Pontificia Universidad Católica del Ecuador

Sede Ibarra

ESCUELA DE INGENIERIA

INFORME FINAL DEL PROYECTO

TEMA:

IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION(SGSI) PARA EL CENTRO MEDICO ¨COTACACHI¨, BASADO EN LA NORMA ISO 27001:2013

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO EN TECNOLOGIAS DE LA INFORMACION

LÍNEAS DE INVESTIGACIÓN:

CULTURA ORGANIZACIONAL E INFORMÁTICA

AUTOR: **JULIO FABIAN VACA BAEZ**

ASESOR: **Mgs. DIEGO FERNANDO BAROJA**

IBARRA, AGOSTO – 2023

Mgs. **DIEGO FERNANDO BAROJA**

ASESOR

CERTIFICA:

Haber revisado el presente informe final de investigación, el mismo que se ajusta a las normas vigentes en la Escuela de Ingeniería (ENCI), de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI); en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f:) ……

Mgs. **DIEGO FERNANDO BAROJA**

C.C.: 1002402061

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El jurado examinador, aprueba el presente informe de investigación en nombre de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCESI):

(f): …….

Mgs. **DIEGO FERNANDO BAROJA**

C.C.: 1002402061

(f): …….

Mgs. Luis David Narváez

C.C.: 1002868378

(f): …….

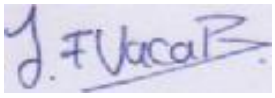
Mgs. Darwin Pillo

C.C.: 1003319660

ACTA DE CESIÓN DE DERECHOS

Yo: JULIO FABIAN VACA BAEZ declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: “Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones, a título gratuito u oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia”.

Ibarra, 8 de agosto de 2023



f): ……

JULIO FABIAN VACA BAEZ

C.C.: 0401643234

AUTORÍA

Yo, JULIO FABIAN VACA BAEZ, portador de la cédula de ciudadanía No 0401643234, declaro que la presente investigación es de total responsabilidad del (los) autor (es), y eximo expresamente a la Pontificia Universidad Católica del Ecuador Sede Ibarra de posibles reclamos o acciones legales.

f): ……..

JULIO FABIAN VACA BAEZ

C.C.: 0401643234

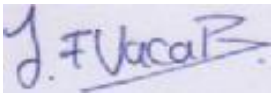
DECLARACIÓN y AUTORIZACIÓN

Yo: JULIO FABIAN VACA BAEZ, con CC: 0401643234 autor del trabajo de grado intitulado: ("IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION(SGSI) PARA EL CENTRO MEDICO ¨COTACACHI¨, BASADO EN LA NORMA ISO 27001:2013"), previo a la obtención del título profesional de ("TECNOLOGIAS DE LA INFORMACION**"**), en la Escuela de (Escuela de Ingeniería)

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador Sede- Ibarra, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador Sede Ibarra a difundir a través de sitio web de la Biblioteca de la PUCESI el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ibarra, (08, agosto del 2023)



(f.)……

JULIO FABIAN VACA BAEZ

C.C.: 0401643234

CERTIFICACIÓN ANTIPLAGIO

Yo **DIEGO FERNANDO BAROJA**, declaro que luego del proceso de revisión en el sistema anti-plagio TURNITIN el porcentaje de similitud del trabajo de titulación denominado: "**IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION(SGSI) PARA EL CENTRO MEDICO ¨COTACACHI¨, BASADO EN LA NORMA ISO 27001:2013"** es del 8% de acuerdo con el documento Id: 1833322426.

En base a lo anterior, considero que el trabajo de titulación NO ☐ **SÍ** ☐ cumple los requisitos de originalidad y autenticidad, de acuerdo con los requisitos establecidos por la ley.

Ibarra, 25 de agosto 2023

(Firma)

DIEGO FERNANDO BAROJA

C.C.: 1002402061

ÍNDICE DE CONTENIDO

RESUMEN Y PALABRAS CLAVE 1

ABSTRACT 2

INTRODUCCIÓN 3

CAPITULO 1 7

ESTADO DEL ARTE 7

1.1INVESTIGACIONES PREVIAS 7

1.1.1NORMA ISO 27001:2013 8

1.2MARCO TEÓRICO Y CONCEPTUAL 9

1.2.1 METODOLOGIAS 9

1.2.2OWASP 9

1.2.3MAGERIT 9

1.3.CONCEPTOS 11

1.3.1LA INFORMACIÓN 11

1.3.2 SEGURIDAD DE LA INFORMACIÓN 11

1.3.3 CALIDAD DE LA INFORMACIÓN 12

1.3.4 SEGURIDAD INFORMÁTICA 13

1.3.5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 14

1.35 LA NORMA ISO/27001 15

CAPITULO II 17

METODOLOGÍA DE LA INVESTIGACIÓN 17

2.1 ASPECTOS GENERALES DE LA INVESTIGACIÓN 17

2.1.1 TIPO DE INVESTIGACIÓN 17

2.1.2 ENFOQUE 18

2.1.3 ANÁLISIS COMPARATIVO DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGOS TI 20

2.2 METODOLOGÍA DEL DESARROLLO DE LA PROPUESTA 28

2.2.1 MAGERIT 28

2.2.2 DESARROLLO DE LA METODOLOGÍA 28
2.2.3 IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS 28
2.3 REQUISITOS FUNCIONALES 31
2.4 HISTORIAS DE USUARIOS 33
2.5 SPRINT BACK LOG 34
2.5.1 SPRINT 1 34
2.5.2 SPRINT 2 34
CAPÍTULO III 35
3.1 FASE DE DIAGNÓSTICO 36
3.2 FASE DE AUDITORÍA INICIAL 36
3.3ANÁLISIS DE ACTIVOS 42
FASE I. IDENTIFICAR ACTIVOS 42
4.1FASE II IDENTIFICACIÓN DE AMENAZAS 50
4.1.1 AMENAZAS ORIGEN DESASTRE NATURAL 51
4.1.2 AMENAZAS ORIGEN ERRORES Y FALLAS NO INTENCIONADOS 53
5.1 FASE IV IDENTIFICACIÓN SALVAGUARDAS 56
6.1FASE V EVALUAR EL RIESGO 57
6.1.1DETERMINACIÓN DEL IMPACTO POTENCIAL 57
6.1.2DETERMINACIÓN DEL RIESGO POTENCIAL 60
7.1 METODOLOGÍA GESTIÓN DE LOS RIESGOS MAGERIT 61
7.1.1 EVALUACIÓN: INTERPRETACIÓN DE LOS VALORES DE IMPACTO Y RIESGOS RESIDUALES 61
7.1.2 ACEPTACIÓN DEL RIESGO 62
7.1.3 TRATAMIENTO 62
7.1.4 ESTUDIO CUANTITATIVO DE COSTE BENEFICIO 64
7.1.5 ESTUDIO CUALITATIVO DE COSTE/ BENEFICIO 64
7.1.6 FORMALIZACIÓN DE ACTIVIDADES 65
7.1.7 ROLES Y FUNCIONES 66
8.1 CHECK LIST DE EVALUACIÓN 67

8.1.1 PLAN DE SEGURIDAD 67
8.1.2 CHECK LIST DE EVALUACIÓN (ESTADO DE MADUREZ)..... 67
CONCLUSIONES Y RECOMENDACIONES..... 92
REFERENCIAS BIBLIOGRAFICAS 94
ANEXOS 97

ÍNDICE DE TABLAS

Tabla 1. ANÁLISIS COMPARATIVO DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGOS TI....20
Tabla 2. IDENTIFICACIÓN DE ACTIVOS. 29
Tabla 3. VALORACIÓN CUALITATIVA. 30
Tabla 4. ESCALA DE VALORACIÓN DE ACTIVOS. 31
Tabla 5. HISTORIAS DE USUARIOS....33
Tabla 6. PRODUCTBACKLOG 33
Tabla 7. SPRINT 1....34
Tabla 8. SPRINT 2....34
Tabla 9. RESULTADOS DE ENCUESTA EN EL CENTRO MÉDICO ¨COTACACHI¨....38
Tabla 10. ACTIVOS TANGIBLES....42
Tabla 11. ACTIVOS INTANGIBLES....44
Tabla 12. ETIQUETADO DE ACTIVOS....46
Tabla 13. CRITERIOS DE VALORACIÓN DE ACTIVOS....47
Tabla 14. DIMENSIÓN DE VALORACIÓN DE ACTIVOS 48
Tabla 15. CRITERIOS DE VALORACIÓN DE ACTIVOS....49
Tabla 16. CODIFICACIÓN SEGÚN TIPO DE AMENAZA....51
Tabla 18. AMENAZAS ORIGEN DESASTRE NATURAL 51
Tabla 19. AMENAZAS ORIGEN ERRORES Y FALLAS NO INTENCIONADOS....53
Tabla 20. AMENAZAS ORIGEN ATAQUES INTENCIONADOS....55
Tabla 21. DEGRADACIÓN DE VALOR 57
Tabla 22. PROBABILIDAD DE OCURRENCIA 58
Tabla 23. NIVEL DE MADUREZ 68
Tabla 24. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD TOMANDO COMO BASE LA NORMA ISO 27001:2013....88

ÍNDICE DE GRÁFICOS

Gráfico 1. ACTIVOS DE LA INFORMACIÓN 11
Gráfico 2. PROYECTOS QUE CONSTITUYEN UN SGSI 14
Gráfico 3. NORMA ISO 27001 16
Gráfico 4. RESULTADOS DEL ANÁLISIS DE RIESGOS 40
Gráfico 5. PORCENTAJE DE RESPUESTAS 41
Gráfico 6. EL RIESGO EN FUNCIÓN DEL IMPACTO Y LA PROBABILIDAD 59
Gráfico 7. EL RIESGO EN FUNCIÓN DEL IMPACTO Y LA PROBABILIDAD 60
Gráfico 8. DETERMINACIÓN DEL RIESGO POTENCIAL 61
Gráfico 9. PROCESO DE GESTIÓN DE RIESGO (MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS 65
Gráfico 10. FASE I DIAGNOSTICO 70
Gráfico 11. RESULTADO DEL DIAGNÓSTICO 72
Gráfico 12. FASE III 74
Gráfico 13. AMENAZAS IDENTIFICADAS Y EL NÚMERO DE LOS ACTIVOS DE INFORMACIÓN 74
Gráfico 14. VULNERABILIDADES Y EL NÚMERO DE AMENAZAS 75
Gráfico 15. NRO. DE AMENAZAS QUE PUEDAN EXPLOTARLAS 76
Gráfico 16. NÚMERO DE VULNERABILIDADES QUE PUEDE SER EXPLOTADA 77
Gráfico 17. CODIFICACIÓN DE RIESGOS DEL PROCESO DE TECNOLOGÍA 78
Gráfico 18. LA PROBABILIDAD DE OCURRENCIA DE LOS RIESGOS IDENTIFICADOS 79
Gráfico 19. NÚMERO DE RIESGOS QUE PUEDE MITIGAR CADA UNO DE LOS CONTROLES 80
Gráfico 20. RELACIÓN DE LAS CANTIDADES DE CONTROLES QUE SE IDENTIFICARON 81
Gráfico 21. DISMINUCIÓN EN EL NIVEL DE LOS RIESGOS QUE GENERO LOS RESPECTIVOS CONTROLES IDENTIFICADOS 82
Gráfico 22. PORCENTAJE DE DISMINUCIÓN QUE GÉNERO LOS CONTROLES IDENTIFICADOS 83
Gráfico 23. PORCENTAJE DE DISMINUCIÓN EN EL NIVEL DE RIESGO QUE GENERO LOS RESPECTIVOS CONTROLES VALORADOS 84
Gráfico 24. MATRICES DE RIESGOS INHERENTE Y RESIDUAL DEL PROCESO DEL PROCESO DE TECNOLOGÍA 85
Gráfico 25. DISTRIBUCIÓN RIESGO RESIDUAL PROCESO DE TECNOLOGÍA 87

RESUMEN Y PALABRAS CLAVE

El presente trabajo aborda la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en el Centro Médico "Cotacachi", con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de la información sensible y crítica relacionada con los pacientes y las operaciones médicas. La norma ISO 27001:2013 se adopta como marco de referencia para guiar la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI.

La tesis se estructura en varias etapas clave. En primer lugar, se realiza una revisión exhaustiva de la norma ISO 27001:2013, identificando sus requisitos y directrices para el establecimiento de un SGSI efectivo. Luego, se lleva a cabo un análisis detallado de la situación actual del Centro Médico "Cotacachi" en cuanto a la seguridad de la información, identificando vulnerabilidades, amenazas y riesgos potenciales.

Basándose en este análisis, se procede a diseñar un plan detallado de implementación del SGSI, que incluye la definición de políticas de seguridad, la identificación de roles y responsabilidades, la realización de evaluaciones de riesgos y la definición de medidas de control adecuadas para mitigar dichos riesgos. Además, se establece un programa de concientización y capacitación en seguridad de la información para el personal del centro médico.

Durante la fase de implementación, se integran los controles de seguridad necesarios, se establecen procedimientos operativos y se realiza una auditoría interna para asegurar que el SGSI cumple con los requisitos de la norma ISO 27001:2013. Finalmente, se lleva a cabo una revisión exhaustiva del proceso de implementación, se identifican lecciones aprendidas y se proponen recomendaciones para la mejora continua del SGSI en el Centro Médico "Cotacachi".

Palabras Claves:

Confidencialidad, Integridad de datos, disponibilidad de datos, gestión de incidentes de seguridad, evaluación de riesgos, continuidad del negocio, proceso de certificación, mejora continua.

ABSTRACT

This thesis addresses the implementation of an Information Security Management System (ISMS) at "Cotacachi" Medical Center, with the aim of safeguarding the confidentiality, integrity, and availability of sensitive and critical information related to patients and medical operations. The ISO 27001:2013 standard is adopted as a framework to guide the planning, establishment, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS.

The thesis is structured into several key stages. Firstly, a comprehensive review of the ISO 27001:2013 standard is conducted, identifying its requirements and guidelines for establishing an effective ISMS. Subsequently, a detailed analysis of the current state of "Cotacachi" Medical Center's information security is performed, identifying vulnerabilities, threats, and potential risks.

Based on this analysis, a detailed ISMS implementation plan is designed. This plan includes defining security policies, identifying roles and responsibilities, conducting risk assessments, and defining appropriate control measures to mitigate identified risks. Additionally, an information security awareness and training program is established for the medical center's personnel.

During the implementation phase, necessary security controls are integrated, operational procedures are established, and an internal audit is conducted to ensure that the ISMS complies with the ISO 27001:2013 requirements. Finally, a thorough review of the implementation process is carried out, lessons learned are identified, and recommendations for the continuous improvement of the ISMS at "Cotacachi" Medical Center are proposed.

Keywords:

Confidentiality, Data integrity, data availability, security incident management, risk assessment, business continuity, certification process, continuous improvement.

INTRODUCCIÓN

Al vivir en un planeta globalizado y el florecimiento de la tecnología, así como el internet y las redes sociales hacen que la información ya no se la disponga sólo a través de un papel modelo o escrito o mediante charlas predestinadas, que la podemos guardar o retransmitir a través de un formato electrónico, mediante imágenes o mensajes digitales es decir que existe un grupo cada vez más grande de personas que tienen vínculos a la información ya que se vuelve más difícil porque está más expuesta al combatir las diferentes amenazas. Por la cantidad de información el resumen se requiere que cumpla con la progresión de medidas de acompañamiento que sean adecuadas como su importancia y criticidad para obtener la confianza de la información

Los Sistemas de Gestión de Seguridad de la Información son descritos por la Norma ISO/IEC de forma ordenada, la infraestructura tecnológica y los sistemas de información del sistema de historias clínicas del área de recursos humanos, es por esta razón que las falencias por la falta de controles oportunos y de un plan de tratamiento han hecho que los objetivos que tienen como institución no se cumplan a cabalidad, por lo tanto se debería de tener un plan plenamente efectivo y con controles que minimicen los riesgos, amenazas.

