UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA DIRECCION DE TI EN UNA PRESTADORA DE SERVICIOS CLINICOS.

AUTOR

CHÁVEZ YAGUAL DANNY SAUL

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN CIBERSEGURIDAD

TUTOR

CHACÓN LUNA ANA EVA

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
ANA EVA CHACON LUNA

Ing. Ana Chacón Luna, Ph.D.
TUTOR

Firmado electrónicamente por:
OSCAR OMAR APOLINARIO ARZUBE

Lic. Oscar Apolinario Arzube, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA DANIELA ALVAREZ GALARZA

Ing. María Alvarez Galarza, Ph.D.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera González, MSc.
SECRETARIO GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Chávez Yagual Danny Saul, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

TUTOR

Firmado electrónicamente por:
ANA EVA CHACON LUNA

Chacón Luna Ana Eva

Santa Elena, 21 de octubre del 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Chávez Yagual Danny Saul**

DECLARO QUE:

El trabajo de Titulación, DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA DIRECCIÓN DE TI EN UNA PRESTADORA DE SERVICIOS CLINICOS, previo a la obtención del título en Magister en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 21 de octubre del 2024

AUTOR

Firmado electrónicamente por:
DANNY SAUL CHAVEZ YAGUAL

Chávez Yagual Danny Saul

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA DIRECCIÓN DE TI EN UNA PRESTADORA DE SERVICIOS CLINICOS, presentado por el estudiante, Chávez Yagual Danny Saul fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 1%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

COMPONENTE TEORICO - CHAVEZ DANNY pdf

< 1% Textos sospechosos

< 1% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
0% Idiomas no reconocidos

Nombre del documento: COMPONENTE TEORICO - CHAVEZ DANNY pdf.pdf
ID del documento: 91eb699901372d2d76b1286a1ec990c585b29d07
Tamaño del documento original: 1 MB
Autores: []

Depositante: ANA EVA CHACON LUNA
Fecha de depósito: 15/10/2024
Tipo de carga: interface
fecha de fin de análisis: 15/10/2024

Número de palabras: 23.817
Número de caracteres: 165.990

TUTOR

Firmado electrónicamente por:
ANA EVA CHACON LUNA

Chacón Luna Ana Eva

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **Chávez Yagual Danny Saul**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo de examen complexivo con fines de difusión pública, además apruebo la reproducción de este trabajo de examen de carácter complexivo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, 21 de octubre del 2024

AUTOR

Firmado electrónicamente por:
DANNY SAUL CHAVEZ YAGUAL

Chávez Yagual Danny Saul

AGRADECIMIENTO

A Dios, por haberme acompañado a lo largo de mi carrera de postgrado nuevamente y guiándome siempre por un buen camino;

A mis padres, les agradezco por su incondicional apoyo y comprensión en cada momento de este recorrido académico, por ser mi mayor fuente de inspiración y fortaleza

A los docentes a mi asesora que me impartieron sus conocimientos y guía constante hicieron posible el desarrollo de este trabajo.

Extiendo mi gratitud a mi familia, cuyo amor y paciencia me han acompañado en cada paso de este camino y que hoy he podido acabar un nuevo proyecto profesional.

Chávez Yagual Danny Saúl

DEDICATORIA

Lleno de regocijo, de amor y esperanza dedico este trabajo a Dios, porque me bendice y me guía en cada momento de mi vida. A mis abuelos, Alejandro especialmente a mi abuelita Virginia, cuya bendición diaria ha sido mi escudo y mi guía en mi camino. A mis Hermanos, a mis padres, Pedro y María de Lourdes, les agradezco por inculcarme los valores que me definen, este trabajo es una ofrenda de agradecimiento por su paciencia, sacrificio y el inmenso amor de madre y padre.

Dedico este trabajo a aquellos que, y a una persona especial que, con sus palabras de aliento, motivación y apoyo me han impulsado a continuar incluso en los momentos más difíciles, este proyecto no es solo el fruto de mi esfuerzo, sino el reflejo del apoyo y la confianza de todos ustedes. ¡Gracias por estar siempre a mi lado!

Chávez Yagual Danny Saúl

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

El siguiente trabajo se denomina “DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA DIRECCIÓN DE TI EN UNA PRESTADORA DE SERVICIOS CLINICOS”, clínica a la que llamaremos “Gamma Smart S.A.” por temas de confidencialidad, es una empresa privada con prestaciones externas al seguro social ecuatoriano, la presente tesis tuvo como único objetivo diseñar un sistema de gestión de seguridad de la información mediante estándares de calidad y metodologías fundamentada en la norma ISO 27001 que cumplan con tres principios fundamentales como la confidencialidad, integridad y disponibilidad de la información.

A través de una investigación exploratoria y diagnóstica, se identificaron riesgos y vulnerabilidades en los procesos clínicos, revelando la falta de procedimientos formales de seguridad. La metodología utilizada es el ciclo PDCA, asegurando la mejora continua de los procesos. Concluimos que esto no solo mejora la infraestructura de seguridad, sino que también fomenta una cultura de protección de la información, lo que es clave para garantizar la confianza de los pacientes y la eficiencia operativa de la organización.

Palabras claves: Sistema de gestión de seguridad de la información, Estándares de calidad, Mejora continua.

ABSTRACT

The following work is called “DESIGN OF AN ISMS BASED ON THE ISO 27001 STANDARD FOR IT MANAGEMENT IN A CLINICAL SERVICES PROVIDER”, a clinic that we will call “Gamma Smart S.A.” Due to confidentiality issues, it is a private company with benefits external to the Ecuadorian social security. The sole objective of this thesis was to design an information security management system through quality standards and methodologies based on the ISO 27001 standard that comply with three fundamental principles such as confidentiality, integrity and availability of information.

Through an exploratory and diagnostic investigation, risks and vulnerabilities in clinical processes were identified, revealing the lack of formal security procedures. The methodology used is the PDCA cycle, ensuring continuous improvement of processes. We conclude that this not only improves the security infrastructure, but also fosters a culture of information protection, which is key to ensuring patient trust and the operational efficiency of the organization.

Keywords: Information security management system, Quality standards, Continuous improvement.

CAPITULO I

INTRODUCCIÓN

En estos tiempos de donde nacen cada día nuevas tecnologías y en un mundo totalmente caracterizado por la globalización, la complejidad de las infraestructuras de tecnologías de la información y comunicación es comprensible que las organizaciones se esfuercen por salvaguardar los activos de información. (Miguel Angel Cruz Diaz, 2017) Hoy en la actualidad muchas empresas manipulan información que se encuentra digitalmente acoplada en los sistemas informáticos, por tal motivo es considerar que la protección, privacidad, confidencialidad y disponibilidad del sistema de información, pueda encontrar riesgo o vulnerabilidad. (Bach. Jácome Sanchez, 2022)

La información hoy en día es un activo de mucha importancia en las empresas (Raúl J. Martelo, 2014), esto implica tener la interpretación de datos para ser utilizados en la toma de decisiones o de solucionar problemas, la información en la seguridad de la información nos hace énfasis a los activos de datos de cualquier valor en una empresa, la misma que buscan salvaguardar de posibles vulneraciones, esto incluyen datos como documentos digitales, archivos, correos electrónicos, contraseñas o propiedad intelectual.

La seguridad de la información se basa en tres principios sustanciales como la integridad, disponibilidad y confidencialidad de la información que son aspectos fundamentales para la gestión y protección de la información para evitar daños y amenazas a las empresas (Morales Osorio & López Trujillo, 2018), como el acceso no autorizado, perdida de información o ataques cibernéticos, en principio crucial como pilares fundamentales para prevenir incidentes y reducir la vulnerabilidad frente a amenazas que comprometan a los activos críticos de una empresa o de una persona en común.

La seguridad de la información implica salvaguardar datos sensibles, confidenciales de una empresa (Guevara-Vega, Delgado-Deza, & Mendoza-de-los-Santos, 2023), pero no solo abarca en situaciones como delitos y amenazas de vulnerabilidades, sino que también abarca a factores humanos y físicos. La seguridad de la información es un conjunto de prácticas y medidas que son destinadas a proteger los activos e información de una empresa frente a diversas amenazas que en la actualidad se puedan presentar, como los ciberataques entre ellos, el malware, phishing, fallas técnicas,

errores humanos y desastres naturales (Pacheco & Suárez, 2015), así mismo para mitigar estos riesgos se diseñan en ciertos casos o se implementan controles de seguridad, físicos, técnicos y administrativos.

Además, la seguridad de la información está basada en normas y estándares de calidad como la norma ISO/IEC 27001 que nos brinda un marco de gestión para la seguridad de la información, que nos obliga a tomar las directrices para poder manejar datos confidenciales y sensibles.

Una estrategia para dar solución a una organización que se ve afectada por diversos factores de riesgo es la implementación de políticas, procesos y controles diseñados para gestionar los riesgos relacionados a la seguridad, enmarcado en un plan de normativas basadas en la estandarización de la ISO 270001, que nos permitirá tener un campo extenso de información sobre la evaluación de los riesgos de seguridad de una empresa, la implementación de un sistema de seguridad de la información nos brinda la facilidad de realizar una auditoría, mitigación y tratamiento de riesgos tomando en cuenta a futuro posibles vulneraciones a los sistemas de información de una organización.

El diseño de un plan para ejecutar un sistema de gestión de seguridad de la información es una herramienta que sirve de gran ayuda para las organizaciones controlar y mitigar sistemáticamente los riesgos rendimientos y niveles de seguridad de la información (Bayona Ore Luz, 2017). El sistema de gestión de seguridad de la información nos ofrece un marco estructurado para proteger la información de una empresa proporcionando una estructura de mejora en las políticas, procesos y tecnologías de seguridad que se adapta a las nuevas formas de ataques cibernéticos en el entorno, minimizando el impacto de posibles altercados e incidentes de seguridad, mejorando la capacidad de respuesta ante incidentes, implementar un SGSI es la clave para garantizar ante una organización un enfoque a la protección de información.

A continuación, se citan tres trabajos de titulación con similitud al tema que se ha propuesto como el proyecto que se titula Diseñar un sistema de gestión de la seguridad de la información (Ramirez & Angarita, 2017) a la empresa UNITRANSA S.A ubicada en la ciudad de Bucaramanga que desea implementar controles necesarios para la gestión de activos de información complementando con la creación de políticas de seguridad y

documentada que le permita a la organización adquirir niveles de seguridad aceptable (Ramirez & Angarita, 2017).

El siguiente trabajo de titulación es un Informe de evaluación de seguridad en la información basada en la norma ISO 27001 en el departamento de TI de una empresa de lácteos en la que se considera necesario que se desarrollen políticas y procedimientos basados en la norma ISO 27001, ya que esta permite regular y gestionar los riesgos a lo que está expuesta la organización de esta forma se pretende evitar incidentes que causen perdida de información, indispensable de servicios, violación de seguridades entre otros, permitiendo así mejorar las políticas existentes y definir procedimientos alineados a una metodología por el estándar ISO 27001 (Troya & Poveda, 2015).

En base a lo antes expuesto el siguiente trabajo de titulación se diseña un sistema de gestión de seguridad de la información basada en la norma ISO 27001 para la dirección de TI de una prestadora de servicios clínicos, que garantizara la reducción de vulnerabilidades y llevando a cabo políticas y procedimientos alineados a los objetivos de la empresa, con la única finalidad de que la información este de manera resguardada de cualquier tipo de vulneración y riesgo que se pueda presentar y así contribuir al control de seguridad y calidad en base a la normativa y gestión de seguridad ISO 27001.

El siguiente trabajo se compone de 3 capítulos clave, el primer capítulo tiene como fundamentación el marco teórico donde se elaboran las teorías del desarrollo del proyecto proporcionando el sustento conceptual y contextual permitiendo identificar las principales teorías del trabajo que se va a presentar, el segundo capítulo contempla la metodología de desarrollo y de investigación del proyecto que se implementó detallando los enfoques de investigación y de desarrollo que fueron aplicados para diseñar e implementar el sistema, asegurando que cada etapa del proceso esté respaldada por un enfoque sistemático y riguroso, finalmente el tercer capítulo se dedica a la documentación y propuesta del sistema, donde se presentan los resultados obtenidos, las soluciones implementadas y un análisis detallado de las fases de la metodología empleada.

Adicionalmente, este trabajo destaca la importancia de garantizar la alineación del sistema con los objetivos de la empresa, asegurando que la gestión de la seguridad de la información no solo cumpla con los estándares establecidos por la norma ISO 27001, sino

que también contribuya a mejorar la eficiencia operativa y la calidad en la prestación de los servicios clínicos. La propuesta final no solo busca mitigar riesgos, sino también establecer un marco sostenible de mejora continua para la seguridad de la información.

1.1 PLANTEAMIENTO DEL PROBLEMA

Una vez que se ha realizado la recolección de información en la dirección de tecnologías de la información de la clínica a la que llamaremos “Gamma Smart SA” por motivos de confidencialidad, se identificaron todos los activos de información de la entidad. Como prestadora de servicios clínicos, Gamma Smart SA cuenta con sistemas de información que permiten registrar, almacenar y ejecutar los procesos clínicos en sus operaciones diarias. Sin embargo, se ha evidenciado que la clínica no dispone de procedimientos ni normativas formalmente establecidos para la gestión de la seguridad de la información.

La clínica enfrenta serios problemas de seguridad en el manejo de su información, que es altamente sensible y crítica. Los historiales clínicos, hojas de interconsultas, derivaciones y exámenes de laboratorio contienen datos confidenciales que deben ser resguardados de manera adecuada. Estos datos están protegidos por la Ley Orgánica de Protección de Datos Personales de Ecuador (Asamblea Nacional del Ecuador, 2021), la cual establece medidas estrictas para su seguridad y confidencialidad. El incumplimiento de estas normativas expone a la clínica a sanciones legales, lo que hace urgente la implementación de un sistema efectivo de gestión de seguridad de la información que garantice la protección y privacidad de estos datos

Es crucial que la clínica asegure la disponibilidad, integridad y confidencialidad de la información de los pacientes y de sus principales activos de información. La disponibilidad garantiza que los datos estén accesibles en todo momento, lo cual es vital para realizar exámenes o procedimientos médicos y diagnósticos de manera eficiente y sin interrupciones. La integridad asegura que la información se mantenga precisa y sin modificaciones no autorizadas, evitando así errores que puedan comprometer la atención médica. Por último, la confidencialidad protege los datos sensibles, asegurando que solo el personal autorizado tenga acceso, cumpliendo con la normativa de protección de datos personales.

La clínica no ha identificado claramente sus activos de información ni ha realizado un análisis exhaustivo de sus vulnerabilidades. Aunque cuentan con algunos controles o mitigantes para ciertos riesgos, esto no significa que dispongan de un marco estándar o estructurado para mejorar su seguridad de manera integral. La ausencia de un enfoque sistemático para identificar y gestionar los activos y vulnerabilidades deja a la clínica expuesta a posibles brechas de seguridad, comprometiendo la confidencialidad, integridad y disponibilidad de la información crítica. Esto resalta la necesidad de adoptar un sistema de gestión de políticas y controles que sigan un estándar reconocido, como la norma ISO 27001, para fortalecer sus controles y mejorar su capacidad de respuesta ante amenazas.

Esta situación plantea un riesgo significativo, ya que no se están garantizando los principios fundamentales de la seguridad de la información: disponibilidad, confidencialidad e integridad. La falta de controles formales impide la identificación adecuada de los riesgos y vulnerabilidades que podrían comprometer la información sensible de la clínica. Esto expone a la organización a posibles incidentes que afecten tanto la continuidad operativa como la confianza de los pacientes.

Además, al no contar con un enfoque formal para la gestión de la seguridad de la información, la clínica también está en riesgo de incumplir con normativas regulatorias del sector salud que exigen el manejo adecuado de los datos clínicos y personales. La creciente amenaza de ciberataques y el aumento de requisitos legales subrayan la necesidad de una estructura clara y documentada que garantice la protección de los datos frente a accesos no autorizados, modificaciones indebidas o pérdida de información crítica.

Por lo tanto, resulta indispensable llevar a cabo un Sistema de Gestión de Seguridad de la Información, fundamentada en el estándar ISO 27001. Este marco normativo proporcionará a Gamma Smart SA una estructura formal para gestionar y mitigar los riesgos de seguridad a través de políticas documentadas y procedimientos estandarizados, garantizando que cualquier cambio en los sistemas de información esté adecuadamente controlado y monitoreado. Con la implementación de este SGSI, la organización podrá proteger mejor sus activos críticos y asegurar la confidencialidad, integridad y disponibilidad de su información.

1.1.1 FORMULACION DEL PROBLEMA

1.1.2 PREGUNTA GENERAL

¿De qué manera puede la clínica establecer un marco de políticas y procedimientos fundamentados en la norma ISO 27001, que aseguren un análisis adecuado de riesgos y la mitigación de vulnerabilidades garantizando así la seguridad de la información?

1.2 OBJETIVOS DEL PROYECTO

1.2.1 OBJETIVO GENERAL

Diseñar una propuesta de sistema de gestión de seguridad de la información mediante estándares de calidad y metodologías fundamentada en la norma ISO 27001 para el aseguramiento de confidencialidad integridad y disponibilidad de la información organizacional de la prestadora de servicios clínicos.

1.2.2 OBJETIVOS ESPECIFICOS

- Realizar el levantamiento de información de los riesgos de seguridad de los activos de información de la prestadora de servicios clínicos para proponer planes de acción que permitan mitigar los riesgos y vulnerabilidades.
- Identificar las vulnerabilidades y riesgos a las cuales están propenso los activos de información y procesos dirigidos por la dirección de informática y tecnologías.
- Identificar los posibles controles y establecer las políticas con la única finalidad de poder mitigar las vulnerabilidades de la clínica.

1.3 ALCANCE

El resultado de este proyecto es el diseño de un Sistema de Gestión de Seguridad de la Información fundamentada en el estándar ISO 27001, que permitirá a la clínica gestionar de manera efectiva la protección de sus activos de información. A través de este sistema, la clínica podrá identificar sus activos críticos, evaluar sus vulnerabilidades y riesgos, y aplicar controles adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información sensible, como los historiales clínicos y los datos de los pacientes. Además, se alineará con la Ley de Protección de Datos Personales de Ecuador,

reduciendo el riesgo de sanciones y fortaleciendo la confianza en la gestión de la información por parte de los pacientes y colaboradores.

El proyecto se centrará en los activos de información vinculados a los siguientes procesos clave de la clínica: gestión de registros de pacientes, atención médica, procesos de datos, procedimientos médicos, facturación electrónica, sistemas de información. El proyecto incluye la identificación de activos, evaluación de riesgos, y establecimiento de controles para garantizar la confidencialidad, integridad y disponibilidad de la información. Además, se abarcarán los sistemas tecnológicos, procesos internos, y el personal relacionado con el manejo de la información, asegurando que todos los elementos involucrados cumplan con la normativa ISO 27001 y la Ley de Protección de Datos Personales de Ecuador.

El proyecto propuesto enfrentará limitaciones, siendo el tiempo un factor crucial en la fase inicial de implementación. Aunque se implementarán controles iniciales para abordar algunas de las vulnerabilidades existentes, la presión por cumplir con los plazos establecidos podría restringir la capacidad de realizar un análisis detallado y exhaustivo, lo que comprometería la efectividad a largo plazo del sistema. Además, se desarrollarán siete de las once etapas recomendadas por la norma ISO 27001, abarcando desde la fase de planificación hasta la fase de actuación. Las fases que no se abordarán incluyen:

1. **Asignación de recursos** (Etapa Act), Implica identificar y asignar los recursos necesarios para el SGSI.
2. **Certificación** (Etapa Check), Consiste en la evaluación formal del SGSI por un organismo externo.
3. **Auditoría** (Etapa Check), Incluye la realización de auditorías internas y externas para evaluar el cumplimiento y la efectividad del SGSI.
4. **Mejora continua** (Etapa Act), Se centra en evaluar y mejorar continuamente la efectividad del SGSI

A esto se suma que la implementación de controles también requerirá un presupuesto de inversión para la empresa.

