se debe definir y ejecutar cronograma de tareas periódicas por parte de los propietarios de los activos para las revisiones derecho de acceso de los usuarios.			
R125	SW5		A.11.2.8 Equipos de usuario desatendido	Se debe concientizar a los usuarios sobre los requisitos y procedimiento de seguridad en los equipos desatendidos, así como implementar en lo posible controles para automatizar el bloqueo de sesiones inactivas.			
R126	SW5	4	A.9.1.1 Política de control de acceso	Se debe establecer y divulgar una política documentada para el control de acceso a la información y los activos de información del negocio, basada en los requisitos de seguridad de la información.	1	1	2
R126	SW5		A.9.4.1 Restricción de acceso a la información	Se debe establecer e implementar los controles para limitar el acceso a la información basados en el mínimo acceso requerido por el usuario para desarrollar sus funciones de acuerdo con la política de control de acceso.			
R126	SW5		A.11.2.8 Equipos de usuario desatendido	Se debe concientizar a los usuarios sobre los requisitos y procedimiento de seguridad en los equipos desatendidos, así como implementar en lo posible controles para automatizar el bloqueo de sesiones inactivas.			
R128	SW6	3	A.9.4.1 Restricción de acceso a la información	Se debe implementar controles técnicos y procedimentales para restringir el acceso a sistemas de acuerdo con una política.	1	0	1
R128	SW6		A.12.2.1 Controles contra códigos maliciosos	Se debe evaluar periódicamente la efectividad de los controles y ajustarlos para cumplir los requerimientos de seguridad de la información.			
R128	SW6		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R128	SW6		A.12.6.1 Gestión de vulnerabilidades técnicas	Se debe desarrollar un plan de detección y mitigación de vulnerabilidades técnicas para los activos de información.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R130	SW6	4	A.11.2.4 Mantenimiento de equipos	Se debe planificar y ejecutar un plan de mantenimiento preventivo para equipos, así como una estrategia de mantenimientos correctivos.	0	1	1
R130	SW6		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R132	SW6	4	A.9.2.2 Suministro de acceso de usuarios	Se debe desarrollar e implementar un proceso formal para asignar y revocar el acceso a usuarios para todos los sistemas de información y servicios.	0	1	1
R132	SW6		A.9.2.5 Revisión de los derechos de acceso de los usuarios	Se debe definir y ejecutar cronograma de tareas periódicas por parte de los propietarios de los activos para las revisiones derecho de acceso de los usuarios.			
R132	SW6		A.11.2.8 Equipos de usuario desatendido	Se debe concientizar a los usuarios sobre los requisitos y procedimiento de seguridad en los equipos desatendidos, así como implementar en lo posible controles para automatizar el bloqueo de sesiones inactivas.			
R133	SW6	4	A.9.1.1 Política de control de acceso	Se debe establecer y divulgar una política documentada para el control de acceso a la información y los activos de información del negocio, basada en los requisitos de seguridad de la información.	2	0	2
R133	SW6		A.9.4.1 Restricción de acceso a la información	Se debe establecer e implementar los controles para limitar el acceso a la información basados en el mínimo acceso requerido por el usuario para desarrollar sus funciones de acuerdo con la política de control de acceso.			
R133	SW6		A.11.2.8 Equipos de usuario desatendido	Se debe concientizar a los usuarios sobre los requisitos y procedimiento de seguridad en los equipos desatendidos, así como implementar en lo posible controles para automatizar el bloqueo de sesiones inactivas.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R137	SW8	4	A.9.4.1 Restricción de acceso a la información	Se debe implementar controles técnicos y procedimentales para restringir el acceso a sistemas de acuerdo con una política.	2	0	2
R137	SW8		A.12.2.1 Controles contra códigos maliciosos	Se debe evaluar periódicamente la efectividad de los controles y ajustarlos para cumplir los requerimientos de seguridad de la información.			
R137	SW8		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R137	SW8		A.12.6.1 Gestión de vulnerabilidades técnicas	Se debe desarrollar un plan de detección y mitigación de vulnerabilidades técnicas para los activos de información.			
R138	SW8	6	A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.	1	1	2
R138	SW8		A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	Se deben definir los protocolos de verificación del servicio prestado por proveedores para la verificación de los acuerdos de niveles de servicio y planificar auditorias periódicas, así como hacer seguimiento a la solución de cualquier problema identificado.			
R138	SW8		A.15.2.2. Gestión de cambios en los servicios de los proveedores	Se debe analiza, evaluar y monitorear los cambios en los servicios entregados por proveedores, los mantenimientos, las mejoras y los ajustes de controles con la finalidad de no generar impacto a los procesos del negocio.			
R139	SW8	7	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	1	1	2
R139	SW8		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			
R139	SW8		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R139	SW8		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R145	RD1	3	A.9.4.1 Restricción de acceso a la información	Se debe implementar controles técnicos y procedimentales para restringir el acceso a sistemas de acuerdo con una política.	1	1	2
R145	RD1		A.12.2.1 Controles contra códigos maliciosos	Se debe evaluar periódicamente la efectividad de los controles y ajustarlos para cumplir los requerimientos de seguridad de la información.			
R145	RD1		A.12.4.1 Registro de eventos	Se debe hacer revisión regular de los registros de eventos de acceso, cambios y eventos para los usuarios y los equipos.			
R145	RD1		A.12.6.1 Gestión de vulnerabilidades técnicas	Se debe desarrollar un plan de detección y mitigación de vulnerabilidades técnicas para los activos de información.			
R150	RD2	3	A.11.2.4 Mantenimiento de equipos	Se debe planificar y ejecutar un plan de mantenimiento preventivo para equipos, así como una estrategia de mantenimientos correctivos.	1	0	2
R150	RD2		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R150	RD2		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R171	RD8	3	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	1	0	1
R171	RD8		A.8.1.3 Uso aceptable de los activos	Se debe establecer una política que contemple el uso aceptable de activos de información donde se concientice sobre los requisitos de seguridad de la información en la organización.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R171	RD8		A.11.2.1 Ubicación y protección de los equipos	Se debe definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R172	RD8	4	A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.	1	1	2
R172	RD8		A.11.2.1 Ubicación y protección de los equipos	Se debe definir, documentar y divulgar con los usuarios las condiciones inseguras que atenten con los activos de seguridad de información; para exigirles el cumplimiento de buenas prácticas en el manejo de los activos.			
R172	RD8		A.11.2.3 Seguridad en el cableado	Se deben realizar auditorías y verificación de ubicación de equipos y su disposición para la protección de los elementos del cableado estructurado.			
R173	RH1	5	A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.	1	1	2
R173	RH1		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R173	RH1		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R173	RH1		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R174	RH1	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R174	RH1		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R174	RH1		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R174	RH1		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R174	RH1		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			
R176	RH1	5	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	1	1
R176	RH1		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R176	RH1		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R176	RH1		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R176	RH1		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R176	RH1		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R178	RH2	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R178	RH2		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R178	RH2		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R178	RH2		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R178	RH2		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R180	RH2	3	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	1	1
R180	RH2		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R180	RH2		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R180	RH2		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R180	RH2		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R180	RH2		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R182	RH3	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R182	RH3		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R182	RH3		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R182	RH3		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R182	RH3		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			
R186	RH4	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R186	RH4		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R186	RH4		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R186	RH4		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R186	RH4		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R188	RH4	3	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	1	1
R188	RH4		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R188	RH4		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R188	RH4		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R188	RH4		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R188	RH4		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R190	RH5	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R190	RH5		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R190	RH5		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R190	RH5		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R190	RH5		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			
R194	RH6	5	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R194	RH6		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R194	RH6		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R194	RH6		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R194	RH6		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R196	RH6	3	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	1	1
R196	RH6		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R196	RH6		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R196	RH6		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R196	RH6		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R196	RH6		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R198	RH7	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R198	RH7		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R198	RH7		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R198	RH7		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R198	RH7		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			
R200	RH7	3	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	1	1	2
R200	RH7		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R200	RH7		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R200	RH7		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R200	RH7		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R200	RH7		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R201	RH8	5	A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.	1	1	2
R201	RH8		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R201	RH8		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R201	RH8		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R202	RH8	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R202	RH8		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R202	RH8		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R202	RH8		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R202	RH8		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y Procedimentales necesarios para garantizar su cumplimiento			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R204	RH8	5	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	2	2
R204	RH8		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R204	RH8		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R204	RH8		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R204	RH8		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R204	RH8		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R206	RH9	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R206	RH9		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R206	RH9		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R206	RH9		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R206	RH9		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			
R208	RH9	3	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	1	1
R208	RH9		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R208	RH9		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			
R208	RH9		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R208	RH9		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R208	RH9		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R210	RH10	7	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la confidencialidad y la no divulgación de información de los pacientes.	1	1	2
R210	RH10		A.7.2.2 Toma de conciencia, educacion y formación en la seguridad de la información	Todos los usuarios deben recibir educacion sobre los requisitos de seguridad de la información para el proceso, las políticas y el cumplimento de la legislación aplicable en telemedicina.			
R210	RH10		A.9.3.1 Uso de información de autenticación secreta	Se debe definir y socializar con los usuarios una política para el buen uso de la información secreta.			
R210	RH10		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de seguridad, así como ajustar los acuerdos de confidencialidad con los empleados con relación a las necesidades de la organización.			
R210	RH10		A.18.1.4 Privacidad y protección de información de datos personales	Se debe desarrollar e implementar una política para procurar la seguridad y protección de datos personales, así como implementar los controles técnicos y procedimentales necesarios para garantizar su cumplimiento.			
R212	RH10	3	A.7.1.2 Términos y condiciones del empleo	Dentro de los acuerdos contractuales con los empleados se deben definir sus responsabilidades con respecto a la disponibilidad y procedimiento que realizar donde por un caso de fuerza mayo no pueda cumplir con sus funciones.	0	2	2
R212	RH10		A.12.1.1 Procedimiento de operación documentados	Los procedimientos operacionales del proceso de telemedicina en Colombiana de Trasplantes deben estar documentados y disponibles para los usuarios en caso de ser necesarios.			
R212	RH10		A.12.3.1 Respaldo de información	Se debe definir una política de copias de respaldo periódicas de la información de utilizan los usuarios bajo requisitos definidos por la Colombiana de Trasplantes, así como probarlas regularmente.			

Cuadro 19. (Continuación)

Código riesgo	Código activo	Riesgo Inherente	Control ISO27001	Estrategia de Tratamiento	Impacto residual	Probabilidad residual	Riesgo residual
R212	RH10		A.16.1.2 Reporte de eventos de seguridad de la información	Se debe definir un procedimiento de reporte de eventos que contemple afectaciones a la disponibilidad como la ausencia de personal.			
R212	RH10		A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			
R212	RH10		A.17.1.2 Implementación de la continuidad de la seguridad de la información	Se debe planificar e implementar un plan de continuidad de seguridad de la información frente a situaciones adversas que atenten contra los objetivos del negocio.			

Fuente: elaboración propia.

5.3.9 Riesgo residual. Con la implantación de los controles propuestos se procura reducir el riesgo residual al nivel aceptable definido por Colombiana de Trasplantes como se puede evidenciar en el mapa de calor del riesgo residual, sin embargo, como ya se mencionó con anterioridad, es indispensable evaluar periódicamente la efectividad de los controles después de su implementación y en caso de detectar que el control no reduce el riesgo a los niveles aceptables, se debe reevaluar la estrategia modificando o remplazando los controles propuestos.

En el cuadro 20, se muestra la ubicación de cada uno de los riesgos residuales esperados en su respectivo cuadrante del mapa de calor, presentando todos los riesgos en nivel bajo después de la implementación de los controles propuestos, identificables visualmente de color verde, que son aceptables para Colombiana de Trasplantes en el proceso de telemedicina.

Cuadro 20. Mapa de calor del riesgo residual

Matriz de valoración del riesgo						
		Probabilidad				
		Muy baja (0)	Baja (1)	Media (2)	Alta (3)	Muy Alta (4)
Impacto	Muy Bajo (0)	R156 R20	R155 R159 R160 R163 R164 R4 R50 R53 R59 R60 R61 R69 R76 R77 R79 R80 R83 R84 R85 R92 R93 R100 R101 R102 R110 R119 R123 R125 R130 R132 R176 R180 R188 R196 R208	R124 R204 R212	–	–
	Bajo (1)	R15 R16 R23 R24 R31 R32 R35 R36 R39 R40 R47 R48 R51 R63 R64 R67 R71 R72 R75 R87 R88 R89 R91 R95 R96 R99 R131 R134 R135 R142 R143 R152 R153 R165 R166 R168 R169 R177 R181 R185 R189 R193 R197 R205 R209 R11 R12 R14 R17 R18 R25 R29 R33 R34 R37 R38 R41 R42 R46 R49 R54 R57 R58 R65 R73 R86 R106 R107 R120 R128 R150 R171	R19 R27 R55 R56 R90 R108 R109 R112 R136 R141 R147 R151 R154 R157 R158 R161 R162 R167 R170 R175 R179 R183 R184 R187 R191 R192 R195 R199 R203 R207 R211 R1 R2 R3 R5 R6 R7 R8 R9 R10 R11 R12 R14 R17 R18 R25 R26 R29 R33 R34 R37 R38 R41 R42 R44 R46 R49 R52 R54 R57 R58 R62 R65 R66 R68 R70 R73 R74 R78 R81 R82 R86 R94 R97 R98 R106 R107 R111 R113 R114 115 R117 R120 R121 R122 R126 R128 R138 R139 R145 R150 R171 R172 R173 R174 R178 R182 R186 R190 R194 R198 R200 R201 R202 R206 R210	-	-	-
	Medio (2)	R22 R30 R118 R127 R129 R140 R144 R146 R148 R149 R13 R103 R104 R105 R116 R133 R137	-	-	-	-
	Alto (3)	-	-	-	-	-
	Muy Alto (4)	-	-	-	-	-

Fuente: elaboración propia.