Existen muchas herramientas que se han implementado como la Norma ISO 27001:2013 con la finalidad de prevenir cualquier ataque. Las tecnologías que van a la par con la administración de la seguridad de dicha información, la gestión de la seguridad de la información, y por lo tanto está sujeto a cambios en la seguridad de la información se mezclan muchos aspectos tales como combinación de herramientas, estrategias y técnicas de seguridad, y factores humanos para la detección de fugas de información, ataques de hackers maliciosos; por

lo consecuente hay que tratar de apartar las vulnerabilidades y amenazas que atenten a la seguridad de la información.

El Centro Médico ¨Cotacachi¨, brinda servicios médicos eficientes, tales como Medicina general, Medicina preventiva, Pediatría, Dermatología. La población cercana al centro médico se ve beneficiada de manera sustancial, al contar con dicho servicio especializado y de primera.

El sistema de seguridad de la información del Centro médico ¨Cotacachi¨ provincia de Imbabura cantón Cotacachi no cuenta con controles adecuados en seguridad de la información, ni con un plan de tratamiento de riesgo para la gestión de seguridad de la información, tampoco con un diseño de plan de seguridad de la información. Hay muchos factores que no favorecen a la inseguridad del sistema de la información los cuales son, pocas políticas de seguridad, falta de controles, alta perdida de información no existe documentación en manuales de funciones, procedimientos y políticas de seguridad, falta de planes de capacitación, inexistencia de la continuidad en los planes de crecimiento y carencia de un diseño de sistema integral de seguridad de la información.

Existen muchas inoperancias en el sistema de seguridad en donde la información puede estar sujeta a pérdidas, ya que no se manejan los procesos de historias clínicas y con políticas de seguridad. No obstante, estos procesos están expuesto a riesgos y amenazas, ya que la red de ordenadores del área médica no cuenta con un respaldo en los protocolos de comunicación y sumado a eso se manejan IPs públicas

El departamento de computación del centro médico “Cotacachi” tiene entre sus funciones, la implementación y manejo de infraestructura tecnológica, redes, desarrollo de aplicaciones y servicios de capacitación tecnológica al sistema de intranet. forma ordenada la

infraestructura tecnológica y los sistemas de información. Por lo que se hace acreedor y responsable de las obligaciones en el manejo de la seguridad de los activos de información de las historias clínicas del área de recursos humanos de la institución, es por esta razón que las falencias por la falta de controles oportunos, y de un plan de tratamiento los objetivos que tienen como institución,

Por tales razones, la carencia de un sistema de seguridad con un diseño de un plan de gestión de la seguridad de la información y de un tratamiento de riesgo se puede decir que ha retrasado de manera muy agravante los objetivos organizacionales que tiene el centro médico y esto implica niveles muy bajos e ineficientes en la labor interina del departamento; una vez detectada la necesidad que tiene el sistema de historias clínicas y con la intención de mejorar sus procesos de los servicios que brinda, se plantea implementar "UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION(SGSI) PARA EL CENTRO MEDICO ¨COTACACHI¨, BASADO EN LA NORMA ISO 27001:2013"

En este sentido se establecen los siguientes objetivos

OBJETIVO GENERAL

Implementar un sistema de gestión de la seguridad de la información (SGSI) para el centro médico ¨Cotacachi¨, basado en la norma ISO 27001:2013.

OBJETIVOS ESPECÍFICOS

- Analizar las bases teóricas y científicas relacionadas directamente con las metodologías y normativas ISO para el diseño del estado del arte.
- Diagnosticar las necesidades y manejo de la información que el centro de médico “Cotacachi” procesa para conocer los procesos de funcionalidad en cada uno de sus departamentos.
- Implementar una metodología para la gestión de la seguridad de la información del centro médico “Cotacachi”.
- Socializar la implementación del sistema de la seguridad de la información en el centro médico “Cotacachi” a sus propietarios y empleados para su conocimiento.

CAPITULO 1

ESTADO DEL ARTE

1.1 INVESTIGACIONES PREVIAS

Con el pasar de los años los centros médicos o consultorios clínicos se han preocupado por mejorar de manera radical todos los sistemas de seguridad de los datos, dando como resultado que la seguridad de la información sea casi nula. La transformación de los sistemas computacionales, del internet y de las telecomunicaciones han dilatado varias puertas para que todas las personas puedan descubrir el valor de la seguridad de la información y lo que conlleva al fácil acceso a los datos.

Lastimosamente el fácil acceso a la información nos expone de manera potencial ante el acceso a personas no autorizadas. Al existir infinidad de hackers que se dedican a los ataques cibernéticos para cometer ilícitos, de esta manera poder afectar los datos sensibles de las empresas.

El monitoreo relacionado a la Seguridad de la Información y de los sistemas tecnológicos se vincula directamente a todo un conjunto de normas como es la ISO 27001:2013 para buscar los mecanismos para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de datos y la información utilizada por los empleados de la organización.

Al tener conocimiento que la información formar parte proactiva dentro de la organización. Tenemos la necesidad de adaptar a su gestión de negocio o emprendimiento,

controles de seguridad que permita a la organización que la información aquí mesurada sea confiable y esté disponible en todo momento, por lo cual al incorporar todos los lineamientos de seguridad minimizaremos los riegos de un manejo poco ético de la información.

1.1.1 NORMA ISO 27001:2013

Es una norma internacional que detalla lineamientos de seguridad de la información, los cuales permiten implementar en la gestión de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información, ayudando así a proteger la información de posibles robos o daños. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (Kosutic, 2014)

1.2 MARCO TEÓRICO Y CONCEPTUAL

1.2.1 METODOLOGIAS

1.2.2 OWASP

El sistema OWASP a lo largo del tiempo ha evolucionado en un estándar en el mundo de la ciberseguridad para detectar y corregir debilidades en el desarrollo de software y hardware.

Su propósito es identificar amenazas y ayudar a los desarrolladores de todo el mundo a mantenerse al día con las aplicaciones y los dispositivos que consumimos.

El proceso OWASP logra dos objetivos. Así mismo, es un recordatorio constante de estas amenazas, para que los desarrolladores las tengan siempre en cuenta. Por otro lado, brinda acceso gratuito a los dispositivos para probar debilidades y evitar que lleguen al producto final.

Las guías de prueba son el primer método de prueba de ciberseguridad para desarrolladores de aplicaciones y profesionales de la seguridad. Hay instrucciones para web y móvil, incluye instrucciones de revisión del código de seguridad.

1.2.3 MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos que proporciona un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para así poder implementar las medidas de control más adecuadas que permitan mitigar los riesgos. Magerit se basa en analizar el impacto que puede tener para la empresa la

violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser aprovechadas por estas amenazas, obteniendo una identificación clara de las medidas preventivas y correctivas más apropiadas.

- Esta metodología es muy útil, ya que permite enfocar los esfuerzos en los riesgos que pueden ser más críticos para la empresa, aquellos relacionados con los sistemas de información.

- Magerit persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.

- Ofrecer un método sistemático para analizar tales riesgos.

- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

1.3. CONCEPTOS

1.3.1 LA INFORMACIÓN

El gráfico 1 muestra que, la información podría ser clasificada de distintas maneras, sin embargo, por la forma de comunicarse poseemos: Hablada en reuniones, impresa o redactada en papel, almacenada electrónicamente, transmitida por correspondencia común o electrónicamente, Exhibido por clip de videos corporativos. Los activos de la información son todo lo cual tiene costo para la organización como: Programa, servicios, intangibles como la fama e imagen, personas y sus capacidades, certificaciones, PC, servidor etc.

Gráfico 1. ACTIVOS DE LA INFORMACIÓN

Nota: Tomado de Bendermacher

1.3.2 SEGURIDAD DE LA INFORMACIÓN

"Seguridad de información es establecer que necesita ser salvaguardado y por qué, de que debería ser salvaguardado y cómo protegerlo", es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos tienen la

posibilidad de conllevar males sobre la información, comprometer su confidencialidad, veracidad o totalidad y disponibilidad, reduciendo el rendimiento de los conjuntos o bloquear la entrada a usuarios autorizados al sistema.

No obstante, esta administración puede servir parcialmente, poco o nada si hay fallas de hardware, de programa, fallas humanas, desastres naturales, ataques terroristas, entre otros, sin que la organización haya estado preparada para estos sucesos Es fundamental que, en todo este proceso, saber de qué defender, de quien defender y cómo defender, esta es el término clave para lograr direccionar el diseño y el mejoramiento constante del SGSI.

1.3.3 CALIDAD DE LA INFORMACIÓN

Se caracteriza por la preservación de los próximos puntos:

• Confidencialidad: Se garantiza que la información sea accesible solo para esos que se encuentren autorizados.

• Totalidad: Protegiendo la precisión de la información en su procesamiento, así como su modificación autorizada.

• Disponibilidad: Asegurando que los usuarios autorizados tengan ingreso a la información y a los activos asociados una vez que sea primordial.

1.3.4 SEGURIDAD INFORMÁTICA

Los desastres naturales (Incendios, inundaciones, terremotos, etcétera.), los poseemos presente en el momento de localizar los emplazamientos del centro de proceso de datos donde alojamos los primordiales servidores de la compañía; sin embargo, aunque tengamos el mejor sistema de extinción de incendios o la sala se encuentre perfectamente sellada, continuamente deberíamos tener un segundo CPD (centro de procesamiento de datos) para que la actividad no pare. Debemos defender la entrada a la sala del CPD por medio de diversas medidas de estabilidad: vigilantes, tarjetas de ingreso, identificación por medio de cliente y contraseña, etcétera. Dichos servicios los contrataremos con determinados suministradores, empero debemos estar preparados para las situaciones en que no logren proporcionarlo: unas baterías o un conjunto electrógeno por si fracasa la corriente eléctrica, una segunda conexión a internet como línea de backup, inclusive tenemos la posibilidad de optar por una solución inalámbrica para estar salvaguardados frente a un corte del servicio. Como pasa con el spam en la correspondencia electrónica, el malware es programa no anhelado y que debemos borrar, perdida de datos generalmente.

1.3.5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El gráfico 2 muestra la porción del sistema general de administración, que comprende la política, la composición organizativa, los métodos, los procesos y los recursos necesarios para implantar la administración de la estabilidad de la información en una organización se llama SGSI. Para llevar a cabo un sistema de administración de estabilidad de información en una organización, debería tener en cuenta lo próximo: Formalizar la administración de estabilidad de información, Examinar y gestionar los peligros. Implantar los procesos de administración de estabilidad con base a la metodología, Afirmar la administración de la estabilidad.

Gráfico 2. PROYECTOS QUE CONSTITUYEN UN SGSI

Nota: Tomado de Gómez.

1.35 LA NORMA ISO/27001

El gráfico 3 muestra la regla ISO 27001, es un estándar desarrollado como modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y optimización de un SGSI para cualquier tipo de organización.

El ISO 27001:2013 es el exclusivo estándar certificable, aceptado internacionalmente de forma universal para la administración de la estabilidad de información; aplica a toda clase de empresas, tanto por su tamaño como su actividad. La aplicación de unos sistemas de procesos, en la organización, junto con la identificación y las intersecciones de dichos procesos, así como su administración, puede denominarse como enfoque con base en procesos. El enfoque con base en procesos para la administración de la estabilidad de información presentada en esta regla, enfatiza a los usuarios, el valor de: La comprensión de los requisitos de la estabilidad de una organización y la necesidad de implantar políticas y fines para la estabilidad de información, Llevar a cabo y operar controles para guiar los peligros de la estabilidad de información de una organización con el entorno de los peligros globales del comercio de la organización, Hacer seguimiento y verificar el manejo y la eficiencia del SGSI, Optimización continua basado en mediciones fines. Encierra a los individuos, los procesos y las tecnologías de información.

Gráfico 3. NORMA ISO 27001

Nota: Tomado de https://elizabthtebazile.wordpress.com/

CAPITULO II

METODOLOGÍA DE LA INVESTIGACIÓN

En este caso la metodología de investigación constituye un marco, a utilizarse para resolver el problema de investigación mediante la recopilación de datos utilizando diversas técnicas, haciendo uso de los métodos convenientes.

2.1 ASPECTOS GENERALES DE LA INVESTIGACIÓN

2.1.1 TIPO DE INVESTIGACIÓN

INVESTIGACIÓN APLICADA

La investigación aplicada es aquella que busca modificar una realidad presente con alguna finalidad práctica, es decir, tiende a la resolución de problemas o al desarrollo de ideas a corto o mediano plazo, dirigidas a conseguir innovaciones (Leiva, 2001).

Para Ibáñez la investigación aplicada o también llamada tecnológica depende de las nociones básicas cuyo objetivo se basa en la aplicación práctica de manera instantánea, lo que significa, que no se enfoca en desarrollar teorías o principios sino en solucionar problemas específicos (Ibáñez, 2015).

La razón por la cual se va a utilizar la investigación aplicada es porque se anhela innovar el proceso de gestión de la seguridad de la información mediante el estudio, análisis e implementación de un modelo de seguridad lógica de la información.

2.1.2 ENFOQUE

El presente proyecto de investigación se basará en un enfoque mixto (cualitativo-cuantitativo)

El investigador que quiere saber algo sobre la experiencia subjetiva de una enfermedad mental crónica, debe realizar entrevistas biográficas con algunos pacientes y analizarlas muy detalladamente. El Investigador que desee averiguar algo sobre la frecuencia y la distribución de estas enfermedades en la población debe efectuar un estudio epidemiológico sobre este asunto. Para la primera pregunta, son apropiados los métodos cualitativos; para la segunda pregunta son adecuados los cuantitativos, cada método se abstiene de entrar en el territorio del otro (Flick, 2012, p. 278).

Según Báez y Pérez el método cualitativo se adhiere a la corriente de pensamiento fenomenológica cuya meta principal se basa en conocer las razones, cuestionamientos del porqué acontece lo que acontece. Por tal razón se fundamenta en lo que se observa y habla con los actores entre ellos empleados, clientes, consumidores, expertos, entre otros, de la realidad, para que con esto se explique lo que causa sus comportamientos, como se perciben los acontecimientos y que actitudes sustentan sus actos (Báez & Pérez, 2007).

El método cuantitativo se basa principalmente en la medición de las características de los fenómenos sociales, lo cual supone derivar un marco conceptual pertinente al problema analizado. Este método tiende a generalizar y normalizar resultados (Bernal Torres, 2006).

Además (Packer, 2013) da conocer la visión común de la investigación cualitativa y cuantitativa.