CAPITULO II

MARCO TEORICO Y METODOLOGIA DEL PROYECTO

2.1 MARCO CONCEPTUAL

Software: Es el conjunto de programas que se ejecutan en una computadora, permitiendo realizar diversas tareas como redactar un documento, navegar por Internet o editar una imagen, el componente más crucial de cualquier computadora es el sistema operativo. (Jacovkis, 2009).

Hardware: Es el conjunto de componentes físicos que conforman un ordenador, la parte más esencial del hardware es el procesador central, ya que es el dispositivo encargado de ejecutar todas las instrucciones que permiten el funcionamiento del equipo(Jacovkis, 2009).

Hacker: Se definen a sí mismos como personas que se dedican a programar de manera apasionada y creen que es un deber para ellos compartir la información y elaborar software gratuito, un hacker es un experto o un entusiasta de cualquier tipo que puede dedicarse o no a la informática (Peka, 2015).

Redes de comunicación: Una red de comunicación es una imagen parcial de la escena en la que se opera y contiene la imagen virtual de la totalidad de esa escena. El soporte fundamental de la escena tiene un basamento cuaternario: espacio, tiempo, movimiento y sociedad lo componen (Hernández, 2010). De entrada, la red no puede ser percibida con plenitud, leída productivamente ni operada de manera eficaz sin la consideración de ese hecho, el manejo de la red supone concebir la historia como un movimiento de la sociedad en el tiempo, en una cierta área (Hernández, 2010).

Seguridad de la información: Se refiere a la implementación de medidas que minimicen al máximo la vulnerabilidad de la información y los recursos, aunque no es posible alcanzar una seguridad del 100%, el objetivo debe ser aproximarse a ese nivel extremo (Velasco, 2008).

Activos de información: Son todos los recursos que contienen información valiosa para una organización, incluyendo datos, documentos, correos electrónicos, software, sistemas, redes, dispositivos y bases de datos (Technology, 2024).

Los activos relacionados con los sistemas de información de una organización se pueden clasificar de la siguiente manera:

- Recursos de información: Incluyen bases de datos, manuales de usuario, procedimientos operativos o de soporte, planes de continuidad, información archivada y disposiciones de emergencia para la recuperación de datos (Velasco, 2008).
- Software: Programas diseñados para realizar tareas específicas, como procesamiento de texto, hojas de cálculo o gestión de bases de datos (Velasco, 2008).

La seguridad debe garantizar la protección de las siguientes características de la información:

- Confidencialidad: La información debe ser accesible únicamente a personas autorizadas(Velasco, 2008).
- Integridad: El contenido de la información no debe ser modificado, excepto por personal autorizado (Velasco, 2008).
- Disponibilidad: La información debe estar siempre disponible para ser procesada por las personas autorizadas (Velasco, 2008).
- Control: Solo las personas autorizadas deben tener la capacidad de decidir cuándo y cómo acceder a la información (Velasco, 2008).

Amenazas a la seguridad de la información

Entre las amenazas más frecuentes se encuentran:

- Catástrofes naturales: Este tipo de amenazas suelen provocar interrupciones en los servicios, afectando principalmente la disponibilidad de la información, por ejemplo, catástrofes naturales incluyen inundaciones, terremotos y tornados entre otros (Velasco, 2008).
- Amenazas físicas: Se relacionan con el acceso físico a los recursos, lo que puede resultar en robos, daños a los equipos y actos de sabotaje, también incluye el acceso no autorizado logrado a través de ingeniería social, aprovechando la confianza de los empleados de la organización (Velasco, 2008).

- Fraude Informático: Implica engañar a los clientes en la venta de productos y servicios a través de promociones o agencias que no existen (Velasco, 2008).
- Software ilegal: La copia de software sin licencia puede llevar a vulnerabilidades en los sistemas informáticos, ya que no se reciben las actualizaciones proporcionadas por los desarrolladores, este tipo de software también puede incluir otras amenazas, como códigos maliciosos(Velasco, 2008).
- Códigos maliciosos: Se refiere a cualquier programa o parte de un programa que causa problemas en los sistemas informáticos, incluidos virus, troyanos, gusanos y puertas traseras, que se activan en los sistemas finales, esta amenaza ha evolucionado debido a la creciente conectividad a Internet y las técnicas de engaño utilizadas por los atacantes(Velasco, 2008).

ISO/IEC 27001: La norma ISO/IEC 27001 es la norma más conocida del mundo para sistemas de gestión de seguridad de la información (SGSI) (ISO/IEC, 2022). Define los requisitos que debe cumplir un SGSI (ISO/IEC, 2022). La norma ISO/IEC 27001 ofrece a las organizaciones de todos los tamaños y sectores directrices para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información (ISO/IEC, 2022). La conformidad con la norma ISO/IEC 27001 significa que una organización o empresa ha puesto en marcha un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja la empresa, y que este sistema respeta todas las mejores prácticas y principios consagrados en esta Norma Internacional.

ISO/IEC 27005: La norma ISO/IEC 27005 es esencial para cualquier organización que busque establecer un marco robusto de gestión de riesgos relacionados con la seguridad de la información, al proporcionar directrices claras, permite a las empresas identificar y evaluar sus necesidades y requisitos específicos en materia de seguridad (PECB, s.f.).

ISO/IEC 27002: Es un estándar internacional que proporciona directrices sobre las mejores prácticas para la gestión de la seguridad de la información, es un complemento a la norma ISO/IEC 27001, que establece los requisitos para un Sistema de Gestión de Seguridad de la Información ((PECB, s.f.).

La ISO/IEC 27002 es crucial para ayudar a las organizaciones a proteger sus activos de información, asegurar la confidencialidad, integridad y disponibilidad de los datos, y

cumplir con regulaciones y requisitos legales relacionados con la seguridad de la información. Su implementación contribuye a una cultura de seguridad dentro de la organización y fortalece la confianza de los clientes y partes interesadas. (PECB, s.f.).

2.2 MARCO TEORICO

FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS

El amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos, la comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido (A., S., & María, 2011).

La norma ISO 27000 es certificable, esto significa que una empresa puede solicitar una auditoría a una entidad certificadora acreditada y si la supera, obtener la certificación (A., S., & María, 2011). Antes de solicitar la auditoría, las empresas necesitan contar con procesos, políticas y controles (A., S., & María, 2011). El SGSI debe estar implementado en la empresa como mínimo con tres meses de antelación, cada uno de los puntos exigidos en la norma pertenece a una etapa de un proceso: Plan – Do –Check –Act (Planificar-Hacer-Verificar-Actuar), que se aplica para estructurar todos los procesos del SGSI (A., S., & María, 2011).

ISO/IEC 27001 ASEGURAMIENTO DE LA CALIDAD DE LA INFORMACIÓN

En la actualidad los datos son esenciales en la vida cotidiana de todas las personas, empresas, organizaciones, entre otras. Desafortunadamente el riesgo de fraude cada vez es mayor. Ciberataques, hacking de los datos digitales, pérdida de información se ha convertido en algo común de esta década (Cruz-Gavilánez & Martinez-Santande, 2018). La aparición de nuevos sistemas acoplados a la parte industrial, de salud, energía, servicios básicos, los han convertido en infraestructuras críticas, si incurre en un ataque, puede traer consigo la paralización de una ciudad, además de las pérdidas económicas (Cruz-Gavilánez & Martinez-Santande, 2018). Por tanto, el riesgo es cada vez mayor. Una de las medidas efectivas para contrarrestar en un alto porcentaje estos problemas, sería implementar un sistema de gestión de la seguridad de la información (SGSI) (Cruz-

Gavilánez & Martinez-Santande, 2018). Esto proporciona un marco detallado para el desarrollo, implementación y gestión de seguridad de la información ISO/IEC27001, representa un propósito importante para proteger su TI (Tecnología Informática), infraestructura y aseguramiento de los datos para una empresa u organización ya sea pública o privada (Cruz-Gavilánez & Martinez-Santande, 2018). EL objetivo de este artículo es discutir el origen y evolución de la ISO / IEC 27001, además se hace una comparación entre la ISO 27001: 2005 y 2013 que es el estándar actual e implementado en la mayoría de las organizaciones.

BENEFICIOS DE IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE UNA ORGANIZACIÓN

El estándar ISO/IEC 27001 es una norma que se desarrolló para ayudar a definir los requisitos que permitirán establecer, implementar, mantener y mejorar continuamente la gestión de seguridad de una empresa, mediante el Sistema de Gestión de Seguridad de la Información (SGSI) (Burgos & Olmedo, 2018). El estándar ISO/IEC 27001 se puede implementar dentro de una organización para evaluar el estado de la organización en cuanto a seguridad de la información se refiere, ayudarlos a saber si los mismos podrían cumplir con sus propios requisitos en materia de seguridad de la información (Burgos & Olmedo, 2018).

El principal beneficio que se logra al implementar un Sistema de Seguridad de la Información (SGSI) es estar preparados para mejorar la gestión de seguridad de la información en la organización (Burgos & Olmedo, 2018). Es por esto por lo que debemos estar conscientes que con una buena gestión de riesgos lograríamos el conocimiento preciso para poder manejar los riesgos, las amenazas y las vulnerabilidades para dotar a la organización de los recursos necesarios para salvaguardar sus activos de información (Burgos & Olmedo, 2018). Dicho de otra manera, podríamos ver a un sistema de seguridad de la información como un enfoque sistemático para la gestión de información de carácter confidencial en la organización para que la misma siga siendo segura, la cual abarca personas, procesos y activos de TI, el implementar un SGSI con la ayuda del estándar ISO/IEC 27001 dará confianza a clientes internos y externo en cuanto a lo referente de la seguridad de la información y mostrará un compromiso con la seguridad, mostrando estar a la vanguardia en la aplicación de la técnica de procesos para

hacer frente a las amenazas de la información y problemas de seguridad (Burgos & Olmedo, 2018).

2.3 METODOLOGIA

2.3.1 CONTEXTO DE LA INVESTIGACION

La clínica Gamma Smart S.A es una empresa privada con prestaciones externas al seguro social ecuatoriano que actualmente ofrece servicios médicos generales, odontológicos y especializados, la clínica también les brinda a los afiliados y pacientes particulares los servicios de hospitalización, procedimientos de mediana complejidad, en aquella empresa cuenta con 250 colaboradores entre médicos especialistas, generales, odontólogos, cirujanos, licenciados y auxiliares en enfermería, adicional cuenta con la planta administrativa y de tecnologías de la información que incluyen 5 Ingenieros con diversos campos de conocimientos en el área de Informática y Tecnologías.

En cuanto a su infraestructura tecnológica, cuenta son servidores propios, historias clínicas digitales, infraestructura de red y dispositivos tecnológicos conectados, cuenta un sistema de gestión hospitalaria que se enfoca en la administración y control de citas médicas, registros de historias clínicas y otro sistema de facturación electrónica para la venta de consultas y control de inventarios, la clínica está sujeta a normativas y reglamentos entre ellas la ley de protección de datos personales del Ecuador (Asamblea Nacional del Ecuador, 2021), incluyendo la ISO 27001 para la gestión de seguridad de la información.

Para que la clínica pueda garantizar la seguridad de la información de sus activos debe de priorizar la disponibilidad de sus sistemas de información que estén operativos todas las 24 horas del día, la integridad para que los usuarios y la planta medica aseguren que los datos ingresados sean fiables, confiables y precisos, la confidencialidad para que la información este únicamente disponible para el personal autorizado y restringida de cualquier bien que quiera hacer uso de la misma sin autorización.

El diseño del sistema de seguridad de la información para el desarrollo de este proyecto deberá enfocarse a una mejora continua, mediante auditorias y actualizaciones constantes que evidencien los cambios y las reducciones de amenazas y vulneraciones a

la infraestructura tecnológica de la organización, así como la capacitación constante al personal de la empresa en base a seguridad de la información.

2.3.2 METODOLOGIAS DEL PROYECTO

2.3.2.1 METODOLOGIA DE LA INVESTIGACION

Para el desarrollo de este proyecto de diseño se realizará una investigación de tipo exploratorio (Sampieri, 2010), el propósito de esto es entender y proponer un sistema de gestión de seguridad de la información en base a las necesidades de la empresa, una organización privada que actualmente maneja una amplia gama de servicios médicos que cada día enfrenta retos en protección y gestión de la seguridad de la información requieren de una visión integral de seguridad, mediante el cual se espera contar con datos introductorios que ayuden a desarrollar y entender teorías del tema propuesto en base a trabajos similares con el fin de ofrecer una propuesta eficaz para el desarrollo de este proyecto.

Así también se desarrollará la investigación de tipo diagnostica (Sampieri, 2010) mediante una entrevista a los dueños de la clínica, con el único objetivo de conocer los procesos clínicos y ver sus necesidades, déficit para poder reducir los impactos en los riesgos que puedan causar daños a su infraestructura tecnológica permitiendo así tener una visión clara con el objetivo.

Con la propuesta ya establecida y habiendo estudiado las metodologías y técnicas de recolección de información se busca proponer un sistema de gestión de seguridad de la información, que reduzca los impactos en los riesgos que afectan los activos de información de la empresa.

2.3.2.2 TECNICAS DE RECOLECCION DE INFORMACION

En el siguiente proyecto de trabajo se realizó una entrevista a los dueños de la clínica, el cual quedaron en evidencias los procesos médicos, clínicos y administrativos, mediante esta técnica de recolección de información se pudo identificar ciertos procesos y activos de información que tienen vulnerabilidades y amenazas, que en un periodo a largo plazo puede representar una amenaza e impacto en los riesgos de sus activos.

A continuación, se procede a listar las debilidades que se hallaron en la clínica:

- Equipos obsoletos sin el respectivo mantenimiento adecuado.

- Falta de control físico sobre los dispositivos portátiles.
- Dispositivos médicos conectados a la red sin configuraciones de seguridad.
- Falta de licencias oficiales en sus programas.
- Clasificación y protección de información sin aplicar controles adecuados.
- Información sin realizarse una copia de seguridad de la información adecuadamente.
- Falta de cifrado de datos e información sensible.
- Planta médica y administrativa sin formación y capacitación en seguridad de la información y poca concienciación sobre políticas de seguridad.
- No se ha implementado políticas de seguridad formal y clara sobre el uso de sistemas.
- No se realiza monitoreo continuo de los sistemas de información tampoco auditorias periódicas de seguridad para poder identificar fallos o vulnerabilidades.

En base a esta recolección de información que se ha realizado se puede concluir y determinar que la clínica necesita implementar un sistema de gestión de seguridad de la información que les permita identificar y mitigar estas falencias que se han encontrado, sistema que es fundamental para proteger los activos de información y garantizar el cumplimiento normativo en la clínica.

2.3.2.3 METODOLOGIA DE DESARROLLO

Para el desarrollo de esta propuesta se planteó usar como metodología para el diseño del sistema de gestión de seguridad de la información el método Deming o PDCA (Plan-Do-Check-Act), método sugerido por la norma ISO/IEC 27001. (Infantas, 2017).

Este es un método que se usa comúnmente para los sistemas de gestión de calidad, el ciclo PDCA es un método que está conformado por 4 fases, que constantemente se está repitiendo de forma continua, cuando se termina el ciclo se verifica y se realiza un seguimiento de los resultados que se han obtenido y el ciclo vuelve a la primera fase con la información actualizada (Patricia, 2019).

En la siguiente grafica se evidencian las cuatro fases del ciclo de Deming metodología de mejora continua utilizada en la gestión de calidad:

Fuente: 1 Ciclo de Deming (PDCA) Tomado de *(Gobierno Electronico, s.f.)*

Gráfico: 1 Ciclo de Deming PDCA

A continuación, se explicará las fases de desarrollo del diseño del sistema de gestión de seguridad de la información en base a la metodología PDCA

Periodo 1: Planear

En esta fase, se llevó a cabo una investigación exploratoria para entender las necesidades específicas de seguridad de la información de la clínica. Las principales acciones realizadas fueron:

- Se recopiló información mediante entrevistas con los propietarios y responsables de la clínica, donde se identificaron los procesos clínicos y los activos críticos.
- Se realizó un diagnóstico de la situación actual, que permitió detectar brechas de seguridad, riesgos potenciales y vulnerabilidades en los sistemas de información.
- Se definió la política de seguridad de la información, alineada con los objetivos estratégicos de la clínica, enfocada en garantizar la confidencialidad, integridad y disponibilidad de los datos.
- Se establecieron los objetivos específicos del SGSI, tomando como base la norma ISO 27001 para guiar su diseño y futura implementación.

Fase 1: Definir la política de seguridad de la información.

En esta fase, se definieron las políticas de seguridad de la información para la clínica. Se establecieron las directrices para garantizar la protección del historial clínico, la infraestructura tecnológica y la ejecución legislativa. La elaboración de la política se hizo en conjunto con las áreas involucradas y bajo el cumplimiento de los valores institucionales.

Se tuvieron en cuenta los siguientes elementos clave:

- Confidencialidad: Solo el personal autorizado tiene acceso a la información.
- Integridad: Garantiza exactitud de los datos.
- Disponibilidad: La información debe estar accesible.

También, se definieron responsabilidades y roles que deben cumplirse a cabalidad, asegurando que cada empleado de la Gamma Smart comprendiera su función en la protección de la información.

Fase 2: Autorización de Gerencia

Esta fase fue necesaria para obtener la aprobación de gerencia y jefes superiores de la clínica para el desarrollo del Sistema de Gestión de Seguridad de la Información. En el plan de seguridad elaborado en la primera fase se explicó la importancia de la protección de la información de los pacientes, y confidencialidad de datos, de acuerdo con la normativa sanitaria.

Después de una revisión del plan de seguridad, la gerencia aprobó la asignación de los recursos necesarios incluyendo la capacitación del personal. Asimismo, se instauraron los roles de supervisión por parte de la directiva durante el proceso de implementación del SGSI.

Se firmó también, un acuerdo en el que la gerencia respalda el plan con la finalidad de promover la seguridad de la información dentro de la clínica.

Fase 3: Definir el alcance

En esta fase se delimitó el alcance del Sistema de Gestión de Seguridad de la Información para la clínica. Se identificaron las principales áreas que se encargan de procesar y almacenar información del paciente y el historial clínico, incluyendo el departamento de sistemas de información.

Fase 4: Evaluación de Riesgos

En esta fase, se evaluaron los riesgos internos y externos vinculados a la seguridad de la información en la clínica. Las áreas críticas identificadas fueron aquellas donde se encuentran los equipos tecnológicos que contienen la base de datos de los registros médicos, historia clínica de los pacientes e información administrativa.

Se identificaron las siguientes amenazas:

- Acceso no autorizado a la base de datos.
- Perdida de datos o información.
- Alteraciones o errores en el sistema de seguridad.
- Ataques cibernéticos.

Una de las vulnerabilidades internas identificadas fue la falta de capacitación al personal de la clínica sobre temas de seguridad de la información y el uso de dispositivos tecnológicos no seguros dentro de la empresa.

Luego de identificar los posibles riesgos y vulnerabilidades se evaluó el nivel impacto que estos podrían tener sobre la confidencialidad, integridad y disponibilidad de la información de la clínica. Se desarrolló un informe mencionando los riesgos identificados, para posteriormente implementar estrategias de control.

Fase 5: Inventario de Activos

En esta fase, se desarrolló un inventario de todos los activos de información más importantes para la clínica. Se identificaron tanto los activos físicos como los digitales más críticos para el funcionamiento seguro de los sistemas de información.

Se identificaron los sistemas de hardware, como computadoras y dispositivos médicos conectados a la red, así como el software que incluía la base de datos donde se

almacena el historial clínico y aplicaciones internas. Uno de los activos más críticos es la información personal y medica de los pacientes.

Para cada activo se determinó el nivel de protección que se requería de acuerdo con la gravedad del riesgo.