5.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE TELEMEDICINA EN COLOMBIANA DE TRASPLANTES

El numeral 5.2 y el objetivo de control A.5 del anexo A de la norma ISO/IEC 27001:2013 establece la necesidad de las políticas de seguridad de la información definidas y respaldadas desde la alta gerencia para soportar el sistema de gestión de seguridad de la información, donde estas deben cumplir con los requisitos que se establecen en la norma, además, como se evidencia en el tratamiento de riesgos, proporciona la línea base para respaldar los controles.

Como referencia para la elaboración de las políticas de seguridad de la información para el proceso de telemedicina en Colombiana de Trasplantes se toman los temas de ejemplo del numeral 5.1.1 de la norma ISO/IEC 27002:2015, además de la guía para implementar las políticas planteadas en el Modelo de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia.

A continuación, se formulan las políticas de seguridad de la información que permitirán el tratamiento de los riesgos identificados en el proceso de Telemedicina en Colombiana de Trasplantes que deberán ser respaldadas por la alta gerencia y comunicadas a todos los empleados y partes externas interesadas de la forma más conveniente, accesible y clara.

5.4.1 Política general de seguridad de la información.

5.4.1.1 Objetivo. Establecer desde la alta dirección los lineamientos para el sistema de gestión de seguridad de la información en Colombiana de Trasplantes con la finalidad de alinear los procesos de acuerdo con los requisitos del negocio, los requerimientos de ley y de la norma ISO/IEC27001:2013, para la protección de los activos de información y la mejora continua del sistema.

5.4.1.2 Alcance. Esta política es de estricto cumplimiento tanto por empleados, contratistas y terceros de Colombiana de Trasplantes que obran en función de encargados del tratamiento de activos de información y que deben adoptar estas directrices en el cumplimiento de sus funciones y/o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole**.**

5.4.1.3 Declaración. La IPS Colombiana de Trasplantes S.A.S. cuyo objeto principal es la prestación de servicios de salud en cualquiera de sus manifestaciones y en particular la prestación del servicio de trasplante renal, hígado, páncreas o cualquier parte del cuerpo

humano susceptible de trasplante que sufran o requieran de este procedimiento, donde se compromete al análisis y tratamiento de riesgos de seguridad de la información, con base en la norma ISO/IEC27001:2013, teniendo el objetivo de garantizar la protección de la información, el cumplimiento de la ley aplicable y la mejora continua del sistema de gestión de seguridad de la información.

Esta política está enfocada en proteger los activos de información e incentivar a los funcionarios, contratistas y partes interesadas en aplicar buenas prácticas de seguridad, así como en cumplir con las directrices definidas por la organización para garantizar la seguridad en el proceso.

Colombiana de Trasplantes se compromete a fomentar la cultura de seguridad de la información mediante un programa de toma de conciencia de obligatorio cumplimiento para todos los empleados y partes externas interesadas.

5.4.1.4 Roles y responsabilidades. Desde la alta dirección de Colombiana de Trasplantes se tiene el compromiso de definir, aprobar y divulgar los lineamientos generales de seguridad de la información, así como con el apoyo y los recursos necesarios para la implementación y mantenimiento del sistema de gestión para la seguridad de la información. También se compromete a realizar el seguimiento periódico de la política, del sistema y al seguimiento del cumplimiento de las políticas definidas.

Los empleados, contratistas y terceros tienen la responsabilidad de conocer las políticas de seguridad de la información para Colombiana de Trasplantes, cumplirlas y ayudar con la mejora continua del sistema de gestión de seguridad de la información, así como de participar en las actividades del programa de toma de conciencia en seguridad de la información.

Los responsables de los activos de información tienen la obligación de garantizar la seguridad de la información mediante la disposición de controles apropiados que mitiguen los riesgos encontrados, así como de apoyar todas las tareas de análisis con el oficial de seguridad, de evaluar la efectividad de la estrategia y el impacto de los cambios sobre el proceso.

El oficial de seguridad nombrado por la alta dirección tiene la responsabilidad de desarrollar la estrategia de seguridad apoyado por los responsables de los activos de información, así como de velar por el cumplimiento del programa de concientización, garantizar la evaluación y tratamiento periódicos de los riesgos, también es responsable de definir y gestionar los indicadores para la evaluación del sistema de gestión. De la misma forma el oficial de seguridad y la alta dirección son los únicos autorizados como interlocutores válidos para el contacto con las autoridades y grupos de interés especial.

5.4.1.5 Sanciones. El incumplimiento de las directrices definidas en la presente política implicará un proceso disciplinario para los empleados involucrados en un incidente de seguridad y/o las acciones legales pertinentes que el área jurídica de Colombiana de Trasplantes determine apropiadas ya sea para empleados, contratistas o terceros. Adicionalmente, los eventos de seguridad deben ser documentados y analizados por un comité de seguridad que involucre la alta dirección, los responsables de los activos de información afectados y los responsables del sistema de seguridad de la información, con el fin de determinar el impacto generado, así como la responsabilidad de las partes involucradas.

5.4.2 Política de dispositivos móviles y teletrabajo. Objetivo: Garantizar la seguridad de la información en el uso de dispositivos móviles y el teletrabajo.

Alcance: Esta política aplica para todos los dispositivos asignados por Colombiana de Trasplantes que realizan algún tipo de tratamiento de datos en los procesos, así como a los empleados, contratistas y terceros.

Lineamientos:

- Ningún funcionario, contratista o tercero de Colombiana de Trasplantes debe usar su dispositivo móvil personal para el tratamiento de información confidencial, solo se deberán emplear equipos corporativos que cuenten con los controles de seguridad descritos en esta política.
- Todos los dispositivos móviles de Colombiana de Trasplantes deben estar inventariados y asignados a un responsable específico.
- Los dispositivos móviles de Colombiana de Trasplantes deben tener controles para impedir la instalación de *software* que represente un riesgo de seguridad.
- Las versiones aprobadas de sistema operativo para los dispositivos móviles de Colombiana de Trasplantes deben ser monitoreadas y aprobadas por el proceso de tecnologías de la información.
- El proceso de tecnologías de la información debe restringir las conexiones a puntos de acceso inseguros en los dispositivos móviles de Colombiana de Trasplantes.
- Todos los dispositivos móviles de Colombiana de Trasplantes deben tener controles de acceso con contraseñas seguras y complejas, incluyendo mínimo 5 caracteres alfanuméricos y un carácter especial.
- El proceso de tecnologías de la información debe cifrar las memorias internas y extendidas de los dispositivos móviles de Colombiana de Trasplantes.
- Los dispositivos móviles de Colombiana de Trasplantes deben estar vinculados a un control de administración remota que permita ubicación, bloqueo y borrado remoto.
- Se deben instalar controles de detección de *malware* y aplicaciones sospechosas o maliciosas en los dispositivos móviles de Colombiana de Trasplantes.

- Los empleados de Colombiana de Trasplantes en modalidad de teletrabajo deben disponer de un sitio con la seguridad física y del entorno necesaria para garantizar la integridad, confidencialidad y disponibilidad de la información.
- Las conexiones de comunicación a los servicios tecnológicos de los empleados de Colombiana de Trasplantes en modalidad de teletrabajo deben ser mediante canales seguros y privados como redes privadas virtuales (VPN), estas deben ser solicitadas al proceso de tecnologías de la información y autorizadas por el jefe del funcionario.
- Las actividades laborales en la modalidad de teletrabajo se deben desarrollar desde los equipos corporativos asignados a los empleados de Colombiana de Trasplantes, ya que estos cuentan con los controles de seguridad para garantizar la protección de la información.
- Todos los medios de información digitales y físicos que custodian los empleados de Colombiana de Trasplantes en la modalidad de teletrabajo deben ser almacenados de forma segura, sin que estén expuestos a factores externos como destrucción, robo o manipulación por parte de terceros.

5.4.3 Política de seguridad en el recurso humano. Objetivo: Asegurar que empleados y contratistas de Colombiana de Trasplantes cumplan con los requisitos del cargo, además que conozcan y acepten las responsabilidades de sus funciones, así como sus obligaciones con respecto a la seguridad de la información.

Alcance**:** Esta política aplica para todos los procesos de selección y desvinculación de personal que desarrolle el proceso de talento humano, así como para todas las actividades de seguimiento y manejo de personal.

Lineamientos:

- El proceso de talento humano debe verificar los antecedentes y referencias de todos los candidatos que se postulen a un cargo en Colombiana de Trasplantes.
- El proceso de talento humano en Colombiana de Trasplantes debe verificar la veracidad de la información entregada por los aspirantes en la hoja de vida y garantizar que cumplan con el perfil del cargo al que aspiran.
- El proceso de talento humano en Colombiana de Trasplantes debe verificar los títulos académicos de los aspirantes con los organismos de control que conserven registros, tales como, asociaciones, consejos y facultades.
- Los aspirantes seleccionados antes de asumir un cargo en Colombiana de Trasplantes deben aceptar y firmar un acuerdo de confidencialidad y no divulgación, donde ratifiquen que entienden y aceptan las condiciones de confidencialidad.
- Colombiana de Trasplantes revisará periódicamente los acuerdos de confidencialidad y ajustará, en caso de ser necesario, las condiciones ya sea por cambios en la legislación o en los objetivos de negocio.

- En el contrato laboral y en el acuerdo de confidencialidad según corresponda, se discriminarán las acciones que Colombiana de Trasplantes tomará tanto legal como disciplinariamente frente a las faltas de la seguridad de la información por parte de los empleados.
- Los empleados de Colombiana de Trasplantes deberán estar plenamente informados de sus roles y responsabilidades en cuanto al manejo de activos de información.
- La alta dirección de Colombiana de Trasplantes hará seguimiento e incentivará a los empleados al cumplimiento de las políticas de seguridad de la información.
- El proceso de talento humano en Colombiana de Trasplantes deberá informar oportunamente la terminación o cambio de contrato laboral al proceso de tecnologías de la información, con el fin de cancelar o ajustar los permisos de acceso a los activos.

5.4.4 Política de gestión y uso aceptable de activos. Objetivo: Definir la responsabilidad sobre los activos de información en cuanto a inventarios, uso, clasificación y manejo, para garantizar el correcto tratamiento dentro de los procesos en Colombiana de Trasplantes.

Alcance: Esta política aplica para el manejo de todos los activos de información que se tratan en los procesos de Colombiana de Trasplantes.

Lineamientos:

- Colombiana de Trasplantes debe hacer la identificación de activos de información vinculados a sus procesos con una periodicidad máxima de un año o cuando un cambio importante ocurra, con la finalidad de mantener el inventario actualizado y depurado, esta actividad estará a cargo del proceso de tecnologías de la información y el proceso de logística.
- Colombiana de Trasplantes debe definir el propietario o responsable de cada activo de información en el inventario durante todo su ciclo de vida, asegurarse que la información permanezca actualizada en el inventario, que estén correctamente almacenados y protegidos.
- Colombiana de Trasplantes determinará la clasificación en el inventario para cada activo de información basándose en los criterios de confidencialidad, integridad y disponibilidad.
- Colombiana de Trasplantes etiquetará los activos de información según su clasificación en el inventario, adicionalmente definirá el mecanismo y el responsable para el desarrollo de esta actividad.
- El propietario o responsable de cada activo de información en Colombiana de Trasplantes debe garantizar una disposición segura de los mismos cuando cumplan su ciclo de vida, sean descartados, devueltos, reasignados o eliminados.
- El proceso de tecnologías de la información en Colombiana de Trasplantes debe programar y ejecutar un cronograma de mantenimientos preventivos a los equipos con una periodicidad de seis meses, al cronograma se le debe hacer seguimiento y

conservar evidencia de la actividad. De igual forma, se deben mantener documentados los procedimientos de mantenimiento.

- Los activos de información de propiedad o en custodia de Colombiana de Trasplantes deben ser utilizados específicamente para las actividades relacionadas a las responsabilidades a cargo del proceso o del empleado, en ninguna circunstancia, estos activos se deben emplear para fines particulares, de otras empresas o externos a la finalidad a la que el responsable del activo dispuso.
- Los empleados de Colombiana de Trasplantes no deberán almacenar información personal en equipos de cómputo, de almacenamiento y/o en servicios de la organización.
- Los activos de información asignados a los empleados de Colombiana de Trasplantes deben ser formalmente entregados por el responsable, así como una vez termine su contrato o el empleado cambie de responsabilidades se deben regresar formalmente.
- Los activos de información en Colombiana de Trasplantes se deben mantener en las condiciones de seguridad apropiadas para evitar la pérdida, robo, alteración o el daño.
- Los retiros de activos fuera de las instalaciones de Colombiana de Trasplantes deben ser autorizados por el responsable del activo y cumplir con las condiciones de seguridad apropiadas, como la protección de acceso a la información y su respaldo. Adicionalmente, deben contar con registros de entrada y salida.
- Los responsables de los activos de información en Colombiana de Trasplantes deben evaluar y autorizar todos los cambios importantes que puedan llegar a afectarlos o afectar el proceso relacionado, esto mediante un protocolo de pruebas, verificación y análisis de impacto del cambio.
- En Colombiana de Trasplantes está restringido el almacenamiento de información de pacientes o catalogada como restringida en medios removibles, exclusivamente los empleados con una autorización formal del oficial de seguridad podrán utilizar este tipo de medios tales como memorias USB, discos externos, CD/DVD y almacenamiento de teléfonos móviles, entre otros.
- En Colombiana de Trasplantes todos los medios removibles empleados para el almacenamiento de información deberán ser propios de la empresa, estar inventariados y contar con los controles de seguridad implementados por el proceso de tecnologías de la información.
- Todos los medios de almacenamiento en Colombiana de Trasplantes deben ser sanitizados inmediatamente después de cumplir su objetivo, ya sea por destrucción o borrado seguro.
- El proceso de tecnologías de la información en Colombiana de Trasplantes empleará controles para la protección de la información en tránsito que permitan garantizar la confidencialidad e integridad antes, durante y después de cada movimiento.