Para lo cual utilizaremos la técnica de la entrevista en el estudio

2.1.3 ANÁLISIS COMPARATIVO DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGOS TI

Tabla 1. ANÁLISIS COMPARATIVO DE LAS METODOLOGÍAS DE ANÁLISIS DE RIESGOS TI

Metodología	**Características**	**Conceptos**	**Fases**	**Ámbito de aplicación**	**Ventajas**	**Desventajas**
OCTAVE	Desmitificar la falsa creencia: La Seguridad Informática es un asunto meramente técnico. 2- Presentar los principios básicos y la estructura de las mejores prácticas internacionales que	Construcción de los Perfiles de Amenazas Basados en Activos. Identificación de la Infraestructura de	Visión de organización. Visión Tecnológica. Planificación de las medidas y reducción riesgos.	Análisis de riesgos para seguridad de sistemas de información.	Es una metodología auto dirigida, es decir, la organización gestiona y dirige la evaluación de sus riesgos a través de un equipo multidisciplinario. Comprende los	No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. Usa muchos documentos

	guían los asuntos no técnicos. Octave divide los activos en dos tipos que son: 1. Sistemas, (Hardware. Software y Datos). 2. Personas	Vulnerabilidades Desarrollo de Planes y Estrategias de Seguridad			procesos de análisis y gestión de riesgos. - Involucra a todo el personal de la entidad.	anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace tediosa, complicada de entender. Requiere de profundos conocimientos técnicos.
	Creado por el	Escalas de	1. Análisis de	Análisis y	Se le considera	El hecho de tener

MAGERIT	Consejo Superior de Administración Electrónica de España. Orientada a los sistemas de información. Persigue los siguientes objetivos: Concientizar a los responsables de los sistemas de información de la existencia de riesgos	valores cualitativos, cuantitativo s y de indisponibilidad del servicio. Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia. Escala alternativa de	riesgos. 2.Caracterización de los activos: a. Caracterización de las amenazas b. Caracterización de las salvaguardas c. Estimación del estado del riesgo. Gestionar los riesgos	gestión de riesgos de los sistemas de información: Gobierno, Organismos, compañías grandes, PYME.	con un alcance completo, tanto en el análisis como en la gestión de riesgos. Posee un extenso archivo de inventarios en lo referente a Recursos de Información, Amenazas y tipo de Activos. Permite un análisis	que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa. No involucra a los procesos, recursos ni vulnerabilidades

	y de la necesidad de atajarlos a tiempo. Ofrecer un método sistemático para analizar tales riesgos. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría,	estimación del riesgo			completo cualitativo y cuantitativo. De carácter Público	como elementos del modelo a seguir

	certificación o acreditación, según corresponda en cada caso					
ISO/IEC 27005	Creado por la organización para la estandarización (ISO). Para análisis cuantitativos y cualitativos. Presenta ejemplos de vulnerabilidades. Describe formas de	Conciencia Responsabilidad. Respuesta. Evaluación del riesgo. Gestión de la seguridad. Reevaluación	1.Establecimiento del contexto. 2. Valoración del riesgo. 3. Tratamiento del riesgo. 4. Aceptación del riesgo. 5. Comunicación	Estándar para la gestión de riesgos de seguridad de la información: Aplicable a cualquier organización sin importar	Estándar internacional, lo que le faculta mayor aceptación Posee una cláusula completa orientada a la monitorización y revisión de riesgos.	No detalla la forma de valorar las amenazas. No es certificable No posee herramientas, técnicas, ni comparativas de ayuda para su

	valoración. Detalla la forma de identificar activos y hacer su valoración, provee ejemplos. Presenta ejemplos de amenazas típicas, Restringido / de pago.		del riesgo. 6. Monitoreo y revisión.	tipo, tamaño o naturaleza	Se la considera con un alcance completo, tanto en el análisis como en la gestión de Riesgos. Posee la fase de aceptación de riesgos, previa su justificación. Permite un análisis completo cuantitativo	implementación

MEHARI	Método para la evaluación y gestión de riesgos según requerimientos de ISO/IEC27005:2008. Comprende bases de datos de conocimiento, con manuales y guías que describen los diferentes módulos (amenazas, riesgos, vulnerabilidades). Modelo de riesgos	Diagnóstico de Seguridad. Análisis de los Intereses Implicados por la Seguridad Análisis de Riesgos	Establecimiento del contexto Tipología y lista de activos principales. Análisis de activos: activos de respaldo y vulnerabilidades intrínsecas. Daños potenciales: lista de posibles escenarios de	Gobierno, Organismos, Empresas medianas y grandes, compañías comerciales, sin fines de lucro (educación, salud, servicios públicos.	Usa un modelo de análisis de riesgos cualitativo y cuantitativo.	Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio. La recomendación de los controles no la incluye

	cualitativo y cuantitativo. Capacidad para evaluar y simular los niveles de riesgo derivado de medidas adicionales.		riesgos.			dentro del análisis de riesgos sino en la gestión de los riesgos. La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.

2.2 METODOLOGÍA DEL DESARROLLO DE LA PROPUESTA

2.2.1 MAGERIT

Para el análisis de riesgos del Centro Médico ¨Cotacachi¨ se utilizará la metodología MAGERIT, la cual permite determinar las medidas apropiadas para cuantificar y dar el tratamiento adecuado a los activos que posee la empresa.

2.2.2 DESARROLLO DE LA METODOLOGÍA

Como apoyo al desarrollo de esta metodología se utilizará la herramienta EAR/PILAR, la cual es una herramienta de análisis de riesgos que incorpora todos los elementos de la metodología MAGERIT en su 3ra versión.

2.2.3 IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

2.2.3.1 IDENTIFICACIÓN DE ACTIVOS.

Para realizar la identificación de los activos se utilizará el inventario proporcionado por la Gerencia y se determinara el tipo de activo al que pertenece de las áreas seleccionadas en el alcance, los cuales son:

Tabla 2. IDENTIFICACIÓN DE ACTIVOS.

Tabla 2. IDENTIFICACIÓN DE ACTIVOS.

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACION	1. [SRV_PPAL] Servidor Principal
	2. [SRV_MICRO] Servidor Microbiología
	3. [HPLC] Equipos HPLC
	4. [FORM_MTRAS] Formulas Maestras
	5. [BD_SG] BD Sistema de Gestión
	6. [BD_MICRO] BD MICROLAB
	7. [HD_BKP] Disco Duro Backups
SERVICIOS	8. [ANAL_MTRAS] Análisis de Muestras
	9. [RTDO_ANAL] Resultado de Análisis
APLICACIONES	10. [PGN_WEB] Página web
	11. [HER_OFI] Herramientas de ofimática
	12. [ANT_VIR] Antivirus
	13. [SO] Sistema Operativo
	14. [PLAT_SG] Plataforma Sistema de Gestión
	15. [MICROLAB] Plataforma MICROLAB 1.0
EQUIPAMIENTO INFORMATICO	16. [PC] Computadoras
	17. [IMP] Impresoras
	18. [FIREWALL] Firewall
	19. [SWT] Switch
REDES DE COMUNICACIONES	20. [WIFI] Router Wifi
	21. [LAN_SFC] Red LAN
	22. [TEL] Telefonía
	23. [IE] Internet
EQUIPAMIENTO AUXILIAR	24. [UPS] UPS
	25. [SIS_VIG] Sistema de Vigilancia
INSTALACIONES	26. [CPD] CPD
	27. [SFC] Empresa
PERSONAL	28. [DIR_CALIDAD] Directora Aseguramiento de Calidad
	29. [RRHH] Director de Talento Humano/HSE
	30. [DT] Directora técnica
	31. [ASIST_DIR_CALID] Asistente Dirección de Aseguramiento de Calidad
	32. [AN_FQ] Analista de Fisicoquímico
	33. [JF_CC] Jefe de Control de Calidad
	34. [AUX_MICRO] Auxiliar de Microbiología
	35. [JF_MICRO] Jefe de Microbiología
	36. [AN_STM] Analista de sistemas

Nota: Tomado de EAR/PILAR Centro Médico “Cotacachi”

2.2.3.2 VALORACIÓN DE ACTIVOS

Para valorar los activos se tomarán las siguientes dimensiones de seguridad de la metodología MAGERIT:

- [D] Disponibilidad.
- [I] Integridad de los datos.
- [C] Confidencialidad de la información.
- [A] Autenticidad.
- [T] Trazabilidad.

Tabla 3. VALORACIÓN CUALITATIVA.

Tabla 3. VALORACIÓN CUALITATIVA.

Valoración cualitativa	Escala de valor cuantitativo expresado en millones	Valor cuantitativo
Muy Alto (MA)	> $ 100	$ 100.000
Alto (A)	100 <valor> 50	$ 50.000
Medio (M)	50 <valor> 30.000	$ 30.000
Bajo (b)	30.000 <valor> 10.000	$ 10.000
Muy bajo (MB)	10.000 <valor> 5.000	$ 5.000

Nota: Tomado de Fuente: Autor

Tabla 4. ESCALA DE VALORACIÓN DE ACTIVOS.

Tabla 4. ESCALA DE VALORACIÓN DE ACTIVOS.

VALOR		CRITERIO
10	Muy alto	Daño muy grave a la organización.
7 - 9	Alto	Daño grave a la organización.
4 - 6	Medio	Daño importante a la organización.
1 - 3	Bajo	Daño menor a la organización.
0	Despreciable	Irrelevante a efectos prácticos.

Nota: Tomado de Fuente: Autor

2.3 REQUISITOS FUNCIONALES

La seguridad es algo que todas las empresas deben tener, pero ninguna suele utilizar. Pensar de esta manera puede traer muchos problemas, para obtener dicha seguridad se puede utilizar la norma ISO 27001.A menos que el propósito del sistema esté relacionado con la seguridad, los usuarios prestan poca atención sobre cómo encaja la seguridad en un producto, y cómo se garantiza que funcione de manera correcta cuando sea necesario. A los sistemas críticos de un avión o un coche se acceden mediante los sistemas de entretenimiento, ya que la mala interpretación de seguridad y verificación, son claros ejemplos.

Evaluar los requisitos según el valor de la información para el negocio.

La seguridad adecuada refleja el valor de la información para la organización. Todos los requisitos deben priorizarse según con los propósitos de negocio que se encuentran destinados a protegerse.

La integración de los requisitos de gestión en las primeras etapas de un proyecto

Cuanto antes se tenga en consideración la seguridad, más opciones existen de tratar las situaciones de riesgo.

2.4 HISTORIAS DE USUARIOS

Tabla 5. HISTORIAS DE USUARIOS

ID HISTORIA DE USUARIO	TIPO DE USUARIO	TAREA	OBJETIVO
H1	usuario,usuario administrador	Login	ingresar al sistema.
H2	usuario,usuario administrador	Recuperar contraseña	Restablecer contraseña en caso de olvido.
H3	usuario administrador	Registro de usuarios	Registrar la información de los usuarios en el sistema.
H4	usuario administrador	Editar Usuarios	Modificar la información de los usuarios en el sistema.
H5	usuario administrador	Eliminar Usuarios	Eliminar usuarios del sistema

Nota: Tomado de Fuente: Autor

2.4.1 PRODUCTBACKLOG

Tabla 6. PRODUCTBACKLOG

BACKLOG ID	ID HISTORIA DE USUARIO	ESTIMACIÓN	PRIORIDAD
B1	H1	9	Muy Alta
B2	H2	5	Alta
B3	H3	9	Muy Alta
B4	H4	5	Alta
B5	H5	5	Alta

Nota: Tomado de Fuente: Autor

2.5 SPRINT BACK LOG

La tabla 7 muestra cada uno de los Sprint cuenta con una duración de una semana, a continuación, se detalla el Sprint Back log de los realizados.

2.5.1 SPRINT 1

Tabla 7. SPRINT 1

BACKLOG ID	ESTADO
B1	Terminado
B2	Terminado
B13	Terminado

Nota: Tomado de Fuente: Autor

2.5.2 SPRINT 2

Tabla 8. SPRINT 2

BACKLOG ID	ESTADO
B1	Terminado
B2	Terminado
B13	Terminado

Nota: Tomado de Fuente: Autor

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

Los resultados obtenidos en este proyecto son del desarrollo de 3 métodos para proporcionar respeto a la finalidad de poder alcanzar los objetivos generales del proyecto.

Se recomiendan los siguientes pasos para realizar esta tarea:

DIAGNOSTICO. Esta actividad fue creada para hacer un análisis preliminar de la información y así poder enterarse del proceso de realizar todo lo que se hace en el Centro Médico ¨Cotacachi¨

AUDITORIA INICIAL. Para conocer el estado actual del tema de la seguridad de la información en la empresa y así poder hacer un plan preciso de la línea de trabajo que seguirá.

ANÁLISIS Y GESTIÓN DE RIESGOS. Durante este período se realiza el inventario de los activos en el que se determina que amenazas pueden existir en la empresa, además, se procede con la creación de una matriz de riesgos y gestión.

3.1 FASE DE DIAGNÓSTICO

Este proceso permitió tener en cuenta la gestión de la seguridad de información, en términos generales, se han identificado los siguientes:

- Falta de conciencia y conocimiento de los empleados acerca de la seguridad de la información.
- No existe una política de seguridad de la información bien establecida en la empresa en términos de definición de controles y evaluación de riesgos.
- No existe un sistema de información adecuado para la gestión de la seguridad, así como una evaluación adecuada de los riesgos de seguridad.
- La política de seguridad es incompatible con la misión de la empresa.

Este proceso de diagnóstico actual es importante ya que permite obtener pautas necesario para hacer el trabajo.

3.2 FASE DE AUDITORÍA INICIAL

Se ha realizado una auditoría interna, enumerando los controles a auditar en todas las áreas que hay que comprobar. Además, con los datos obtenidos se realiza un análisis preliminar la información de salida, será el espacio general del área tratada para encontrar las debilidades a ser abordadas.

ENTREVISTA VERBAL. Es posible obtener información de primera mano sobre las propiedades de la empresa, es decir, cómo hacer una gestión de activos, los problemas que trae su consolidación, problemas ocurridos en varios activos y cuentas del Centro Médico ¨Cotacachi¨.

Se hizo para conocer la opinión del gerente del Centro Médico ¨Cotacachi¨ y el proceso que controlan todos los días en el que se ven: el conocimiento de tener software seguridad, tener algún conocimiento del manejo adecuado de la información antes capacitación, identificar posibles correos electrónicos maliciosos o maliciosos puede dar lugar a la fuga de información, conocimientos valiosos y derechos de propiedad seguridad general.

La tabla 9 muestra los resultados presentados a continuación en la tabla N°9, son a los empleados dentro de la organización, se describe a continuación:

Tabla 9. Resultados de encuesta en el Centro Médico ¨Cotacachi¨

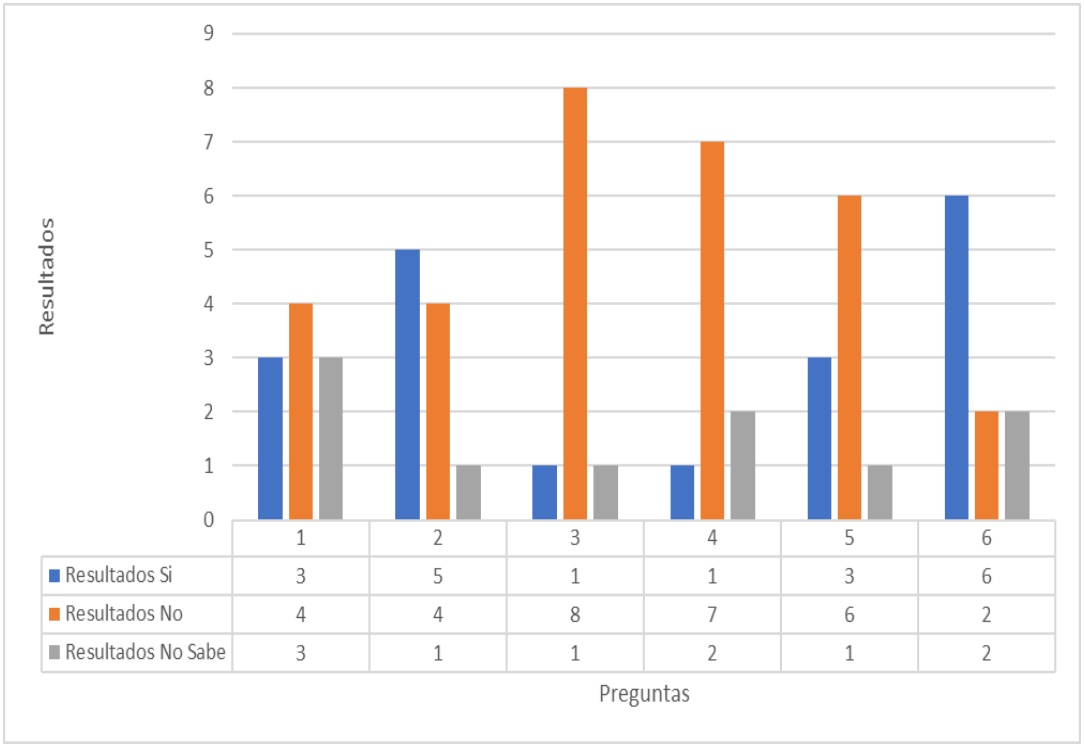
Tabla 9. RESULTADOS DE ENCUESTA EN EL CENTRO MÉDICO ¨COTACACHI¨

	Resultados			
Preguntas:	**Sí**	**No**	**No sabe**	**Comentarios**
¿Tienes software instalado en tu computadora para detectar, bloquear y recuperarse de un ataque de software malicioso, por ejemplo, un ataque de virus científico de la computación?			3	No tienen conocimiento
Como empleado, usted sabe el riesgo de ataques de software ¿Malware o virus informático?			1	No tienen conocimiento
Recibiste todo tipo capacitación y software utilizado para detectar,			1	No tienen conocimiento

prevenir y recuperar ¿Un ataque informático a su organización?				
¿Actualiza usted periódicamente el software antivirus?			2	No tienen conocimiento
¿Al enviar correos electrónicos de carácter profesional con información sensible de su organización, utiliza algún tipo de encriptación?			1	No tienen conocimiento
¿Ha recibido un correo electrónico de dudosa procedencia con información rara? Ejemplo: pidiendo que hagan clic o compartir ¿información personal?			2	Se entrenaron siendo parte del departamento sistema.