Periodo 2: Hacer

Durante esta fase, se procedió a implementar las acciones planificadas en la etapa anterior. Entre las actividades realizadas destacan:

- Se diseñó el SGSI, desarrollando la documentación formal de los procedimientos y responsabilidades para la gestión de la seguridad de la información.
- Se establecieron controles de seguridad que mitigaron los riesgos previamente identificados. Estos incluyeron la gestión de acceso, protección de datos sensibles y procedimientos de respuesta a incidentes.

Fase 6: Gestión de riesgos e incidentes

Es fundamental para asegurar que la organización esté preparada para identificar, mitigar y responder a los riesgos y eventos de seguridad que puedan afectar sus activos de información o procesos críticos. Esta fase no solo se enfoca en la prevención de riesgos, sino también en la respuesta rápida y efectiva ante incidentes, minimizando su impacto en las operaciones de la organización. Se deben seguir los siguientes pasos:

Fase 7: Establecer Políticas de SGSI

Durante esta fase, se establecieron y formalizaron las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) de la clínica. Estas políticas fueron diseñadas con base en los resultados de la evaluación de riesgos y los requerimientos normativos, garantizando la protección de los datos sensibles de los pacientes, así como la seguridad en todos los procesos de manejo de la información.

Se redactaron políticas específicas para el control de acceso, el uso de dispositivos y redes, la protección de la información confidencial y la gestión de incidentes. Además, se definieron procedimientos para la clasificación de la información según su nivel de sensibilidad y medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Periodo 3: Check (Verificar)

En esta fase, se evalúa y verifica el SGSI implementado, realizando las siguientes acciones:

- Se monitorean los controles de seguridad para asegurar su efectividad en función de los objetivos planteados.

4. Periodo 4: Act (Actuar)

Finalmente, en esta fase, se toman medidas correctivas y de mejora continua para optimizar el SGSI:

- Se establece un proceso de revisión periódica, garantizando que el SGSI mantuviera su efectividad a largo plazo.

CAPITULO III

DESARROLLO DEL PROYECTO

3.1 CRONOGRAMA DE IMPLEMENTACION

A continuación, mediante un diagrama de Gantt se evidencia el cronograma de implementación y diseño del SGSI

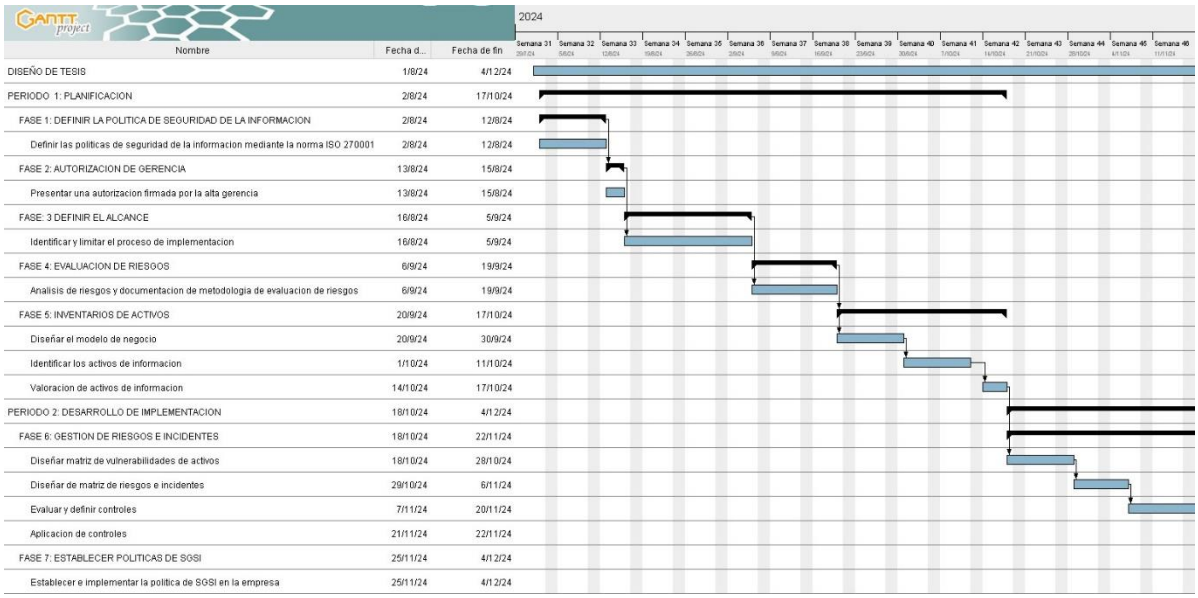

Gráfico: 2 Cronograma de implementación y diseño del SGSI

3.2 DESARROLLO E IMPLEMENTACION DEL SGSI

En base a la metodología Deming (Plan-Do-Check-Act) se ha establecido desarrollar 11 etapas que se desarrollaran a continuación:

- ❖ **Periodo 1: Planeación**

En esta etapa contamos con 5 fases en la que definimos las políticas de seguridad, el alcance, evaluación de riesgos, autorización de la empresa, métodos de evaluación y se realiza el inventario de activos.

- ✓ **Primera Fase: Definir las políticas de seguridad**

A.- Propósito y Alcance:

Establecer los lineamientos para garantizar la protección de datos de la clínica, asegurando su confidencialidad, integridad y disponibilidad de la información

B.- Compromiso de la alta Gerencia:

La Gerencia se compromete a facilitar todos los recursos requeridos para implementar el Sistema de Gestión de Seguridad de la Información, garantizando así el cumplimiento del estándar de calidad ISO 27001.

C.- Objetivo:

Mitigar los riesgos de seguridad relacionados con la perdida de información o accesos no autorizados de la clínica, implementando controles de accesos y cumpliendo con las normativas de seguridad para garantizar la confidencialidad integridad y protección de datos asegurando la confianza de los usuarios

D.- Roles y Responsabilidades:

Todos los empleados y contratistas son responsables de cumplir con esta política de seguridad.

El (OSI) Oficial de Seguridad de la Información es el responsable de supervisar y garantizar la implementación y cumplimientos de los protocolos de seguridad.

E.- Principios Claves de Seguridad:

Los principios claves de esta política que incluyen son:

- Control de Acceso a la Información.
- Gestión de Incidentes de Seguridad.
- Identificación y Tratamiento de Riesgos de Seguridad.

F.- Cumplimiento Legal y Normativo:

La Clínica Gamma Smart SA garantiza el cumplimiento de todas las leyes, normativas y regulaciones incluidas que están expuestas en la ley de protección de datos personales.

G.- Revisión y Mejora Continua:

Esta política será revisada anual y periódicamente cuando sea el caso, esto debido a los cambios en los riesgos de seguridad, asegurando así que esta política siga siendo efectiva para reducir el impacto en riesgos y de acuerdo con los objetivos del SGSI.

- ✓ **Segunda Fase: Autorización de Gerencia**

Se realizo un acta de constitución del proyecto en la cual se detalla los objetivos y el alcance del proyecto, este documento formaliza la creación del proyecto y proporciona una breve descripción general, el mismo que se entregó de manera física y digital a la parte pertinente de la alta gerencia para su aprobación. (Ver Anexo 1 – Acta de Constitución)

- ✓ **Tercera Fase: Definir el Alcance**

El alcance de este proyecto se basa en brindar un sistema de gestión de seguridad de la información, en el cual se lograron determinar e identificar los procesos del negocio en la que esta expuesta a ser vulnerada su información, los procesos que se han incluido en el alcance se detallan a continuación:

Registro de Pacientes: A partir de esta sección empiezan los procesos de la clínica, los pacientes al ingresar a la clínica toman un turno, las recepcionistas registran los datos del paciente en el sistema, realizando la verificación cruzada, procedimiento mediante el cual el prestador de salud identifica al usuario, una vez registrado el paciente se dirige hasta el departamento de signos vitales para que los licenciados registren sus signos vitales en el sistema y luego a la espera de ser atendido por el medico de acuerdo a su cita.

Atención Medica al Paciente: El medico atiende la cita del paciente, en este proceso el medico registra la atención, llena la historia clínica del paciente en el sistema clínico, el medico puede generar ordenes de exámenes de laboratorio, estudios de imágenes o procedimientos de acuerdo a la atención.

Proceso de Datos: En esta sección luego de que el medico genero las ordenes médicas, el o los licenciados registran los resultados de los estudios en el sistema, al paciente se le entrega una copia de sus resultados de forma física mientras que el documento digital queda guardado en el sistema, de otro modo sucede con los médicos de imagenología que informan los estudios de imágenes ellos lo hacen vía remota informando luego suben al sistema sus resultados, cuando existen ordenes de procedimientos al paciente le asignan una cita para revisar los resultados de estudios que deben realizarse antes de hacer algún tipo de procedimiento de mediana y alta complejidad, cuando le toque

realizarse el procedimiento los licenciados o licenciadas y las auxiliares registran los consentimientos informados, formularios, registran los resultado que han obtenidos en el sistema clínico después de realizarle un procedimiento médico, una parte de archivos suben al sistema y la otra parte de documentación se coloca en una carpeta compartida donde se tiene acceso sin ningún tipo de restricción.

Procedimientos Médicos: Cuando hay procedimientos de mediana complejidad se realizan varios documentos, estos son archivos con información confidencial del paciente la misma que no puede ser expuesta por ningún medio.

Auditoria Medica: En esta parte los ingenieros del área de validaciones realizan las revisiones en el sistema en cuanto desde las recepcionistas hasta los médicos hayan registrado correctamente la historia clínica del paciente, en caso que haya algún error pues el personal de validación envía a corregir, seguido los auditores médicos también revisan los procedimientos médicos que se hayan desarrollado correctamente, revisión de archivos médicos compartidos en una carpeta publica y sin restricción.

Facturación Electrónica: Una vez haber pasado por auditoria, los planilladores comienzan a generar archivos planos, documentación que es generada del sistema clínico administrativo y de forma manual en documentos Excel para luego proceder a realizar la facturación

Cuarta Fase: Evaluación de Riesgos

En esta sección, se aplicó la ISO 27005 en donde nos facilitó un listado de amenazas y de vulnerabilidades (Ver Anexo 1 Listado de amenazas y vulnerabilidades) para identificar, analizar y gestionar los riesgos para cada uno de los activos de información de la empresa.

Para poder implementar esta evaluación también se tuvo que elaborar matrices de riesgos para poder identificar y relacionar cada activo con las amenazas y vulnerabilidades, los riesgos fueron identificados en diferentes niveles como alto, medio, bajo y crítico. Los riesgos altos y críticos se clasificaron para poder recibir un tratamiento siguiendo un plan de respuesta efectiva a través de la mitigación, transferencia o aceptación del riesgo, este enfoque permitió que la clínica tome decisiones de cómo gestionar y cuidar sus activos de información asegurando la continuidad de su funcionamiento y reduciendo el impacto

de posibles incidentes de seguridad. En la siguiente tabla se muestran los criterios de ocurrencia, una vez que se ha relacionado las vulnerabilidades con las amenazas se inicia el proceso de vincular los riesgos con sus consecuencias y en base de la consecuencia se estipula la criticidad de los riesgos.

Principios de Probabilidad	
Probabilidad	Frecuencia
Rara Vez	1 vez cada 6 años
Incierto	3 veces cada 6 años
Posible	1 vez al año
Probable	2 veces al año
Alta Probabilidad	4 veces al año

Tabla 1 Criterios de probabilidad para evaluar los riesgos

Para poder determinar cuánto es el impacto se realizaron criterios que nos ayudaran a desarrollar e interpretar el nivel de impacto que tendrían los activos de información, según la ISO/IEC 27005, cada organización debe definir su apetito de riesgo como parte fundamental de los procesos evaluativos y de la gestión de riesgos, tomando en cuenta hasta que parte se puede tolerar una vulnerabilidad o amenaza que pueda colocar en riesgo sus operaciones o de comprometer los activos de información. (ISO/IEC, 2018).

En la siguiente tabla se muestra las características del impacto que nos ayudaran a determinar el nivel de criticidad de los riesgos.

Atributos para determinar el impacto de activos	
Impacto	Criterio
Bajo	No existen daños o impacto directo sobre la empresa, tampoco existen sanciones legales ni daño a la reputación.
Moderado	Puede existir un tipo de riesgo, pero aceptable, no existen sanciones legales, ni daño a la reputación y su impacto operacional es mínimo
Importante	El riesgo en la empresa es de manera directa, pero a nivel medio, existen penalizaciones y sanciones por infracciones leves, la empresa podría caer en gastos de recursos tanto operativos como económicos.
Alto	El impacto en la empresa es directo y el daño mayor, existen sanciones por faltas graves, la alta gerencia pudiera estar involucrada, la empresa generaría gastos operativos, económicos y pérdidas financieras.
Catastrófico	El daño a la empresa es catastrófico, perdidas financieras y económicas, sanciones por infracciones graves, el directorio y la alta gerencia involucrada, perdida de la cartera de clientes a gran volumen.

Tabla 2 Atributos para determinar el impacto de activos

Una vez que hemos definidos los conceptos para el impacto y establecer la frecuencia de la probabilidad para poder determinar los niveles de criticidad, vamos a fijarnos previamente en la siguiente representación, la misma que nos permitirá establecer el riesgo de acuerdo con la probabilidad y el impacto definidos por la organización.

A continuación, se ilustra la siguiente grafica para definir un nivel de criticidad.

Impacto	Catastrófico	Medio	Alto	Alto	Critico	Critico
	Alto	Bajo	Medio	Alto	Alto	Critico
	Importante	Bajo	Medio	Medio	Alto	Alto
	Moderado	Bajo	Bajo	Medio	Medio	Medio
	Bajo	Bajo	Bajo	Bajo	Bajo	Medio
		Rara Vez	Incierto	Posible	Probable	Alta Probabilidad
	Probabilidad					

Tabla 3 Niveles de criticidad

Quinta Fase: Inventarios de Activos

En esta sección, se realizó el levantamiento de información y la identificación de los activos de información que nos implica un análisis exhaustivo de los recursos informáticos de la impresa, posterior a ello se procede a valorar estos activos considerando su importancia en términos de confidencialidad, integridad y disponibilidad.

Atributo	Descripción
ID del Activo	Un identificador único para cada activo de información
Nombre del Activo:	Nombre descriptivo del activo.
Descripción:	Detalles del activo y su función.
Propietario:	La persona o departamento responsable de la gestión del activo.

Ubicación:	Dónde se encuentra el activo (físicamente o en la nube).
Clasificación:	Tipo de información o función que desempeña el activo (por ejemplo, Operacional, Información Crítica, Información Sensible, etc.).

Tabla 4 Atributos para la identificación de activos

A continuación, se listan los activos de información de la clínica (Ver Tabla 2)

Listado de Activos de Información

ID Activos	Tipo de Activo	Nombre de Activo	Descripción de Activo	Propietario	Ubicación	Clasificación
A001	Software	Sistema web Gamma Smart 2.0	Sistema web que permite el registro de las atenciones médicas de los pacientes	TI	Cloud	Operacional
A002	Datos e Información	Bases de datos	Información que se guarda en un gestor de base de datos que incluye información de historiales clínicos, datos personales de clientes, documentos, facturas, archivos planos de los sistemas clínico y de inventario	TI	Cloud	Información Sensible
A003	Hardware	Servidor de Correo Electrónico	Servidor de correos que es utilizado para las comunicaciones internas y externas	TI	Data Center	Información Confidencial
A004	Hardware	Red de Comunicaciones	Infraestructura de red que permite conectividad interna y externa en toda la planta hospitalaria	TI	Clínica	Infraestructura Critica
A005	Datos e Información	Backups	Copias de seguridad de la documentación confidencial de la clínica, Informes Laboratorios, Imágenes, Procedimientos, Formularios, Facturación, Archivos Planos	TI	Almacenamiento Externo	Información Critica
A006	Software	Software de Facturación	Sistema de escritorio utilizado para la gestión de facturación electrónica	Administración, TI, Finanzas	Admisión, Administración y Bodega	Operacional
A007	Software	Software de Inventario	Sistema de escritorio que permite el registro de entrada y salida de insumos médicos	Finanzas	Administración y Bodega	Operacional

A008	Hardware	Servidor de Local de Facturación	Servidor que aloja el sistema de facturación	TI	Sala de Servidores	Infraestructura
B001	Hardware	Computadoras de Escritorios	Equipo de cómputo que permite a los usuarios realizar sus actividades de trabajo de acuerdo con sus funciones	TI	Consultorios y Área Administrativa	Operacional
B002	Hardware	Computadoras Laptops	Equipo de cómputo que permite a los usuarios realizar sus actividades de trabajo de acuerdo con sus funciones	TI	Bodega	Operacional
B003	Hardware	Biométrico	Dispositivo que permite tomar la lectura de la huella digital	TI	Entrada de la Clínica	Operacional
B004	Hardware	Impresora	Dispositivo que permite ser utilizado para documentos administrativos, y médicos	Administración	Salas de Procedimientos, Agendamiento, Recepción, Administración, Gerencia	Operacional
B005	Hardware	Escáner	Equipo utilizado para digitalizar documentos	Administración	Recepción, Administración	Operacional
C001	Hardware	Electrocardiograma	Equipo que es utilizado para ver la actividad eléctrica del corazón	Gerencia	Área de Cardiología	Información Sensible
C002	Hardware	Ecocardiograma	Equipo que es utilizado para realizar ecografías de como fluye la sangre por el corazón y las válvulas cardiacas	Gerencia	Área de Cardiología	Información Sensible
C003	Hardware	Ecógrafos	Equipo que realiza toma de imágenes de ultrasonidos de diferentes tipos en el cuerpo del paciente	Gerencia	Área de Ecografía	Información sensible

C004	Hardware	Equipo de Rayos X	Equipo que utiliza radiación electromagnética ionizante que permite la toma de imágenes en representación gráfica de sistema óseo del paciente	Gerencia	Area de Rayos X	Informacion Sencible
C005	Hardware	Equipo de Endoscopia y Colonoscopia	Equipo que permite explorar y tomar muestras de Tejido del estomago y el colon para poder biopsiar	Gerencia	Sala de Procedimientos de Mediana Complejidad	Información Confidencial
C006	Hardware	Equipo de Cistoscopia	Equipo que permite explorar y tomar muestras de Tejido de órganos reproductores masculinos y femeninos	Gerencia	Sala de Procedimientos de Mediana Complejidad	Información Confidencial
C007	Hardware	Equipo de Colposcopia	Equipo que permite explorar y tomar muestras del tejido de cuello uterino	Gerencia	Sala de Procedimientos de Mediana Complejidad	Información Confidencial
C008	Hardware	Equipo de Tomografía	Equipo que permite realizar la captura de imágenes detalladas en el interior del cuerpo mediante radiación ionizante	Gerencia	Sala de Tomografia	Informacion Cofidencial
C009	Hardware	Equipo de Rayos X Panorámico	Equipo que permite la toma de una imagen panorámica dental mediante radiación ionizante	Gerencia	Sala de RX Panoramico	Informacion Sencible
C010	Hardware	Equipo de Electroencefalograma	Equipo que permite la toma de ondas y actividades eléctricas del cerebro	Gerencia	Sala de Electroencefalograma	Información Sencible
C011	Hardware	Equipo de Fibroscan	Equipo que mide la velocidad de ondas elásticas a través del hígado que sirve para detectar el grado de fibrosis hepatica	Gerencia	Sala de Fibroscan	Informacion Sencible
C012	Hardware	Equipos de Laboratorio	Equipos que permiten realizar los procedimientos bioquímicos sobre las muestras de los pacientes	Gerencia de Laboratorio	Laboratorio	Información Confidencial

E001	Datos e Información	Historia Clinica	Documentación medica-legal donde contiene la información de una paciente almacenada en el sistema web	Gerencia	Cloud	Información Confidencial
E002	Datos e Información	Formularios de Historia Clínica Ocupacional	Documentos que se llenan con información del paciente en base a un procedimiento médico o tratamiento	Gerencia, Sala de Procedimientos	Carpeta Compartida	Información Confidencial
E003	Datos e Información	Consentimientos Informados	Documentos en el cual el paciente firma autorizando a realizarse un procedimiento con su consentimiento	Gerencia, Médicos, Sala de Procedimientos	Carpeta Compartida	Información Confidencial
E004	Datos en Información	Hoja de Interconsulta	Documento médico legal donde se detalla los datos relativos de un paciente, antecedentes, evolución, tratamientos y demás procedimientos.	Gerencia, Médicos, Sala de Procedimientos	Carpeta Compartida	Información Confidencial

Tabla 5 Listado de Activos de Información

Luego de haber identificado los activos de información de la empresa se procederá a dar una valoración a cada uno de los activos siguiendo las directrices del estándar ISO 27001, tomando en cuenta sus 3 principios de seguridad, integridad, confidencialidad y disponibilidad de la información, a cada una de las dimensiones se les asignará una escala del 1 al 4 tal como se ilustra en la grafica

DIMENSION DEL ACTIVO				
	ESCALA			
DIMENSION	1.- BAJA	2.- MEDIA	3.- ALTA	4.- CRITICO
DISPONIBILIDAD	Activo que puede estar inaccesible sin afectar al resto de operaciones	Activo que puede tolerar pequeñas interrupciones	Activo que tiene que estar disponible casi siempre	Activo que necesita estar operativo 24/7, cualquier caída o inactividad es critica
CONFIDENCIALIDAD	Información de dominio público o de acceso libre de bajo riesgo	Activo de información sensible con acceso restringido, si se filtra no ocasionaría algún riesgo	Activo de información confidencial protegida, si se filtra causaría graves daños o un riesgo moderado	Activo de información sumamente confidencial, su divulgación o filtración causaría un riesgo catastrófico
INTEGRIDAD	Los errores en datos no suman y no generan ningún riesgo	Son errores tolerables, pero deben corregirse porque si no generarían un impacto leve	La información debe ser con precisión, los errores afectan gravemente	La información debe ser exacta, cualquier alteración generaría un impacto grave y critico

Tabla 6 Dimensión del activo y su escala

Luego de haber dado a cada dimensión e identificado su valoración ahora se va a realizar la media de cada uno de los activos de información para obtener su valor solo se seleccionarán los activos mayores a 3 que representen un riesgo con mayor impacto para poder realizar seguidamente el análisis, tratamiento y sus políticas de seguridad y de controles para proteger su información, a continuación, se listan los activos de información junto a su valoración de activos.