5.4.5 Política de control de acceso. Objetivo: Definir las condiciones apropiadas para el acceso a la información basados en las necesidades específicas de los usuarios y los procesos, así como el seguimiento a los permisos y actividades sobre los activos de información.

Alcance: Esta política aplica al acceso, los permisos y restricciones de acceso a activos de información por parte de todos los empleados, contratistas y terceros que participan en los procesos en Colombiana de Trasplantes.

Lineamientos:

- El acceso a los recursos de información para los usuarios en Colombiana de Trasplantes debe estar aprobado por el jefe directo especificando los recursos a los que se puede acceder y el nivel de acceso, siempre respaldado mediante un comunicado escrito que soporte el trámite de suministro de control de acceso al coordinador del proceso de tecnologías de información.
- Los responsables o dueños de los activos de información en Colombiana de Trasplantes deben definir roles de acceso y restricción a los activos de información a su cargo para la asignación ágil y efectiva de derechos de acceso a los usuarios, teniendo en cuenta el nivel de acceso y los derechos como leer, escribir o borrar.
- El control de acceso a redes, aplicaciones y/o sistemas en Colombiana de Trasplantes debe ser mediante usuario y contraseña, ajustados a los roles definidos al perfil del usuario por el responsable del activo de información y suministrados desde el proceso de tecnologías de la información.
- El proceso de talento humano en Colombiana de Trasplantes debe solicitar el retiro los derechos de acceso a la información cuando un funcionario se desvincula de su cargo, siempre mediante un comunicado escrito al coordinador de tecnologías de la información.
- Los responsables de los activos de información y los jefes de proceso en Colombiana de Trasplantes deben solicitar formalmente al coordinador de tecnologías de la información, los cambios en el suministro de control de acceso a los activos de información cuando un funcionario cambia de rol o responsabilidades, además de hacer auditorías de seguimientos periódicos a los accesos asignados para los recursos de información, donde deben ajustarlos o retirarlos de ser necesario.
- Los activos de información digital en Colombiana de Trasplantes deben estar protegidos para su autenticación con estándares de calidad de contraseñas seguras. Las contraseñas deben tener un mínimo de 9 caracteres alfanuméricos incluidos caracteres especiales, también se debe solicitar cambios periódicos de contraseñas por lo menos cada 45 días con un histórico mínimo de 12 contraseñas sin repetición; en casos donde se identifiquen riesgos altos de acceso no autorizado se deben adicionar controles de doble factor de autenticación.
- En Colombiana de Trasplantes toda la información de autenticación para los usuarios debe ser personal e intransferible, donde los usuarios que compartan su información

de acceso se verán sometidos a acciones disciplinarias y deberán asumir el no repudio de las actividades que se realicen usando sus credenciales.

- Los administradores de servicios informáticos en Colombiana de Trasplantes deben utilizar controles para bloqueos automáticos de sesiones de usuarios después de tiempos superiores a 10 minutos sin actividad en los sistemas de información.
- Los sistemas de información en Colombiana de Trasplantes deben generar registros de acceso a los activos de información lógicos y físicos, que deben ser almacenados de forma segura durante el tiempo de retención que el responsable de información defina como apropiado o necesario según los requerimientos de ley o de los requisitos del negocio.
- El responsable de cada activo de información en Colombiana de Trasplantes debe identificar las circunstancias que necesiten acceso privilegiado a los activos o sistemas de información, y con apoyo del oficial de seguridad definir la práctica apropiada de uso en condiciones específicas que no comprendan actividades cotidianas o regulares del proceso. Las actividades frecuentes deben tener privilegios de acceso limitados para la ejecución de las tareas rutinarias.
- El proceso de tecnologías de la información en Colombiana de Trasplantes limitará el tráfico de información con contraseñas en texto plano para la autenticación en las aplicaciones y recursos de red.
- El proceso de tecnologías de la información en Colombiana de Trasplantes restringirá el uso de programas con la capacidad de anular los sistemas de información o los controles de seguridad sobre los mismos, en caso de que se requieran es necesaria la aprobación formal del responsable del activo y el oficial de seguridad, donde se justifique su uso y se establezca el alcance.
- El proceso de tecnologías de la información en Colombiana de Trasplantes restringirá el acceso a código fuente de programas mediante el almacenamiento seguro y los permisos basados en roles.

5.4.6 Política de tratamiento de historias clínicas. Objetivo: Definir como debe ser el tratamiento apropiado de la información implícita en la historia clínica de los pacientes en Colombiana de Trasplantes, con la finalidad de cumplir con la legislación aplicable y evitar fugas de información sensible.

Alcance: Esta política aplica al acceso, los permisos y restricciones centrados en los procesos que impliquen el manejo de las historias clínicas de los pacientes en Colombiana de Trasplantes.

Lineamientos:

- La Historia Clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene

en su atención. En Colombiana de Trasplantes dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

- La identificación de la historia clínica en Colombiana de Trasplantes se hará con el número de la cédula de ciudadanía para los mayores de edad.
- En Colombiana de Trasplantes toda información sensible debe estar ubicada en el archivo respectivo de acuerdo con los tiempos de retención, y se debe organizar un sistema que le permita saber en todo momento, en qué lugar de la institución se encuentra la historia clínica, y a quien y en qué fecha ha sido entregada.
- En Colombiana de Trasplantes se debe tener un archivo único de historias clínicas en las etapas de archivo de gestión, central e histórico, el cual será organizado y prestará los servicios pertinentes guardando los principios generales establecidos en el Acuerdo 07 de 1994, referente al Reglamento General de Archivos, expedido por el Archivo General de la Nación y demás normas que lo modifiquen o adicionen.
- Colombiana de Trasplantes podrá entregar copia de la historia clínica al usuario o a su representante legal cuando este lo solicite, para los efectos previstos en las disposiciones legales vigentes.
- En Colombiana de Trasplantes para el traslado, entre prestadores de servicios de salud, de la historia clínica de un usuario, debe dejarse constancia en las actas de entrega o de devolución, suscritas por los funcionarios responsables de las entidades encargadas de su custodia.
- En Colombiana de Trasplantes la historia clínica debe conservarse por un periodo mínimo de 20 años contados a partir de la fecha de la última atención. Mínimo cinco (5) años en el archivo de gestión del prestador de servicios de salud, y mínimo quince (15) años en el archivo central.
- Colombiana de Trasplantes como prestador de servicios de salud debe archivar la historia clínica en un área restringida, con acceso limitado al personal de salud autorizado, conservando las historias clínicas en condiciones que garanticen la integridad física y técnica, sin adulteración o alteración de la información.
- En Colombiana de Trasplantes los programas automatizados que se diseñen y utilicen para el manejo de las historias clínicas, así como sus equipos y soportes documentales, deben estar provistos de mecanismos de seguridad, que imposibiliten la incorporación de modificaciones a la historia clínica una vez se registren y guarden los datos.
- En todo caso en Colombiana de Trasplantes debe protegerse la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado para conocerla y adoptar las medidas tendientes a evitar la destrucción de los registros en forma accidental o provocada.
- En Colombiana de Trasplantes la información en aplicaciones de video, fotografía, huellas dactilares y cualquier información considerada sensible debe mantenerse bajo estrictas medidas de seguridad y siempre debe contar con las autorizaciones de titulares, que deben encontrase centralizadas en alguna aplicación de gestión documental para su rápida consulta.

5.4.7 Política de controles criptográficos. Objetivo: Definir el uso de controles criptográficos para asegurar la confidencialidad, integridad, autenticidad y el acceso a los activos de información en los procesos de Colombiana de Trasplantes.

Alcance: Esta política aplica para la protección de los activos de información que contengan información almacenada y/o que están vinculados de alguna forma en la transferencia de información.

Lineamientos:

- Todos los dispositivos institucionales en Colombiana de Trasplantes que manejen información reservada deben contar con controles de cifrado de información, tales como los portátiles y los equipos de escritorio que deberán tener el disco cifrado; para el caso de dispositivos de almacenamiento externos y exclusivamente donde su uso este autorizado de acuerdo con la política de dispositivos móviles y teletrabajo, deberán tener la información cifrada o en su defecto todo el dispositivo cifrado.
- La administración de los controles de cifrado de información en Colombiana de Trasplantes debe estar coordinada por el proceso de tecnologías de la información, que mantendrá los medios de recuperación debidamente almacenados y protegidos para uso en caso de ser necesarios.
- Colombiana de Trasplantes utilizara algoritmos de cifrados seguros y reconocidos por estándares internacionales.
- Toda la información reservada en Colombiana de Trasplantes que viaje por medio de canales de comunicación digital como correos electrónicos, portales web, trasferencias de carpetas compartidas o cualquier otro similar, deberá estar cifrada o en su defecto el canal deberá estar cifrado mediante protocolos seguros, previniendo en cualquier caso que información confidencial viaje en texto plano.
- El proceso de tecnologías de la información en Colombiana de Trasplantes realizará la gestión efectiva y segura de las llaves de cifrado y su ciclo de vida, mediante la generación, distribución, respaldo y eliminación.
- Colombiana de Trasplantes utilizará llaves públicas válidas en los casos que sean necesarios, manteniendo un seguimiento y renovación periódica antes que caduquen, donde la emisión debe hacerse por entidades de certificación públicas válidas, que cumplan todos los estándares de seguridad y calidad para este proceso. No se emplearán llaves auto firmadas para los servicios de información ya que estas presentan altos riesgos de suplantación y acceso no autorizado.
- Colombiana de Trasplantes debe garantizar que todos los servicios de proveedores cumplan con el uso de llaves públicas válidas y buenas prácticas en controles criptográficos con algoritmos seguros.

5.4.8 Política de seguridad física y del entorno. Objetivo: Definir las condiciones apropiadas para prevenir el acceso físico no autorizado, la alteración física no autorizada de activos de información y/o la incursión no autorizada a las instalaciones.

Alcance: Esta política aplica al acceso de todas las ubicaciones físicas que contiene activos de información y están expuestas a empleados, contratistas y terceros en Colombiana de Trasplantes.

Lineamientos:

- Colombiana de Trasplantes definirá y divulgará las restricciones de acceso a los perímetros de seguridad donde se procese o almacenen activos de información.
- Colombiana de Trasplantes definirá los controles de acceso físicos sobre los perímetros de seguridad definidos, tales como cámaras, detectores de movimiento, detectores de humo, demarcación visual, personal de vigilancia, alarmas, puertas con cerraduras y controles biométricos, los cuales siempre deben estar bloqueados.
- En Colombiana de Trasplantes el acceso a perímetros de seguridad está habilitado exclusivamente para el personal autorizado y en caso de requerir acceso de personal sin autorización debe contar con aprobación del responsable autorizado, además de estar siempre acompañado durante la permanencia y todo el trayecto.
- Los activos de información de Colombiana de Trasplantes deben estar ubicados en sitios seguros donde se minimice el riesgo de robo, espionaje o cualquier riesgo asociado al acceso físico, esto incluye ubicaciones fuera de las instalaciones de la empresa.
- El proceso de tecnologías de la información en Colombiana de Trasplantes realizará revisiones periódicas a los requisitos de seguridad del cableado eléctrico y de comunicaciones.
- El personal de seguridad física en Colombiana de Trasplantes monitoreará el retiro de activos de información de las instalaciones, verificando la autorización del responsable valido, así como las condiciones de tiempo y naturaleza del retiro. Para cualquier caso se debe llevar una bitácora detallando el responsable del retiro, persona que autoriza, motivo y tiempo que el activo estará fuera.
- Colombiana de Trasplantes establecerá y divulgará el procedimiento de seguridad para los activos fuera de las instalaciones, adicionalmente se debe garantizar los controles de seguridad definidos para la confidencialidad, disponibilidad e integridad.
- El proceso de tecnologías de la información en Colombiana de Trasplantes debe garantizar el borrado seguro o destrucción de medios de almacenamiento en equipos y medios externos que se den de baja por obsolescencia, daño o deterioro; de igual forma para la reasignación de equipos o la devolución en caso de equipos rentados.

5.4.9 Política de seguridad en las operaciones. Objetivo: Definir las condiciones apropiadas para garantizar la continuidad de las operaciones de los procesos en Colombiana de Trasplantes.

Alcance: Esta política aplica al desarrollo de actividades por parte empleados, contratistas y terceros en Colombiana de Trasplantes.

Lineamientos:

- Todos los procedimientos de la operación en Colombiana de Trasplantes deben estar documentados y se deben hacer revisiones periódicas.
- El proceso de tecnologías de la información en Colombiana de Trasplantes debe definir y documentar la línea base de configuración para todos los sistemas de información y periódicamente se debe actualizar con respecto a los nuevos cambios que se aprueben.
- La gestión de cambios en los procesos operativos para Colombiana de Trasplantes debe contemplar el análisis del cambio y debe ser autorizado por el responsable o responsables de los activos involucrados, de este análisis se deben definir las condiciones necesarias en recursos, tiempos y amenazas que traiga el cambio para concretar la mejor estrategia de ejecución.
- Los cambios autorizados en Colombiana de Trasplantes deben tener un plan de trabajo con tiempos y responsabilidades, además de una estrategia de recuperación en caso de que el cambio no sea exitoso y se necesite revertir.
- Los equipos y servicios en Colombiana de Trasplantes que contengan información o acceso a información deben contar con controles para la detección, respuesta, mitigación y prevención frente a ataques, así como a códigos maliciosos (*malware*) conocidos y desconocidos. Los controles deben incluir, pero no estar limitados a: bloqueo de sitios web maliciosos, sospechosos o en listas negras, restricciones a la trasferencia de archivos desde o hacia redes externas o sitios desconocidos, revisión de archivos en tránsito o en reposo, filtrado de correos electrónicos y sus adjuntos.
- El proceso de tecnologías de la información en Colombiana de Trasplantes monitoreara el estado funcional y de actualización de definiciones de las soluciones de seguridad perimetral y en punto final, tales como: *firewall,* Detector de intrusos de red, *anti-malware, anti-spyaware, anti-phishing*, sistema de detección de fuga de información; entre otros.
- El proceso de tecnologías de la información en Colombiana de Trasplantes al detectar en un equipo un comportamiento relacionado a un riesgo de seguridad lo aislará de la red, adicionalmente el acceso del usuario a los servicios será restringido.
- El proceso de tecnologías de la información en Colombiana de Trasplantes limitará que los usuarios finales deshabiliten los controles de detección de código malicioso en sus equipos.