Nota: Tomado de Fuente: Autor

Gráfico 4. RESULTADOS DEL ANÁLISIS DE RIESGOS

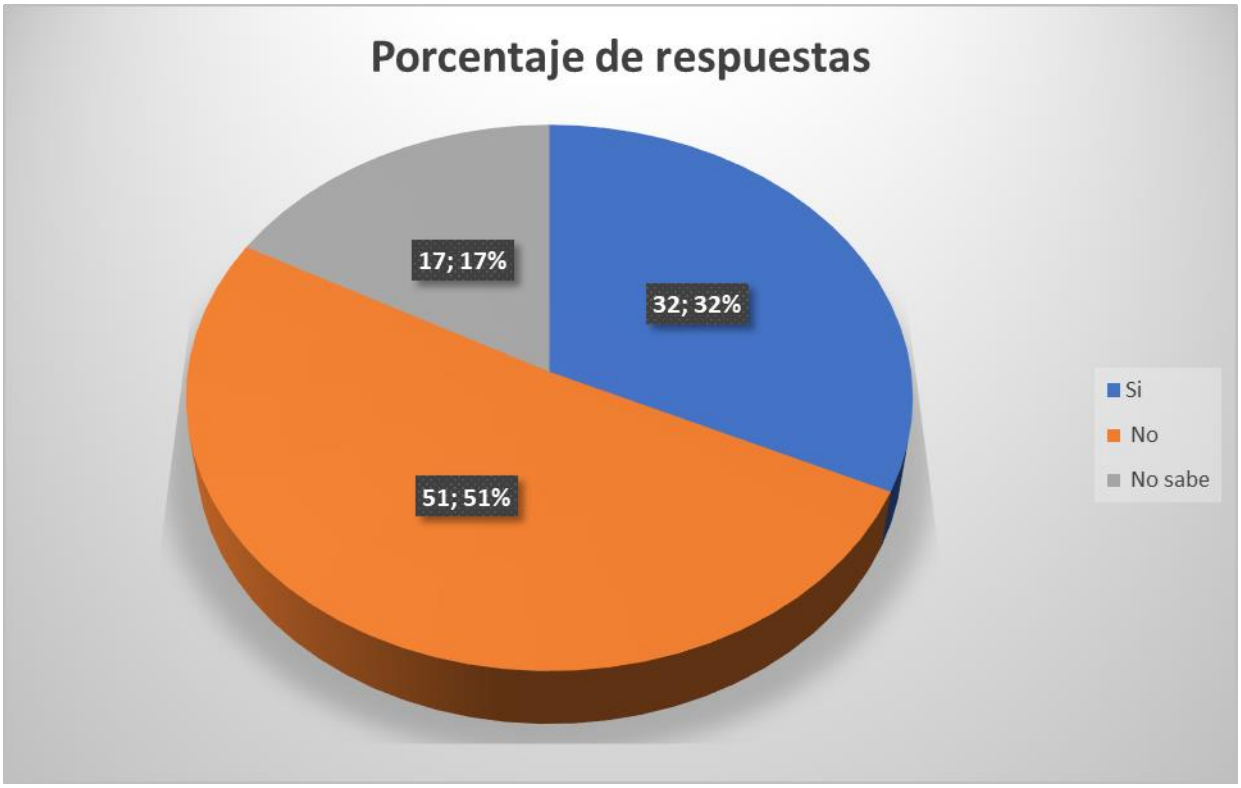


Nota: Tomado de Fuente: Autor

.

El gráfico 5 muestra que el 51% de las respuestas recibidas fueron negativas, lo que sugiere que era falta de conocimiento sobre la gestión de la información y el uso de la tecnología de la información para su protección. Mientras que el 32% de las respuestas positivas y el 17% de los participantes no sabían nada ante las dudas planteadas en cada pregunta. Se diseña un plan para ello. en capacitación a todos los funcionarios del Centro Médico ¨Cotacachi¨ para que sean actualizados en sus conocimientos tecnológicos y uso adecuado de la información para su protección.

Gráfico 5. PORCENTAJE DE RESPUESTAS



Nota: Tomado de Fuente: Autor

3.3 ANÁLISIS DE ACTIVOS

FASE I. IDENTIFICAR ACTIVOS

3.3.1.1 ACTIVOS

El centro médico ¨Cotacachi¨ cuenta con activos tangibles e intangibles que permiten su operación en el logro del cumplimiento el ámbito de la salud, estos se clasifican así:

3.3.1.2 CLASIFICACIÓN ACTIVOS

La tabla 10 muestra la clasificación de los activos del centro médico.

Tabla 10. ACTIVOS TANGIBLES

Infraestructura
• Red de Datos
• Red Eléctrica
• Instalación de red de datos • Instalación de red de Eléctrica • Planta de la Organización

• **Personas**
• Analista
• Pacientes
• Funcionales • Personal administrativo • Proveedores
• Usuarios Externos
• Usuarios Internos

• **Hardware / Equipo Informático**
• Cámaras de Seguridad • CD/DVD • Computadores de Escritorio
• Discos Portables
• Dispositivos Móviles
• Equipos Multifuncional
• Impresoras • Memoria USB
• Módems
• Portátiles
• Routers
• Servidores

• Teléfonos

Nota: Tomado de Fuente: Autor

La tabla 11 muestra la clasificación de los activos intangibles del centro médico.

Tabla 11. ACTIVOS INTANGIBLES

• **Datos/Información**
• Archivos de Datos
• Base de Datos
• Contratos
• Documentación del Sistema
• Documentos Internos
• Entregables (CD/DVD)
• Formatos
• Hojas de Vida
• Información Disco Portables
• Información en Carpetas compartidas en Red
• Información Memorias USB
• Manuales de Usuario
• Material Físico (Impreso)

• **Software/Aplicaciones Informáticas**
• Antivirus
• Desarrollo - IDE • Desarrollos a medida y/o propios de la Organización • Licencias
• Motor Base de Datos
• Navegadores
• Office
• Sistemas Operativos

• **Servicios Auxiliares**
• Almacenamiento de Información • Capacitaciones • Fluido Eléctrico
• Internet
• Red Inalámbrica
• Telefonía

Nota: Tomado de Fuente: Autor

3.3.1.3 ETIQUETADO DE ACTIVOS

Existe una gran importancia en identificar los activos mediante un sistema lógico y ordenado de etiquetas ejemplo:

La tabla 12 muestra la clasificación el etiquetado de los activos del centro médico.

Tabla 12. ETIQUETADO DE ACTIVOS

• **ACTIVO**	**ETIQUETA**
• Hardware	HW-000000
• Información	IF-000000
• Infraestructura	IFR-000000
• Personas	RH-000000
• Servicios	SRV-000000
• Software	SW-000000
• Equipamiento Auxiliar	AUX-000000

Nota: Tomado de Fuente: Autor

3.3.1.4 CRITERIOS DE VALORACIÓN DE ACTIVOS

La tabla 13 muestra la valoración de los activos del centro médico.

Tabla 13. CRITERIOS DE VALORACIÓN DE ACTIVOS

CONCEPTO	**ID**
Confidencialidad de la información	C
Disponibilidad Integridad de los datos Autenticidad	D I A
Trazabilidad	T

Nota: Tomado de Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html

La tabla 14 muestra la dimensión de valoración de los activos del centro médico.

Tabla 14. DIMENSIÓN DE VALORACIÓN DE ACTIVOS

Nivel de Valor	Valor	Criterio
10	Extremo	Daños extremadamente graves
9	Muy Alto	Daño muy grave
6 a 8	Alto	Daño grave
3 a 5	Medio	Daño importante
1 a 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Nota: Tomado de Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html

La tabla 15 muestra criterios de valoración de los activos del centro médico.

Tabla 15. CRITERIOS DE VALORACIÓN DE ACTIVOS

NIVEL DE VALOR	CRITERIO
8 – 10	Restringido
4 – 7	Uso Interno
0 – 3	Pública

Nota: Tomado de Fuente:https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html

RESTRINGIDO: información que no se permite divulgar entre las diferentes áreas de la organización, afectando la intimidad del personal o trabajo de cada área o simplemente es información vital para el debido funcionamiento de la organización. Ej.: información de la base de datos, contraseñas de servidores, hojas de vida etc.

USO INTERNO: información que circula al interior de una empresa u organización. Busca llevar un mensaje para mantener la coordinación entre las distintas áreas, permite la introducción, difusión y aceptación de pautas para el desarrollo organizacional. Los trabajadores necesitan estar informados para sentirse una parte activa de la organización. Esta información es útil para tomar decisiones.

PÚBLICA: información a la cual toda persona interna y externa de la organización tiene acceso por cualquier medio de comunicación, sin previa autorización, sin censura o impedimento. Eje: página web de la organización.

4.1 FASE II IDENTIFICACIÓN DE AMENAZAS

Una vez identificados los activos es necesario relacionarlos con aquellos riesgos que se pueden materializar y generar una degradación, pérdida total o parcial de cada uno de ellos.

Amenaza causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008].

De acuerdo con Magerit y en general las metodologías de riesgos y amenazas se pueden clasificar en cinco grandes grupos así:

- De origen natural
- Del entorno (de origen industrial)
- Defectos de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada

La tabla 16 muestra la codificación según el tipo de amenaza.

Tabla 16. CODIFICACIÓN SEGÚN TIPO DE AMENAZA

Tipo de amenaza	**ID**
Desastre Natural	[N]
Origen Industrial	[I]
Errores y Fallos no intencionados	[E]
Ataques intencionados	[A]

Nota: Tomado de Fuente:https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html

4.1.1 AMENAZAS ORIGEN DESASTRE NATURAL

La tabla 18 muestra las amenazas de origen natural.

Tabla 17. AMENAZAS ORIGEN DESASTRE NATURAL

[N.1] AGUA	
Tipos de Activos	Dimensiones
• [HW] equipos informáticos (hardware)	1.D

• [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	
Descripción:	
Eventualidad ocasionada por fuga de agua o desastre natural, maremotos, tsunami etc. Ver: **CMC: 02 - PERJUICIOS OCASIONADOS POR EL AGUA**	

[N.2] FUEGO	
Tipos de Activos	Dimensiones
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	1.D

• [L] instalaciones	
Descripción:	
Eventualidad de que el fuego ocasione daño sobre los activos del sistema Ver: **CMC: 01- INCENDIO**	

Nota: Tomado de Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html

4.1.2 AMENAZAS ORIGEN ERRORES Y FALLAS NO INTENCIONADOS

La tabla 19 muestra las amenazas de origen errores y fallas no intencionados del centro médico.

Tabla 18. AMENAZAS ORIGEN ERRORES Y FALLAS NO INTENCIONADOS

[E.1] ERRORES DE USUARIO	
Tipos de Activos	**Dimensiones**
• [D] datos / información • [keys] claves criptográficas • [S] servicios	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad

• [SW] aplicaciones • [Media] soportes de información	
Descripción:	
Equivocaciones de las personas cuando usan los servicios, datos, etc.	

[E.2] ERRORES DE ADMINISTRADOR	
Tipos de Activos	**Dimensiones**
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones • [HW] equipos informáticos	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad

• [COM] redes • [Media] soportes de información	
Descripción:	
Equivocaciones de personas con responsabilidades de instalación y operación	

Nota: Tomado de Fuente: Autor

4.1.3 AMENAZAS ORIGEN ATAQUES INTENCIONADOS

La tabla 20 muestra las amenazas origen ataques intencionados.

Tabla 19. AMENAZAS ORIGEN ATAQUES INTENCIONADOS

[A.1] MANIPULACIÓN DE REGISTROS DE LOG	
Tipos de Activos	Dimensiones
• [D.log] registro de actividad	1. [I] integridad (Trazabilidad)
Descripción:	
Edición de los datos originales registrados por los sistemas informáticos	

[A.2] MANIPULACIÓN DE LA CONFIGURACIÓN	
Tipos de Activos	Dimensiones
• [D.log] registro de actividad	1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
DESCRIPCIÓN:	
prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: Privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

Nota: Tomado de Fuente: Autor

5.1 FASE IV IDENTIFICACIÓN SALVAGUARDAS

Una vez que nuestros activos y amenazas ocultas estén expuestos varios riesgos, se deben establecer mecanismos de defensa, aquí están las cosas más importantes. total, por DNI Y tipo de protección.

6.1 FASE V EVALUAR EL RIESGO

6.1.1 DETERMINACIÓN DEL IMPACTO POTENCIAL

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos7:

Nota: riesgo e impacto potencial son valoraciones que se introducen como teóricas.

PROBABILIDAD: cuán probable o improbable es que se materialice la amenaza

La tabla 21 muestra la degradación de valor.

Tabla 20. DEGRADACIÓN DE VALOR

ID	PROBABILIDAD	OCURRENCIA
MA	Casi seguro	fácil
A	Muy alto	medio
M	posible	difícil
B	Poco probable	Muy difícil
MB	Muy raro	Extremadamente difícil

Nota: Tomado de Fuente: Autor

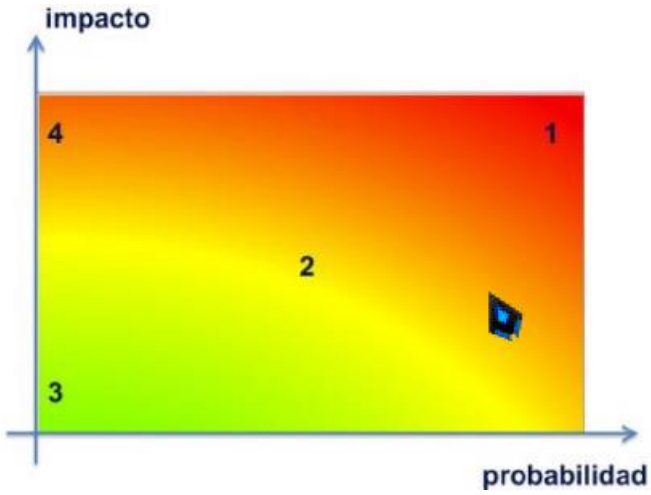
La tabla 22 muestra la probabilidad de ocurrencia.