VALORACION DE ACTIVO					
CRITERIO DE VALORACION					
ID ACTIVO	ACTIVO	DISPONIBILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	PROMEDIO
A001	Sistema web Gamma Smart 2.0	4	4	4	4
A002	Bases de datos	3	4	4	4
A003	Servidor de Correo Electrónico	2	4	2	3
A004	Red de Comunicaciones	2	2	4	3
A005	Backups	2	4	4	3
A006	Software de Facturación	3	3	3	3
A007	Software de Inventario	4	4	4	4
A008	Servidor de Local de Facturación	4	4	4	4
B001	Computadoras de Escritorios	2	2	3	2
B002	Computadoras Laptops	3	2	3	3
B003	Biométrico	1	1	2	1
B004	Impresora	1	2	2	2
B005	Escáner	2	1	1	1
C001	Electrocardiograma	1	3	3	2
C002	Ecocardiograma	3	2	2	2
C003	Ecografos	1	3	2	2
C004	Equipo de Rayos X	1	3	3	2
C005	Equipo de Endoscopia y Colonoscopia	3	4	4	4
C006	Equipo de Cistoscopia	2	3	2	2
C007	Equipo de Colposcopia	3	4	4	4
C008	Equipo de Tomografía	4	4	4	4
C009	Equipo de Rayos X Panorámico	2	2	3	2
C010	Equipo de Electroencefalograma	1	3	3	2
C011	Equipo de Fibroscan	3	2	2	2
C012	Equipos de Laboratorio	3	4	4	4
E001	Historia Clinica Digital	4	4	4	4
E002	Formularios de Historia Clínica Ocupacional	4	4	4	4
E003	Consentimientos Informados	3	4	3	3
E004	Hoja de Interconsulta	4	4	4	4

Tabla 7 Valoración de activos de información de la empresa

Periodo 2: Desarrollo

En esta fase se centra en la identificación, evaluación y tratamiento del riesgo, asociados a los activos de información en base a las vulnerabilidades y amenazas encontradas.

Sexta Fase: Gestión de Riesgos e Incidentes

En esta sección vamos a identificar las amenazas y vulnerabilidades a la que están expuestas los activos de información de la empresa, también se tomara en cuenta la probabilidad de que cada riesgo tenga un impacto potencial en la empresa.

IDENTIFICACION DE AMENAZAS DE LOS ACTIVOS				
CRITERIO DE VALORACION				
ID ACTIVO	ACTIVO	VULNERABILIDAD	AMENAZA	PROMEDIO
A001	Sistema web Gamma Smart 2.0	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.	Abuso de los derechos	4
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Software ampliamente distribuido	Corrupción de datos	
		Configuración incorrecta de parámetros	Error en el uso	
		Gestión deficiente de las contraseñas	Falsificación de derechos	
A002	Bases de datos	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	4
		Asignación errada de los derechos de acceso	Abuso de los derechos	
		Configuración incorrecta de parámetros	Error en el uso	
		Fechas incorrectas	Error en el uso	
		Tablas de contraseñas sin protección	Falsificación de derechos	
		Gestión deficiente de las contraseñas	Falsificación de derechos	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Parámetros incorrectamente configurados	Mal funcionamiento del software	
A003	Servidor de Correo Electrónico	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	3
		Susceptibilidad a la humedad, el polvo y la suciedad.	Susceptibilidad a la humedad, el polvo y la suciedad.	

		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
		Almacenamiento sin protección	Hurto de medios o documentos	
A004	Red de Comunicaciones	Líneas de comunicación sin protección	Escucha encubierta	3
		Tráfico sensible sin protección	Escucha encubierta	
		Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones	
		Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos	
		Arquitectura insegura de la red	Espionaje remoto	
		Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información	
		Conexiones de red pública sin protección	Uso no autorizado del equipo	
****99A005	Backups	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	3
		Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Almacenamiento sin protección	Hurto de medios o documentos	
		Copia no controlada	Hurto de medios o documentos	
		Falta de backups o redundancia en el almacenamiento	Destrucción del equipo o los medios	
A006	Software de Facturación	Defectos bien conocidos en el software	Abuso de los derechos	3
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
		Software ampliamente distribuido	Corrupción de datos	
		Interfaz de usuario compleja	Error en el uso	

		Configuración incorrecta de parámetros	Error en el uso	
		Fechas incorrectas	Error en el uso	
		Software nuevo o inmaduro	Mal funcionamiento del software	
		Fallos para registros y eliminación de usuarios	Error en el uso	
A007	Software de Inventario	Defectos bien conocidos en el software	Abuso de los derechos	4
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
		Software ampliamente distribuido	Corrupción de datos	
		Interfaz de usuario compleja	Error en el uso	
		Configuración incorrecta de parámetros	Error en el uso	
		Falta de respaldos	Error en el uso	
A008	Servidor de Local de Facturación	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	4
		Susceptibilidad a la humedad, el polvo y la suciedad.	Susceptibilidad a la humedad, el polvo y la suciedad.	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
		Almacenamiento sin protección	Hurto de medios o documentos	
B002	Computadoras Laptops	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	3
		Uso incorrecto de software y hardware	Error en el uso	
		Equipos sin protección impermeable, falta de drenaje	Daño por agua	
		Ausencia de sistemas de filtración de aire y mantenimiento adecuado	Contaminación (polvo, humo, etc.)	
		Equipos expuestos a ambientes hostiles, falta de monitoreo ambiental	Polvo, corrosión, congelamiento	

		Susceptibilidad a la humedad, el polvo y la suciedad.	Susceptibilidad a la humedad, el polvo y la suciedad.	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
		Almacenamiento sin protección	Hurto de medios o documentos	
		Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo	
C005	Equipo de Endoscopia y Colonoscopia	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	4
		Ausencia de un eficiente control de cambios en la configuración	Error en el uso	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
		Almacenamiento sin protección	Hurto de medios o documentos	
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
		Interfaz de usuario compleja	Error en el uso	
		Configuración incorrecta de parámetros	Error en el uso	
		Ausencia del personal	Incumplimiento en la disponibilidad del personal	
		Habilitación de servicios innecesarios	Procesamiento ilegal de datos	
		Descarga y usos no controlados de software	Manipulación con software	

		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Uso incorrecto de software y hardware	Error en el uso	
C007	Equipo de Colposcopia	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	4
		Ausencia de un eficiente control de cambios en la configuración	Error en el uso	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Ausencia del personal	Incumplimiento en la disponibilidad del personal	
		Habilitación de servicios innecesarios	Procesamiento ilegal de datos	
		Descarga y usos no controlados de software	Manipulación con software	
		Almacenamiento sin protección	Hurto de medios o documentos	
C008	Equipo de Tomografía	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	4
		Ausencia de un eficiente control de cambios en la configuración	Error en el uso	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
		Almacenamiento sin protección	Hurto de medios o documentos	
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
		Interfaz de usuario compleja	Error en el uso	

		Configuración incorrecta de parámetros	Error en el uso	
		Ausencia del personal	Incumplimiento en la disponibilidad del personal	
		Habilitación de servicios innecesarios	Procesamiento ilegal de datos	
		Descarga y usos no controlados de software	Manipulación con software	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Uso incorrecto de software y hardware	Error en el uso	
		Sensibilidad a la radiación electromagnética	Radiación electromagnética	
		Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos	
C012	Equipos de Laboratorio	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información	4
		Ausencia de un eficiente control de cambios en la configuración	Error en el uso	
		Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía	
		Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos	
		Almacenamiento sin protección	Hurto de medios o documentos	
		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos	
		Interfaz de usuario compleja	Error en el uso	
		Habilitación de servicios innecesarios	Procesamiento ilegal de datos	
		Ausencia de copias de respaldo	Manipulación con software	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones	

		Arquitectura insegura de la red	Espionaje remoto	
		Ausencia del personal	Incumplimiento en la disponibilidad del personal	
		Uso incorrecto de software y hardware	Error en el uso	
		Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo	
E001	Historia Clínica Digital	Copia no controlada	Hurto de medios o documentos	4
		Fechas incorrectas	Error en el uso	
		Ausencia de copias de respaldo	Manipulación con software	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Falta de conciencia acerca de la seguridad	Error en el uso	
		Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables	
		Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	
		Uso incorrecto de software y hardware	Error en el uso	
E002	Formularios de Historia Clínica Ocupacional	Copia no controlada	Hurto de medios o documentos	4
		Fechas incorrectas	Error en el uso	
		Ausencia de copias de respaldo	Manipulación con software	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Falta de conciencia acerca de la seguridad	Error en el uso	

		Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables	
		Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	
		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	
		Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos	
E003	Consentimientos Informados	Copia no controlada	Hurto de medios o documentos	3
		Fechas incorrectas	Error en el uso	
		Ausencia de copias de respaldo	Manipulación con software	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Falta de conciencia acerca de la seguridad	Error en el uso	
		Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables	
		Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	
		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	
		Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos	
		Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos	

E004	Hoja de Interconsulta	Copia no controlada	Hurto de medios o documentos	4
		Fechas incorrectas	Error en el uso	
		Ausencia de copias de respaldo	Manipulación con software	
		Falla en la producción de informes de gestión	Uso no autorizado del equipo	
		Falta de conciencia acerca de la seguridad	Error en el uso	
		Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables	
		Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos	
		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos	
		Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos	

Tabla 8 Identificación de amenazas y vulneración de los activos

Luego de haber realizado la identificación de los activos con sus amenazas y vulnerabilidades se procede a crear la matriz de riesgos que nos ayudara para evaluar y gestionar los riesgos, realizando una combinación de probabilidad con el impacto para luego permitir priorizar los riesgos según su criticidad para poder tomar decisiones.

Dependiendo de su criticidad se le da un tratamiento al riesgo son acciones que se van a tomar para mitigar o gestionar los riesgos, también se refiere a ciertas acciones o estrategias que se implementan para gestionar los riesgos identificados en la empresa, dentro del tratamiento tenemos 4 alternativas como: reducir, retener, transferir o evitar el riesgo, a continuación, se muestra la matriz de riesgo.

	IDENTIFICACION DE AMENAZAS DE LOS ACTIVOS							
	CRITERIO DE VALORACION							
ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R001	Sistema web Gamma Smart 2.0	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo.	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Incierta	Catastrófico	Alto	Reducir el riesgo
R002		Falla en la producción de informes de gestión	Datos de los informes no se registran correctamente.	Toma de decisiones incorrectas por falta de visibilidad de la actividad del equipo	Posible	Alto	Alto	Reducir el riesgo
R003		Software ampliamente distribuido	Software ampliamente utilizado y pueden ser explotados por atacantes	Perdida de o alteración de información confidencial	Incierta	Alto	Medio	Retener el riesgo
R004		Configuración incorrecta de parámetros	Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Deficiencia en la parte operativa o resultados erróneos que afectan a la toma de decisiones.	Probable	Alto	Alto	Reducir el riesgo
R005		Gestión deficiente de las contraseñas	Contraseñas cortas, débiles que pueden ayudar al atacante a obtener acceso y hacerse pasar por un usuario no autorizado.	Acceso no autorizado a sistemas podría llevar a un robo y fuga de datos confidenciales	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R007	Bases de datos	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Posible	Alto	Alto	Reducir el riesgo
R008		Asignación errada de los derechos de acceso	Usuarios con accesos y permisos excesivos	Acciones no autorizadas, alteración de información	Posible	Alto	Alto	Reducir el riesgo
R009		Configuración incorrecta de parámetros	Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Deficiencia en la parte operativa o resultados erróneos que afectan a la toma de decisiones.	Posible	Importante	Medio	Retener el riesgo
R010		Fechas incorrectas	Fechas incorrectas afectan el proceso de la información	Fallos en los reportes	Posible	Bajo	Bajo	Retener el riesgo
R011		Tablas de contraseñas sin protección	Acceso de contraseñas sin protección y a los sistemas de información.	Accesos no autorizados a los sistemas de información.	Alta Probabilidad	Alto	Crítico	Reducir el riesgo
R012		Gestión deficiente de las contraseñas	Contraseñas cortas, débiles que pueden ayudar al atacante a obtener acceso y hacerse pasar por un usuario no autorizado.	Acceso no autorizado a sistemas podría llevar a un robo y fuga de datos confidenciales	Alta Probabilidad	Alto	Critico	Reducir el riesgo
R013		Falla en la producción de informes de gestión	Datos de los informes no se registran correctamente.	Toma de decisiones incorrectas por falta de visibilidad de la actividad del equipo	Posible	Importante	Medio	Retener el riesgo
R014		Parámetros incorrectamente configurados	Configuración incorrecta altera y afecta la productividad del software	Interrupciones que afectan a la disponibilidad del software	Posible	Alto	Alto	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R015	Servidor de Correo Electrónico	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Alto	Reducir el riesgo
R016		Susceptibilidad a la humedad, el polvo y la suciedad.	Equipos de Hardware expuesto a la corrosión y suciedad	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Alta Probabilidad	Catastrófico	Alto	Reducir el riesgo
R017		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos y perdida de información.	Caída del servicio y daños en los componentes electrónicos del hardware	Probable	Catastrófico	Critico	Reducir el riesgo
R018		Susceptibilidad a las variaciones de temperatura	Las variaciones de temperatura pueden sobrecalentar los equipos	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Incierto	Catastrófico	Alto	Reducir el riesgo
R019		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo
R020	Red de Comunicaciones	Líneas de comunicación sin protección	Interceptación de comunicaciones	Robo de información confidencial	Posible	Moderado	Medio	Retener el riesgo
R021		Tráfico sensible sin protección	Captura de paquetes de datos durante el tráfico de red	Exposición de datos e información confidencial	Posible	Alto	Alto	Reducir el riesgo
R022		Conexión deficiente de los cables.	Mal funcionamiento de los equipos de redes	Interrupción de conectividad y perdida de comunicación	Incierto	Alto	Medio	Retener el riesgo
R023		Ausencia de identificación y autentificación de emisor y receptor	Usuarios no autorizados pueden acceder a los sistemas de información	Accesos no autorizados comprometen la seguridad del sistema de información	Posible	Alto	Alto	Reducir el riesgo

R024		Arquitectura insegura de la red	Acceso no autorizado a través de vulnerabilidades	Robo de información en tiempo real	Probable	Alto	Alto	Reducir el riesgo
R025		Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	El sistema de red no puede con sobrecargas de tráfico pesado	Falla en el rendimiento o caída total de la infraestructura de red	Incierto	Alto	Medio	Retener el riesgo
R026		Conexiones de red pública sin protección	Acceso no autorizado de dispositivos a redes publicas	Robo de información y uso indebido de recursos	Probable	Catastrófico	Critico	Reducir el riesgo
R027	Backups	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Alto	Reducir el riesgo
R028		Susceptibilidad a la humedad, el polvo y la suciedad.	Equipos de Hardware expuesto a la corrosión y suciedad	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Alta Probabilidad	Catastrófico	Alto	Reducir el riesgo
R029		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos y perdida de información.	Caída del servicio y daños en los componentes electrónicos del hardware	Probable	Catastrófico	Critico	Reducir el riesgo
R030		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo
R031		Copia no controlada	Duplicidad de documentos o medios electrónicos	Divulgación y perdida de información	Posible	Alto	Alto	Reducir el riesgo
R032		Falta de backups o redundancia en el almacenamiento	Perdida de información	Pérdida total de información almacenada	Posible	Alto	Alto	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R033	Software de Facturación	Defectos bien conocidos en el software	Explotación de vulnerabilidades	Accesos no autorizados que pudieran manipular los sistemas de información	Posible	Alto	Alto	Reducir el riesgo
R034		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Incierta	Alto	Medio	Retener el riesgo
R035		Software ampliamente distribuido	Software ampliamente utilizado y puede ser explotados por atacantes	Perdida de o alteración de información confidencial	Incierta	Alto	Medio	Retener el riesgo
R036		Interfaz de usuario compleja	Dificultad para el usuario al utilizar el sistema	Errores y fallos en la ejecución de tareas	Incierto	Moderado	Bajo	Retener el riesgo
R037		Configuración incorrecta de parámetros	Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Deficiencia en la parte operativa o resultados erróneos que afectan a la toma de decisiones.	Posible	Importante	Medio	Retener el riesgo
R038		Fechas incorrectas	Fechas incorrectas afectan el proceso de la información	Fallos en los reportes	Posible	Bajo	Bajo	Retener el riesgo
R039		Software nuevo o inmaduro	Inestabilidad y falta de pruebas de errores del software	Fallos inesperados en el sistema que afectan su funcionabilidad	Posible	Alto	Alto	Reducir el riesgo
R040		Fallos para registros y eliminación de usuarios	Dificultad al crear usuarios o eliminar cuentas de usuario	Error en la gestion de usuarios y problemas de seguridad.	Posible	Alto	Alto	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R041	Software de Inventario	Defectos bien conocidos en el software	Explotación de vulnerabilidades	Accesos no autorizados que pudieran manipular los sistemas de información	Posible	Alto	Alto	Reducir el riesgo
R042		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Incierta	Alto	Medio	Retener el riesgo
R043		Software ampliamente distribuido	Software ampliamente utilizado y pueden ser explotados por atacantes	Perdida de o alteración de información confidencial	Incierta	Alto	Medio	Retener el riesgo
R044		Interfaz de usuario compleja	Dificultad para el usuario al utilizar el sistema	Errores y fallos en la ejecución de tareas	Incierto	Moderado	Bajo	Retener el riesgo
R045		Configuración incorrecta de parámetros	Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Deficiencia en la parte operativa o resultados erróneos que afectan a la toma de decisiones.	Posible	Importante	Medio	Retener el riesgo
R046		Falta de respaldos	Perdida de datos debido a errores o fallas en el sistema	Perdida de información definidita	Incierto	Alto	Alto	Reducir el riesgo
R047	Servidor de Local de Facturación	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software.	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R048		Susceptibilidad a la humedad, el polvo y la suciedad.	Equipos de Hardware expuesto a la corrosión y suciedad	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R049		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos de Hardware y perdida de información.	Caída del servicio y daños en los componentes electrónicos del hardware	Incierto	Alto	Medio	Retener el riesgo