- El proceso de tecnologías de la información en Colombiana de Trasplantes realizará periódicamente las copias de seguridad de los activos de información y garantizará su integridad mediante pruebas de restauración.
- El proceso de tecnologías de la información en Colombiana de Trasplantes realizará una copia de seguridad en línea y otra copia de seguridad fuera de línea para garantizar el acceso a la información de los activos más críticos.
- El proceso de tecnologías de la información en Colombiana de Trasplantes garantizará la preservación y retención de los eventos de seguridad generados por las soluciones desplegadas, los sistemas de información, los registros de acceso y los registros de auditoría por un periodo mínimo de dos años, con el fin de conservar la evidencia para análisis futuros.
- El proceso de tecnologías de la información en Colombiana de Trasplantes garantizará que todos los relojes de los sistemas de información y seguridad estén sincronizados con una única fuente.
- El proceso de tecnologías de la información en Colombiana de Trasplantes es el único autorizado para la instalación de *software* en la organización e implementará los controles para el bloqueo de ejecución y/o instalación de *software*.
- En Colombiana de Trasplantes toda instalación de *software* debe ser previamente aprobada por el jefe inmediato del usuario y solicitado al proceso de tecnologías de la información, que verificará la disponibilidad de licenciamiento antes de proceder con la actividad.
- Todas las versiones de los productos de *software* instalados en Colombiana de Trasplantes deben ser probados por el proceso de tecnologías de la información para garantizar su operatividad con pruebas exitosas.
- Colombiana de Trasplantes realizará análisis regulares de vulnerabilidades a los activos de información para detectar los riesgos expuestos y tratarlos.
- Colombiana de Trasplantes creará planes de mitigación para los riesgos encontrados, que contemplen acciones de tratamiento y seguimiento de efectividad.
- En Colombiana de Trasplantes todas las pruebas y auditorías sobre los sistemas de información deben estar alineadas a un cronograma y se acordará el alcance en conjunto con las partes interesadas.
- El proceso de tecnologías de la información en Colombiana de Trasplantes hará seguimiento periódico a la vigencia de los contratos de servicio y soporte para las soluciones tecnológicas administradas.

5.4.10 Política de seguridad de las comunicaciones. Objetivo: Definir las condiciones apropiadas para garantizar la seguridad en las redes y en la trasferencia de información para los procesos en Colombiana de Trasplantes.

Alcance: Esta política aplica a los servicios de red y la trasferencia de información en Colombiana de Trasplantes.

Lineamientos:

- El proceso de tecnologías de la información en Colombiana de Trasplantes aplicará controles para el uso de los servicios de red de los usuarios, también, monitoreará los niveles de cumplimiento de acuerdos para el servicio y la detección de eventos de seguridad.
- Los funcionarios de Colombiana de Trasplantes no deben usar servicios personales de correo, almacenamiento en nube o mensajería, para el desarrollo de sus actividades organizacionales. El proceso de tecnologías de la información restringirá el acceso a este tipo de contenido o cualquier otro que represente un riesgo para los usuarios o los procesos de la organización.
- El proceso de tecnologías de la información en Colombiana de Trasplantes separará y limitará el acceso entre las diferentes redes para garantizar el servicio con los mínimos permisos de acceso necesarios.
- El proceso de tecnologías de la información en Colombiana de Trasplantes proveerá una conexión de invitados aislada y segura a los terceros que requieran servicio de internet.
- La información reservada de los pacientes en los procesos de Colombiana de Trasplantes solo se debe compartir y distribuir con el personal autorizado para actividades propias de la organización.
- La información reservada en Colombiana de Trasplantes solo se debe compartir por canales de comunicación institucionales y que la organización haya definido como autorizados.
- El envío de información a terceros catalogada como reservada en Colombiana de Trasplantes, debe ser autorizado por el representante legal o su encargado.
- El proceso de tecnologías de la información en Colombiana de Trasplantes monitoreará los flujos de información en los vectores comunes de fuga tales como correo electrónico, servicios para compartir archivos en línea y medios de almacenamiento externo, con la finalidad de aplicar los bloqueos y generar los reportes al oficial de seguridad y a proceso de talento humano.

5.4.11 Política de seguridad en la relación con proveedores. Objetivo: Establecer las condiciones que se deben cumplir para la protección de activos de información en custodia o manejo de proveedores en los procesos de Colombiana de Trasplantes.

Alcance: Esta política aplica a todos los proveedores de Colombiana de Trasplantes.

Lineamientos:

- Todos los proveedores que intervienen en los procesos de Colombiana de Trasplantes deben estar identificados y catalogados según el tipo de servicio que prestan y el nivel de acceso a la información que manejan.
- Los proveedores de Colombiana de Trasplantes deben conocer y aceptar la política de seguridad de la información.
- Los proveedores de Colombiana de Trasplantes deben garantizar que tiene los controles y cumplen los requisitos de seguridad necesarios para la prestación del servicio, así como aceptar la realización de auditorías para verificar el cumplimiento.
- El proceso de logística con el acompañamiento del oficial de seguridad realizará seguimiento periódico a los acuerdos de servicio con cada uno de los proveedores.
- Colombiana de Trasplantes debe acordar con los proveedores cuando se realicen cambios sobre el servicio que pueda afectar la operación, generando un procedimiento para la gestión del cambio que incluya estrategia, planes de trabajo, notificaciones oportunas, cronogramas de mantenimiento y reportes sobre cada actividad.

5.4.12 Política para la gestión de incidentes de seguridad de la información. Objetivo: Establecer las responsabilidades y procedimientos para el tratamiento de incidentes de seguridad en Colombiana de Trasplantes.

Alcance: Aplica a todos los empleados, contratistas y terceros involucrados en los procesos de Colombiana de Trasplantes.

Lineamientos:

- La alta dirección en Colombiana de Trasplantes asignará un responsable para liderar el tratamiento de incidentes de seguridad de la información, este debe recopilar los eventos, convocar a las partes interesadas, dirigir la investigación del evento y liderar el grupo de trabajo para decidir si se cataloga como un incidente de seguridad para posteriormente tomar las acciones necesarias.
- Todas las partes involucradas en los procesos de Colombiana de Trasplantes deben reportar los eventos de seguridad y comportamientos que vayan en contravía de las políticas de seguridad establecidas por la organización, así como los comportamientos inseguros encontrados en el desarrollo de las actividades que atenten contra la disponibilidad, integridad y confidencialidad de los activos de información. Los reportes se deben hacer directamente al responsable designado por la alta dirección, mediante los canales válidos definidos.
- Durante el tratamiento de incidentes de seguridad de la información en Colombiana de Trasplantes se debe formalizar el reporte del evento, hacer el levantamiento de información preliminar, realizar la evaluación del evento y definir si se clasifica con incidente dentro de la escala previamente establecida, dar respuesta al incidente con los protocolos preestablecidos en los procedimientos para el tratamiento. Después del

manejo de incidente se deberá presentar el reporte a la alta gerencia y a las partes interesadas, incluyendo las lecciones aprendidas.

- Para el tratamiento de incidentes de seguridad de la información en Colombiana de Trasplantes se mantendrán una retención mínima de dos años de los registros de eventos de los sistemas de información, para permitir analizar los comportamientos detectados y generar informes consolidados de ser necesarios.
- El designado por la alta dirección de Colombiana de Trasplantes deberá definir, documentar y divulgar los procedimientos para el tratamiento de incidentes de seguridad, que contemplen como mínimo el reporte, canales de comunicación, responsabilidades, recolección de evidencia, estrategia de análisis, valoración, procedimientos preestablecidos de respuesta y evaluación de resultados, así como las lecciones aprendidas.
- El grupo de trabajo que desarrollará las actividades de tratamiento de incidentes de seguridad en Colombiana de Trasplantes debe contar con: el responsable principal designado por la alta dirección, un representante de la alta dirección, un especialista forense interno o externo y los responsables de los activos de información afectados. En caso de que sea necesario se debe incluir a un representante del equipo Legal de Colombiana de Trasplantes.

5.4.13 Política para la gestión de continuidad del negocio. Objetivo: Desarrollar una política de gestión de la continuidad del negocio incluyendo la continuidad de la seguridad de la información para los procesos en Colombiana de Trasplantes.

Alcance: Esta política aplica a los procesos en Colombiana de Trasplantes que requieren asegurar, recuperar y restablecer la disponibilidad, así como para el sistema de gestión de seguridad de la información.

Lineamientos:

- Colombiana de Trasplantes definirá las directrices para la continuidad del negocio y recuperación en situaciones adversas, mediante un plan de continuidad para recuperar y restablecer la disponibilidad de los procesos, que incluya los requisitos de seguridad de la información.
- Colombiana de Trasplantes definirá los niveles de disponibilidad de servicio en cada uno de sus procesos de acuerdo con las necesidades del negocio con sus clientes, proveedores y partes interesadas.
- Colombiana de Trasplantes debe establecer, implementar y mantener actualizados los procesos, procedimientos y controles de continuidad del negocio, realizando anualmente simulacros de continuidad y recuperación.
- Colombiana de Trasplantes definirá los responsables de autorizar y ejecutar los procedimientos de continuidad, que deben contar con las capacidades y autoridad suficiente para su ejecución.

- Los planes de recuperación en Colombiana de Trasplantes se deben revisar con regularidad o cuando un cambio significativo ocurra, con el fin de ajustar los procedimientos de acuerdo con las necesidades de seguridad del proceso.
- Colombiana de Trasplantes deberá evaluar periódicamente las estrategias de redundancia para los servicios con el fin de garantizar la disponibilidad en casos de eventos adversos que afecten la operación.
- Los componentes de los servicios de internet y energía en Colombiana de Trasplantes deben contar con estrategias de respaldo en caso de que por algún motivo sea suspendidos parcial o totalmente, en lo posible deben tener controles automáticos de detección de fallos; estos respaldos se deben probar regularmente para garantizar su operatividad.

5.4.14 Política de cumplimiento. Objetivo: Asegurar el cumplimiento de requisitos legales y contractuales relacionados con la seguridad de la información en Colombiana de Trasplantes.

Alcance: Esta política aplica para todos los requisitos legales y contractuales relacionados con los procesos de Colombiana de Trasplantes.

Lineamientos:

- Colombiana de Trasplantes en cabeza del oficial de seguridad y el área jurídica debe revisar constantemente los requisitos legales y contractuales con terceros que tengan injerencia en la seguridad de la información, así mismo deberá generar planes de acción para implementar cuando se identifique un posible riesgo de incumplimiento.
- Colombiana de Trasplantes velará por el cumplimiento de los derechos de los titulares y los principios del tratamiento de datos personales, tales como: principio de la legalidad, principio de finalidad, principio de libertad, principio de veracidad, principio de transparencia, principio de acceso y circulación restringida, principio de seguridad y principio de confidencialidad.
- Toda adquisición de *software* y servicios relacionados en Colombiana de Trasplantes se debe realizar por medio del proceso de tecnologías de la información que garantizará el cumplimiento de las condiciones de uso del fabricante y la legislación asociada.
- Colombiana de Trasplantes debe garantizar el cumplimiento de las leyes de propiedad intelectual y derechos de autor en el *software.*
- El proceso de tecnologías de la información en Colombiana de Trasplantes debe realizar revisiones periódicas para la identificación de *software* no autorizado, vigencia y cobertura de licenciamiento de acuerdo con la disponibilidad adquirida.
- Es de obligatorio cumplimiento que todos los empleados y terceros involucrados en los procesos de Colombiana de Trasplantes conozcan y cumplan a cabalidad la legislación aplicable para la protección de datos personales, además que realicen un

manejo adecuado dentro de lo que enmarca la ley de la información reservada de los pacientes, funcionarios y terceros.

- Colombiana de Trasplantes monitoreará y controlará los flujos de información reservada desde sus instalaciones y equipos hacia externos para prevenir los movimientos de datos no autorizados.
- El oficial de seguridad de Colombiana de Trasplantes con el apoyo del proceso de mejoramiento de la calidad desarrollará las auditorías semestrales periódicas a los procesos y sistemas relacionados con activos de información, e informarán a la alta gerencia los resultados.

5.4.15 Capacitación y sensibilización en seguridad de la información. Objetivo: Asegurar el conocimiento, la comprensión y cumplimiento de todos los procedimientos, políticas y legislación relacionada con temas de protección enfocados en la seguridad de la información en Colombiana de Trasplantes.

Alcance: Aplica a todos los empleados, contratistas y terceros involucrados en los procesos de Colombiana de Trasplantes.