Tabla 21. PROBABILIDAD DE OCURRENCIA

ID	**FRECUENCIA**	**PERIODO**
MA	Muy frecuente	A diario
A	frecuente	mensual
M	normal	Una vez al año
B	Poco frecuente	Cada varios años
MB	Muy poco frecuente	siglos

Nota: Tomado de Fuente: Autor

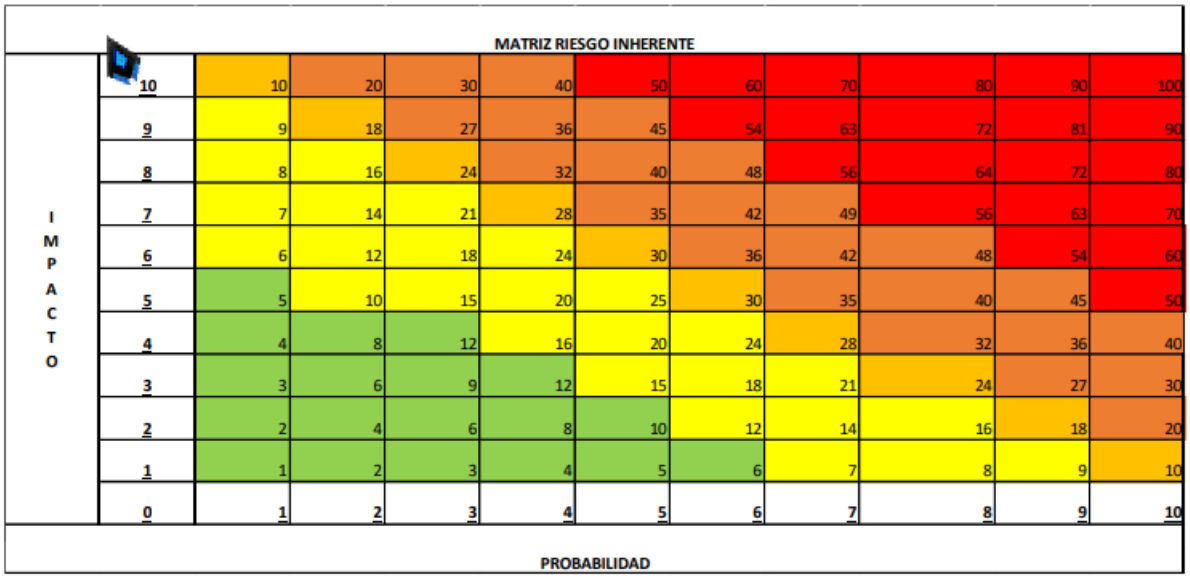
Gráfico 6. EL RIESGO EN FUNCIÓN DEL IMPACTO Y LA PROBABILIDAD



Nota: Tomado de Fuente:https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-imetodo/file.html

El gráfico 7 muestra la valoración hecha por el analista a través del análisis se da en el anexo los daños que puedan causarse a dichos bienes y la probabilidad de que se produzca el hecho peligroso materializar.

Gráfico 7. EL RIESGO EN FUNCIÓN DEL IMPACTO Y LA PROBABILIDAD



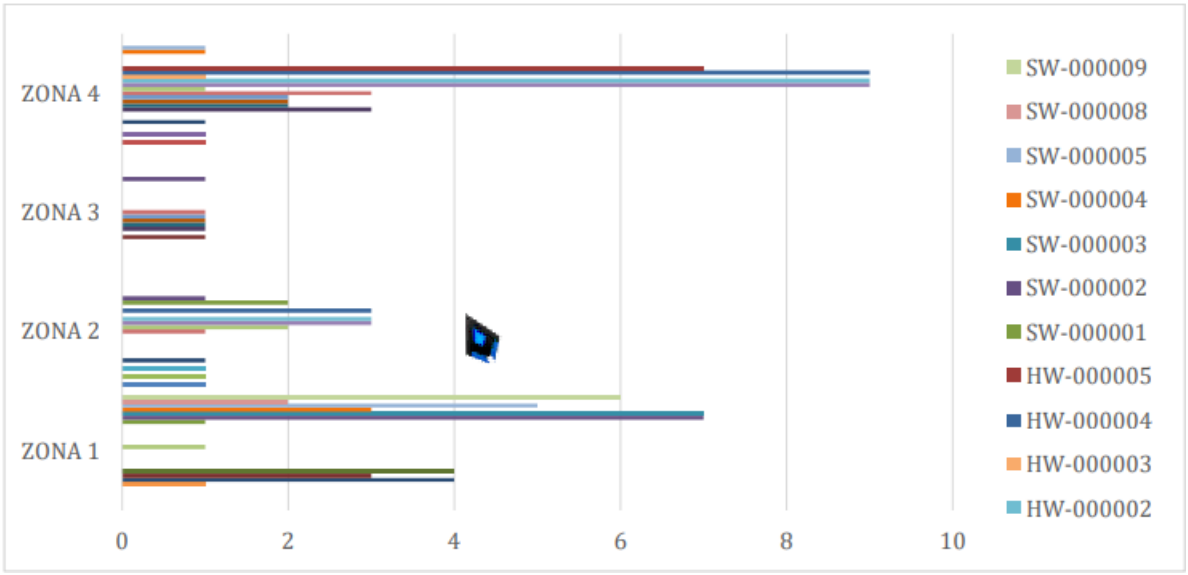
10	10	20	30	40	50	60	70	80	90	100
9	9	18	27	36	45	54	63	72	81	90
8	8	16	24	32	40	48	56	64	72	80
7	7	14	21	28	35	42	49	56	63	70
6	6	12	18	24	30	36	42	48	54	60
5	5	10	15	20	25	30	35	40	45	50
4	4	8	12	16	20	24	28	32	36	40
3	3	6	9	12	15	18	21	24	27	30
2	2	4	6	8	10	12	14	16	18	20
1	1	2	3	4	5	6	7	8	9	10
0	1	2	3	4	5	6	7	8	9	10

Nota: Tomado de Fuente: Autor

6.1.2 DETERMINACIÓN DEL RIESGO POTENCIAL

El gráfico 8 muestra la evaluación teórica que muestra el supuesto de que no hay protección activa, este índice (riesgo potencial) crece con influencia y probabilidad, puede causar daños al sistema.

Gráfico 8. DETERMINACIÓN DEL RIESGO POTENCIAL



Nota: Tomado de Fuente: Autor

7.1 METODOLOGÍA GESTIÓN DE LOS RIESGOS MAGERIT

7.1.1 EVALUACIÓN: INTERPRETACIÓN DE LOS VALORES DE IMPACTO Y RIESGOS RESIDUALES

El impacto y el riesgo residual es una medida de la situación actual en medio de la incertidumbre potencialmente sin salvaguardas y medidas adecuadas que reduzcan el impacto y el riesgo valores aceptables. Si estos dos valores son iguales, es señal de que la protección Lo que se implementó no fue efectivo, y no porque no se hizo nada, sino por elementos que quedaron básicamente sin cuidado.

El valor residual por sí mismo no es más que un número a menos que se combine con relación con lo que se debe y no se debe hacer de la debilidad Sistema. Los tomadores de decisiones deben ser conscientes de estas tareas que faltan y mantener un informe sobre debilidades y vulnerabilidades.

7.1.2 ACEPTACIÓN DEL RIESGO

Es responsabilidad de la alta dirección de la organización determinar si el nivel el impacto y el riesgo son aceptables después de las garantías. Debes aceptar la responsabilidad de deficiencias porque esta decisión no es técnica. Puede ser una decisión política o administrativa o esto puede ser estipulado por la ley o por obligaciones contractuales de proveedores o clientes. y Los niveles de aceptación se pueden asignar a activos o departamentos. No existe un nivel óptimo de riesgo. de lo contrario tomar mi conocimiento y aceptar formalmente la dirección.

7.1.3 TRATAMIENTO

Hay dos opciones a considerar para administrar la creación decidió utilizar algún tratamiento del sistema de seguridad desplegado para proteger el sistema de información: reducir el riesgo residual (aceptar un menor riesgo) y ampliar el riesgo residual (aceptar un mayor riesgo).

Se puede observar un comportamiento de ganancia-pérdida en el riesgo residual promedio. que puedan verse afectados por el escenario actual, incluido el análisis de la situación el sector donde trabaja frente a la 'norma'.

Existen 4 zonas de riesgo:

- Zona 1: aquí se encuentran los riesgos muy probables y de alto impacto la meta es sacarlos de esta zona
- Zona 2: se ubican los riesgos de probabilidad relativa y con un impacto medio, se deben tomar acciones.
- Zona 3: están los riesgos poco probables y de impacto bajo. Comúnmente se deja con esta o se les permite subir un poco si esto nos genera ganancias en otra área.
- Zona 4: riesgos improbables, pero de gran impacto: son un desafío para la toma de decisiones ya que su bajo índice de ocurrencia no justifica que se tomen medidas preventivas, pero su elevado impacto exige que se tenga previsto la reacción en su ocurrencia y la recuperación.

En general, estos escenarios de incertidumbre afectan a las Zonas 3 y 4 cuanto mayor sea la posibilidad, más rápido puede llegar a usted mismo o a otra persona y salir en la incertidumbre, En cualquier caso, la incertidumbre debe considerarse mala y necesaria. hacer algo como: encontrar formas de predecir mejor el efecto, revisar los foros, centros de reacción o expertos en la materia. Otra forma es cambiar algunos

aspectos, arquitectura de componentes o sistemas. Por último, preparar los sistemas de alarma. o procedimientos flexibles de retención y renovación.

7.1.4 ESTUDIO CUANTITATIVO DE COSTE BENEFICIO

Por razones lógicas, no se puede invertir en protección más de su valor quieres estar seguro, pero el conjunto de estas razones lógicas en la práctica no es evidente ni siquiera por cálculo. riesgo o calcular el costo de las medidas de seguridad.

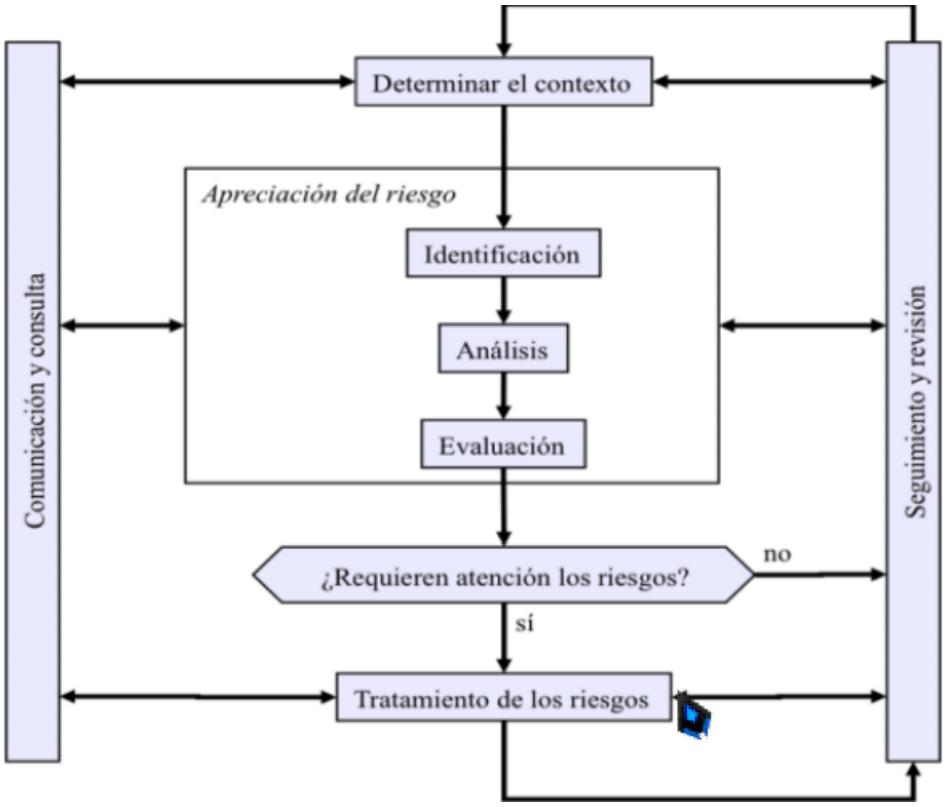
7.1.5 ESTUDIO CUALITATIVO DE COSTE/ BENEFICIO

Cuando los beneficios intangibles se ven en la relación costo-beneficio, dificultan el cálculo punto de equilibrio numérico, algunos aspectos intangibles que se suelen considerar son:

- Beneficios en la reputación o en la imagen.
- Beneficios en la competencia en comparación con otras organizaciones del mismo sector productivo.
- Cumplimiento en normas obligatorias o voluntarias.
- Mejoras en la capacidad de la operación.
- Mejoras en la productividad.

7.1.6 FORMALIZACIÓN DE ACTIVIDADES

Gráfico 9. PROCESO DE GESTIÓN DE RIESGO (MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS



Nota: Tomado de Fuente:https://www.ccncert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)

7.1.7 ROLES Y FUNCIONES

Muchos actores implementadores intervienen en el proceso de gestión de riesgos las siguientes funciones y responsabilidades:

- Órganos de gobierno
- Dirección ejecutiva
- Dirección operacional

A continuación, se identifican algunos roles que están involucrados en el proceso de gestión de riesgos.

- Responsables de la información
- Responsables del servicio
- Responsables de la seguridad
- Responsables del sistema

8.1 CHECK LIST DE EVALUACIÓN

8.1.1 PLAN DE SEGURIDAD

Describe la forma en que se llevan a cabo los proyectos para su cumplimiento. decisiones tomadas de acuerdo con el enfoque de gestión de riesgos.

8.1.2 CHECK LIST DE EVALUACIÓN (ESTADO DE MADUREZ)

Entidad Auditada: Centro Médico ¨Cotacachi¨

ALCANCE DE LA AUDITORÍA: Se auditó el área de Departamento de seguridad informática en la forma como se garantiza la seguridad de los sistemas.

El departamento de seguridad de TI dentro de la organización apoya todo operaciones porque se realizan a través de redes informáticas donde se transmiten y almacenan toda la información comercial.

Objetivos del área auditada dentro de la organización:

- Identificar el estado actual del SGSI en la organización
- Asegurar el funcionamiento y disponibilidad de las plataformas tecnológicas.
- Ofrecer oportunidades de mejora al SGSI

NIVEL DE MADUREZ

La tabla 23 muestra el nivel de madurez es métodos "reproducibles pero intuitivos L2" seguridad básica, sin metodología definida con precisión, documentación, modelo o para medirlo, no hay conocimientos de seguridad dentro de la organización, es necesario Trabajar duro para crear conciencia entre la alta dirección porque no hay una política clara, no es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando sea necesario Los procesos no están funcionando de manera eficiente.

Tabla 22. NIVEL DE MADUREZ

FACTOR	NIVEL	SIGNIFICADO
0%	L0	inexistente
20%	L1	inicial
40%	L2	reproducible pero intuitivo
60%	L3	proceso definido
80%	L4	gestionado y medible
100%	L5	optimizado

Nota: Tomado de Fuente: Autor

MARGO LEGAL

En esta sección se describen cuestiones relacionadas con las reglamentaciones que se aplican tanto a ser útil y complementario a la gestión de riesgos a nivel nacional e internacional.

- Seguridad en el ámbito de la Administración electrónica
- Protección de datos de carácter personal (Habeas Data)
- Firma electrónica
- Seguridad de las redes y de la información

RESULTADOS OBTENIDOS LUEGO DE APLICAR EL SGSI AL CENTRO MÉDICO ¨COTACACHI¨

FASE I DIAGNÓSTICO.