R050		Susceptibilidad a las variaciones de temperatura	Las variaciones de temperatura pueden sobrecalentar los equipos	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Incierto	Catastrófico	Alto	Reducir el riesgo
R051		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo
ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R052	Computadoras Laptops	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Alto	Reducir el riesgo
R053		Uso incorrecto de software y hardware	Mal uso de las herramientas	Fallos operativos y en su productividad	Alta Probabilidad	Catastrófico	Medio	Retener el riesgo
R054		Equipos sin protección impermeable, falta de drenaje	Daño físico a los equipos	Daño del equipo y perdida de datos e interrupción del servicio	Posible	Alto	Alto	Reducir el riesgo
R055		Ausencia de sistemas de filtración de aire y mantenimiento adecuado	Daño físico a los equipos y mal funcionamiento de los equipos	Daños físicos y bajo rendimiento de los equipos	Posible	Alto	Alto	Reducir el riesgo
R056		Equipos expuestos a ambientes hostiles, falta de monitoreo ambiental	Daños periódicamente de equipos	Fallos de hardware y bajo rendimiento de equipos	Posible	Moderado	Medio	Retener el riesgo
R057		Susceptibilidad a la humedad, el polvo y la suciedad.	Equipos de Hardware expuesto a la corrosión y suciedad	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo

R058		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos de Hardware y perdida de información.	Caída del servicio y daños en los componentes electrónicos del hardware	Incierto	Alto	Medio	Retener el riesgo
R059		Susceptibilidad a las variaciones de temperatura	Las variaciones de temperatura pueden sobrecalentar los equipos	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Incierto	Catastrófico	Alto	Reducir el riesgo
R060		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo
R061		Ausencia de política formal sobre la utilización de computadores portátiles	Robo o extravío de equipos portátiles	Pérdida de información y de equipos	Incierto	Catastrófico	Alto	Reducir el riesgo
R062	Equipo de Endoscopia y Colonoscopia	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R063		Ausencia de un eficiente control de cambios en la configuración	Alteraciones de las configuraciones no controladas	Mal funcionamiento de los sistemas de información puede ocasionar perdidas.	Incierto	Moderado	Bajo	Retener el riesgo
R064		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos y perdida de datos	Caída del servicio y daños en los componentes electrónicos del hardware	Posible	Alto	Alto	Reducir el riesgo
R065		Susceptibilidad a las variaciones de temperatura	Las variaciones de temperatura pueden sobrecalentar los equipos	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Incierto	Catastrófico	Alto	Reducir el riesgo
R066		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo

R067		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Incierto	Alto	Medio	Retener el riesgo
R068		Interfaz de usuario compleja	Dificultad para el usuario al utilizar el sistema	Errores y fallos en la ejecución de tareas	Incierto	Moderado	Bajo	Retener el riesgo
R069		Configuración incorrecta de parámetros	Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Deficiencia en la parte operativa o resultados erróneos que afectan a la toma de decisiones.	Posible	Importante	Medio	Retener el riesgo
R070		Ausencia del personal	Falta de operaciones para operatividad	Interrupción y retrasos en su operatividad	Posible	Importante	Medio	Retener el riesgo
R071		Habilitación de servicios innecesarios	Usos indebidos de servicios habilitados	Violación de políticas de privacidad y cumplimiento	Posible	Alto	Alto	Reducir el riesgo
R072		Descarga y usos no controlados de software	Instalación de programas y aplicaciones no autorizadas	Aplicaciones y software maliciosos que afecten la integridad que comprometan a la empresa.	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R073		Falla en la producción de informes de gestión	Datos de los informes no se registran correctamente.	Toma de decisiones incorrectas por falta de visibilidad de la actividad del equipo	Posible	Importante	Medio	Retener el riesgo
R074		Uso incorrecto de software y hardware	Mal uso de las herramientas	Fallos operativos y en su productividad	Alta Probabilidad	Moderado	Medio	Retener el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R075	Equipo de Colposcopia	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R076		Ausencia de un eficiente control de cambios en la configuración	Cambios no supervisados en la configuración	Errores y fallos en la ejecución de tareas	Posible	Moderado	Medio	Retener el riesgo
R077		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos y perdida de datos	Caída del servicio y daños en los componentes electrónicos del hardware	Posible	Alto	Alto	Reducir el riesgo
R078		Ausencia del personal	Falta de operaciones para operatividad	Interrupción y retrasos en su operatividad	Posible	Importante	Medio	Retener el riesgo
R079		Habilitación de servicios innecesarios	Usos indebidos de servicios habilitados	Violación de políticas de privacidad y cumplimiento	Posible	Alto	Alto	Reducir el riesgo
R080		Descarga y usos no controlados de software	Instalación de programas y aplicaciones no autorizadas	Aplicaciones y software maliciosos que afecten la integridad que comprometan a la empresa.	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R081		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R082	Equipo de Tomografía	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R083		Ausencia de un eficiente control de cambios en la configuración	Cambios no supervisados en la configuración	Errores y fallos en la ejecución de tareas	Posible	Moderado	Medio	Retener el riesgo
R084		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos y perdida de información.	Caída del servicio y daños en los componentes electrónicos del hardware	Posible	Alto	Alto	Reducir el riesgo
R085		Susceptibilidad a las variaciones de temperatura	Las variaciones de temperatura pueden sobrecalentar los equipos	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Incierto	Catastrófico	Alto	Reducir el riesgo
R086		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Catastrófico	Alto	Reducir el riesgo
R087		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Incierto	Alto	Medio	Retener el riesgo

R088		Interfaz de usuario compleja	Dificultad para el usuario al utilizar el sistema	Errores y fallos en la ejecución de tareas	Incierto	Moderado	Bajo	Retener el riesgo
R089		Configuración incorrecta de parámetros	Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Deficiencia en la parte operativa o resultados erróneos que afectan a la toma de decisiones.	Posible	Importante	Medio	Retener el riesgo
R090		Ausencia del personal	Falta de operaciones para operatividad	Interrupción y retrasos en su operatividad	Posible	Importante	Medio	Retener el riesgo
R091		Habilitación de servicios innecesarios	Usos indebidos de servicios habilitados	Violación de políticas de privacidad y cumplimiento	Posible	Alto	Alto	Reducir el riesgo
R092		Descarga y usos no controlados de software	Instalación de programas y aplicaciones no autorizadas	Aplicaciones y software maliciosos que afecten la integridad que comprometan a la empresa.	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R093		Falla en la producción de informes de gestión	Datos de los informes no se registran correctamente.	Toma de decisiones incorrectas por falta de visibilidad de la actividad del equipo	Posible	Importante	Medio	Reducir el riesgo
R094		Uso incorrecto de software y hardware	Mal uso de las herramientas	Fallos operativos y en su productividad	Posible	Moderado	Medio	Reducir el riesgo
R095		Sensibilidad a la radiación electromagnética	Interferencia o daños en los equipos	Mal funcionamiento de equipos	Rara Vez	Alto	Bajo	Retener el riesgo
R096		Ausencia de protección física de la edificación, puertas y ventanas	Robo de información y de equipos	Perdida de datos confidenciales y de equipos	Posible	Moderado	Medio	Retener el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R097	Equipos de Laboratorio	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Fallos en el hardware que puede resultar en pérdidas de datos	Hardware no disponible y fallo en la disponibilidad de software que llevaría a perdida de datos	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R098		Ausencia de un eficiente control de cambios en la configuración	Cambios no supervisados en la configuración	Errores y fallos en la ejecución de tareas	Posible	Moderado	Medio	Retener el riesgo
R099		Susceptibilidad a las variaciones de voltaje	Variaciones de voltaje pueden causar daños en los equipos de Hardware y perdida de información.	Caída del servicio y daños en los componentes electrónicos del hardware	Posible	Alto	Alto	Reducir el riesgo
R100		Susceptibilidad a las variaciones de temperatura	Las variaciones de temperatura pueden sobrecalentar los equipos	Equipos expuestos a los daños físicos y perdida de funcionabilidad	Posible	Catastrófico	Alto	Reducir el riesgo
R101		Almacenamiento sin protección	Documentos pueden ser hurtados	Perdida de información sensible y confidencial	Incierto	Alto	Medio	Retener el riesgo
R102		Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Alteración de información sensible que comprometan a la integridad del sistema.	Probable	Alto	Alto	Reducir el riesgo
R103		Interfaz de usuario compleja	Dificultad para el usuario al utilizar el sistema	Errores y fallos en la ejecución de tareas	Posible	Importante	Medio	Retener el riesgo

R104		Habilitación de servicios innecesarios	Usos indebidos de servicios habilitados	Violación de políticas de privacidad y cumplimiento	Posible	Alto	Alto	Reducir el riesgo
R105		Ausencia de copias de respaldo	Perdida definitiva de información	Perdida de información crítica y manipulación de datos	Posible	Alto	Alto	Reducir el riesgo
R106		Falla en la producción de informes de gestión	Acceso no controlado de los equipos de oficina	Mal uso de recursos	Posible	Alto	Alto	Reducir el riesgo
R107		Ausencia de pruebas de envío o recepción de mensajes	Fallos al enviar o recepción de comunicación	Dificultad para identificar problemas de comunicación	Rara Vez	Importante	Bajo	Retener el riesgo
R108		Arquitectura insegura de la red	Acceso no autorizado a información confidencial	Robo de información, espionaje o violación a la privacidad	Incierto	Catastrófico	Alto	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R109		Ausencia del personal	Falta de operaciones para operatividad	Interrupción y retrasos en su operatividad	Posible	Importante	Medio	Retener el riesgo
R110		Uso incorrecto de software y hardware	Mal uso de las herramientas	Fallos operativos y en su productividad	Posible	Moderado	Medio	Retener el riesgo
R111		Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso indebido de los equipos de la empresa	Mal uso y perdida de información confidencial	Posible	Alto	Alto	Reducir el riesgo
R112	Historia Clínica Digital	Copia no controlada	Duplicidad de documentos o medios electrónicos	Divulgación y perdida de información	Probable	Alto	Alto	Reducir el riesgo
R113		Fechas incorrectas	Fechas incorrectas afectan el proceso de la información	Fallos en los reportes	Probable	Bajo	Bajo	Retener el riesgo
R114		Ausencia de copias de respaldo	Perdida definitiva de información	Perdida de información crítica	Posible	Alto	Alto	Reducir el riesgo
R115		Falla en la producción de informes de gestión	Acceso no controlado de los equipos de oficina	Mal uso de recursos	Probable	Alto	Alto	Reducir el riesgo
R116		Falta de conciencia acerca de la seguridad	Uso indebido de los sistemas de información	Perdida de datos	Posible	Alto	Alto	Reducir el riesgo
R117		Ausencia de procedimiento formal para la autorización de la información disponible al público	Divulgación de información incorrecta o comprometida	Riesgos reputacionales, uso de información no verificada	Alta Probabilidad	Alto	Critico	Reducir el riesgo
R118		Ausencia de procedimientos de identificación y valoración de riesgos	Vulnerabilidades no detectadas	Uso indebido de recursos	Incierto	Importante	Medio	Retener el riesgo
R119		Uso incorrecto de software y hardware	Mal uso de las herramientas	Fallos operativos y en su productividad	Posible	Moderado	Medio	Retener el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R120	Formularios de Historia Clínica Ocupacional	Copia no controlada	Duplicidad de documentos o medios electrónicos	Divulgación y perdida de información	Probable	Alto	Alto	Reducir el riesgo
R121		Fechas incorrectas	Fechas incorrectas afectan el proceso de la información	Fallos en los reportes	Probable	Bajo	Bajo	Retener el riesgo
R122		Ausencia de copias de respaldo	Perdida definitiva de información	Perdida de información crítica y manipulación de datos	Posible	Alto	Alto	Reducir el riesgo
R123		Falla en la producción de informes de gestión	Acceso no controlado de los equipos de oficina	Mal uso de recursos	Probable	Alto	Alto	Reducir el riesgo
R124		Falta de conciencia acerca de la seguridad	Uso indebido de los sistemas de información	Perdida de datos	Posible	Alto	Alto	Reducir el riesgo
R125		Ausencia de procedimiento formal para la autorización de la información disponible al público	Divulgación de información incorrecta o comprometida	Riesgos reputacionales, uso de información no verificada	Alta Probabilidad	Catastrófico	Critico	Reducir el riesgo
R126		Ausencia de procedimientos de identificación y valoración de riesgos	Vulnerabilidades no detectadas	Uso indebido de recursos	Incierto	Importante	Medio	Retener el riesgo
R127		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Robo de documentos confidenciales expuesto en lugar publico	Robo de documentación confidencial no autorizada	Probable	Catastrófico	Critico	Reducir el riesgo
R128		Ausencia de autorización de los recursos de procesamiento de la información	Uso no autorizado de recursos	Información expuesta en lugar publico y mal uso de recursos	Probable	Alto	Alto	Reducir r el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R129	Consentimientos Informados	Copia no controlada	Duplicidad de documentos o medios electrónicos	Divulgación y perdida de información	Probable	Catastrófico	Critico	Reducir el riesgo
R130		Fechas incorrectas	Fechas incorrectas afectan el proceso de la información	Fallos en los reportes	Probable	Bajo	Bajo	Retener el riesgo
R131		Ausencia de copias de respaldo	Perdida definitiva de información	Perdida de información crítica y manipulación de datos	Posible	Alto	Alto	Reducir el riesgo
R132		Falla en la producción de informes de gestión	Acceso no controlado de los equipos de oficina	Mal uso de recursos	Probable	Alto	Alto	Reducir el riesgo
R133		Falta de conciencia acerca de la seguridad	Uso indebido de los sistemas de información	Perdida de datos	Posible	Alto	Alto	Reducir el riesgo
R134		Ausencia de procedimiento formal para la autorización de la información disponible al público	Divulgación de información incorrecta o comprometida	Riesgos reputacionales, uso de información no verificada	Alta Probabilidad	Alto	Critico	Reducir el riesgo
R135		Ausencia de procedimientos de identificación y valoración de riesgos	Vulnerabilidades no detectadas	Uso indebido de recursos	Incierto	Catastrófico	Alto	Reducir el riesgo
R136		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Robo de documentos confidenciales expuesto en lugar publico	Robo de documentación confidencial no autorizada	Probable	Catastrófico	Critico	Reducir el riesgo
R137		Ausencia de autorización de los recursos de procesamiento de la información	Uso no autorizado de recursos	Información expuesta en lugar público y mal uso de recursos	Probable	Alto	Alto	Reducir el riesgo
R138		Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	No detección de accesos no autorizados	Pérdida de información sensible, violación de la seguridad	Posible	Alto	Alto	Reducir el riesgo

ID RIESGO	ACTIVO	VULNERABILIDAD	RIESGO	CONSECUENCIA	PROB.	IMPACTO	CRITICIDAD	TRATAMIENTO
R139	Hoja de Interconsulta	Copia no controlada	Duplicidad de documentos o medios electrónicos	Divulgación y perdida de información	Probable	Catastrófico	Critico	Reducir el riesgo
R140		Fechas incorrectas	Fechas incorrectas afectan el proceso de la información	Fallos en los reportes	Rara vez	Bajo	Bajo	Retener el riesgo
R141		Ausencia de copias de respaldo	Perdida definitiva de información	Perdida de información crítica y manipulación de datos	Posible	Alto	Alto	Reducir el riesgo
R142		Falla en la producción de informes de gestión	Acceso no controlado de los equipos de oficina	Mal uso de recursos	Probable	Importante	Alto	Reducir el riesgo
R143		Falta de conciencia acerca de la seguridad	Uso indebido de los sistemas de información	Perdida de datos	Posible	Importante	Medio	Retener el riesgo
R144		Ausencia de procedimiento formal para la autorización de la información disponible al público	Divulgación de información incorrecta o comprometida	Riesgos reputacionales, uso de información no verificada	Alta Probabilidad	Alto	Critico	Reducir el riesgo
R145		Ausencia de procedimientos de identificación y valoración de riesgos	Vulnerabilidades no detectadas	Uso indebido de recursos	Incierto	Catastrófico	Alto	Reducir el riesgo
R146		Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Robo de documentos confidenciales expuesto en lugar publico	Robo de documentación confidencial no autorizada	Probable	Catastrófico	Critico	Reducir el riesgo
R147		Ausencia de autorización de los recursos de procesamiento de la información	Uso no autorizado de recursos	Información expuesta en lugar público y mal uso de recursos	Probable	Alto	Alto	Reducir el riesgo

Tabla 9 Identificación de amenazas y criterio de valoración

Identificación de Controles

ID RIESGO	ACTIVO	RIESGO	DOMINIOS	CRITICIDAD	CONTROLES ISO 27002:2013
R001	Sistema web Gamma Smart 2.0	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Dom: 9 Control de Acceso	Alto	**9.4.3 Gestión de contraseñas de usuario.:** Las contraseñas de los sistemas de información deben ser fiables con caracteres especiales y longitud máxima. **9.4.2 Procedimientos seguros de inicio de sesión.:** Asegurar que los usuarios inicien sesión de forma correcta y así minimizar para que usuarios no identificados accedan al sistema.
R002		Datos de los informes no se registran correctamente.	Dom: 12 Seguridad en la operatividad	Alto	**12.4.1 Registro y gestión de eventos de actividad.:** Implementar mecanismos de validación y verificación de datos que aseguren que los informes se registren correctamente. **12.1.1 Documentación de procedimientos de operación**: Asegurar que toda la documentación este correctamente registrada que detallen como generar y registrar los informes
R004		Los parámetros mal configurados llevan a un mal funcionamiento del sistema.	Dom: 12 Seguridad en la operatividad Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Alto	**12.1 Responsabilidades y procedimientos de operación.** **12.1.2 Gestión de cambios:** Crear unas políticas de gestión de cambios que incluya la revisión y aprobación de todas las configuraciones antes de aplicar cambios. **14.2.2 Procedimientos de control de cambios en los sistemas:** Implementar procedimientos para documentar y revisar las modificaciones en la configuración del sistema, asegurando que los parámetros establecidos y configurados funcionen de manera correcta sin causar algún tipo de fallo

R005		Contraseñas cortas, débiles que pueden ayudar al atacante a obtener acceso y hacerse pasar por un usuario no autorizado.	Dom: 9 Control de Acceso	Critico	**9.4.3 Gestión de contraseñas de usuario.:** Las contraseñas de los sistemas de información deben ser fiables con caracteres especiales y longitud máxima. **9.4.2 Procedimientos seguros de inicio de sesión.:** Aplicar métodos de bloqueo o inactivación de cuenta después de un numero de intentos fallidos, esto reduce el acceso de usuarios no autorizados.
R007	Bases de datos	Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Dom: 9 Control de Acceso	Alto	**9.4.3 Gestión de contraseñas de usuario.:** Las contraseñas de los sistemas de información deben ser fiables con caracteres especiales y longitud máxima. **9.4.2 Procedimientos seguros de inicio de sesión.:** Asegurar que los usuarios inicien sesión de forma correcta y así minimizar para que usuarios no identificados accedan al sistema.
R008		Usuarios con accesos y permisos excesivos	Dom: 9 Control de Acceso	Alto	**9.2.5 Revisión de los derechos de acceso de los usuarios.:** Revisar periódicamente los derechos de accesos de los usuarios para evitar que tengan accesos de permisos excesivos y solo tengan accesos a las funciones necesarias para desarrollar sus actividades.
R011		Acceso de contraseñas sin protección y a los sistemas de información.	Dom: 9 Control de Acceso Dom: 10 Cifrado	Crítico	**9.4.1 Restricción del acceso a la información.:** Restringir el acceso a los sistemas de información y datos sensibles de usuarios no autorizados y configuración para así evitar manipulación de información crítica. **10.1.1 Política de uso de los controles criptográficos.:** Aplicar criptografía para proteger contraseñas e información confidencial que vayan en tráfico de red e incluir protocolos seguros como TLS para la transmisión de contraseñas, modo que las contraseñas no sean accesibles con facilidad.