Lineamientos:

- La alta dirección de Colombiana de Trasplantes se compromete a apoyar y destinará los recursos necesarios para el entrenamiento del personal de seguridad de la información, y el desarrollo del plan de concientización a los empleados, contratistas y partes interesadas en los procesos de la organización, los cuales serán sensibilizados y tendrán la obligación de asistir a las actividades programadas.
- El oficial de seguridad y el proceso de cultura y liderazgo en Colombiana de Trasplantes son los responsables del diseño, la planeación y desarrollo del plan de concientización, donde analizarán el resultado de las actividades y ajustarán periódicamente el plan para lograr una mejora continua.
- Colombiana de Trasplantes instruirá sobre comportamientos seguros para uso y manipulación de dispositivos móviles.
- En Colombiana de Trasplantes los empleados antes de asumir el cargo y durante su permanencia serán capacitados en las políticas y los aspectos concernientes a seguridad de la información.
- Los empleados de Colombiana de Trasplantes deben estar sensibilizados con las buenas prácticas para el manejo de activos de información, particularmente con la normativa y legislación aplicable a la información de pacientes, y en consecuencia deben cumplirla a cabalidad.
- Dentro del plan de concientización en Colombiana de Trasplantes se debe motivar a los usuarios a cambiar regularmente sus credenciales de acceso a los activos de información, cumpliendo con las definiciones de complejidad y caducidad entregadas por el oficial de seguridad y acordes a las necesidades del negocio.

- Colombiana de Trasplantes debe capacitar a los usuarios sobre la importancia del escritorio limpio para mantener la confidencialidad en la información expuesta ya sea digital o física, principalmente la información ubicada sobre sus puestos de trabajo, en medios de almacenamiento de fácil acceso, en impresiones o fotocopias olvidadas, así como en la información visible en los escritorios de las sesiones de sus equipos y documentos abiertos permanentemente sin uso.
- Colombiana de Trasplantes divulgará a todos los empleados, contratistas y terceros involucrados en los procesos, la política de uso aceptable de *software* donde se especifique la prohibición de uso de *software* no autorizado.
- Colombiana de Trasplantes divulgará a los usuarios la responsabilidad y actividades a cargo en los procesos de generación de copias de respaldo de información.
- Colombiana de Trasplantes divulgará las directrices de obligatorio cumplimiento para la trasferencia de información en Colombiana de Trasplantes.

5.5 PLAN DE CONCIENTIZACIÓN

5.5.1 Objetivo. El plan de concientización tiene como objetivo asegurar que los integrantes de la organización conozcan, comprendan y cumplan todos los procedimientos, políticas y legislación relacionada con temas de protección enfocados en la seguridad de la información, donde principalmente se dé a conocer las políticas y directrices de seguridad definidas por Colombiana de Trasplantes, además de los riesgos que se pueden tener al dar mal uso a los activos de información que diariamente se manejan.

5.5.2 Alcance. Se propone la ejecución de tres fases esenciales que se conforman por el diseño, desarrollo e implementación, que permitirán llevar a cabo la ejecución efectiva del plan de concientización del SGSI con el fin de fomentar la apropiación de todas las temáticas definidas alineadas a las estrategias y objetivos de la organización al sistema de gestión de seguridad, esto basado en la NIST SP 800-50.

5.5.2.1 Diseño. En esta etapa se identifican las necesidades y prioridades dentro del SGSI donde se determina el alcance del plan de la concientización donde se definen las diferentes actividades a realizar para cumplir con las metas propuestas en el entorno de la sensibilización y capacitación de todos los integrantes de la organización, adoptando una cultura organizacional que cubra las necesidades del negocio. Por consiguiente, se proponen estos puntos a:

- Evaluación de las necesidades. La evaluación de necesidades nos proporciona un resultado general de lo que se debe aplicar para determinar necesidades para la sensibilización y capacitación, para así justificar ante la alta gerencia los recursos requeridos con el objetivo de iniciar con el desarrollo del plan de concientización y para lograr este proceso se proponen las siguientes actividades:
- Entrevistas con grupos claves.
- Auditorías internas.
- Verificación de comportamientos.
- Actividades de ingeniería social.
- Identificar incidentes de seguridad.
- Colaboración de otras áreas, para proceder con las diferentes actividades del plan de concientización es importante tener el apoyo del área de talento humano o logística para la programación de dichas actividades, definir la disponibilidad del personal y espacios para dictar las capacitaciones.

5.5.2.2 Desarrollo del plan de concientización. Al tener definidas las necesidades con la información recolectada se podrá continuar con el desarrollo del plan de concientización donde se debe definir la estrategia de desarrollo e implementación, igual contar con la viabilidad y el apoyo presupuestal por parte de la alta gerencia, cumpliendo con lo anteriormente mencionado, se debe definir:

- Definir las temáticas
- Definir actividades y estrategias
- A quién va dirigido
- Fechas de ejecución
- Registro de asistencia

5.5.2.3 Definir material y herramientas. Los materiales y herramientas se definen según la complejidad de la temática y el grupo objetivo, es importante identificar el tipo de aprendizaje que se va a aplicar (Sensibilización, capacitación o educación), tomando en cuenta lo anteriormente mencionado se recomienda elegir los siguientes materiales y herramientas:

- Pósters
- Presentaciones (PowerPoint, Prezzi, videos, etc.)
- Juegos
- Publicidad en medios electrónicos

5.5.2.4 Desarrollo. En el desarrollo se define las fuentes disponibles para los temas a difundir, cuál es el alcance, contenido, materiales a utilizar y las herramientas de apoyo.

En el desarrollo del material se debe garantizar que la temática a difundir sea de fácil entendimiento y que desarrolle las habilidades y destrezas que se pretenden, de igual forma sensibilizar al público objetivo de las implicaciones legales y responsabilidades que incurren al no aplicar lo aprendido. En el cuadro 21, se presentan las temáticas a desarrollar dentro del plan de concientización y los puntos a tratar.

Cuadro 21. Temáticas plan de concientización

Temática	Puntos a tratar
Información activo imprescindible de la organización	Importancia de la información Los tres pilares de la seguridad Protección de datos personales Privacidad y la ley
Contraseñas	Importancia de las contraseñas Buenas prácticas en su uso Robustez No compartirla No usar la misma Doble factor de autenticación Gestores de contraseñas
Puestos de trabajo	Importancia de proteger el puesto de trabajo Buenas practicas Mesas limpias Bloqueo de sesión *Software* actualizado Antivirus
Correo electrónico: principales fraudes y riesgo	Correo electrónico como herramienta Tipos de correo fraudulentos *Phishing* *Spam* *Malware*
Dispositivos móviles y teletrabajo: riesgos y protección	Riesgos asociados Medidas de protección Protección antimalware y sitios web peligrosos Protección contra accesos no autorizados Protección de la información Aplicaciones legitimas No recordar la contraseña No utilizar redes wifi-inseguras Otras medidas de protección en el teletrabajo
Redes sociales: medidas de seguridad para perfiles de empresa	El valor de las redes sociales Posibles riesgos de su uso Medidas de seguridad

Fuente: elaboración propia.

- **Ejecución capacitación información activo imprescindible de la organización.**
- Duración: 1 Hora.
- Fecha de ejecución: Mes 2.
- Modalidad: Virtual.
- Dirigido: Todo el personal de Colombiana de Trasplantes.
- Temas para tratar: importancia de la información, los tres pilares de la seguridad, protección de datos personales, privacidad y la ley.
- Consejo: Los datos son el pilar de tu empresa. ¡PROTÉGELOS!
- Consejo: Dale a tus DATOS el valor que tienen.

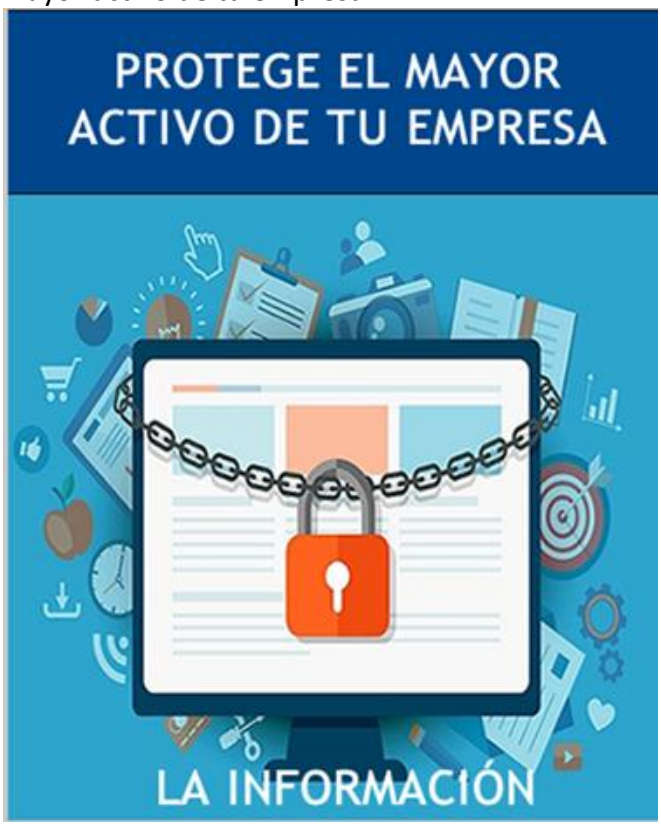
Con la figura 7, se busca concientizar a los usuarios sobre el valor de la información y el impacto de perderla.

Figura 7. Nunca se valora lo suficiente la información

Fuente: elaboración propia.

En la figura 8, se busca enfatizar la importancia de la información con activo de Colombiana de Trasplantes.

Figura 8. Protege el mayor activo de tu empresa



Fuente: elaboración propia.

- **Test evaluativo información activo imprescindible de la organización.**

1. Llamamos activos de información a toda información que tiene valor para la empresa y que, por tanto, tendremos que proteger. ¿En qué formato se encuentran los activos de información de las empresas hoy en día?
a) Solo en formato digital en ordenadores y dispositivos electrónicos como móviles.
b) Fundamentalmente en papel.
c) En la cabeza de las personas, los activos de información son su conocimiento del negocio.
d) En papel, en formato digital y en las personas, con su conocimiento.

2. Los tres pilares sobre los que se sostiene la seguridad de la información son:
a) Disponibilidad, integridad y confidencialidad.
b) Disponibilidad, autenticidad e integridad.
c) Disponibilidad, integridad y criticidad.
d) Integridad, autenticidad y criticidad.

3. Un dato personal es:
a) Una fotografía.
b) Todas las respuestas.
c) Un documento de identificación como el DNI.
d) Un correo electrónico si se puede asociar a una persona física.

4. ¿Qué afirmación es más correcta sobre los incidentes que pueden afectar a la seguridad de la información de la empresa?
a) Están exclusivamente provocados por ciberdelincuentes, es la única forma de que la información pueda verse comprometida.
b) Son siempre accidentales o causados por empleados de la empresa malintencionados o descuidados, también llamados *insiders*.
c) Los *insiders* son ciberdelincuentes que sobornan o influencian a empleados insatisfechos para causar incidentes.
d) Los ciberdelincuentes en ocasiones se aprovechan de nuestra ingenuidad o falta de preparación.

5. Si la empresa recoge datos personales, desde ese momento tiene capacidad para hacer con ellos lo que más convenga a la organización, sin que los usuarios puedan hacer ejercer ningún tipo de derecho:
a) Sí, porque así lo establece el Reglamento General de Protección de Datos.
b) No, ya que existen derechos y libertades que deben ser respetados de acuerdo con lo indicado en la ley.
c) Sí, siempre que el usuario haya aceptado los términos y condiciones del servicio.
d) Sí, siempre que los datos personales se encuentren en formato físico.

- **Ejecución capacitación contraseñas.**
- Duración: 1 Hora.
- Fecha de ejecución: Mes 3.
- Modalidad: Virtual.
- Dirigido a: Personal de telemedicina.
- Temas para tratar: importancia de las contraseñas, buenas prácticas en su uso, robustez, no compartirla, no usar la misma, doble factor de autenticación y gestores de contraseñas.
- Consejo: La CONTRASEÑA es la puerta de entrada a tu información.
- Consejo: Las contraseñas son como tu cepillo de dientes son solo para TU USO.

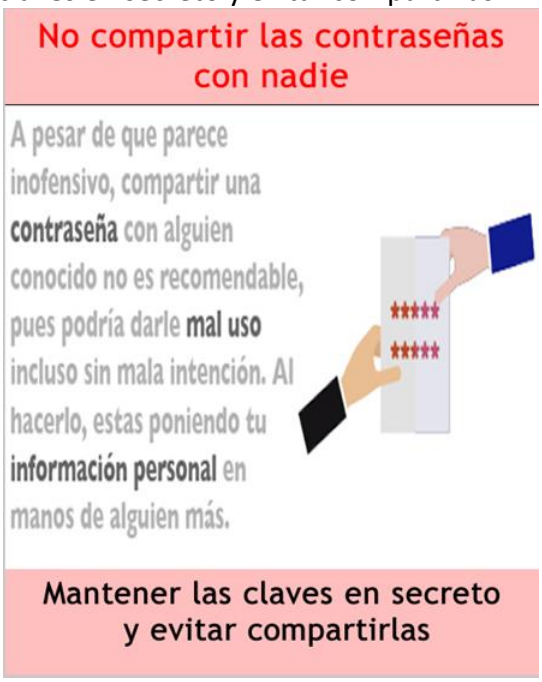
Con la figura 9, se pretende promover en los usuarios de Colombiana de Trasplantes el uso de buenas prácticas en las contraseñas de acceso a los servicios.

Figura 9. Una contraseña robusta para cada servicio

Fuente: elaboración propia.

Con la figura 10, se pretende evitar que los usuarios compartan sus contraseñas de acceso a servicios de Colombiana de Trasplantes.

Figura 10. Mantener las claves en secreto y evitar compartirlas



Fuente: elaboración propia.