Gráfico 10. FASE I DIAGNOSTICO

A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	33.33%
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	33%
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	24.17%
A.6.1 Organización Interna	48.33%
A.6.2 Dispositivos móviles y teletrabajo	0.00%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	47.04%
A.7.1 Antes de asumir el empleo	100.00%
A.7.2 Durante la ejecución del empleo	41.11%
A.7.3 Terminación y cambio de empleo	0.00%
A.8 GESTION DE ACTIVOS	43.06%
A.8.1 Responsabilidad por los activos	62.50%
A.8.2 Clasificación de la información	66.67%
A.8.3 Manejo de Medios	0.00%
A.9 CONTROL DE ACCESO	61.15%
A.9.1 Requisitos de negocio para control de acceso.	69.05%
A.9.2 Gestión de acceso de usuarios	38.89%
A.9.3 Responsabilidad de los usuarios	50.00%

A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	33.33%
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información	33%
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	24.17%
A.6.1 Organización Interna	48.33%
A.6.2 Dispositivos móviles y teletrabajo	0.00%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	47.04%
A.7.1 Antes de asumir el empleo	100.00%
A.7.2 Durante la ejecución del empleo	41.11%
A.7.3 Terminación y cambio de empleo	0.00%
A.8 GESTION DE ACTIVOS	43.06%
A.8.1 Responsabilidad por los activos	62.50%
A.8.2 Clasificación de la información	66.67%
A.8.3 Manejo de Medios	0.00%
A.9 CONTROL DE ACCESO	61.15%
A.9.1 Requisitos de negocio para control de acceso.	69.05%
A.9.2 Gestión de acceso de usuarios	38.89%
A.9.3 Responsabilidad de los usuarios	50.00%

Nota: Tomado de Fuente: Autor

Gráfico 11. RESULTADO DEL DIAGNÓSTICO

OBJETIVO DE CONTROL	% CUMPLE	CAUSA	PLAN DE ACCION	
A.10 CRIPTOGRAFIA	0%	No existen mecanismos para cifrar la información que se intercambio al interior de la entidad o con terceros.	PA1	Implementar cuanto antes los debidos mecanismos de cifrado con el objetivo de asegurar la confidencialidad, autenticidad e integridad de la información, tales como: cifrado de correos, portal de intercambio seguro y cifrado del almacenamiento de dispositivos movibles.
A.16 GESTIÓN INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14%	La entidad no cuenta con un proceso para de gestión de incidentes de seguridad de la información.	PA2	Establecer cuenta antes el proceso de gestión de incidentes de seguridad para contar un enfoque coherente y eficaz para la debida gestión de los incidentes de seguridad y proveer a la entidad de un mecanismo para el reporte, evaluación y respuesta a los incidentes de seguridad de la información
		Los encargados de la seguridad de la información no mantienen un contacto con grupos de interés especializados en seguridad de la información	PA3	Los encargado de la seguridad de la información deben participar en eventos, foros, asociaciones y otros organizamos relacionados con seguridad de la información, para conocer las tendencias del mercado y las nuevas amenazas que surgen y que atentan contra la seguridad de la información
A.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION	24%	La entidad no tiene definidos todos los roles y responsabilidades de la seguridad de la información.	PA4	Este es un entregable del proyecto. Se requiere que el respectivo documento sea aprobado por la Alta Dirección.
A.18 CUMPLIMIENTO	30%	No cumple el control A.18.1.5 Reglamentación de controles criptográficos		Implementar mecanismo de cifrado. (Asociado al PA1)
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION	33%	Las políticas relacionadas con seguridad de la información están definidas en el Manual de Políticas de Seguridad Informática del proceso de tecnología, manual no está aprobado ni es revisado por la Alta Dirección	PA5	Elaborar unas políticas de seguridad aprobadas por la Alta Dirección para garantizar su debida implementación, actualización y cumplimiento.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA	37%	No se incluyen los requisitos relacionados con seguridad de la información en las ciclo de vida de desarrollo. (control A.14.1.1 del Anexo A de la norma ISO/IEC 27001:2013)	PA6	Es indispensable implementar controles adecuados y efectivos, o fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del ciclo de vida del desarrollo de aplicaciones de la entidad y con ello garantizar que los cambios que se realizan en producción no afecten la seguridad de la información, para lo cual, se debe crear un documento que contengan las mejorar practicas para el desarrollo de software seguro.
		No siempre se realizan las verificaciones técnicas a las aplicaciones críticas del negocio cuando se realizan cambios en producción, situación que no garantiza la normal operación, disponibilidad y seguridad de los servicios de TI una vez realizado los cambios.		
		No existe con un procedimiento adecuado de control de versionamiento del software		
		Durante el desarrollo de las aplicaciones no se incluyen pruebas de seguridad		
A.8 GESTION DE ACTIVOS	43%	La entidad no tiene identificados todos los activos de información a través de los cuales se gestiona la información del negocio	PA7	En el proyecto se identifico los activos de información de acuerdo al alcance de SGSI.
		La entidad no tiene establecidos los lineamientos para el uso aceptable de los activos de información asociados con la información e instalaciones de procesamiento de información		Se requiere definir la respectiva política (Asociada al PA5)
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	47%	No se cuenta con un mecanismo que permite garantizar que los colaboradores o terceras, estén debidamente informados sobre las funciones y las responsabilidades respecto a la seguridad de la información	PA8	La Vicepresidencia de Riesgo debe capacitar a los colaboradores de la entidad para que conozcan las Políticas de Seguridad de la Información y las adopten en sus actividades diarias.
		La entidad no cuenta con un plan anual de capacitación y formación en seguridad de la información para sus empleados, lo que genera en algunos casos la poca efectividad de los		El área de gestiona humana realizar un plan de capacitación en temas de seguridad de la información. (Asociado al PA8)

		controles implementados.		
A.17 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION	58%	Dentro del plan de continuidad del negocio de la entidad no se tiene contemplados los requisitos para garantizar la seguridad de la información	PA9	Documentar, implementar y mantener los procedimientos y controles necesarios para asegurar el nivel de continuidad requerido con el objetivo de garantizar la seguridad de la información en situaciones adversas.
A.9 CONTROL DE ACCESO	61%	La identificación del equipo no hace parte del esquema de autenticación de los usuarios al directorio activo.	PA10	La Dirección de Tecnológica deberá verificar la viabilidad de implementar este control
		La entidad no cuenta con un procedimiento formal para la asignación, control y restricción de derechos de acceso y privilegios sobre sus recursos tecnológicos y aplicaciones.	PA11	La Dirección de Tecnología deberá crear el respectivo procedimiento
		No se cuenta con un procedimiento para la gestión de contraseñas en los sistemas base de la entidad.	PA12	La Dirección de Tecnología deberá crear el respectivo procedimiento
A.13 SEGURIDAD DE LAS COMUNICACIONES	75%	No se cuenta con mecanismo adecuados para proteger la información confidencial que se envía por correo electrónico (control A.13.2.3 Anexo A de la norma ISO/IEC 27001:2013)		Garantizar la debida protección y cifrado de la información incluida en la mensajería electrónica (Asociado al PA1)
A.11 SEGURIDAD FISICA Y DEL ENTORNO	76%	No se cuenta con los procedimientos para trabajo en áreas seguras (control A.11.1.5 del Anexo A de la ISO/IEC 27001:2013)	PA13	Establecer el respectivo procedimiento
		No se cuenta con un mecanismo efectivo de seguridad que permita validar que los equipos que se conecta a la red interna de la entidad sea una estación de trabajo segura y valida	PA14	Implementar una solución de NAC (Control de acceso de la Red)
		No se cuenta con una política de escritorio limpio		Se requiere definir y establecer la respectiva política (Asociado al PA5)

Nota: Tomado de Fuente: Autor

El resultado del diagnóstico indico que el nivel de cumplimiento o desarrollo de la entidad frente al Anexo A de la norma ISO/IEC 27001:2013 es del 46.09%, debió a que no cuenta con algunos controles, o los existentes no son adecuados o no están documentos y que por la tanto requieren su revisión en un medio plazo para mejorar su efectividad y su cumplimiento. Esta situación representa un riesgo Medio para el centro médico ¨Cotacachi¨ debido a la ausencia de controles o la presencia de algunos con debilidades, la cual, puede ser aprovechado por amenazas internas o externas para atentar contra la seguridad de la información de la entidad.

Gráfico 12. FASE III

FASE III

IDENTIFICAR Y VALORAR ACTIVOS DE INFORMACION	• Identificar los activos de información • Determinar el tipo de activo • Identificar los dueños de los riesgos • Identificar el responsable del activo • Identificar el contenedor del activo • Valorar los activos • Determinar el valor de criticidad del activo • Establecer el nivel de criticidad del activo • Determinar los activos para la valoración de riegos
IDENTIFICAR Y VALORAR ACTIVOS DE INFORMACION VALORACION DE RIESGOS	• Identificar de amenazas y vulnerabilidades • Analizar el riesgo inherente • Mapa de calor • Elaborar Matriz de Riesgo Inherente • Evaluar controles existentes para mitigar los riesgos • Determinar Riesgo Residual • Elaborar Matriz de Riesgo Residual • Establecer opciones y/o planes de tratamiento de riesgos

Nota: Tomado de Fuente: Autor

Gráfico 13. AMENAZAS IDENTIFICADAS Y EL NÚMERO DE LOS ACTIVOS DE INFORMACIÓN

Tipo de activo	No
Datos / Información	9
Equipos informáticos	14
Instalaciones	4
Redes de comunicaciones	4
Servicios	6
Software	20
Total	**57**

Nota: Tomado de Fuente: Autor

El gráfico 14 muestra las amenazas identificadas y el número de los activos de información seleccionados que pueden ser afectados por estas:

Gráfico 14. VULNERABILIDADES Y EL NÚMERO DE AMENAZAS

Nota: Tomado de Fuente: Autor

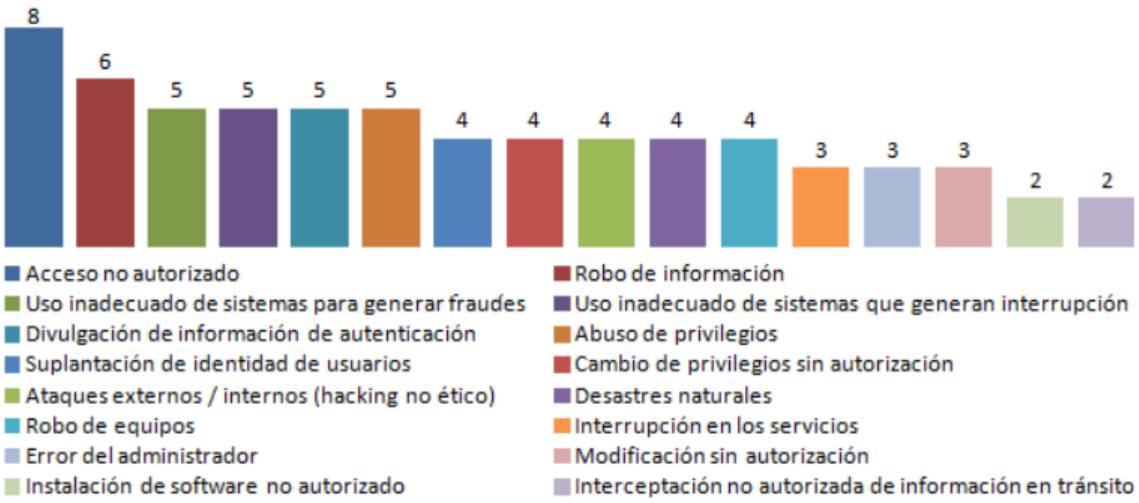
El gráfico 15 muestra el resultado de esta labor se identificaron las siguientes vulnerabilidades y el número de amenazas que pueden explotarlas:

Gráfico 15. NRO. DE AMENAZAS QUE PUEDAN EXPLOTARLAS

Nota: Tomado de Fuente: Autor

El gráfico 16 muestra el número de vulnerabilidades que puede ser explotada por cada una de las amenazas identificadas:

Gráfico 16. NÚMERO DE VULNERABILIDADES QUE PUEDE SER EXPLOTADA



Nota: Tomado de Fuente: Autor

El gráfico 17 muestra la Codificación de riesgos del proceso de tecnología

Gráfico 17. CODIFICACIÓN DE RIESGOS DEL PROCESO DE TECNOLOGÍA

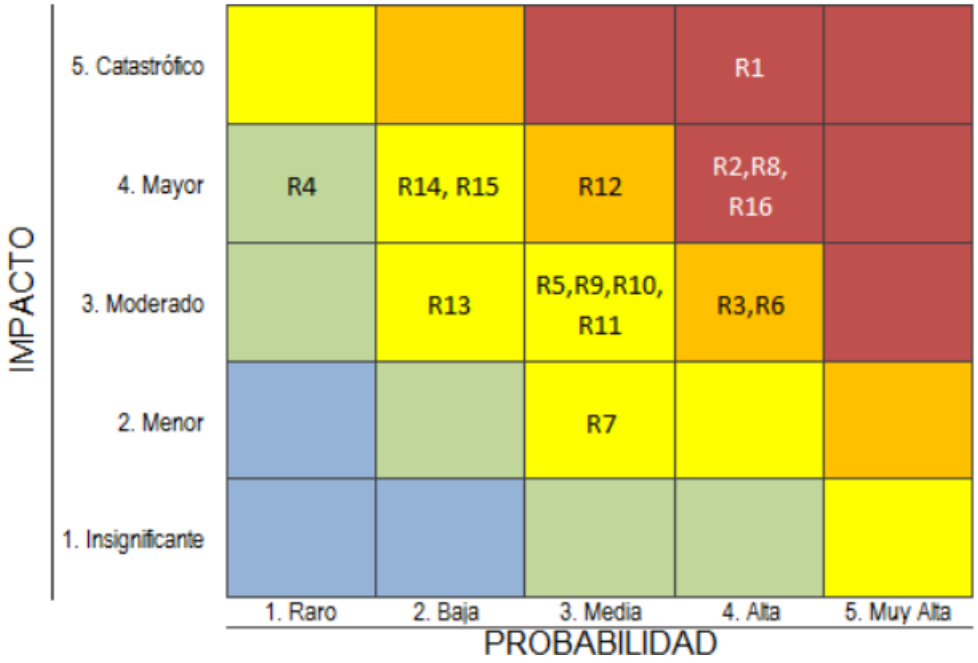
R1	Acceso no autorizado
R2	Ataques externos / internos (hacking no ético)
R3	Cambio de privilegios sin autorización
R4	Desastres naturales (Terremotos, Incendios, Inundaciones, etc.)
R5	Divulgación de información de autenticación
R6	Error del administrador
R7	Instalación de software no autorizado
R8	Interceptación no autorizada de información en tránsito
R9	Interrupción en los servicios
R10	Modificación sin autorización
R11	Robo de equipos
R12	Robo de información
R13	Suplantación de identidad de usuarios
R14	Uso inadecuado de sistemas para generar fraudes
R15	Uso inadecuado de sistemas que generan interrupción
R16	Abuso de privilegios

Nota: Tomado de Fuente: Autor

El gráfico 18 muestra el riesgo inherente se valoró la probabilidad de ocurrencia de los riesgos identificados, así como el impacto de los mismos en caso de su materialización.