R012		Contraseñas cortas, débiles que pueden ayudar al atacante a obtener acceso y hacerse pasar por un usuario no autorizado.	Dom: 9 Control de Acceso	Critico	**9.4.3 Gestión de contraseñas de usuario.:** Las contraseñas de los sistemas de información deben ser fiables con caracteres especiales y longitud máxima. **9.4.2 Procedimientos seguros de inicio de sesión.:** Asegurar que los usuarios inicien sesión de forma correcta y así minimizar para que usuarios no identificados accedan al sistema.
R014		Configuración incorrecta altera y afecta la productividad del software	Dom: 12 Seguridad en la operatividad	Alto	**12.1.1 Documentación de procedimientos de operación**: Asegurar que toda la documentación este correctamente registrada que detallen como generar y registrar los informes. **12.1.2 Gestión de cambios:** Crear unas políticas de gestión de cambios que incluya la revisión y aprobación de todas las configuraciones antes de aplicar cambios.
R015	Servidor de Correo Electrónico	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Alto	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar perdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R016		Equipos de Hardware expuesto a la corrosión y suciedad	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad.
R017		Variaciones de voltaje pueden causar daños en los equipos y perdida de información.	Dom: 11. Seguridad física y ambiental.	Critico	**11.2.2 Instalaciones de suministro:** Instalar en los equipos de cómputo, servidores, UPS y reguladores de voltaje para estabilizar la

			Dom: 12 Seguridad en la operatividad		alimentación eléctrica y salvaguardar los equipos de fluctuaciones y tensiones en la energía. **12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R018		Susceptibilidad a las variaciones de temperatura	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R019		Documentos pueden ser hurtados	Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de activos que se movilicen fuera de la empresa y así evitar posibles robos de información.

R021	Red de comuni-cación	Captura de paquetes de datos durante el tráfico de red	Dom: 13. Seguridad en las telecomunicaciones. Dom: 10. Cifrado.	Alto	**13.1.1 Controles de red:** Implementar controles de seguridad en la red, usar firewall, sistemas de detección y prevención de intrusiones, limitar el uso de acceso no autorizado, adicional monitorear los comportamientos inusuales que puedan indicar intentos de interceptación de datos. **10.1.1 Política de uso de los controles criptográficos.:** Aplicar criptografía para proteger contraseñas e información confidencial que vayan en tráfico de red e incluir protocolos seguros como TLS para la transmisión de contraseñas, modo que las contraseñas no sean accesibles con facilidad.
R023		Usuarios no autorizados pueden acceder a los sistemas de información	Dom: 9 Control de Acceso	Alto	**9.4.1 Restricción del acceso a la información.:** Restringir el acceso a los sistemas de información y datos sensibles de usuarios no autorizados y configuración para así evitar manipulación de información crítica. **9.2.1 Gestión de altas/bajas en el registro de usuarios:** Crear procedimientos para la creación, modificación y eliminación de cuentas de usuarios.
R024		Acceso no autorizado a través de vulnerabilidades	Dom: 9 Control de Acceso Dom: 12 Seguridad en la operatividad	Alto	**12.6.1 Gestión de las vulnerabilidades técnicas:** Realizar análisis de vulnerabilidades, aplicar parches de seguridad y actualizaciones de software. **9.2.5 Revisión de los derechos de acceso de los usuarios.:** Revisar periódicamente los derechos de accesos de los usuarios para evitar que tengan accesos de permisos excesivos y solo tengan accesos a las funciones necesarias para desarrollar sus actividades.

R026		Acceso no autorizado de dispositivos a redes publicas	Dom: 13. Seguridad en las telecomunicaciones. Dom: 6. Aspectos organizativos de la seguridad de la información		**13.1.1 Controles de red:** Implementar controles de seguridad en la red, usar firewall, sistemas de detección y prevención de intrusiones, limitar el uso de acceso no autorizado, adicional monitorear los comportamientos inusuales que puedan indicar intentos de interceptación de datos. **6.2.1 Política de uso de dispositivos para movilidad:** Crear políticas sobre el uso de dispositivos móviles y personales que contenga el uso de medidas de seguridad, monitorear dispositivos conectados y establecer limites de acceso a las redes publicas
R027	Backups	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Alto	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R028		Equipos de Hardware expuesto a la corrosión y suciedad	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad.
R029		Variaciones de voltaje pueden causar daños en los equipos y perdida de información.	Dom: 11. Seguridad física y ambiental. Dom: 12 Seguridad en la operatividad	Critico	**11.2.2 Instalaciones de suministro:** Instalar en los equipos de cómputo, servidores, UPS y reguladores de voltaje para estabilizar la alimentación eléctrica y salvaguardar los equipos de fluctuaciones y tensiones en la energía.

					. **12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R030		Documentos pueden ser hurtados	Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de activos que se movilicen fuera de la empresa y así evitar posibles robos de información.
R031		Duplicidad de documentos o medios electrónicos	Dom: 8. Gestión de activos. Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios. **14.1.1 Análisis y especificación de los requisitos de seguridad:** Crear procedimientos de análisis para la creación de almacenamiento de datos y eliminación de documentos de copias redundantes asegurando que existan documentos necesarios y actualizados lo que ayuda a reducir la duplicidad de información

R032		Perdida de información	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R033	Software de facturación	Explotación de vulnerabilidades	Dom: 12 Seguridad en la operatividad	Alto	**12.6.1 Gestión de las vulnerabilidades técnicas:** Realizar análisis de vulnerabilidades, aplicar parches de seguridad y actualizaciones de software. **12.5.1 Instalación del software en sistemas en producción:** Asegurar que solo el software autorizado sea instalado en los sistemas de producción e implementar controles y revisiones de seguridad ante las instalaciones de nuevo software para prevenir la explotación de vulnerabilidad derivadas de un software no autorizado o malicioso
R039		Inestabilidad y falta de pruebas de errores del software	Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Alto	**Control: 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas:** Asegurar que todas las funciones del sistema se prueben en escenarios reales y de producción para identificar posibles fallos antes de la implementación. **Control: 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo:** Realizar revisiones técnicas del sistema después de realizar cualquier modificación, esto asegura que el sistema se vea afectado por errores o inestabilidad.
R040		Dificultad al crear usuarios o eliminar cuentas de usuario	Dom: 9 Control de Acceso	Alto	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Crear procedimientos para la creación, modificación y eliminación de cuentas de usuarios.
R041	Software de inventario	Explotación de vulnerabilidades	Dom: 12 Seguridad en la operatividad	Alto	**12.6.1 Gestión de las vulnerabilidades técnicas:** Realizar análisis de vulnerabilidades, aplicar parches de seguridad y actualizaciones de software.

					12.5.1 Instalación del software en sistemas en producción: Asegurar que solo el software autorizado sea instalado en los sistemas de producción e implementar controles y revisiones de seguridad ante las instalaciones de nuevo software para prevenir la explotación de vulnerabilidad derivadas de un software no autorizado o malicioso
R046		Perdida de datos debido a errores o fallas en el sistema	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R047	Servidor local de facturación	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Critico	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R048		Equipos de Hardware expuesto a la corrosión y suciedad	Dom: 11. Seguridad física y ambiental.	Critico	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad.
R050		Las variaciones de temperatura pueden sobrecalentar los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad.

					11.2.1 Emplazamiento y protección de equipos: Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R051		Documentos pueden ser hurtados	Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de activos que se movilicen fuera de la empresa y así evitar posibles robos de información.
R052	Compu-tadoras Laptops	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Alto	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R054		Daño físico a los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.

					Control: 11.1.1 Perímetro de seguridad física: Establecer un perímetro de seguridad física con barreras, sistemas de vigilancia y controles de acceso para evitar accesos de personas no autorizadas y que puedan causar daños a los equipos
R055		Daño físico a los equipos y mal funcionamiento de los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID. **Control: 11.1.1 Perímetro de seguridad física:** Establecer un perímetro de seguridad física con barreras, sistemas de vigilancia y controles de acceso para evitar accesos de personas no autorizadas y que puedan causar daños a los equipos
R057		Equipos de Hardware expuesto a la corrosión y suciedad	Dom: 11. Seguridad física y ambiental.	Critico	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad.
R059		Las variaciones de temperatura pueden sobrecalentar los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R060			Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso

		Documentos pueden ser hurtados			restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de activos que se movilicen fuera de la empresa y así evitar posibles robos de información.
R061		Robo o extravío de equipos portátiles	Dom: 11. Seguridad física y ambiental. Dom: 8 Gestión de activos	Alto	**Control: 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones:** Crear políticas y procedimientos para el uso de movilización de equipos portátiles fuera de la organización y crear políticas de seguimiento remoto en caso de robo o perdida. **Control: 8.3.2 Eliminación de soportes:** **A**segurarse que cualquier tipo de información que este almacenada en dispositivos portátiles este cifrada y que se pueda eliminar remotamente en caso de que se pueda extraviar o que se roben el dispositivo.
R062	Equipo de endoscopia y colonos copia	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Critico	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.

R064		Variaciones de voltaje pueden causar daños en los equipos y perdida de datos	Dom: 11. Seguridad física y ambiental. Dom: 12 Seguridad en la operatividad	Alto	**11.2.2 Instalaciones de suministro:** Instalar en los equipos de cómputo, servidores, UPS y reguladores de voltaje para estabilizar la alimentación eléctrica y salvaguardar los equipos de fluctuaciones y tensiones en la energía. **12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R065		Las variaciones de temperatura pueden sobrecalentar los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R066		Documentos pueden ser hurtados	Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este

					autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de activos que se movilicen fuera de la empresa y así evitar posibles robos de información.
R071		Usos indebidos de servicios habilitados	Dom: 9 Control de Acceso	Alto	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Crear procedimientos para la creación, modificación y eliminación de cuentas de usuarios.
R072	Equipo de colpos-copia	Instalación de programas y aplicaciones no autorizadas	Dom: 12 Seguridad en la operatividad	Alto	**12.6.2 Restricciones en la instalación de software:** Crear políticas que restrinjan la instalación de sistemas o software no autorizados y controlar los sistemas instalados en los sistemas. **12.5.1 Instalación del software en sistemas en producción:** Asegurar que solo el software autorizado sea instalado en los sistemas de producción e implementar controles y revisiones de seguridad ante las instalaciones de nuevo software para prevenir la explotación de vulnerabilidad derivadas de un software no autorizado o malicioso
R075		Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Critico	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R077		Variaciones de voltaje pueden causar daños en los equipos y perdida de datos	Dom: 11. Seguridad física y ambiental. Dom: 12 Seguridad en la operatividad	Alto	**11.2.2 Instalaciones de suministro:** Instalar en los equipos de cómputo, servidores, UPS y reguladores de voltaje para estabilizar la alimentación eléctrica y salvaguardar los equipos de fluctuaciones y tensiones en la energía.

					12.3.1 Copias de seguridad de la información: Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R079		Usos indebidos de servicios habilitados	Dom: 9 Control de Acceso	Alto	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Crear procedimientos para la creación, modificación y eliminación de cuentas de usuarios.
R080		Instalación de programas y aplicaciones no autorizadas	Dom: 12 Seguridad en la operatividad	Critico	**12.6.2 Restricciones en la instalación de software:** Crear políticas que restrinjan la instalación de sistemas o software no autorizados y controlar los sistemas instalados en los sistemas. **12.5.1 Instalación del software en sistemas en producción:** Asegurar que solo el software autorizado sea instalado en los sistemas de producción e implementar controles y revisiones de seguridad ante las instalaciones de nuevo software para prevenir la explotación de vulnerabilidad derivadas de un software no autorizado o malicioso
R081		Documentos pueden ser hurtados	Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de

					activos que se movilicen fuera de la empresa y así evitar posibles robos de información.
R082	Equiipo de tomogra-fia	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad Dom: 11. Seguridad física y ambiental.	Critico	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R084		Variaciones de voltaje pueden causar daños en los equipos y perdida de información.	Dom: 11. Seguridad física y ambiental. Dom: 12 Seguridad en la operatividad	Alto	**11.2.2 Instalaciones de suministro:** Instalar en los equipos de cómputo, servidores, UPS y reguladores de voltaje para estabilizar la alimentación eléctrica y salvaguardar los equipos de fluctuaciones y tensiones en la energía. **12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R085		Las variaciones de temperatura pueden sobrecalentar los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.

R086		Documentos pueden ser hurtados	Dom: 8. Gestión de activos. Dom: 11. Seguridad física y ambiental.	Alto	**8.2.3 Manipulación de activos** Crear políticas para el uso y almacenamiento de documentos asegurando que estén protegidos mediante cifrado y con el acceso restringido y controlado, estos documentos deben estar en sitios seguros ya sea en cajas fuertes o gabinetes, gavetas archivadoras con cerraduras para evitar el acceso no autorizado y mitigar el hurto **11.2.5 Salida de activos fuera de las dependencias de la empresa** Crear políticas que regulen la movilización de documentos físicos fueras de las instalaciones de la organización y que solo el personal que este autorizado tenga permiso para poder realizarlo. Implementar un sistema de monitoreo y registros de activos que se movilicen fuera de la empresa y así evitar posibles robos de información.
R091		Usos indebidos de servicios habilitados	Dom: 9 Control de Acceso	Alto	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Crear procedimientos para la creación, modificación y eliminación de cuentas de usuarios.
R092		Instalación de programas y aplicaciones no autorizadas	Dom: 12 Seguridad en la operatividad	Critico	**12.6.2 Restricciones en la instalación de software:** Crear políticas que restrinjan la instalación de sistemas o software no autorizados y controlar los sistemas instalados en los sistemas. **12.5.1 Instalación del software en sistemas en producción:** Asegurar que solo el software autorizado sea instalado en los sistemas de producción e implementar controles y revisiones de seguridad ante las instalaciones de nuevo software para prevenir la explotación de vulnerabilidad derivadas de un software no autorizado o malicioso
R097	Equipos de laboratorio	Fallos en el hardware que puede resultar en pérdidas de datos	Dom: 12 Seguridad en la operatividad	Critico	**12.3.1 Copias de seguridad de la información.:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias

			Dom: 11. Seguridad física y ambiental.		de seguridad se deben almacenar en lugares seguras y separadas del hardware principal. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R099		Variaciones de voltaje pueden causar daños en los equipos de Hardware y perdida de información.	Dom: 11. Seguridad física y ambiental. Dom: 12 Seguridad en la operatividad	Alto	**11.2.2 Instalaciones de suministro:** Instalar en los equipos de cómputo, servidores, UPS y reguladores de voltaje para estabilizar la alimentación eléctrica y salvaguardar los equipos de fluctuaciones y tensiones en la energía. **12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R100		Las variaciones de temperatura pueden sobrecalentar los equipos	Dom: 11. Seguridad física y ambiental.	Alto	**11.1.4 Protección contra las amenazas externas y ambientales:** Realizar controles ambientales en áreas donde estén los equipos críticos, estas áreas deben estar con sistema de climatización, deshumificadores y filtros de aires para reducir los niveles de humedad polvo y suciedad. **11.2.1 Emplazamiento y protección de equipos:** Ubicar los equipos de nivel crítico en áreas con protección física y seguras e implementar servidores en alta disponibilidad o en almacenamiento RAID.
R102		Usuario no autorizado puede acceder al sistema con privilegios con la sesión abierta.	Dom: 9 Control de Acceso	Alto	**9.4.3 Gestión de contraseñas de usuario.:** Las contraseñas de los sistemas de información deben ser fiables con caracteres especiales y longitud máxima. **9.4.2 Procedimientos seguros de inicio de sesión.:** Asegurar que los usuarios inicien sesión de forma

					correcta y así minimizar para que usuarios no identificados accedan al sistema.
R104		Usos indebidos de servicios habilitados	Dom: 9 Control de Acceso	Alto	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Crear procedimientos para la creación, modificación y eliminación de cuentas de usuarios.
R105		Perdida definitiva de información	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R106		Acceso no controlado de los equipos de oficina	Dom: 11. Seguridad física y ambiental.	Alto	**Control: 11.1.1 Perímetro de seguridad física:** Establecer perímetros de seguridad que limite el acceso a los equipos de oficina esto puede incluir cercas, sistema de control de acceso y vigilancia para evitar el acceso no autorizado de usuarios no autorizados **Control: 11.1.2 Controles físicos de entrada:** Crear controles de acceso físico como tarjetas, biométricos o cerraduras eléctricas para restringir el acceso a lugares prohibido o áreas sensibles.
R108		Acceso no autorizado a información confidencial	Dom: 9 Control de Acceso	Alto	**9.2.5 Revisión de los derechos de acceso de los usuarios.:** Revisar periódicamente los derechos de accesos de los usuarios para evitar que tengan accesos de permisos excesivos y solo tengan accesos a las funciones necesarias para desarrollar sus actividades. **Control: 9.1.1 Política de control de accesos: Crear políticas de usos y de control de accesos que** defina a los usuarios que roles y permisos puedan tener.
R111		Uso indebido de los equipos de la empresa	Dom: 8. Gestión de activos.	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga

					una copia oficial y se minimice el riesgo de duplicados incensarios.
R112	Historia clinica digital	Duplicidad de documentos o medios electrónicos	Dom: 8. Gestión de activos. Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios. **14.1.1 Análisis y especificación de los requisitos de seguridad:** Crear procedimientos de análisis para la creación de almacenamiento de datos y eliminación de documentos de copias redundantes asegurando que existan documentos necesarios y actualizados lo que ayuda a reducir la duplicidad de información
R114		Perdida definitiva de información	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R115		Acceso no controlado de los equipos de oficina	Dom: 11. Seguridad física y ambiental.	Alto	**Control: 11.1.1 Perímetro de seguridad física:** Establecer perímetros de seguridad que limite el acceso a los equipos de oficina esto puede incluir cercas, sistema de control de acceso y vigilancia para evitar el acceso no autorizado de usuarios no autorizados **Control: 11.1.2 Controles físicos de entrada:** Crear controles de acceso físico como tarjetas, biométricos o cerraduras eléctricas para restringir el acceso a lugares prohibido o áreas sensibles.
R116		Uso indebido de los sistemas de información	Dom: 8. Gestión de activos.	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga

					una copia oficial y se minimice el riesgo de duplicados incensarios.
R117		Divulgación de información incorrecta o comprometida	Dom: 12 Seguridad en la operatividad	Critico	**12.4.1 Registro y gestión de eventos de actividad.:** Implementar mecanismos de validación y verificación de datos que aseguren que los informes se registren correctamente. **Control: 18.1.4 Protección de datos y privacidad de la información personal:** Crear políticas sobre manejo de información y clasificación, se debe proporcionar capacitación a los empleados sobre la importancia de la protección de datos y su consecuencia en caso de divulgación.
R120	Formularios de Historia Clínica Ocupacional	Duplicidad de documentos o medios electrónicos	Dom: 8. Gestión de activos. Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios. **14.1.1 Análisis y especificación de los requisitos de seguridad:** Crear procedimientos de análisis para la creación de almacenamiento de datos y eliminación de documentos de copias redundantes asegurando que existan documentos necesarios y actualizados lo que ayuda a reducir la duplicidad de información
R122		Perdida definitiva de información	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R123		Acceso no controlado de los equipos de oficina	Dom: 11. Seguridad física y ambiental.	Alto	**Control: 11.1.1 Perímetro de seguridad física:** Establecer perímetros de seguridad que limite el acceso a los equipos de oficina esto puede incluir cercas, sistema de control de acceso y vigilancia para

					evitar el acceso no autorizado de usuarios no autorizados **Control: 11.1.2 Controles físicos de entrada:** Crear controles de acceso físico como tarjetas, biométricos o cerraduras eléctricas para restringir el acceso a lugares prohibido o áreas sensibles.
R124		Uso indebido de los sistemas de información	Dom: 8. Gestión de activos.	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios.
R125		Divulgación de información incorrecta o comprometida	Dom: 12 Seguridad en la operatividad	Critico	**12.4.1 Registro y gestión de eventos de actividad.:** Implementar mecanismos de validación y verificación de datos que aseguren que los informes se registren correctamente. **Control: 18.1.4 Protección de datos y privacidad de la información personal:** Crear políticas sobre manejo de información y clasificación, se debe proporcionar capacitación a los empleados sobre la importancia de la protección de datos y su consecuencia en caso de divulgación.
R127		Robo de documentos confidenciales expuesto en lugar publico	Dom: 11. Seguridad física y ambiental.	Critico	**Control: 11.1.5 El trabajo en áreas seguras:** Crear políticas que regulen el manejo de información confidencial en departamentos o áreas públicas. **Control: 8.2.2 Etiquetado y manipulado de la información:** Asegurarse que la información de carácter confidencial este correctamente membretada y etiquetada con advertencia que es información sensible.
R128		Uso no autorizado de recursos	Dom: 12 Seguridad en la operatividad. Dom 9: Control de acceso.	Alto	**12.6.2 Restricciones en la instalación de software:** Crear políticas que restrinjan la instalación de sistemas o software no autorizados y controlar los sistemas instalados en los sistemas.