- **Test evaluativo contraseñas.**

1. La robustez es una característica fundamental de las contraseñas basada principalmente en:
a) La longitud de esta y el tipo de caracteres utilizados.
b) Lo difícil que sea de recordar.
c) El número de letras mayúsculas utilizadas.
d) Todas las anteriores.

2. Una contraseña robusta debe estar compuesta por:
a) Un mínimo de 8 caracteres y que contenga números y letras.
b) Un mínimo de 8 caracteres y que contenga números, letras mayúsculas, minúsculas y símbolos.
c) Un mínimo de 8 caracteres y que contenga letras mayúsculas, minúsculas y símbolos.
d) Un mínimo de 16 caracteres y que sean números.

3. Los gestores de contraseñas son:
a) Funciones que incorporan las aplicaciones web para verificar si una contraseña es correcta o no.
b) Herramientas que permiten almacenar múltiples contraseñas de diferentes servicios.
c) Herramientas que utilizan los ciberdelincuentes para «adivinar» las contraseñas de sus víctimas.
d) Ninguna de las anteriores.

4. Uno de los errores más habituales cuando se utilizan contraseñas es:
a) Utilizar una contraseña débil.
b) Utilizar la misma contraseña para múltiples servicios.
c) Escribirla en un *post-it* o similar a la vista de cualquiera.
d) Todas las anteriores.

5. El doble factor de autenticación es:
a) Un mecanismo que añade una capa extra de seguridad a los servicios que requieren de usuario y contraseña para su uso por medio una nueva clave que, generalmente, es de un solo uso.
b) Un mecanismo que permite a dos usuarios acceder a un mismo servicio por medio de una única contraseña.
c) Un mecanismo utilizado en exclusiva por las redes sociales para verificar la identidad del usuario.
d) Una estrategia que utilizan algunos servicios en Internet que permite su acceso por medio de dos contraseñas distintas.

- **Ejecución capacitación puestos de trabajo.**
- Duración: 1 Hora.
- Fecha de ejecución: Mes 4.
- Modalidad: Virtual.
- Dirigido a: Todo el personal de Colombiana de Trasplantes.
- Temas para tratar: importancia de proteger el puesto de trabajo, buenas prácticas, mesas limpias, bloqueo de sesión, *software* actualizado y Antivirus.
- Consejo: Utiliza WIN + L cada vez que te levantes de tu puesto.
- Consejo: Practica el PARCHEADO y evita problemas. ¡Actualización OK!

Con la figura 11, se pretende concientizar a los usuarios de Colombiana de Trasplantes acerca de su responsabilidad en aseguramiento de su puesto de trabajo, para evitar pérdidas o divulgación no autorizada de información.

Figura 11. Tu puesto de trabajo es tu responsabilidad

Fuente: elaboración propia.

- **Test evaluativo puestos de trabajo**

1. El puesto de trabajo, desde el punto de vista de la ciberseguridad para la empresa:
a) Es clave, ya que de este dependerá en gran medida que la compañía no sufra un incidente que puede afectar a su continuidad.
b) Está expuesto a múltiples riesgos como pérdida de confidencialidad, infecciones por *malware* o información en formato físico accesible por terceras partes.
c) Debe ser protegido por el propio empleado siguiendo las políticas y recomendaciones indicadas por los responsables de la empresa.
d) Todas las anteriores**.**

2. Indica la respuesta correcta sobre el bloqueo de sesión:
a) Cualquier dispositivo debe estar bloqueado siempre que no se esté en presencia de este, a excepción de *tablets* y *smartphones*.
b) Cualquier dispositivo debe estar bloqueado siempre que no se esté en presencia de este, excepto si se encuentra dentro de la empresa, ya que es un lugar seguro.
c) Cualquier dispositivo debe estar bloqueado siempre que no se esté en presencia de este.
d) No es necesario habilitar un bloqueo de sesión.

4. El atajo de teclado para bloquear un dispositivo con sistema operativo *Windows* es:
a) Win + L
b) Win + B
c) Win + X
d) Win + Fin

5. Cuando el s*oftware* de un equipo esta desactualizado, se corre el riesgo de:
a) Contar con medidas de seguridad que pueden haber quedado obsoletas.
b) Todas las respuestas son ciertas.
c) Que un ciberdelincuente utilice alguna vulnerabilidad para tomar el control del dispositivo.
d) No poder utilizar las últimas funcionalidades ofrecidas por el fabricante.

6. ¿Cuáles son buenas prácticas para la protección del puesto de trabajo?
a) Disponer de una política de mesas limpias, difundirla y hacerla cumplir.
b) Mantener todo el *software* actualizado.
c) Instalar, activar y mantener actualizados los antivirus y cortafuegos.
d) Todas las anteriores, además de bloquear la sesión cuando no estemos frente a nuestros dispositivos.

- **Ejecución capacitación correo electrónico: principales fraudes y riesgo.**
- Duración: 1 Hora.
- Fecha de ejecución: Mes 5.
- Modalidad: Virtual.
- Dirigido a: Personal de telemedicina.
- Temas para tratar: correo electrónico como herramienta, tipos de correo fraudulentos, *Phishing, Spam y Malware.*
- Consejo: Envíos a múltiples destinatarios, siempre en COPIA OCULTA.
- Consejo: Correo SOSPECHOSO No dar clic sobre estos enlaces.

Con la figura 12, se busaca informar a los usuarios sobre las diferentes amenazas en los correos electrónicos que los pueden engañar para robar su información.

Figura 12. Los correos electronicos fraudulentos se esconden donde menos los esperas

Fuente: elaboración propia.

- **Test evaluativo correo electrónico: principales fraudes y riesgo.**

1. El *phishing* es un tipo de correo electrónico malicioso:
a) Cuyo objetivo, generalmente, es infectar los equipos de las víctimas con *malware*.
b) Cuyo objetivo es ofrecer información falsa.
c) Que suplanta a una empresa o entidad fiable y cuyo objetivo es generalmente hacerse con claves de acceso o información sensible.
d) Que hará que el dispositivo de la víctima funcione de manera anómala e imposibilitando realizar cualquier tarea con él.

2. Las campañas de envío de *software* malicioso o *malware* que realizan los ciberdelincuentes por correo electrónico generalmente se realizan utilizando una de las siguientes técnicas:
a) *Malware* incrustado en el propio correo que en el momento de ser abierto infecta el equipo.
b) Documentos adjuntos maliciosos.
c) Enlaces maliciosos a páginas web.
d) La «b» y la «c».

3. Ante una comunicación por correo electrónico cuyo remitente parece legítimo pero existen sospechas sobre su legitimidad, la mejor forma de proceder es:
a) Acceder a lo que solicita el correo, pero esto solamente si es abrir un archivo adjunto ya que los enlaces son más peligrosos.
b) Comprobar las cabeceras del correo con una herramienta especializada y ante la menor duda no interactuar con el correo de ninguna manera. Además, es recomendable borrarlo directamente para evitar futuras situaciones peligrosas.
c) Acceder a lo que solicita el correo, pero esto solamente si solicita abrir un enlace o responder a la propia comunicación ya que los archivos adjuntos son más peligrosos.
d) Ninguna de las anteriores.

4. La ingeniería social consiste en:
a) Intentar forzar a la víctima a realizar una determinada acción que beneficie al ciberdelincuente como revelar información confidencial, abrir un enlace o descargar y ejecutar un archivo adjunto.
b) Suplantar a una entidad conocida, como a un banco, cambiando su página web.
c) Realizar campañas masivas de envío de correos electrónicos fraudulentos.
d) Enviar correos electrónicos de spam.

5. Cuando se recibe un correo electrónico sospechoso, para verificar si es fraudulento nos fijaremos en:

a) En el remitente que puede estar falseado, para ver si es conocido y si está bien escrito.
b) En el remitente que puede estar falseado, en el cuerpo y asunto para detectar posibles engaños, en los adjuntos que pueden ser maliciosos y en los enlaces que pueden estar falseados.
c) En el cuerpo para ver si están bien escritos, si se dirige a nosotros de manera impersonal y si nos insta a realizar una descarga o visitar una web.
d) En los adjuntos que pueden ser maliciosos y en si lleva enlaces que pueden estar falseados.

- **Ejecución capacitación dispositivos móviles y teletrabajo: riesgos y protección.**
- Duración: 1 Hora.
- Fecha de ejecución: Mes 6.
- Modalidad: Virtual.
- Dirigido a: Personal de telemedicina.
- Temas para tratar: riesgos asociados, medidas de protección, protección antimalware, sitios web peligrosos, protección contra accesos no autorizados, protección de la información, aplicaciones legítimas, no recordar la contraseña, no utilizar redes wifi-inseguras y otras medidas de protección en el teletrabajo.
- Consejo: Desconfía de las redes WIFI abiertas
- Consejo: Suministrar a tu smartphone siempre un método de bloqueo.

Con la figura 13, se quiere resaltar la necesidad de proteger los dispositivos móviles de los usuarios en Colombiana de Trasplantes, ya que contienen información sensible y están constantemente expuestos.

Figura 13. Dispositivos móviles en tu empresa

Fuente: elaboración propia.

Con la figura 14, se busca informar a los usuarios de Colombiana de Trasplantes acerca de los riesgos del trabajo remoto y la necesidad de medidas para contenerlos.

Figura 14. Riesgos de la información en el teletrabajo

Fuente: elaboración propia.

- **Test evaluativo dispositivos móviles y teletrabajo: riesgos y protección.**

1. ¿Los dispositivos móviles, como *smartphones* y *tablets*, pueden infectarse con *malware*?
a) No, están diseñados para no infectarse.
b) Sí, todos los dispositivos pueden infectarse.
c) Solamente los dispositivos basados en Android.
d) Sí, pero solamente si se descargan aplicaciones de tiendas no oficiales.

2. Utilizar redes wifi de lugares públicos es:
a) Una práctica recomendable, ya que así se reduce el consumo de datos de la tarifa móvil.
b) Una práctica recomendable y segura, ya que actualmente debido al cifrado implementado en este tipo de redes es imposible espiar las comunicaciones.

c) Una práctica desaconsejable, ya que la red puede estar bajo el control de un ciberdelincuente y toda la información que se envía y recibe puede ser espiada.
d) Una práctica desaconsejable, pero si la conexión es lo suficientemente ágil los ciberdelincuentes no tendrían tiempo de espiar las comunicaciones.

3. Habilitar la función «recordar contraseña» con la que cuentan los navegadores web es:
a) Recomendable, ya que así se agiliza enormemente el flujo de trabajo.
b) Desaconsejable, ante un acceso fraudulento al dispositivo el ciberdelincuente podrá acceder a los servicios en los que está habilitada esta función.
c) Desaconsejable, ya que los controles de seguridad de este tipo de funciones suelen ser débiles.
d) Recomendable, ya que de esta forma se pueden establecer contraseñas únicas para cada servicio sin riesgo a que se olviden.

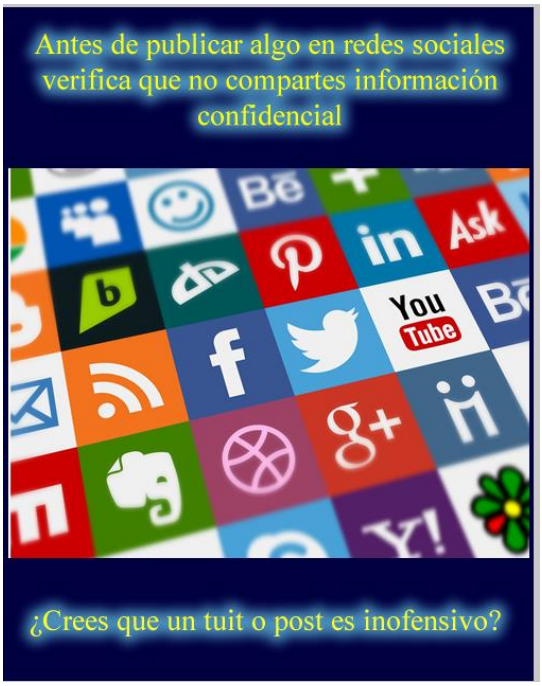
4. Una VPN permite:
a) Aumentar la velocidad de descarga de Internet.
b) Proteger el dispositivo contra las infecciones por *malware*.
c) Establecer una conexión segura y cifrada entre dos puntos cuando se usa una red insegura, como las redes *wifi* públicas.
d) Todas las respuestas son ciertas.

5. Los dispositivos móviles deben:
a) Contar con cifrado.
b) Tener un sistema de control de accesos robusto.
c) Estar actualizados a la última versión disponible.
d) Todas las respuestas son ciertas.

- **Ejecución capacitación redes sociales: medidas de seguridad para perfiles de empresa.**
- Duración: 1 Hora.
- Fecha de ejecución: Mes 7.
- Modalidad: Virtual.
- Dirigido a: Personal de telemedicina.
- Temas para tratar: el valor de las redes sociales, posibles riesgos de su uso y medidas de seguridad.
- Consejo: Aplicar siempre el sentido común y recordar que el internet tiene memoria.
- Consejo: Comprueba siempre la PRIVACIDAD y SEGURIDAD de RRSS.

Con la figura 15, se quiere concientizar a los usuarios de Colombiana de Trasplantes sobre la reserva que deben tener con la información que exponen abiertamente en las redes sociales.

Figura 15. Antes de publicar algo en redes sociales verifica que no compartas información confidencial



Fuente: elaboración propia.

- **Test evaluativo redes sociales: medidas de seguridad para perfiles de empresa.**

1. En los perfiles empresariales de redes sociales se debe:
a) Evitar realizar juicios de valor personal e intercambiar comentarios en tono elevado.
b) Interaccionar con los usuarios.
c) Actualizar los contenidos, ya que ese no es el objetivo de una red social.
d) La «b» y «c».