Cada zona dentro del mapa de calor corresponde a un tipo de riesgo e indica las acciones de tratamiento del riesgo a seguir. El siguiente es el mapa de riesgos inherente del proceso de tecnología:

Gráfico 18. LA PROBABILIDAD DE OCURRENCIA DE LOS RIESGOS IDENTIFICADOS



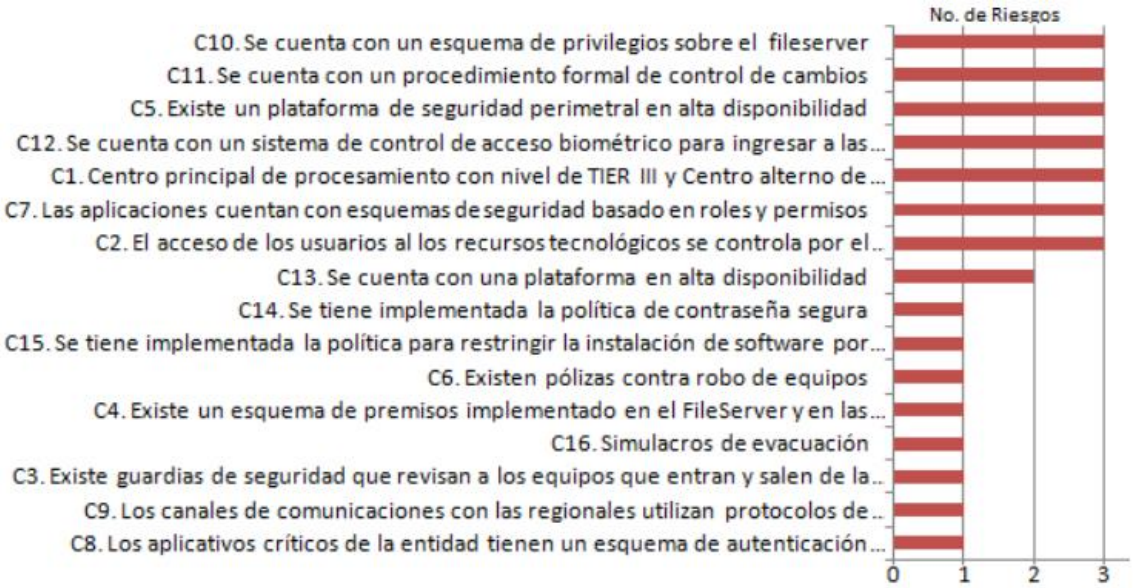
Nota: Tomado de Fuente: Autor

Dentro de los riesgos clasificados como riesgo extremo, se encuentra el riesgo 'R16. Abuso de privilegios', el cual representa uno de los mayores riesgos que atentan contra la seguridad de las organizaciones de acuerdo con estudios realizados. La empresa Oracle en su informe ''DBA – Security Superhero: 2014 IOUG Enterprise Data Security Survey', indica que el 54% de los encuestados ven el abuso de los privilegios de acceso como uno de los mayores riesgos para los datos de las empresas80. La empresa Raytheon Company, en su informe 'Privileged User Abuse & The Insider Threat' publicado en mayo de 2014, indica que las personas con acceso a los datos

privilegiados frecuentemente ponen en riesgos la información sensible de la organización81. El abuso de privilegios es un riesgo que por su naturaleza y los efectos que conlleva, genera la posibilidad de la materialización de otros riesgos, como son, el cambio de privilegios sin autorización, accesos no autorizados, pérdida o robo de información y uso inadecuado de sistemas para generar fraudes o interrupción en los servicios.

El gráfico 19 muestra la información proporcionada por tecnología, se identificaron el número de riesgos que puede mitigar cada uno de los controles, lo cual, inicialmente indicaría el nivel de efectividad del control. La siguiente grafica muestra esta situación:

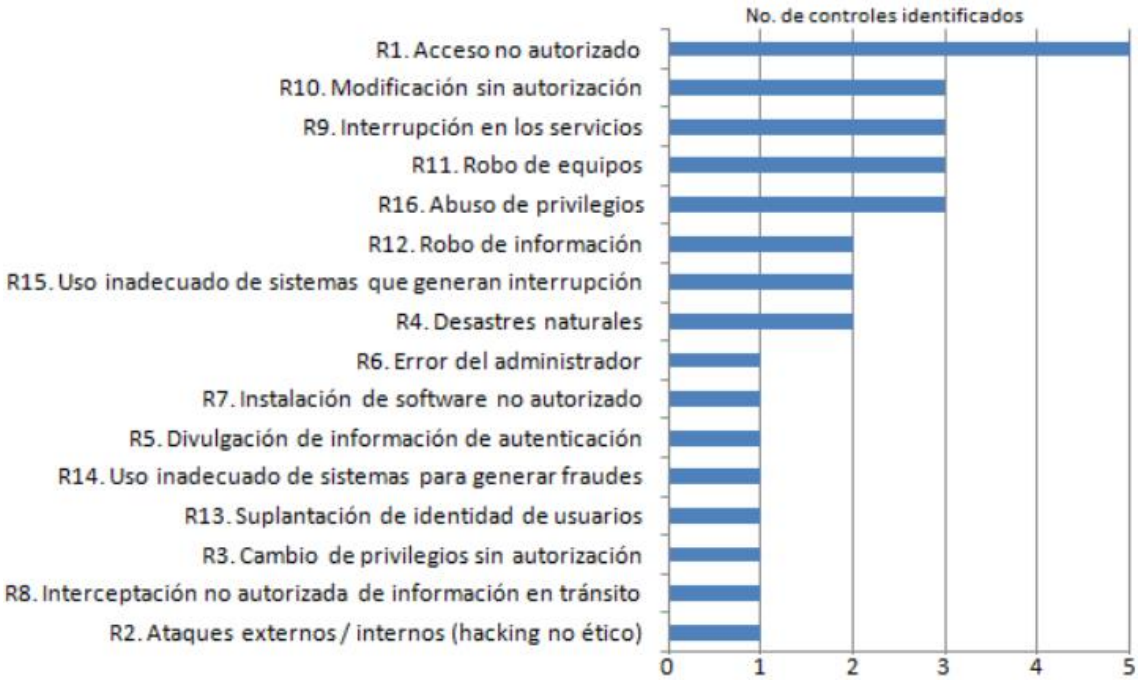
Gráfico 19. NÚMERO DE RIESGOS QUE PUEDE MITIGAR CADA UNO DE LOS CONTROLES



Nota: Tomado de Fuente: Autor

El gráfico 20 muestra la relación de las cantidades de controles que se identificaron para cada uno de los riesgos evaluados:

Gráfico 20. RELACIÓN DE LAS CANTIDADES DE CONTROLES QUE SE IDENTIFICARON



En esta gráfica se puede observar que para cada riesgo por lo menos se identificó un control que puede generar el desplazamiento del riesgo a una zona menor en el mapa de calor, lo cual, es algo positivo ya que ayuda a mitigar el nivel de riesgo inherente del proceso de tecnología.

El gráfico 21 muestra las siguientes graficas muestras la disminución en el nivel de los riesgos que genero los respectivos controles identificados:

Gráfico 21. DISMINUCIÓN EN EL NIVEL DE LOS RIESGOS QUE GENERO LOS RESPECTIVOS CONTROLES IDENTIFICADOS

Nota: Tomado de Fuente: Autor

El gráfico 22 muestra el porcentaje de disminución que género los controles identificados para mitigar cada uno de los riesgos:

Gráfico 22. PORCENTAJE DE DISMINUCIÓN QUE GÉNERO LOS CONTROLES IDENTIFICADOS

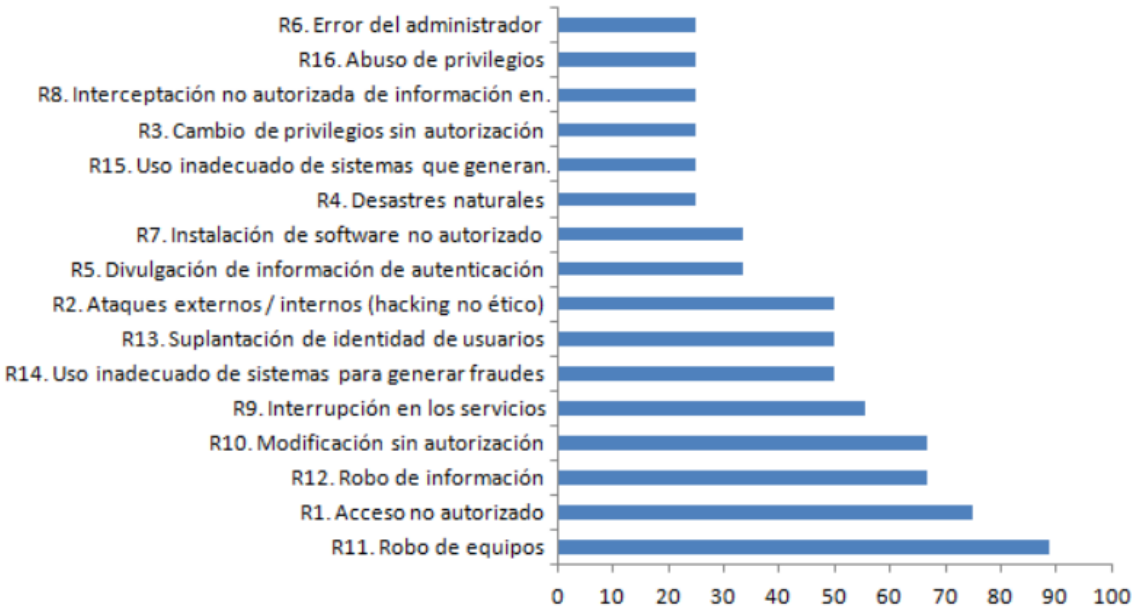
	Riesgo Inherente				Riesgo Residual				
RIESGO	Probabilidad	Impacto	PxI	Nivel Riesgo	Probabilidad	Impacto	PxI	Nivel riesgo	% Disminución
R1. Acceso no autorizado	4	5	**20**	Riesgo Extremo	1	5	**5**	Riesgo Medio	75.00%
R2. Ataques externos / internos (hacking no ético)	4	4	**16**	Riesgo Extremo	2	4	**8**	Riesgo Medio	50.00%
R3. Cambio de privilegios sin autorización	4	3	**12**	Riesgo Alto	3	3	**9**	Riesgo Medio	25.00%
R4. Desastres naturales	1	4	**4**	Riesgo Bajo	1	3	**3**	Riesgo Bajo	25.00%
R5. Divulgación de información de autenticación	3	3	**9**	Riesgo Medio	2	3	**6**	Riesgo Medio	33.33%
R6. Error del administrador	4	3	**12**	Riesgo Alto	3	3	**9**	Riesgo Medio	25.00%
R7. Instalación de software no autorizado	3	2	**6**	Riesgo Medio	2	2	**4**	Riesgo Bajo	33.33%
R8. Interceptación no autorizada de información en tránsito	4	4	**16**	Riesgo Extremo	3	4	**12**	Riesgo Alto	25.00%
R9. Interrupción en los servicios	3	3	**9**	Riesgo Medio	2	2	**4**	Riesgo Bajo	55.56%
R10. Modificación sin autorización	3	3	**9**	Riesgo Medio	1	3	**3**	Riesgo Bajo	66.67%
R11. Robo de equipos	3	3	**9**	Riesgo Medio	1	1	**1**	Riesgo Inusual	88.89%
R12. Robo de información	3	4	**12**	Riesgo Alto	1	4	**4**	Riesgo Bajo	66.67%
R13. Suplantación de identidad de usuarios	2	3	**6**	Riesgo Medio	1	3	**3**	Riesgo Bajo	50.00%
R14. Uso inadecuado de sistemas para generar fraudes	2	4	**8**	Riesgo Medio	1	4	**4**	Riesgo Bajo	50.00%
R15. Uso inadecuado de sistemas que generan interrupción	2	4	**8**	Riesgo Medio	2	3	**6**	Riesgo Medio	25.00%
R16. Abuso de privilegios	4	4	**16**	Riesgo Extremo	3	4	**12**	Riesgo Alto	25.00%
								Promedio disminución de controles	**44.97%**

Nota: Tomado de Fuente: Autor

De acuerdo con estos datos los controles valoradores generaron una disminución del 44.97% en el nivel de los riesgos del proceso de tecnología.

El gráfico 23 muestra el porcentaje de disminución en el nivel de riesgo que genero los respectivos controles valorados:

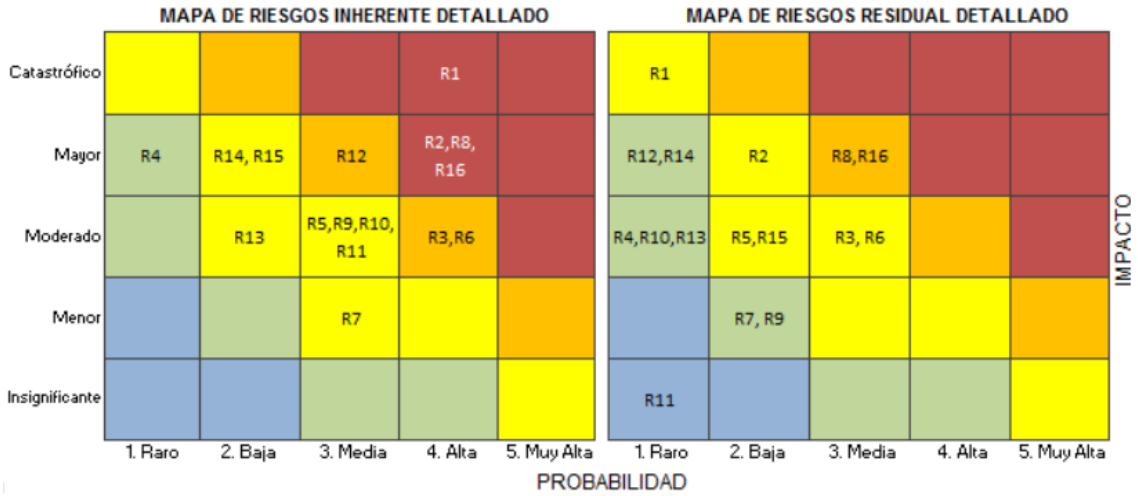
Gráfico 23. PORCENTAJE DE DISMINUCIÓN EN EL NIVEL DE RIESGO QUE GENERO LOS RESPECTIVOS CONTROLES VALORADOS



Nota: Tomado de Fuente: Autor

El gráfico 24 muestra las matrices de riesgos inherente y residual del proceso del proceso de tecnología, donde se puede observar el desplazamiento que género los controles identificados para cada uno de los riesgos:

Gráfico 24. MATRICES DE RIESGOS INHERENTE Y RESIDUAL DEL PROCESO DEL PROCESO DE TECNOLOGÍA



Nota: Tomado de Fuente: Autor

Los siguientes son algunos de los análisis que se pueden establecer de acuerdo a la disminución del nivel de los riesgos que se presenta en el mapa de riesgo residual del proceso de tecnología:

• La efectividad de los controles identificados permitió la disminución del nivel de los riesgos que estaban en la zona extrema, que correspondían a riesgos que requerían acciones inmediatas de tratamiento orientadas a reducir, compartir el riesgo, transferirlo o incluso evitarlo. Esta disminución permitió que todos los riesgos extremos se movieran a otras zonas del mapa de calor.

• Los controles identificados y valorados para el riesgo R1 - Acceso no autorizado, permitieron que este riesgo de moviera de la zona extrema a una de las zonas de riesgo medio. Esta reducción fue una de las más efectivas en el mapa de calor, debido a que genero una disminución del 75% en el nivel de este riesgo. A pesar de la reducción del nivel de este riesgo, el mismo quedo es una zona de riesgo medio que requiere de medidas adecuadas que permitan seguir disminuyendo el riesgo a un nivel bajo o inusual.

• El Riesgos R2 - Ataques externos / internos (hacking no ético), paso de la zona extrema a la zona de riesgo medio, debido a una disminución en su nivel de riesgo del 50% generada por los controles identificados. Este riesgo requiere de acciones prontas y adecuadas para reducir el riesgo a niveles más bajos.

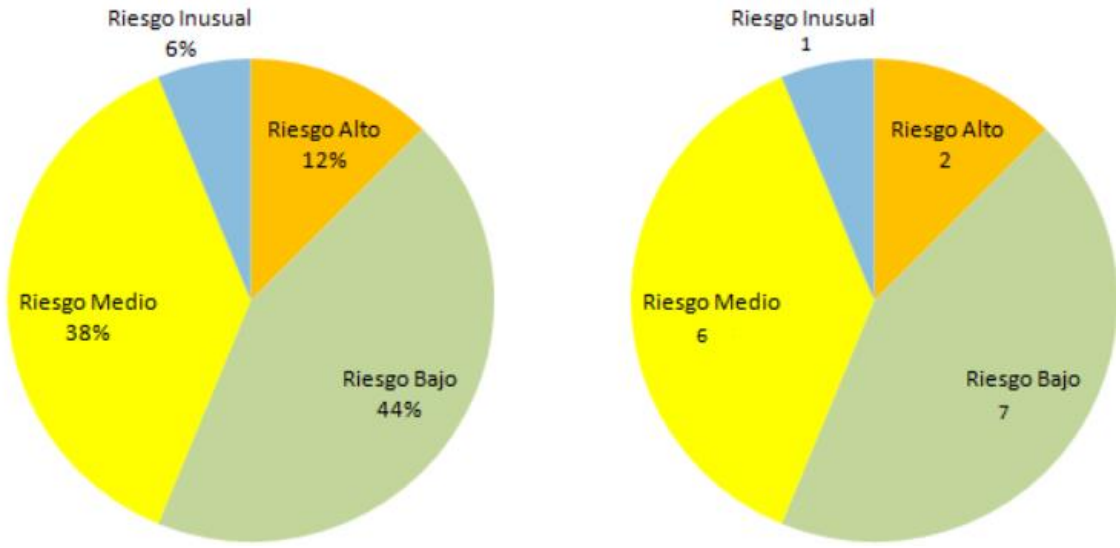
• Los Riesgo R8 - Interceptación no autorizada de información en tránsito y R16 - Abuso de privilegios, que estaban en la zona extrema, solo tuvieron una reducción del 25% generada por sus respectivos controles, quedando en la zona riesgo alto que requiere de una atención y medidas urgentes para reducir el nivel del riesgo.

• Los controles valorados para el riesgo R11 - Robo de equipos, generaron el mayor nivel desplazamiento en el mapa de calor, correspondiente a una disminución del nivel de riesgos del 89%, permitiendo que este riesgo pasara de la zona media a la zona más baja de riesgo inusual. Este riesgo se asume y no necesita tratamiento.

• El riesgo R12 - Robo de información pasó de la zona de riesgo alta a la zona de riesgo media, debido a que los controles valorados generaron una disminución del 66.67%. Este riesgo al quedar en una zona de riesgo med

El gráfico 25 muestra la DISTRIBUCIÓN RIESGO RESIDUAL PROCESO DE TECNOLOGÍA

Gráfico 25. DISTRIBUCIÓN RIESGO RESIDUAL PROCESO DE TECNOLOGÍA



Nota: Tomado de Fuente: Autor

Estas graficas permiten establecer:

• Existe dos riesgos altos, que requieren atención urgente y la implementación medidas para reducir el nivel del riesgo, los cuales son: R16. Abuso de privilegios y R8. Interceptación no autorizada de información en tránsito.

• Existen seis riesgos (R1, R2, R5, R15, R3 y R6) en la zona media que requieren de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual.

• Existen siete riesgos en la zona baja (R12, R14, R4, R10, R13, R7, R9) donde el riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo.

• Existe un riesgo en la zona inusual (R11), que por esta en esta zona se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes.

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD TOMANDO COMO BASE LA NORMA ISO 27001:2013.

Para el desarrollo de las políticas de Seguridad de la Información, se tuvo en cuentas los dominios, objetivos de control y controles que están definidos en el Anexo A de la Norma ISO/IEC 27001:2013.

Tabla 23. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD TOMANDO COMO BASE LA NORMA ISO 27001:2013.

Dominio de control	**Nombre de la Política de seguridad**
A.5.	Política General de Seguridad de la Información
A.6.	Organización de Seguridad de la Información

A.7.	Seguridad de los Recursos Humanos
A.8.	Gestión de Activos
A.9.	Control de Acceso
A.10.	Criptografía
A.11.	Seguridad Física y del Entorno
A.12.	Seguridad de las Operaciones
A.13.	Seguridad de las Comunicaciones
A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas
A.15.	Relaciones con los Proveedores
A.16.	Gestión de Incidentes de Seguridad de la Información
A.17.	Seguridad de la Información en la Continuidad del Negocio
A.18.	Cumplimiento de Requisitos Legales y Contractuales

Nota: Tomado de Fuente: Autor

Las políticas, normas y lineamientos que regirán la seguridad de la información en la entidad y las responsabilidades y obligaciones de todos los colaboradores y terceros que tengan acceso a la información de la entidad.

DEFINIR UN MECANISMO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD.

Para alcanzar este objetivo específico del proyecto, se elaboró el procedimiento para el reporte y atención de incidentes de seguridad.

El procedimiento para el reporte y atención de incidentes de seguridad de la información, comienza con la identificación del evento de seguridad que pueda afectar la disponibilidad, integridad y confidencialidad de la información de la entidad, continua con el análisis del evento para determinar si se clasifica o no como una incidencia de seguridad para así determinar e implementar las medidas de Contención, Erradicación y Recuperación y finaliza con la aplicación de mejoras para prevenir la ocurrencia de nuevos incidentes. El procedimiento de reporte y atención de incidentes de seguridad debe ser aprobado por el vicepresidente de riesgos y el área de calidad, para su debida publicación y socialización. Debido a que el presente trabajo de grado solo abarca el diseño de un sistema de gestión de seguridad de la información para centro médico, y no la implementación de este.

MARGO LEGAL SEGÚN LA CONSTITUCIÓN ECUATORIANA

- Acuerdo No. 166, Esquema Gubernamental de Seguridad de la Información EGSI (19 de septiembre de 2013).
- Constitución de la República del Ecuador (Decreto Legislativo 0 / Registro Oficial 449 de 20-oct-2008 / Última modificación: 13-jul-2011).
- Decreto de Creación de la UNIVERSIDAD LAICA ELOY ALFARO DE MANABI (Decreto Ejecutivo número 10 y publicado en el Registro Oficial N.º 313) el 13 de noviembre de 1985.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67).
- Ley Orgánica de Servicio Público, LOSEP (Ley 0 / Registro Oficial Suplemento 294 de 06-oct-2010).
- Ley Orgánica de Transparencia y Acceso a la Información Pública No. 24, publicado en el Registro Oficial Suplemento 337 del 18 de mayo del 2004.
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 Código de Práctica para la Gestión de la Seguridad de la Información.
- Reglamento General a la Ley Orgánica del Servicio Público (Decreto Ejecutivo 710 / Registro Oficial Suplemento 418 de 01-abr-2011 / Última modificación: 10-oct-2011).

CONCLUSIONES Y RECOMENDACIONES

- Se realizó la formulación para la valoración y enmarcar los riesgos, en el centro médico ¨Cotacachi¨ usada como patrón de referencia.

- La metodología de análisis de los riesgos se realizó por medio de la guía proporcionada por Magerit V 3.0.

- Se expresó la realización de proceso de gestión de los riesgos de acuerdo con Magerit V 3.0 basado en la empresa utilizada como ejemplo de referencia.

- Se realizó el diagnóstico y se pudo evidenciar las falencias de cada uno de los activos y de esta manera analizar y cubrir con los requerimientos individuales del negocio.

- Magerit sitúa al acatamiento de los fundamentos de confiabilidad, integridad y disponibilidad de la información.

- Se implemento la guía práctica con ejemplos y fórmulas para la implementación básica de un SGSI basado en Magerit v3.0, de esta manera su implementación del SGSI proporciona a las empresas un agregado de confianza y poder de mercado.

- Magerit es un marco de trabajo para el gobierno de T.I estructural que comprende bien todos los roles y su participación en pro de una guía integra de trabajo.

- El conocimiento y la comunicación son factores clave para avanzar y acertar implementación de la política de seguridad, ya que de esta manera se socializó la implementación del sistema de la seguridad de la información en el centro médico “Cotacachi” a sus propietarios y empleados.

REFERENCIAS BIBLIOGRAFICAS

Báez, M., & Pérez, M. (2017). Metodología de la Investigación Cualitativa. Editorial Académica Española.,

Fernández, E. (2020). ISO 27001: Estándar de Seguridad de la Información. *International Journal of Cybersecurity, 6*(1), 56-72.

Fernández, M. (2017). Métodos Cuantitativos en Investigación Social. *Social Science Research, 25*(1), 87-102.

Flick, U. (2018). Introducción a la Investigación Cualitativa (5ª ed.). Morata.

García, A. (2018). Enfoque Mixto en Investigación Cualitativa y Cuantitativa. *Journal of Mixed Methods Research, 14*(2), 189-204.

García, M. (2019). MAGERIT: Análisis y Gestión de Riesgos. *Revista de Seguridad Informática, 5*(1), 45-62.

Gómez, L. (2017). Ciberseguridad y Riesgos Asociados. *Cybersecurity Review, 8*(1), 67-82.

González, A. (2019). Gestión de Desastres en Seguridad Informática. *Disaster Management Journal, 24*(4), 421-435.

Ibáñez, J. (2015). Métodos de Investigación. Ediciones de la Universidad de Murcia.

ISO. (2019). ISO 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. ISO.

Johnson, A. (2018). OWASP: Estándar en Ciberseguridad. *International Journal of Information Security, 12*(4), 367-382.

Kendall, K. E., & Kendall, J. E. (2011). Análisis y Diseño de Sistemas. Pearson Educación.

López, R. (2017). Seguridad de la Información en la Era Digital. *International Journal of Information Management, 34*(6), 749-762.

Magerit. (s.f.). Guía para la Gestión de Riesgos en la Seguridad de la Información. https://www.ccn-cert.cni.es/publico/estrategias-y-herramientas/normativa/magerit.html

Martínez, P. (2018). Calidad de la Información en SGSI. *Journal of Information Quality, 15*(2), 123-138.

OWASP Foundation. (s.f.). OWASP Top Ten. https://owasp.org/www-project-top-ten/

Pérez, J. (2019). Entrevistas en Investigación Cualitativa. *Qualitative Research Journal, 32*(4), 412-427.

Pérez, L. (2016). La Clasificación de la Información en SGSI. *Revista de Tecnología y Seguridad Informática, 8*(3), 89-104.

Ramírez, C. (2018). Modelos de Innovación en la Gestión de la Seguridad de la Información. *Information Systems Research, 29*(5), 538-552.

Rodríguez, S. (2017). Metodología de Investigación Aplicada. *Research Methods Journal, 41*(3), 287-302.

Senn, J. A. (2011). *ANÁLISIS y DISEÑO de SISTEMAS de INFORMACIÓN* (Segunda edición). [Mig, S.A. de C.V.]

Silberschatz, A., & Korth, H. F. (2014). Fundamentos de Base de Datos y Seguridad de la Información. [PDF]. [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://biblioteca.univalle.edu.ni/files/original/01aebde3cc06dce33f2538aa2724eb2541cb9473.pdf].,

Smith, J. (2017). Metodologías de Evaluación de Vulnerabilidades en SGSI. *Journal of Cybersecurity*, *3*(2), 135-148.

Torres, F. (2020). Gestión de la Seguridad Lógica de la Información. *Journal of Information Security Management*, *11*(3), 211-226.

ANEXOS

Turnitin Originality Report

Processed on: 24-Ago-2023 17:26 -05

ID: 1833322426

Word Count: 2608

Submitted: 1

Similarity Index	Similarity by Source
8%	Internet Sources: 0% Publications: Student Papers: 10%

IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION(SGSI) PARA EL CENTRO MEDICO

4% match (student papers from 01-NoÿCOTACACHI˙, By Julio 2021) Fabian Vaca Baez Submitted to Universidad Anahuac México Sur on 2021-11-01

4% match (student papers from 20-Nov-2020)
Submitted to Universidad Autónoma de Chiapas on 2020-11-20

CARTA DE ACEPTACIÓN DEL PROYECTO DE TITULACIÓN

Φ *CONSULTORIO DE ATENCION MÉDICA*
Dr. FABIAN VACA ECHEVERRÍA
Universidad Nacional de Medicina de Ucrania (Kiev)

Medicina General – Pediatría – Dermatología.- Electrocardiografía Electrocirugía de piel: Eliminación definitiva de verrugas, lunares, lipomas, callos, uñeros. Electro cauterizaciones. -Nebulizaciones Pruebas de Diabetes - Desintoxicación iónica del organismo. OZONOTERAPIA.
DIAGNOSTICO COMPUTARIZADO DEL ESTADO FUNCIONAL DE ORGANOS Y SISTEMAS DEL ORGANISMO HUMANO.

CARTA DE ACEPTACIÓN DEL PROYECTO DE TITULACIÓN

Cotacachi, 02 de mayo del 2023

Julio Fabián Vaca Báez.

Reciba un cordial saludo. A través de la presente, el Consultorio Médico "Cotacachi", tenemos el agrado de notificarle la aceptación del proyecto "Implementación de un sistema de gestión de la seguridad de la información(SGSI)", para el centro médico"Cotacachi", desarrollado por Julio Fabián Vaca Báez.

Durante la realización del proyecto el encargado de su desarrollo será Julio Fabián Vaca Báez y tendrá la labor de Diseñar e implementar el (SGSI) antes mencionado.

Sin más que agregar, esperamos que el proyecto inicie según lo esperado y sea llevado a cabo con completo éxito.

Atentamente,

Dr. Brito Fabián Vaca Echeverría
Dr. Fabián Vaca E.
MÉDICO GENERAL
Cod. M.S.P.: 1000698538

Dirección: Calle Bolívar 6-54 y Segundo Luis Moreno. - Cel. 0994454971

Cotacachi – Imbabura – Ecuador.

CARTA DE RECEPCIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Φ *CONSULTORIO DE ATENCION MÉDICA*
Dr. FABIAN VACA ECHEVERRÍA
Universidad Nacional de Medicina de Ucrania (Kiev)

Medicina General – Pediatría – Dermatología.- Electrocardiografía Electrocirugía de piel: Eliminación definitiva de verrugas, lunares, lipomas, callos, uñeros. Electro cauterizaciones. -Nebulizaciones Pruebas de Diabetes - Desintoxicación iónica del organismo. OZONOTERAPIA.
DIAGNOSTICO COMPUTARIZADO DEL ESTADO FUNCIONAL DE ORGANOS Y SISTEMAS DEL ORGANISMO HUMANO.

CARTA DE RECEPCIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Cotacachi, 09 de agosto del 2023

Julio Fabián Vaca Báez.

Reciba un cordial saludo. A través de la presente, el Consultorio Médico "Cotacachi", nos complace notificarle la recepción del sistema de gestión de la seguridad de la información (SGSI), para el centro médico"Cotacachi", desarrollado por Julio Fabián Vaca Báez.

Se implementó de manera eficiente y con éxito el sistema (SGSI), realizado por Julio Fabián Vaca Báez.

Sin más que agregar, auguramos éxitos en su vida profesional.

Atentamente,

Dr. Brito Fabián Vaca Echeverría

Dr. Fabián Vaca E.
MEDICO GENERAL
Cod. M.S.P.: 1000698538

Dirección: Calle Bolívar 6-54 y Segundo Luis Moreno. - Cel. 0994454971

Cotacachi – Imbabura – Ecuador.