					Control: 9.1.1 Política de control de accesos: Crear políticas de usos y de control de accesos que defina a los usuarios que roles y permisos puedan tener.
R129	Consenti-mientos informados	Duplicidad de documentos o medios electrónicos	Dom: 8. Gestión de activos. Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Critico	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios. **14.1.1 Análisis y especificación de los requisitos de seguridad:** Crear procedimientos de análisis para la creación de almacenamiento de datos y eliminación de documentos de copias redundantes asegurando que existan documentos necesarios y actualizados lo que ayuda a reducir la duplicidad de información
R131		Perdida definitiva de información	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R132		Acceso no controlado de los equipos de oficina	Dom: 11. Seguridad física y ambiental.	Alto	**Control: 11.1.1 Perímetro de seguridad física:** Establecer perímetros de seguridad que limite el acceso a los equipos de oficina esto puede incluir cercas, sistema de control de acceso y vigilancia para evitar el acceso no autorizado de usuarios no autorizados **Control: 11.1.2 Controles físicos de entrada:** Crear controles de acceso físico como tarjetas, biométricos o cerraduras eléctricas para restringir el acceso a lugares prohibido o áreas sensibles.

R133		Uso indebido de los sistemas de información	Dom: 8. Gestión de activos.	Alto	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios.
R134		Divulgación de información incorrecta o comprometida	Dom: 12 Seguridad en la operatividad	Critico	**12.4.1 Registro y gestión de eventos de actividad.:** Implementar mecanismos de validación y verificación de datos que aseguren que los informes se registren correctamente. **Control: 18.1.4 Protección de datos y privacidad de la información personal:** Crear políticas sobre manejo de información y clasificación, se debe proporcionar capacitación a los empleados sobre la importancia de la protección de datos y su consecuencia en caso de divulgación.
R135		Vulnerabilidades no detectadas	Dom: 12 Seguridad en la operatividad.	Alto	**12.6.1 Gestión de las vulnerabilidades técnicas:** Realizar análisis de vulnerabilidades, aplicar parches de seguridad y actualizaciones de software.
R136		Robo de documentos confidenciales expuesto en lugar publico	Dom: 11. Seguridad física y ambiental.	Critico	**Control: 11.1.5 El trabajo en áreas seguras:** Crear políticas que regulen el manejo de información confidencial en departamentos o áreas públicas. **Control: 8.2.2 Etiquetado y manipulado de la información:** Asegurarse que la información de carácter confidencial este correctamente membretada y etiquetada con advertencia que es información sensible.
R137		Uso no autorizado de recursos	Dom: 12 Seguridad en la operatividad. Dom 9: Control de acceso.	Alto	**12.6.2 Restricciones en la instalación de software:** Crear políticas que restrinjan la instalación de sistemas o software no autorizados y controlar los sistemas instalados en los sistemas.

					Control: 9.1.1 Política de control de accesos: Crear políticas de usos y de control de accesos que defina a los usuarios que roles y permisos puedan tener.
R138		No detección de accesos no autorizados	Dom: 12 Seguridad en la operatividad.	Alto	**Control: 12.4.1 Registro y gestión de eventos de actividad:** Crear un sistema de registro de eventos donde se guarden todos los accesos a los sistemas de información incluyendo el uso de registros de auditoria para visualizar y monitorear las actividades de usuarios, accesos a sistemas críticos y cambios en la configuración.
R139	Hoja de Interconsu-ta	Duplicidad de documentos o medios electrónicos	Dom: 8. Gestión de activos. Dom: 14 Adquisición, desarrollo y mantenimiento de los sistemas de información	Critico	**8.1.3 Uso aceptable de los activos:** Crear políticas de gestión de documentos que permitan controlar versiones y limitaciones de acceso y solo contenga una copia oficial y se minimice el riesgo de duplicados incensarios. **14.1.1 Análisis y especificación de los requisitos de seguridad:** Crear procedimientos de análisis para la creación de almacenamiento de datos y eliminación de documentos de copias redundantes asegurando que existan documentos necesarios y actualizados lo que ayuda a reducir la duplicidad de información
R141		Perdida definitiva de información	Dom: 12 Seguridad en la operatividad	Alto	**12.3.1 Copias de seguridad de la información:** Realizar copias de seguridad periódicas y automáticas para evitar pérdidas de datos importantes, las copias de seguridad se deben almacenar en lugares seguras y separadas del hardware principal.
R142		Acceso no controlado de los equipos de oficina	Dom: 11. Seguridad física y ambiental.	Alto	**Control: 11.1.1 Perímetro de seguridad física:** Establecer perímetros de seguridad que limite el acceso a los equipos de oficina esto puede incluir cercas, sistema de control de acceso y vigilancia para evitar el acceso no autorizado de usuarios no autorizados

					Control: 11.1.2 Controles físicos de entrada: Crear controles de acceso físico como tarjetas, biométricos o cerraduras eléctricas para restringir el acceso a lugares prohibido o áreas sensibles.
R144		Divulgación de información incorrecta o comprometida	Dom: 12 Seguridad en la operatividad	Critico	**12.4.1 Registro y gestión de eventos de actividad.:** Implementar mecanismos de validación y verificación de datos que aseguren que los informes se registren correctamente. **Control: 18.1.4 Protección de datos y privacidad de la información personal:** Crear políticas sobre manejo de información y clasificación, se debe proporcionar capacitación a los empleados sobre la importancia de la protección de datos y su consecuencia en caso de divulgación.
R145		Vulnerabilidades no detectadas	Dom: 12 Seguridad en la operatividad.	Alto	**12.6.1 Gestión de las vulnerabilidades técnicas:** Realizar análisis de vulnerabilidades, aplicar parches de seguridad y actualizaciones de software.
R146		Robo de documentos confidenciales expuesto en lugar publico	Dom: 11. Seguridad física y ambiental.	Critico	**Control: 11.1.5 El trabajo en áreas seguras:** Crear políticas que regulen el manejo de información confidencial en departamentos o áreas públicas. **Control: 8.2.2 Etiquetado y manipulado de la información:** Asegurarse que la información de carácter confidencial este correctamente membretada y etiquetada con advertencia que es información sensible.
R147		Uso no autorizado de recursos	Dom: 12 Seguridad en la operatividad. Dom 9: Control de acceso.	Alto	**12.6.2 Restricciones en la instalación de software:** Crear políticas que restrinjan la instalación de sistemas o software no autorizados y controlar los sistemas instalados en los sistemas. **Control: 9.1.1 Política de control de accesos: Crear políticas de usos y de control de accesos que** defina a los usuarios que roles y permisos puedan tener.

Séptima Fase: Establecer políticas de gestión de seguridad de la información

Una vez que se ha realizado la matriz de riesgo y de establecer los controles se elaboran las políticas de seguridad que deberían ser implementadas en la clínica. A continuación, se listan las políticas de seguridad elaboradas:

- Política de Gestión de Contraseñas
- Política de Escritorio Limpio
- Política de Gestión de Accesos
- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de Copias de Respaldo
- Política de Gestión de Activos.
- Política de Gestión de Seguridad Física
- Política de Gestión de Dispositivos Móviles

Las siguientes políticas se pueden evidenciar desde el Anexo # 5

CONCLUSIONES

- Mediante el levantamiento de información, se pudo identificar de manera integral los riesgos de seguridad asociados a los activos de información de clínica; se concluyó que esta evaluación es esencial para proponer planes de acción efectivos que mitiguen las vulnerabilidades y aseguren la protección de datos sensibles.

- En base a los requerimientos se identificaron las vulnerabilidades y riesgos a los que están expuestos los procesos tecnológicos de la clínica, lo que permitirá a la dirección de informática priorizar acciones y mejorar la infraestructura de seguridad.

- Con la realización de una gestión de seguridad de la información establecieron controles y políticas de seguridad que son fundamentales para mitigar dichas vulnerabilidades, se concluye que la implementación y diseño de un Sistema de Gestión de Seguridad de la Información robusto es clave para fortalecer la confianza de los pacientes y la eficacia operativa de la clínica.

RECOMENDACIONES

- Llevar a cabo evaluaciones de riesgo de forma periódica para identificar nuevas amenazas y vulnerabilidades que puedan surgir en el entorno de la clínica, este proceso permitirá mantener actualizado el Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar la protección continua de los activos de información.

- Realizar capacitaciones regulares para todo el personal de la clínica sobre las políticas y procedimientos de seguridad de la información, esto asegurará que todos los empleados comprendan la importancia de la seguridad de los datos y cómo contribuir a proteger la información sensible de los pacientes.

- En una segunda versión del trabajo propuesto, implementar un sistema de monitoreo continuo y realizar auditorías internas de los controles de seguridad establecidos, esto permitirá detectar desviaciones de manera temprana y corregirlas antes de que se conviertan en incidentes de seguridad.

REFERENCIAS

A., M. I., S., P. A., & María, A. L. (30 de Abril de 2011). Fundamentos de ISO 27001 y su aplicacion en las empresas. *Scientia Et Technica, I*(47), 334-339.

Asamblea Nacional del Ecuador. (9 de Noviembre de 2021). *Ley de Proteccion de Datos Personales.* Obtenido de Registros Publicos: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/

Bach. Jácome Sanchez, A. P. (2022). *Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001*. Lima.

Bayona Ore Luz, P. Q. (2017). *Diseño e Implementación De Un Sistema De Gestión De Seguridad De La Información Para Proteger Los Activos De Información De La Clínica Medcam Perú Sac.* Lima.

Burgos, O. D., & Olmedo, M. R. (2018). Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001. *Revista Multidisciplinaria, V*(2).

Cruz-Gavilánez, Y. d., & Martinez-Santande, C. J. (2018). ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo . *Polo del Conocimiento*.

Gobierno Electronico. (s.f.). *Ciclo de Deming (PDCA)*. Recuperado el 7 de Octubre de 2024, de https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

Guevara-Vega, E. M., Delgado-Deza, J. R., & Mendoza-de-los-Santos, A. C. (2023). Vulnerabilidades y amenazas en los activos de información: una revisión sistemática. *Revista Científica de Sistemas e Informática*.

Hernández, P. C. (2010). La red de comunicación un concepto y un instrumento metodológico. *Razon y Palabra*.

Infantas, M. A. (2017). *Diseño E Implementación De Un Sistema De Gestión De Seguridad De La Información Para Proteger Los Activos De Información De La Clínica Medcam Perú Sac.* Lima.

ISO/IEC. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.* Ginebra, Suiza: International Organization for Standardization.

ISO/IEC. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad*. Obtenido de Sistemas de gestión de la seguridad de la información: https://www.iso.org/standard/27001

Jacovkis, D. (2009). El software libre: producción colectiva de conocimiento. *Revisya de Internet Derecho y Politica*.

Miguel Angel Cruz Diaz, S. F. (2017). *Diseño E Implementación De Un Sistema De Gestión De Seguridad De La Información Para Proteger Los Activos De Información De La Clínica Medcam.* Lima.

Morales Osorio, E., & López Trujillo, M. (2018). Sistemas de gestion de seguridad de la informacion para empresas KPO: una aproximacion. *Ventana Informatica*(37).

Pacheco, C. N., & Suárez, N. E. (2015). La seguridad de la información: un activo valioso de la organización.

Patricia, R. C. (2019). *Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS.* Quito.

PECB. (s.f.). *ISO/IEC 27002 Information Security Controls*. Obtenido de https://pecb.com/es/education-and-certification-for-individuals/iso-iec-27002

PECB. (s.f.). *ISO/IEC 27005 Information Security Risk Management*. Obtenido de https://pecb.com/es/education-and-certification-for-individuals/iso-iec-27005

Peka, H. (2015). La ética del hacker y el espíritu de la era de la información.

Ramirez, G. G., & Angarita, J. C. (2017). *Diseñar un sistema de gestión de la seguridad de la información (sgsi) a la empresa Unitransa s.a. ubicada en la ciudad de Bucaramanga.* Bucaramanga.

Raúl J. Martelo, J. E. (2014). *Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI).* (Vol. 26(2)). Cartagena, Colombia: Informacion Tecnologica. doi:10.4067/S0718-07642015000200015

Sampieri, R. H. (2010). *Metodologia de la Investigacion.* Mexico: Mc Graw Hill Education.

Technology, T. U. (2024). *Activos de información.* España. Obtenido de https://msmk.university/activos-de-informacion/

Troya, J. L., & Poveda, R. J. (2015). *Informe de evaluacion de seguridad en la informaicon basada en la norma ISO 27001 en el departamento de TI de una empresa de lácteos.* Guayaquil.

Velasco, W. V. (2008). Politicas y seguridad de la informaicon. *Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*.

ANEXOS

Anexo: 1 Acta de constitución del proyecto

Anexo: 2 Listado de Amenazas de acuerdo con la ISO 27005

ACTA DE CONSTITUCIÓN DEL PROYECTO

Fecha: Agosto, 1 del 2024

Lugar: Guayaquil

Nombre Del Proyecto	Diseño de un SGSI basado en la norma ISO 27001 para la dirección de TI en una prestadora de servicios clínico Gamma Smart S.A.		
Elaborado por:	Ing. Danny Chavez Yagual	Autorizado por:	Gamma Smart S. A
Objetivo:	Diseñar una propuesta de sistema de gestión de seguridad de la información mediante estándares de calidad y metodologías fundamentada en la norma ISO 27001 para el aseguramiento de confidencialidad integridad y disponibilidad de la información organizacional de la prestadora de servicios clínicos		
Alcance del Proyecto	**Áreas Afectadas:** El proyecto abarcará todas las áreas de Gamma Smart S.A. que manejan información sensible, incluyendo recursos humanos, finanzas, y desarrollo de productos. **Recursos Necesarios:** Se utilizarán recursos técnicos, humanos para el desarrollo del SGSI.		
La alta gerencia da paso a continuar con la ejecución del proyecto conforme a los objetivos y el alcance establecidos en este documento.			

Ing. Danny Chavez

GAMMA SMART S.A
PRESTADORA EXTERNA

Gerencia – Gamma Smart S.A

AMENAZAS COMUNES		
Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Anexo: 3 Listado de Vulnerabilidades

VULNERABILIDADES COMUNES	
Tipos	Ejemplos de vulnerabilidades
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.
	Ausencia de esquemas de reemplazo periódico.
	Susceptibilidad a la humedad, el polvo y la suciedad.
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencia de pistas de auditoria
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y usos no controlados de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Falla en la producción de informes de gestión
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables.
	Punto único de falla
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en un área susceptible de inundación
	Red energética inestable
	Ausencia de protección física de la edificación, puertas y ventanas
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso

	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información
	Ausencia de auditorías (supervisiones) regulares
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento del servicio
	Ausencia de acuerdos de niveles del servicio, o insuficiencia en los mismos.
	Ausencia de procedimiento de control de cambios
	Ausencia de procedimiento formal para el control de la documentación del SGSI
	Ausencia de procedimiento formal para la supervisión del registro del SGSI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso del correo electrónico
	Ausencia de procedimientos para la introducción del software en los sistemas operativos
	Ausencia de registros en las bitácoras (logs) de administrador y operario.
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla
	Ausencia de autorización de los recursos de procesamiento de la información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad
	Ausencia de revisiones regulares por parte de la gerencia
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales

Anexo: 4 Dominios, Objetivos y Controles

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Fuente: 2 ISO/IEC 27002:2013

Anexo: 5 Entrevista a los Propietarios y Responsables de la Clínica

Entrevista a los Propietarios y Responsables de la Clínica

Objetivo: Identificar los procesos clínicos, activos de información y necesidades de seguridad para el diseño del Sistema de Gestión de Seguridad de la Información (SGSI).

Sección 1: Procesos Clínicos

1. ¿Cuáles son los principales procesos clínicos que se realizan en la clínica?
2. ¿Cómo se gestionan actualmente los datos clínicos de los pacientes?
3. ¿Cuáles son los sistemas de información clave que se utilizan en la clínica para estos procesos?
4. ¿Qué tipo de información sensible se maneja durante estos procesos?

Sección 2: Gestión de la Información

5. ¿Qué sistemas de almacenamiento de información se utilizan?
6. ¿Cómo se protege actualmente la información clínica frente a pérdidas, accesos no autorizados o errores?
7. ¿Existe un respaldo regular de los datos clínicos?
8. ¿Qué medidas de control de acceso existen para proteger los datos clínicos y quién tiene acceso a ellos?

Sección 3: Seguridad de la Información

9. ¿Han experimentado algún incidente relacionado con la seguridad de la información en los últimos años?
10. ¿Cómo se maneja actualmente el acceso de personal a los sistemas de información?
11. ¿Existen políticas o procedimientos formales sobre la seguridad de la información en la clínica?
12. ¿Hay capacitación regular para el personal sobre las mejores prácticas de seguridad de la información?

Sección 4: Expectativas

13. ¿Cuáles considera que son las principales áreas de mejora en términos de seguridad de la información?
14. ¿Qué aspectos de los procesos clínicos o de los sistemas de información cree que necesitan mayor protección?
15. ¿Qué expectativas tienen respecto a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)?
16. ¿Cuál es el nivel de compromiso de la clínica para implementar políticas formales de seguridad de la información?

Anexo: 6 Política General de la Seguridad de la Información

Política General de la Seguridad de la Información

1. Introducción

Esta política establece los lineamientos fundamentales de seguridad de la información que debe adoptar la organización, abarcando la gestión de activos de información clasificados en diversas categorías. Asimismo, se definen las responsabilidades y las sanciones aplicables en caso de infracción a las normas de seguridad establecidas.

Objetivo

Establecer directrices que aseguren la protección y respaldo de los activos de información ante amenazas intencionales o accidentales, garantizando así la confidencialidad, integridad y disponibilidad de la información.

Alcance

Esta política se aplica en toda la empresa en general, incluyendo sus empleados capacitados y facultativos relacionados al puesto u otras profesiones anexas. El presente documento será analizado y modificado de acuerdo con las correcciones y cambios periódicos de la organización, como la innovación tecnológica, incorporación de nuevos servicios, reconstrucción o renovación de la infraestructura, etc.

2. Generalidades

- Gamma Smart es una organización consciente de la importancia de proteger la información, para reducir los peligros y riesgos a los que son expuestos los activos, evitando que existan pérdidas de datos de la empresa u otros daños irreversibles. Mencionando que dentro de la legislación ecuatoriana es imprescindible salvaguardar los datos personales de los pacientes y empleados.
- El acceso a la información y su uso será acorde a las normas, estándares, reglas, y políticas internas de Gamma Smart.
- Los empleados deben estar capacitados con las políticas, estándares y normas y deberán tener conocimiento de los documentos relacionados con los datos personales y la seguridad de estos.
- Es necesario contar con una adecuada revisión del sistema y seguimiento de las operaciones para la correcta identificación de la información de los pacientes o

empleados; información detallada de las acciones realizadas, el momento y el lugar.

- Para poder prevenir estafas, errores o infracciones debe promoverse la difusión de la información fomentando una cultura de la seguridad de la información entre los trabajadores internos de la organización y solo se podrá acceder a los datos a los que cada colaborador se encuentra autorizado.
- Se instaurarán los recursos necesarios para la protección de la identidad de las personas, software, hardware u otro documento que contenga información de Gamma Smart.
- Cuando exista la salida de un empleado, este debe devolver llaves, equipos, usuarios u otro tipo de activo que contenga información que pueda poner en peligro la seguridad de la empresa. En caso de que existan dudas sobre la absoluta devolución, de procederá a la revisión y comprobación de tener copias o haber creados datos perjudiciales para la organización.
- Niveles de clasificación de la información:
  - Activo libre, información que puede difundirse
  - Activo restringido, información interna, en caso de que se llegue a filtrar no provoca riesgo.
  - Activo protegido información controlada y vigilada para su acceso, en caso de que se llegue a filtrar puede provocar un riesgo moderado para la empresa.
  - Activo confidencial, información que no puede ser difundida en absoluto. En caso de que se llegue a filtrar puede provocar un gran riesgo para la empresa.
- La zona restringida de la empresa debe tener la seguridad necesaria para prevenir la perdida de la información.
- No se podrá almacenar información en medios removibles, los puertos serán desactivados en los equipos de la clínica, si se desea utilizar alguno debe ser justificado en el departamento de administración.
- Si se realiza algún cambio en las políticas de seguridad debe comunicarse inmediatamente a todos los empleados, realizando nuevas capacitaciones de los cambios efectuados.
- La presente política general y las políticas específicas deben revisarse y actualizarse mínimo 1 vez cada año.

3. Responsabilidades

La gerencia general y el área administrativa son responsables de la seguridad de la información de la empresa. Sin embargo, cada trabajador debe comprometerse a cumplir con las normas y políticas de acuerdo con el cargo que realice.

4. Sanciones

La violación de la política general de la seguridad de la información respalda la imposición de penalidades o sanciones disciplinarias siguiendo el reglamento interno de Gamma Smart, y para poder aplicarse se debe tener en cuenta la gravedad de la falta, las circunstancia y frecuencia de la falta.

Las sanciones por aplicarse son las siguientes:

- Amonestación verbal o escrita: Se impondrá cuando la falta se realiza por primera vez.
- Amonestación económica: Se impondrá cuando la falta sea recurrente.
- Suspensión del trabajo: Se impondrá cuando el empleado tenga antecedentes de amonestaciones o la falta sea grave.
- Despido: Se impondrá cuando a pesar de las amonestaciones anteriores el trabajador continúe cometiendo faltas críticas dentro de la empresa.

5. Políticas Específicas

La política general de la información desglosa políticas específicas de seguridad, que se detallan a continuación:

- Política de Gestión de Contraseñas
- Política de Escritorio Limpio
- Política de Gestión de Accesos
- Política de Gestión de Seguridad Física
- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de Dispositivos Móviles
- Política de Gestión de Copias de Respaldo
- Política de Gestión de Activos.

Anexo: 7 Políticas de Gestión de Contraseñas

Políticas de Gestión de Contraseñas

1. **Introducción**

La presente política establece los lineamientos para la creación, uso, almacenamiento y gestión de contraseñas dentro de Gamma Smart, con el objetivo de proteger los activos de información de la organización y garantizar la confidencialidad, integridad y disponibilidad de los datos.

2. **Objetivo**

Prevenir accesos no autorizados a sistemas y datos críticos mediante la implementación de prácticas seguras en la gestión de contraseñas.

3. **Alcance**

El alcance de esta política es aplicable a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información de Gamma Smart. Todos los usuarios deben cumplir con los lineamientos establecidos en esta política.

4. **Creación de Contraseñas**

- Las contraseñas deben tener un mínimo de 12 caracteres y deben incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- Las contraseñas no deben contener información personal fácilmente identificable, como nombres, fechas de nacimiento o números de teléfono.
- Los usuarios deben cambiar sus contraseñas cada 90 días y no deben reutilizar las últimas cinco contraseñas utilizadas.
- Las contraseñas deben ser generadas utilizando un gestor de contraseñas o mediante un proceso aleatorio seguro.

Las contraseñas que se utilizan dentro de la empresa deben ser solamente para el ámbito laboral, para evitar robo de información.

5. **Gestión de Contraseñas de Usuarios**

Las contraseñas deben cambiarse cada 6 meses como máximo y no podrá guardarse la contraseña dentro de algún navegador de internet. Está prohibido compartir la contraseña con otros empleados. En caso de que un miembro de la empresa solicite la contraseña, se debe informar de inmediato a al área administrativa de Gamma Smart y asimismo se solicitará una nueva contraseña cuando exista pérdida u olvido de la contraseña.

6. **Contraseñas para desarrolladores.**

Las aplicaciones o sistemas operativos que gestionen contraseñas de la empresa deben encriptarse y los caracteres no deben ser visibles; en su lugar, se deben mostrar símbolos no alfabéticos. En caso de querer tener acceso se debe utilizar un VPN.

7. **Almacenamiento de Contraseñas**

- Las contraseñas no deben ser almacenadas en texto plano en ningún sistema. Deben utilizarse algoritmos de hashing seguros y salting para el almacenamiento.
- Las contraseñas no deben ser anotadas en papel o en documentos electrónicos de fácil acceso. En caso de ser necesario, se deberá utilizar un gestor de contraseñas confiable para su almacenamiento seguro.

8. **Uso de Contraseñas**

- Las contraseñas deben ser confidenciales y no compartidas con nadie, incluso con colegas o superiores.
- Los usuarios deben cerrar sesión en sus cuentas cuando no estén en uso, especialmente en dispositivos compartidos o públicos.
- Se debe evitar el uso de contraseñas en dispositivos no seguros o en redes Wi-Fi públicas.

9. **Recuperación y Restablecimiento de Contraseñas**

- El proceso de recuperación y restablecimiento de contraseñas debe requerir la verificación de identidad del usuario mediante preguntas de seguridad, autenticación multifactor (MFA) o métodos similares.

- Los usuarios deben ser informados sobre la necesidad de mantener la confidencialidad de las respuestas a las preguntas de seguridad.

10. Responsabilidades

Es responsabilidad de todos los empleados cumplir con esta política y reportar cualquier actividad sospechosa relacionada con el uso de contraseñas.

El departamento de TI es responsable de implementar y mantener las medidas técnicas necesarias para proteger las contraseñas y realizar auditorías periódicas para verificar el cumplimiento de esta política.

11. Sanciones

Las sanciones por aplicarse son las mismas mencionadas en la política general.

El incumplimiento de esta política puede resultar en sanciones disciplinarias, que pueden incluir amonestaciones, suspensiones o despido, dependiendo de la gravedad de la infracción.

Anexo: 8 Política de Escritorio Limpio

Política de Escritorio Limpio

1. Introducción

En este documento se establecerá una política de escritorio limpio, que garantice que ninguna información confidencial quede a la vista o pueda ser alterada cuando el empleado se aparte de su área o lugar de trabajo. Esta política es fundamental, ya que contribuye a reducir de manera significativa el riesgo de filtraciones o sustracción de la información.

2. Objetivo

El objetivo de esta política es garantizar que la información solo sea vista y utilizada por el personal autorizado, estableciendo normas que los empleados deben seguir cuando no estén en su área de trabajo.

3. Alcance

El alcance de esta política abarca a todos los empleados de la empresa.

4. Escritorio Limpio

- El bloqueo de la computadora es obligatorio tras ausentarse del área de trabajo, y al final de la jornada, tiene que ser apagada.
- Los archivos o documentos que contengan información confidencial no deben quedar a la intemperie y al final de la jornada, deben guardarse en su lugar designado bajo llave.
- Las llaves de los escritorios o anaqueles deben estar bajo responsabilidad del trabajador en todo momento.
- Los documentos confidenciales desechados o archivos eliminados deben ser destruidos de manera que no puedan ser reconstruidos.
- Las impresiones deben recogerse de inmediato para evitar que caigan en manos de personal no autorizadas.

5. **Monitoreo del escritorio limpio**

   Al final de cada jornada de trabajo, se realizará un recorrido por todas las instalaciones para asegurarse de que los trabajadores están cumpliendo con las políticas y normas. Si se encuentra alguna información física o digital será guardado por la administración y para recuperarlos el empleado deberá justificar la pérdida.

6. **Responsabilidades**

Los responsables están mencionados en la política general.

7. **Sanciones**

Las sanciones por aplicarse son las mismas mencionadas en la política general.

Anexo: 9 Política de Gestión de Accesos

Política de Gestión de Accesos

1. Introducción

En este documento se describirá la gestión de accesos a los sistemas de la organización, así como la administración de sus activos de información y el monitoreo por parte de los usuarios.

2. Objetivo

Establecer la gestión del control de accesos de la información de la empresa.

3. Alcance

Esta política es aplicable a toda la información proporcionada por la clínica, física o digital, así como a aquellos que las gestionan y utilizan.

4. Acceso a la información

Los empleados únicamente podrán acceder a los activos de información que sean indispensables para llevar a cabo sus funciones dentro de la organización. A cada trabajador que ingrese se le creará un usuario para acceder a las computadoras, junto con una contraseña que deberá cumplir con las directrices de la Política de Gestión de Contraseñas. Los activos de información a los que los trabajadores tendrán acceso, según sus funciones, serán determinados por el jefe inmediato y el área administrativa, si se necesita otorgar acceso a un tercero por auditoría, deberá ser aprobado primero por administración y el usuario deberá firmar un acuerdo de confidencialidad.

Para las aplicaciones y sistemas de Gamma Smart, se debe designar a un único administrador que tenga la autoridad para otorgar acceso a los usuarios.

5. Mantenimiento de los accesos

Se debe llevar a cabo un mantenimiento constante, el cual debe realizarse mínimo una vez cada seis meses. Una vez que se termina la auditoría se debe retirar el acceso al personal no autorizado, si algún empleado cambia de función o de área de trabajo se debe

analizar si se mantiene el acceso a la información o se procede a hacer la devolución de esta y se deberá actualizar sus permisos.

Ante la salida de un empleado se debe solicitar la devolución de toda la información proporcionada y se les retirarán los accesos de inmediato.

6. **Segregación de funciones**

No debe existir acceso por grupos de usuarios, el acceso a la información debe ser individual, y debe basarse en una segregación de funciones, lo que significa que no pueden tener acceso a todas las funciones o transacciones de la empresa.

7. **Responsabilidades**

Los responsables están mencionados en la política general.

8. **Sanciones**

Las sanciones por aplicarse son las mismas mencionadas en la política general.

Anexo: 10 Política de Gestión de Incidentes de Seguridad

Política de Gestión de Incidentes de Seguridad

1. **Introducción**

En este documento se exponen las directrices a seguir en caso de que ocurra algún incidente que afecte la seguridad de la información.

2. **Objetivo**

Establecer directrices para la gestión de incidentes de seguridad de la información, con el fin de minimizar impactos negativos dentro de la empresa.

3. **Alcance**

Esta política es aplicable a todos los empleados de Gamma Smart.

4. **Gestión de incidentes**

- Los empleados tienen la responsabilidad de informar sobre cualquier incidente de seguridad a su jefe inmediato.
- Los incidentes que se reporten deben analizarse para verificar si se trata o no de un incidente de seguridad, y la gravedad, para realizar un plan de respuesta por el personal de seguridad.
- La coordinación con otras instituciones debe ser primordial ante un incidente, especialmente el departamento de policía, bomberos, etc.
- Los incidentes deben ser registrados especificando el nombre del activo afectado, detalles, controles y riesgos asociados del incidente, acciones realizadas durante el incidente, los riesgos ante los cuales queda expuesta la empresa y los planes de acción a realizarse para solucionar el incidente de seguridad.
- La gerencia y el área administrativa son los encargados de analizar y detallar los incidentes de gravedad para verificar que no exista alguna violación de las leyes y desarrollar un plan de acción.
- Después de resolver el incidente, se debe determinar si representa un nuevo riesgo o ya era un riesgo conocido. Si es un nuevo riesgo, se realizará una evaluación detallada de este para la creación de nuevos planes de acción. Y si es un riesgo

anterior ya conocido, se deben establecer nuevos estudios para evaluar su impacto y mejorar los planes de acción ya realizados.

5. Responsabilidades

Los responsables están mencionados en la política general.

6. Sanciones

Las sanciones por aplicarse son las mismas mencionadas en la política general.

Anexo: 11 Política de Gestión de Copias de Seguridad Backups

Política de Gestión de Copias de Seguridad Backups

1. **Introducción**

Esta política establece las directrices para la creación, almacenamiento y recuperación de copias de respaldo de los datos críticos de Gamma Smart, con el objetivo de garantizar la disponibilidad y la integridad de la información ante posibles pérdidas o incidentes.

2. **Objetivo**

El objetivo de esta política es asegurar que todas las copias de respaldo se realicen de manera regular y que los procedimientos de restauración estén documentados y probados, minimizando así el riesgo de pérdida de información.

3. **Alcance**

Se aplica a toda la información proporcionada por Gamma Smart, ya sea de manera física o digital, así como a los trabajadores que las gestionan y utilizan.

4. **Gestión de incidentes**

- Las copias de respaldo se realizarán al menos una vez al día para los datos críticos y semanalmente para datos menos sensibles.
- Las copias de respaldo deben ser almacenadas en un medio seguro y separado del sistema original, preferiblemente en un entorno físico y/o en la nube.
- Se realizarán pruebas periódicas de restauración de datos para garantizar la integridad y la disponibilidad de las copias de respaldo.

5. **Responsabilidades**

Los responsables están mencionados en la política general.

6. **Sanciones**

Las sanciones por aplicarse son las mismas mencionadas en la política general.

Anexo: 12 Política de Gestión de Activos

Política de Gestión de Activos

1. Introducción

En este documento muestran los lineamientos para seguridad de la gestión de activos de información de la empresa.

2. Objetivo

Establecer lineamientos y directrices para la gestión de los activos de información de la empresa, con el fin de prevenir la pérdida de la Confidencialidad, Integridad y Disponibilidad.

3. Alcance

Se aplica a toda la información proporcionada por Gamma Smart, ya sea de manera física o digital, así como a los trabajadores que las gestionan y utilizan.

4. Seguridad de Información digital

Es necesario que el personal esté informado sobre las políticas y estándares del uso de todos los activos de información digital, se debe utilizar obligadamente los sistemas o aplicaciones de la empresa, para la realización de comunicaciones electrónicas. Los trabajadores, por ejemplo, los médicos, no podrán intercambiar información a los pacientes mediante correo personal, esta debe realizarse directamente con los recursos digitales proporcionados por Gamma Smart. Solo el personal autorizado puede interceptar y leer comunicaciones electrónicas, en caso de que terceros lo hagan se recurrirá a una sanción.

Está completamente prohibido almacenar información restringida en celulares o dispositivos personales no autorizados por la empresa. La documentación confidencial debe estar encriptada.

Se debe evitar abrir correos electrónicos de origen sospechoso o desconocido, los antivirus tienen que estar debidamente instalados en todas las computadoras junto con un programa de encriptación. El mantenimiento de información digital debe realizarse por o menos cada 6 meses.

5. Seguridad de Información Física

Es importante estar al tanto de las políticas y estándares relacionados con el uso de todos los activos de información física. El acceso a administración estará restringido únicamente a personal autorizado, mientras que las áreas de consultas, laboratorios y sala de espera estarán abiertas a empleados en general y pacientes. Si es necesario eliminar un documento que contenga datos confidenciales, debe ser destruido completamente. Los escritorios administrativos deben permanecer vacíos (sin ningún documento visible) cuando el empleado no esté presente.

Debe realizarse un mantenimiento por lo menos una vez al año y las historias clínicas al ser consideradas un documento legal, debe ser totalmente confidencial y almacenados bajo llave.

6. Responsabilidades

Los responsables están mencionados en la política general.

7. Sanciones

Las sanciones por aplicarse son las mismas mencionadas en la política general.

Anexo: 13 Política de Seguridad Física

Política de Seguridad Física

1. Introducción

Esta política establece las medidas de seguridad física necesarias para proteger las instalaciones de Gamma Smart, así como los activos de información y los datos sensibles almacenados en ellas.

2. Objetivo

El objetivo de esta política es prevenir el acceso no autorizado a las instalaciones y a los activos de información, así como garantizar la protección de la información contra robos, daños o pérdida.

3. Alcance

Esta política se aplica a todas las instalaciones de la organización, incluidos edificios, oficinas, almacenes y áreas de trabajo donde se manejen datos sensibles.

4. Controles de Acceso Físico

- El acceso a las instalaciones estará restringido a personal autorizado mediante el uso de tarjetas de identificación, cerraduras y sistemas de control de acceso.
- Se llevarán a cabo registros de acceso para monitorear quién entra y sale de las instalaciones, así como para detectar posibles actividades sospechosas.

5. Protección de Activos de Información

- Los equipos y dispositivos que contengan información sensible deben ser asegurados y protegidos adecuadamente cuando no estén en uso.
- Las áreas donde se manejen datos críticos deben estar limitadas al personal autorizado y contar con medidas de seguridad adicionales, como cámaras de vigilancia.

6. Emergencias y Contingencias

- Se desarrollarán procedimientos para situaciones de emergencia, como incendios, inundaciones o accesos no autorizados, que aseguren la protección de los activos de información.

- Se realizarán simulacros periódicos para garantizar que todos los empleados estén familiarizados con los procedimientos de evacuación y protección de la información.

7. **Responsabilidades**

- La gerencia es responsable de implementar y supervisar esta política, así como de garantizar que se cumplan las medidas de seguridad física.
- Todos los empleados deben cumplir con las directrices de seguridad física y reportar cualquier incidente o comportamiento sospechoso.

8. **Revisión de la Política**

Esta política será revisada y actualizada al menos una vez al año o cuando se produzcan cambios significativos en la infraestructura física.

Anexo: 14 Política de Gestión de Dispositivos Móviles

Política de Gestión de Dispositivos Móviles

1. Introducción

Esta política establece los lineamientos para el uso seguro de dispositivos móviles personales y corporativos dentro de Gamma Smart, con el objetivo de proteger la información sensible y los activos de la organización.

2. Objetivo

El objetivo de esta política es garantizar que todos los dispositivos móviles utilizados para acceder a datos sensibles cumplan con las normas de seguridad necesarias para prevenir accesos no autorizados y la pérdida de información.

3. Alcance

Esta política se aplica a todos los empleados y contratistas que utilicen dispositivos móviles para acceder a sistemas y datos de la organización, ya sean dispositivos de propiedad de la empresa o personales.

4. Seguridad de Dispositivos Móviles

- Todos los dispositivos móviles deben estar protegidos mediante contraseñas o métodos de autenticación biométrica.
- Los dispositivos móviles deben contar con software de seguridad actualizado, como antivirus y herramientas de gestión de dispositivos móviles (MDM).
- Se debe activar la función de cifrado de datos en todos los dispositivos móviles que manejen información sensible.

5. Acceso a Datos Sensibles

- El acceso a datos sensibles a través de dispositivos móviles estará restringido y será necesario el uso de una conexión segura (VPN) para acceder a la red de la organización.
- Los empleados no deben utilizar redes Wi-Fi públicas para acceder a datos sensibles de la organización.

6. **Pérdida o Robo de Dispositivos**

- En caso de pérdida o robo de un dispositivo móvil, el empleado debe reportarlo de inmediato al departamento de TI para tomar las medidas adecuadas, como el borrado remoto de datos.
- Se realizarán auditorías periódicas para verificar que los dispositivos móviles cumplan con las políticas de seguridad establecidas.

7. **Responsabilidades**

- El departamento de TI es responsable de proporcionar capacitación sobre la seguridad de los dispositivos móviles y de supervisar su cumplimiento.
- Todos los empleados deben seguir las directrices establecidas en esta política y reportar cualquier incidente de seguridad relacionado con dispositivos móviles.

8. **Revisión de la Política**

Esta política será revisada y actualizada al menos una vez al año o cuando se produzcan cambios significativos en la tecnología o en las necesidades de seguridad de la organización.