2. En los perfiles empresariales, las opciones de privacidad:
a) Deben ser lo más débiles posibles a fin de poder llegar al mayor número de usuarios posibles.
b) Deben revisarse y estar configuradas adecuadamente manteniendo un equilibrio entre privacidad e interacción con los usuarios.
c) Deben estar configuradas lo más restrictivamente posible.
d) No son importantes ya que los perfiles empresariales no presentan ningún riesgo.

3. ¿Las redes sociales pueden ser utilizadas por ciberdelincuentes para cometer fraudes?
a) No, ese tipo de acciones se realizan siempre fuera de las redes sociales.
b) No, ya que las redes sociales cuentan con mecanismos de protección lo suficientemente robustos como para evitar cualquier acción maliciosa.
c) Sí, pueden realizar distintos tipos de fraude como suplantaciones, campañas de *malware* o *phishing*.
d) La «a» y la «b».

4. En los perfiles empresariales se ha de tener precaución con:
a) Las aplicaciones de terceros que tienen acceso a la información de la cuenta.
b) La información que se publica.
c) Todas las respuestas son ciertas.
d) Las configuraciones de privacidad.

5. En caso de recibir un documento adjunto por medio de una red social:
a) Se debe abrir inmediatamente ya que la agilidad de respuesta en este tipo de herramientas es clave para generar confianza en el usuario.
b) Se puede abrir sin ningún riesgo ya que la red social eliminaría todo rastro de *malware* en caso de existir.
c) Se debe abrir sin ningún tipo de riesgo a no ser que la extensión del archivo sea .exe.
d) Se deben seguir las mismas recomendaciones de seguridad que en el caso de archivos adjuntos en el correo electrónico.

- **Encuesta de aplicabilidad.** Al finalizar la ejecución del programa de concientización se consultará con los participantes mediante una encuesta de aplicabilidad presentada en el cuadro 22, para establecer el grado de la receptividad hacia la seguridad de la información, a las políticas de seguridad de la organización y su utilidad durante sus labores cotidianas, de esta forma identificar que los temas sean pertinentes y estén alineados a los objetivos de la organización.

Cuadro 22. Encuesta de aplicabilidad

Tema	Poco útil	Algo útil	Normal	Bastante útil	Muy útil
Información activo imprescindible de la organización					
Importancia de la información	O	O	O	O	O
Los tres pilares de la seguridad	O	O	O	O	O
Protección de datos personales	O	O	O	O	O

Cuadro 22. (Continuación)

Tema	Poco útil	Algo útil	Normal	Bastante útil	Muy útil
Privacidad y la ley	O	O	O	O	O
Contraseñas					
Importancia de las contraseñas	O	O	O	O	O
Buenas prácticas en su uso: Robustez	O	O	O	O	O
Buenas prácticas en su uso: No compartirla	O	O	O	O	O
Buenas prácticas en su uso: No usar la misma	O	O	O	O	O
Buenas prácticas en su uso: Doble factor de autenticación	O	O	O	O	O
Buenas prácticas en su uso: Gestores de contraseñas	O	O	O	O	O
Puestos de trabajo					
Importancia de proteger el puesto de trabajo	O	O	O	O	O
Buenas prácticas: Mesas limpias	O	O	O	O	O
Buenas prácticas: Bloqueo de sesión	O	O	O	O	O
Buenas prácticas*: Software* actualizado	O	O	O	O	O
Buenas prácticas: *Software* actualizado	O	O	O	O	O
Buenas prácticas: Antivirus	O	O	O	O	O
Correo electrónico: principales fraudes y riesgos					
Correo electrónico como herramienta	O	O	O	O	O
Tipos de correo fraudulentos	O	O	O	O	O
Phishing	O	O	O	O	O
Spam	O	O	O	O	O

Cuadro 22. (Continuación)

Malware	O	O	O	O	O
Dispositivos móviles y teletrabajo: riesgos y protección					
Riesgos asociados	O	O	O	O	O
Medidas de protección	O	O	O	O	O
Protección antimalware y sitios web peligrosos	O	O	O	O	O
Protección contra accesos no autorizados	O	O	O	O	O
Protección de la información	O	O	O	O	O
Aplicaciones legítimas	O	O	O	O	O
No recordar la contraseña	O	O	O	O	O
No utilizar redes wifi-inseguras	O	O	O	O	O
Otras medidas de protección en el teletrabajo	O	O	O	O	O
Redes sociales: Medidas de seguridad para perfiles de empresa					
El valor de las redes sociales	O	O	O	O	O
Posibles riesgos de su uso	O	O	O	O	O
Medidas de seguridad	O	O	O	O	O
Fuente: elaboración propia.					

- **Cronograma de concientización.** En el cuadro 23, se presenta el cronograma propuesto para poner en consideración la ejecución del plan de concientización durante un periodo estimado de ocho meses.

Cuadro 23. Cronograma de concientización

Capacitación	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8
Diseño								
Información activo imprescindible de la organización								
Contraseñas								
Puestos de trabajo								
Correo electrónico: principales fraudes y riesgo								
Dispositivos móviles y teletrabajo: riesgos y protección								
Redes sociales: Medidas de seguridad para perfiles de empresa								
Encuesta de satisfacción								

Fuente: elaboración propia.

5.5.3 Implementación. Para la implementación del plan de concientización se deben definir las técnicas que se van a utilizar para difundir la información donde se recomienda:

- Cuenta de Correo electrónico medios@colombianadetrasplantes.com
- Presentaciones con plantilla empresarial PowerPoint
- Videos educativos
- Publicación de videos en canales de *Microsoft Stream*
- Utilizar las charlas académicas programadas
- Controles de Asistencia

5.5.4 Mantenimiento. En la fase de mantenimiento se debe monitorear, retroalimentar y evaluar lo ejecutado dentro del plan de concienciación con el fin de garantizar el compromiso por parte de los colaboradores, donde es importante actualizar el plan de concientización con nuevas temáticas que refuercen lo aprendido y ayuden a prevenir nuevos riesgos que pueden llegar a afectar la organización.

Para un correcto mantenimiento se recomienda lo siguiente:

- Ataques de ingeniería social
- Cuestionarios
- Entrevistas
- Auditorías
- Campañas por medios electrónicos

5.6 PROPUESTA DE IMPLEMENTACIÓN

5.6.1 Objetivo. Ofrecer a Colombiana de Trasplantes una propuesta de implementación del Sistema de Gestión de Seguridad de la Información para el proceso de telemedicina que se está prestando actualmente a fin de poder garantizar el cumplimento de la legislación nacional frente a los riesgos de seguridad que pueden presentar los activos lógicos teniendo presente el CONPES 3995 del 2020 buscando mitigar los riesgos legales, financieros, tecnológicos asociados a la prestación del servicio.

5.6.2 Antecedentes. Colombiana de Trasplantes desde el año 2020 inició el servicio de Telemedicina utilizando las tecnologías y procesos vigentes en la organización para prestar el servicio de atención en medicina al público, este servicio se prestaba en la instalación de la organización ubicadas en Bogotá, Medellín y Cali.

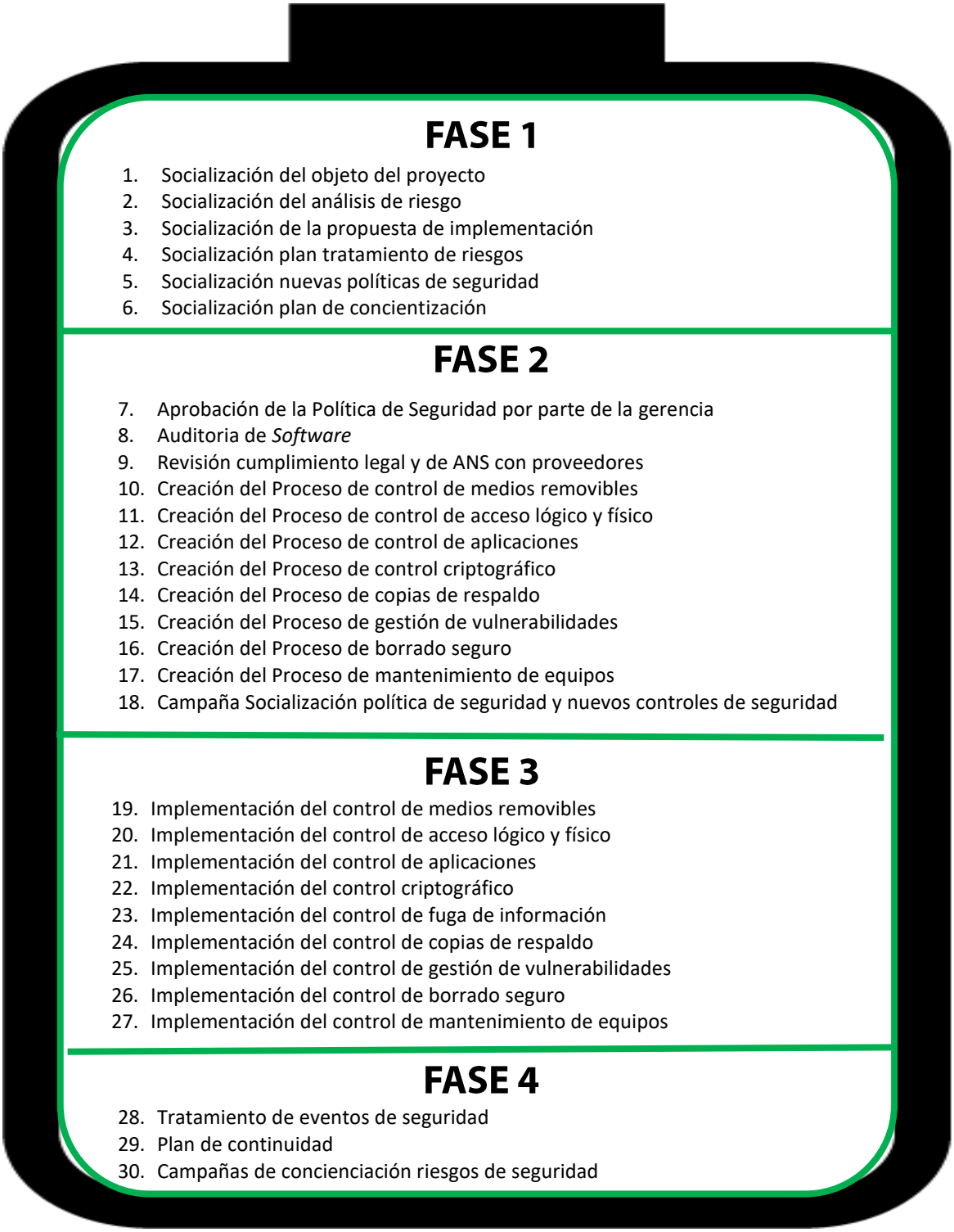
La arquitectura tecnológica de operación del proceso de telemedicina se basa en la disponibilidad y la calidad del servicio buscando la atención de los pacientes y el contacto con ellos mediante el uso del servicio de *Call Center* propietario utilizando la plataforma *Imedical Cloud* que permite el contacto inicial con el paciente para luego vincularlo a la cita mediante el uso de la plataforma de agendamiento *Microsoft Bookings* para luego realizar el proceso de cita mediante la aplicación *Microsoft Teams*, la información del paciente se actualiza luego en la plataforma del *Imedical Cloud*.

5.6.3 Descripción del proyecto. Mediante la realización de cuatro fases se busca la implementación del SGSI en el proceso de telemedicina para Colombiana de Trasplantes:

- La fase uno contempla la socialización del proyecto en sus principales hitos.
- La fase dos contempla como hito la aceptación de la Política de Seguridad por parte de la Gerencia, además de crear y documentar los procesos sobre los cuales se van a efectuar controles de seguridad que estén ligados a los hallazgos del análisis de Riesgos.
- La fase tres contempla la implementación tecnológica y procedimental de los controles previamente tratados y la creación de los documentos con la línea base de configuración.
- La fase cuatro contempla el proceso final del SGSI, abarcando el tratamiento de eventos de seguridad, documentando el plan de continuidad y la realización de las campañas de concientización sobre riesgos de seguridad.

En la figura 16, se presentan las fases propuestas a la alta gerencia para la implementación del del Sistema de Gestión de Seguridad de la Información para el proceso de telemedicina en Colombiana de Trasplantes.

Figura 16. Propuesta implementación



Fuente: elaboración propia.

5.6.4 Cronograma. En el cuadro 24, se presenta el cronograma de implementación donde se plantea una duración estimada de un año para el desarrollo de las actividades propuestas, sin embargo, el sistema debe seguir madurando año tras año, lo que significa que, una vez terminada la etapa de implementación inicial en el proceso de telemedicina en Colombiana de Trasplantes, se debe seguir trabajando para la mejora continua del sistema.

Cuadro 24. Cronograma de implementación

Actividad	Mes											
	1	2	3	4	5	6	7	8	9	10	11	12
Fase 1 - Socialización												
1. Socialización del Objeto del Proyecto												
2. Socialización del Análisis de Riesgo												
3. Socialización de la Propuesta de Implementación												
4. Socialización Plan Tratamiento de Riesgos												
5. Socialización nuevas Políticas de Seguridad												
6. Socialización Plan de Concienciación												
Fase 2 - Estructuración												
7. Aprobación de la Política de Seguridad por parte de la gerencia												
8. Auditoria de Software												
9. Revisión Cumplimiento Legal y de ANS con Proveedores												
10. Creación del Proceso de control de Medios Removibles												
11. Creación del Proceso de control de Acceso lógico y físico												
12. Creación del Proceso de control de Aplicaciones												
13. Creación del Proceso de control Criptográfico												
14. Creación del Proceso de Copias de Respaldo												
15. Creación del Proceso de Gestión de Vulnerabilidades												
16. Creación del Proceso de Borrado Seguro												
17. Creación del Proceso de Mantenimiento de Equipos												
18. Campaña Socialización Política de Seguridad y nuevos Controles de Seguridad												
Fase 3 - Implementación												
19. Implementación del Control de Medios Removibles												
20. Implementación del Control de Acceso lógico y físico												
21. Implementación del Control de Aplicaciones												
22. Implementación del Control Criptográfico												
23. Implementación del Control de Fuga de Información												
24. Implementación del Control de Copias de respaldo												
25. Implementación del Control de Gestión de vulnerabilidades												
26. Implementación del Control de Borrado Seguro												

Cuadro 24. (Continuación)

Actividad	Mes											
	1	2	3	4	5	6	7	8	9	10	11	12
27. Implementación del Control de Mantenimiento de Equipos												
Fase 4 - Implementación II												
28. Tratamiento de Eventos de Seguridad												
29. Plan de Continuidad												
30. Campañas de Concienciación Riesgos de Seguridad												

Fuente: elaboración propia.

5.6.5 Recurso humano y tecnológico. La implementación del Sistema de Gestión de Seguridad de la Información en el proceso de telemedicina para Colombiana de Trasplantes requiere de la participación de todos los integrantes del proceso, la gerencia y adicionalmente el personal que será el encargado de construir el sistema y darle vida. Este último, debe contar con el perfil idóneo para el desarrollo de las actividades propuestas y la disponibilidad suficiente para entregar la dedicación que va a ser crucial en el éxito del proyecto.

El recurso humano vinculado en el proyecto debe estar integrado por:

- **Gerencia**. Brindará el respaldo al proceso y proveerá los recursos financieros.
- **Oficial de seguridad.** Definirá los lineamientos, las actividades y le hará seguimiento a la ejecución oportuna del cronograma. Sera responsable del sistema en general.
- **Analista de seguridad.** Desarrollará la documentación de las políticas, los procesos e instructivos. Apoyará con el monitoreo y tratamiento de eventos de seguridad.
- **Personal del proceso de telemedicina, contratistas y procesos de apoyo.** participará en los planes de concientización y participará activamente en el sistema aportando en el cumplimiento de las políticas de seguridad de la información.
- **Coordinador de tecnología.** Brindará los recursos para la instalación y puesta en operación de los controles de seguridad.
- **Servicios profesionales.** Brindaran apoyo en la ejecución de las actividades del cronograma.

Los recursos tecnológicos que se contemplan incluir para soportar el sistema comprenden:

- **Detección y respuesta a amenazas en punto final.** Solución que permite la detección de amenazas conocidas y desconocidas mediante el monitoreo de comportamiento en los equipos de los usuarios, también permite tomar acciones frente a las anomalías detectadas.
- **Detección de fuga de información en punto final.** Solución que permite analizar la información que sale de los equipos de los usuarios en búsqueda de identificadores previamente definidos para coincidir con la información que se quiere controlar.

- **Cifrado de discos e información en el punto final.** Solución que permite proteger del acceso no autorizado a la información en los equipos de los usuarios mediante el cifrado completo del disco, las unidades extraíbles y/o archivos. Adicionalmente permite un borrado seguro de información.
- **Control de dispositivos y aplicaciones.** Solución que permite restringir o limitar el uso de dispositivos de almacenamiento externo y/o de conexión, así como la instalación y/o ejecución de programas según criterios predefinidos.
- **Detección y respuesta a amenazas en servicios de mensajería y almacenamiento de información.** Solución que permite proteger contra amenazas de códigos maliciosos, suplantación y técnicas de engaño en la información en tránsito o almacenada en servicios de mensajería electrónica y/o almacenamiento en nube.
- **Detección de fuga de información en servicios de mensajería o almacenamiento.** Solución que permite analizar la información que sale de los buzones de correo electrónico de los usuarios, los servicios de mensajería instantánea institucional y los repositorios en nube detectando identificadores previamente definidos para coincidir con la información que se quiere controlar.
- **Respaldo de información local y en nube.** Solución que permite respaldar automáticamente la información almacenada en los equipos de los usuarios, desde todo el sistema operativo hasta carpetas y archivos particulares. También permite hacer respalde de la información almacenada en servicios de nube.
- **Gestión de información y eventos de seguridad.** Solución que permite la recolección de información de los controles desplegados mediante los registros de acciones o eventos encontrados por cada herramienta, para posteriormente, configurar casos de uso que permitan identificar comportamientos maliciosos, analizar eventos de seguridad y generar las acciones de mitigación.

5.6.6 Presupuesto. La implementación del plan de tratamiento para el proceso de Telemedicina en Colombiana de Trasplantes requiere una inversión en diferentes recursos discriminados anteriormente y que son necesarios para poner en marcha los controles. Los recursos asociados a herramientas tecnológicas pueden tener diferentes alternativas en el presupuesto para la estimación se tomaron de referencias los fabricantes Trend Micro Inc.[40] y *Splunk* Inc.[41] que son referentes líderes en el mercado.

En el cuadro 25, se tienen en cuenta opciones reales del mercado con valores promedio para cada una de las fases propuestas, el costo del recurso humano también puede estar

[40] WWW.GARTNER.COM [en línea]. [Consulta 16 de mayo de 2021]. Disponible en internet: https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/trend-micro

[41] WWW.GARTNER.COM [en línea]. [Consulta 16 de mayo de 2021]. Disponible en internet: https://www.gartner.com/reviews/market/security-information-event-management/vendor/splunk/product/splunk-enterprise

sujeto a variaciones por lo que se calculará estimando el esfuerzo en tiempo de dedicación para el proyecto o por aproximaciones a valores de mercado para servicios de consultoría, no se descarta que se pueda emplear recurso humano interno de Colombiana de Trasplantes siempre que este cuente con la idoneidad y la disponibilidad necesaria para el proyecto.

Cuadro 25. Presupuesto

Fase	Actividades	Recursos	Costo en pesos
1	Socialización del Objeto del Proyecto Socialización del Análisis de Riesgo Socialización de la Propuesta de Implementación Socialización Plan Tratamiento de Riesgos Socialización nuevas Políticas de Seguridad Socialización Plan de Concienciación	Humano: Gerencia Oficial de seguridad	$ 5.700.000
2	Aprobación de la Política de Seguridad por parte de la gerencia Auditoria de *Software* Revisión Cumplimiento Legal y de ANS con Proveedores Creación del Proceso de control de Medios Removibles Creación del Proceso de control de Acceso lógico y físico Creación del Proceso de control de Aplicaciones Creación del Proceso de control Criptográfico Creación del Proceso de Copias de Respaldo Creación del Proceso de Gestión de Vulnerabilidades Creación del Proceso de Borrado Seguro Creación del Proceso de Mantenimiento de Equipos Campaña Socialización Política de Seguridad y nuevos Controles de Seguridad	Humano: Gerencia Oficial de seguridad Analista de Seguridad Comunicaciones Consultoría	$52.800.000
3	Implementación del Control de Medios Removibles Implementación del Control de Acceso lógico y físico Implementación del Control de Aplicaciones Implementación del Control Criptográfico Implementación del Control de Fuga de Información Implementación del Control de Copias de respaldo Implementación del Control de Gestión de vulnerabilidades Implementación del Control de Borrado Seguro Implementación del Control de Mantenimiento de equipos	Humano: Oficial de seguridad Analista de Seguridad Consultoría. Tecnológico: Soluciones seguridad punto final, soluciones seguridad mensajería, almacenamiento y correo electrónico	$55.750.000
4	Tratamiento de Eventos de Seguridad Plan de Continuidad Campañas de Concienciación Riesgos de Seguridad	Humano: Oficial de seguridad Analista de Seguridad Comunicaciones Consultoría Tecnológico: Solución de gestión de información y eventos de seguridad	$55.300.000
		Total	$ 169.550.000
Fuente: elaboración propia.			

6. CONCLUSIONES

La elaboración del análisis del estado actual en el proceso de telemedicina en la IPS Colombiana de Trasplantes con respecto a la norma ISO/IEC 27001:2013 para seguridad de la información, permitió identificar el bajo porcentaje de implementación de los controles planteados en esta para el proceso, así como la necesidad de fortalecer la postura de seguridad frente a los requisitos de cumplimento, donde se evidenció que no existe un sistema eficiente para detectar y tratar los riesgos a los que está expuesta la información.

La identificación de los activos de información en el proceso de telemedicina en la IPS Colombiana de Trasplantes es uno de los requisitos necesarios para iniciar con la gestión del riesgo, donde se evidenció que no existía un inventario actualizado de todos los activos involucrados dentro del proceso y en consecuencia tampoco una valoración de estos. Con las actividades desarrolladas se logró valorar la criticidad de cada uno de los activos identificados tomando como referencia la confidencialidad, integridad y disponibilidad.

El proceso de telemedicina en Colombiana de Trasplantes involucra el tratamiento de datos personales de los pacientes y está reglamentado por la ley, en consecuencia, se deben cumplir condiciones de seguridad que permitan proteger los derechos del usuario y su información privada, por lo que la norma ISO/IEC 27001:2013 es un marco de referencia idóneo a implementar.

Trabajando con la metodología de la norma ISO/IEC 27005:2009 se lograron identificar los diferentes riesgos a los que están expuestos los activos de información en el proceso de telemedicina, donde se evaluaron las amenazas de cada uno de los activos con respecto a su impacto para Colombiana de Trasplantes y la estimación de su probabilidad de ocurrencia, teniendo como referencia el nivel de riesgo aceptable y la necesidad de tratamiento de los riesgos medios y altos.

Se definen políticas de seguridad de la información alineadas con los objetivos de la empresa y basados en estas se proponen controles que permitan reducir el nivel de riesgo en los activos de información de la compañía.

El plan de tratamiento propuesto está orientado a reducir los riesgos inaceptables según la definición de Colombiana de Trasplantes hasta un nivel tolerado por la empresa, mediante los diferentes controles del anexo A de la norma ISO/IEC 27001:2013 se plantea reducir tanto el impacto como la probabilidad de ocurrencia de cada uno de los riesgos.

El control y mitigación de los riesgos en Colombiana de Trasplantes debe basarse en políticas de seguridad de la información sólidas y ajustadas a las necesidades del negocio, así como apalancarse en controles efectivos y bien administrados, que deben ser evaluados regularmente para determinar su efectividad según lo estimado en el plan de tratamiento.

La educación de los empleados, usuarios y terceros en el proceso de telemedicina en Colombiana de Trasplantes es parte fundamental para el adecuado tratamiento de los riesgos de seguridad de la información, ya que muchos de los riesgos tienen involucrado el factor humano para su materialización.

Con la propuesta de implementación del sistema de gestión de seguridad de la información en Colombiana de Trasplantes se presenta a la dirección una estrategia viable en tiempos, recursos y costos que le proporcionarán a la empresa la cobertura sobre las necesidades de seguridad en el proceso de telemedicina, y que además puede apalancar una futura cobertura del sistema de gestión de seguridad de la información para otros procesos.

La seguridad de la información es fundamental para todos los procesos de la compañía, sin embargo, actualmente todo el personal no le da importancia a este tema y no da la suficiente prioridad a los activos de información que son vitales para la empresa, con el diseño de este sistema de gestión de seguridad de la información para el proceso de telemedicina, se establecerá una base para implementarlo a todos los procesos de la compañía ayudando a establecer procedimientos y buenas prácticas para el desarrollo de todas las actividades que impliquen un riesgo para la empresa y a cumplir con todos los requisitos legales que esto implique, teniendo en cuenta los tres pilares de la seguridad: confidencialidad, integridad y disponibilidad de la información.

BIBLIOGRAFÍA

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012. [en línea]. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587 de 18 de octubre de 2012. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html, 2019.

--------. Ley 2015 de 2020. [en línea]. (31, enero, 2020). Por la cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones. Diario Oficial No. 51.213 de 31 de enero de 2020. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_2015_2020.html, 2021.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES. Consejo Nacional de Política Económica y Social [en línea]. (1, julio, 2020). [Consulta 15 de mayo de 2021]. Disponible en internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución No. 2654 del 2019. [en línea]. (3, octubre, 2019). Por el cual se establecen disposiciones para la telesalud y parámetros para la práctica de la telemedicina en el país. Disponible en internet: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/resolucion-2654-de-2019.pdf, 2019. p. 1-10.

--------. Resolución No. 839 del 2017. [en línea]. (23, marzo, 2017). Por la cual se modifica la resolución 1995 de 199 y se dictan otras disposiciones. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/Resolucion%20No%20839%20de%202017.pdf, 2017.

--------. Resolución No. 1995 del 1999. [en línea]. (8, julio, 1999). Por la cual se establecen normas para el manejo de la Historia Clínica. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf, 1999.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Elaboración de la política general de seguridad y privacidad de la información. [en línea]. [Consulta: 28 marzo 2021]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

--------. Guía para la Gestión y Clasificación de Activos de Información. [en línea]. [Consulta: 28 marzo 2021]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

--------. Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información [en línea]. [Consulta 8 de abril de 2021]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Información Engañosa [en línea]. [Consulta: 16 junio 2020]. Disponible en internet: https://www.sic.gov.co/sus-derechos.

--------. Sobre la protección de Datos personales -Habeas Data en Colombia. [en línea]. [Consulta: 2 junio 2020]. Disponible en internet: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Compendio Seguridad de la Información. 2 ed. Bogota D.C.: ICONTEC, 2017. ISBN 978-958-8585-53-6.

--------. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. NTC-ISO-IEC 27005:2009. Bogota D.C.: ICONTEC, 2009.

ISO27000.ES. Glosario [en línea]. [Consulta 7 de abril de 2021]. Disponible en internet: https://www.iso27000.es/glosario.html

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY). Special Publication 800-50 Building an Information Technology Security Awareness and Training Program. [en

línea]. (octubre, 2003). [Consulta 15 de mayo de 2021]. Disponible en internet: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf