ESCUELA DE INGENIERIA EN SISTEMAS

Tema:

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EP-EMAPA-A CON LA NORMA ISO/IEC27001:2013

Proyecto de investigación previo a la obtención del título de Ingeniera en de Sistemas de la Información

Línea de Investigación:

Sistemas de información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

Priscilla Lizbeth Aguilar Molina

Director:

Ing. Mg. Darío Javier Robayo Jácome

Ambato – Ecuador

Diciembre 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EP-EMAPA-A CON LA NORMA ISO/IEC27001:2013

Línea de Investigación:

Sistemas de información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

Priscilla Lizbeth Aguilar Molina

Darío Javier Robayo Jácome, Ing. Mg. f._____
CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. Mg. f._____
CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f._____
CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. f._____
DIRECTOR ESCUELA DE SISTEMAS

Hugo Rogelio Altamirano Villarroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato Ecuador
Diciembre - 2022

Pontificia Universidad Católica del Ecuador
BIBLIOTECA

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo, Priscilla Lizbeth Aguilar Molina portador de la cédula de ciudadanía 1803653128, autor del trabajo de graduación intitulado: "PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EP-EMAPA-A CON LA NORMA ISO/IEC 27001:2013", previa a la obtención del título profesional de INGENIERA EN SISTEMAS DE LA INFORMACION, en la escuela de INGENIERÍAS.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontifica Universidad Católica del Ecuador, 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 del autor.

2. Autorizo a la Pontifica Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, diciembre 2022

.....

Priscilla Lizbeth Aguilar Molina

CC. 1803653128

AGRADECIMIENTO

A Dios y a la Virgen María por ser quienes guían mi vida y en silencio me ayudan a tomar las mejores decisiones.

A mis padres Marco y Pathy, y mi abuelita Hilda quienes son mi apoyo en cada momento, quienes me dan fuerza en los peores momentos y celebran conmigo cada logro.

A la universidad “PUCESA”, mis docentes universitarios y mis compañeros quienes me brindaron los instrumentos necesarios para mi desarrollo académico, profesional y personal.

A la empresa “EP-EMAPA-A”, quienes me abrieron las puertas para realizar el presente proyecto.

DEDICATORIA

Este proyecto está dedicado a mis padres que son mi ejemplo a seguir y son mi pilar fundamental.

A mi hijo Gael le dedico todo lo lindo que pasa en mi vida, a él que me acompañó al primer día de la universidad, él mi compañero de estudio.

A mis hermanos Gabriela, Adrián y mis hermanos que están en el cielo por las enseñanzas de vida, por su apoyo incondicional y sus alegrías.

A mis sobrinas Brianna y Raphaella, que con sus demostraciones de amor y fortaleza le dan sentido a mi vida.

Y a mis mejores amigos por estar en las buenas y en las malas y darnos ánimos mutuamente cuando lo necesitamos.

RESUMEN

En la actualidad el manejo de la información dentro de las empresas cobra importancia, esto se debe al incremento de incidentes, que se han generado sobre todo en las empresas del sector público y que ha provocado afectaciones a nivel interno influye en la continuidad operativa de la organización, esto acarrea problemas a nivel económico y legal, bajo este contexto, se plantea el objetivo de esta investigación en desarrollar un plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013 para el centro de la base de datos (cuarto frio). La metodología fue descriptiva con corte transversal, porque permitió observar y describir, como se manejan los activos y procesos, su manipulación, custodia, confidencialidad, integridad y seguridad, a fin de establecer un estudio del análisis y gestión de riesgos. La población de estudio fueron cinco representantes del área de TI, a quienes, se les aplicó entrevistas y, para el diagnóstico de la situación actual, se utilizó la metodología MAGERIT, que se apoya en las Normas ISO 2700. Dentro de los principales hallazgos, se demostró los riesgos potenciales contra los activos de seguridad, es la falta de procedimientos de seguridad y la poca importancia de capacitación en temas de ciberseguridad a los servidores y base de datos. Como una conclusión relevante, se establece la necesidad de desarrollar políticas de seguridad de la información, enfocado en el área de ciberseguridad, y orientada a la protección de los activos de la base de datos.

Palabras Claves: información, activo, norma ISO/IEC 27001:2013

ABSTRACT

The handling of information within businesses has become more crucial in recent years. This is because there have been more incidents, mostly in businesses tied to the public sector. These episodes have damaged the organization from the inside out, disrupting its normal operations and creating issues with the law and the economy. The goal of this research is to create an information security management plan that complies with the ISO/IEC 27001:2013 standard for the database center (cold room) for the EP-EMAPA-A. In order to develop a risk analysis and management research, the technique was descriptive with a cross-sectional view, allowing us to observe and explain how assets and processes are managed, including their handling, custody, confidentiality, integrity, and security. Five IT industry representatives who were subjected to interviews made up the study population. The MAGERIT approach, which is based on the ISO 2700 Standards, was used to diagnose the current condition. One of the primary conclusions was that servers and databases are particularly vulnerable to security concerns due to a lack of security protocols and inadequate training. In conclusion, it is stated that information security policies that are focused on cybersecurity and directed toward safeguarding database assets must be created.

Keywords: information, asset, ISO/IEC 27001:2013 standard

ÍNDICE DE CONTENIDOS

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD iii

AGRADECIMIENTO iv

DEDICATORIA v

RESUMEN vi

ABSTRACT vii

INTRODUCCIÓN xi

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA 9

1.1. Seguridad de la Información 9

1.2. Plan de gestión de seguridad de la información 19

1.3. Norma ISO/IEC 27001:2013 30

CAPÍTULO II. METODOLOGIA DE LA INVESTIGACIÓN 36

2.1. Caracterización de EP-EMAPA-A 36

2.2. Metodología de investigación 38

2.3 Metodología de desarrollo 46

CAPÍTULO III ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN 69

2.3. Plan de Gestión de Seguridad de la Información 69

2.4. Validación del Plan 85

3.2. Análisis de los resultados de la validación 88

CONCLUSIONES 91

RECOMENDACIONES 93

BIBLIOGRAFÍA 94

ANEXOS 100

ÍNDICE DE TABLAS

Tabla 1. Criterios de impacto 28
Tabla 2. Criterios de probabilidad de ocurrencia 29
Tabla 3. Población de estudio 39
Tabla 4. Identificación de activos del Centro de Datos de la EP-EMAPA-A 49
Tabla 5. Disponibilidad de los activos 55
Tabla 6. Análisis de la integridad de los activos 55
Tabla 7. Análisis de confidencialidad de los activos 56
Tabla 8. Análisis de Amenaza 57
Tabla 9. Análisis de vulnerabilidad 59
Tabla 10. Vulnerabilidad - Improbabilidad 60
Tabla 11. Vulnerabilidad - posible 61
Tabla 12. Evaluación del riesgo 61
Tabla 13. Riesgo medio 63
Tabla 14. Riesgo Bajo 63
Tabla 15. Tratamiento del riesgo 66
Tabla 16. Marco legal ISO/IEC 27001:2013 71
Tabla 17. Coeficiente de conocimiento de información 85
Tabla 18. Coeficiente de argumentación 86
Tabla 19. Valoración de la experiencia de los expertos 88
Tabla 20. Coeficiente de argumentación de los expertos 89
Tabla 21. Calificación de criterios por expertos 90

ÍNDICE DE FIGURAS

Figura 1. Ciclo de Deming PDCA 12
Figura 2. Estructura de un SGSI 13
Figura 3. Fases de los SGSI 14
Figura 4. Ciclo de vida de la información 20
Figura 5. Ciclo de vida clásico de un sistema de información, modelo en cascada 22
Figura 6. Gestión de la seguridad de la información 31
Figura 7. Fases para la implementación de un SGSI 32
Figura 8. Metodología de evaluación y tratamiento de riesgo 33
Figura 9. Fases de la metodología MARGERIT 47
Figura 10. Análisis de amenaza 58
Figura 11. Análisis de vulnerabilidad 60
Figura 12. Evaluación del riesgo 62
Figura 13. Estado de los controles de seguridad de la información 64
Figura 14. Estructura Orgánica de EP-EMAPA-A 72
Figura 15. Estructura Orgánica del departamento de Tecnología de Información 73
Figura 16. Arquitectura de las políticas del sistema de seguridad de la información 74
Figura 17. Seguridad Física y del Ambiente 78
Figura 18. Control de acceso 81
Figura 19. Control de acceso 82
Figura 20. Gestión de continuidad 84

ÍNDICE DE CUADROS

Cuadro 1.Clasificación de los activos de información 25
Cuadro 2. Eventos de seguridad de la información 28
Cuadro 3. Organización de la información 77
Cuadro 4. Seguridad personal 78
Cuadro 5. Seguridad de comunicacion y operaciones 79
Cuadro 6. Control de accesos 81
Cuadro 7. Mantenimiento de sistemas de información 83
Cuadro 8. Gestión de continuidad de la empresa 84
Cuadro 9. Valoración de la experiencia de los expertos 85

INTRODUCCIÓN

El uso de las Tecnologías de Información y Comunicación (TIC), se han incrementado de manera vertiginosa, porque contribuyen a la organización, optimización y mejora de las actividades de todos los procesos de una empresa. El uso de las TIC permite a las organizaciones el almacenamiento, mantenimiento, trasmisión y recuperación de la información. Precisamente ese uso ha hecho que, en la actualidad, se presenten una variedad de amenazas que afectan a su confidencialidad, integridad y disponibilidad de su principal activo que es la información. En la mayor parte de empresas, no se precautela la seguridad de este activo y no se cuenta con políticas adecuadas para protegerla, lo que conlleva a la vulnerabilidad de su información.

De acuerdo con Inteco (2014) y Agesic (2016), la información representa un valiosos activo en todas las empresas, pues de esta depende el adecuado funcionamiento y toma de decisiones de las mismas. Para Chiavenato (2006), refiere que la información es un conjunto de datos que tienen cierto significado, y contribuye aumentar o a disminuir la incertidumbre, a su vez incrementa el conocimiento específico de algo. Esta información expresa un mensaje determinado y proporciona orientaciones para una determinada solución.

Toda información es procesada y este procesamiento es de tres tipos, en función de las condiciones del entorno, relativo a la naturaleza de la tarea y el nivel de rendimiento, que se requiere en correspondencia con la tarea específica. Cuando las empresas tienen entornos estables, manejan de mejor manera su información y se apoyan en el empirismo y en los resultados del pasado.

Actualmente, los entornos empresariales, son cada vez más complejos, dinámicos y heterogéneos, por lo que es urgente la necesidad de procesar adecuadamente la información. En el segundo grupo, que se enfoca a la naturaleza de la tarea, la tarea

depende de la diversidad interna de la misma y toda esta demanda información y, por lo tanto, requiere interrelaciones entre sus subunidades. En relación con el nivel de rendimiento esperado, mientras mayor sean las exigencias en el resultado, más se incrementa las exigencias de calidad de los sistemas de procesamiento de información (Sarabia, 2017).

En función de lo expuesto para el procesamiento de la información, es necesario hablar de lo que representan los sistemas, considerados como un conjunto de elementos materiales e inmateriales (hombres, máquinas, métodos y reglas, entre otros), que se interrelacionan para transformar procesos conformados por entradas y salidas (Matheron, 1990).

Sin embargo, O´Brien y Marakas (2006), estiman que el sistema constituye un grupo de componentes, que se interrelacionan y que trabajan por una finalidad común, en donde, se aceptan entradas y se producen salidas. De ahí que surge la necesidad de analizar componentes y características de la Teoría General de Sistemas, considerada desde el paradigma holístico e integrador, como un conjunto de interrelaciones y elementos de comunicación entre especialistas y especialidades. Pues, los sistemas tienen características como. interactividad, límites, objetivos, y, control (Pérez, 2017).

Para dar cumplimiento de manera técnica y adecuada al procesamiento de la información es necesaria contar con un Sistema de Gestión de Seguridad de la Información (SGSI), pues este es el elemento más importante de la norma ISO 27001, este unifica criterios de evaluación de los riesgos asociados al manejo de la información institucional, dentro de los principios, que se manejan es confidencialidad (solo es accesible a quienes, se les autoriza), integridad (la información es la correcta), y disponibilidad (siempre accesible a quienes están autorizados).

Los beneficios que proporcionan los SGSI, se centran en establecer una metodología de gestión de seguridad estructurada; esto reduce los riesgos de pérdida, robo o integridad de la información; los riesgos y controles son continuamente revisados; se

garantiza la continuidad del negocio tras un incidente grave; permite el cumplimiento de la legislación vigente; reduce los costes y el mejoramiento de los procesos, así como del servicio y, también, aumenta la seguridad en base a la gestión de procesos. Se consideraría que solo las empresas del sector TI requieren la aplicación de esta norma, sin embargo, al ser la información uno de los principales activos de las empresas y se requiere en cualquier tipo de actividad, se estima que la gestión de seguridad de la información al momento es una necesidad, dentro del sector empresarial.

La norma ISO 27001: 2013, tiene como aspecto importante la flexibilidad, esto significa que es aplicable a todo tipo y tamaño de empresa, por lo que es importante conocer el contexto completo de la organización, por esta razón los objetivos de seguridad de información tomarían en cuenta los objetivos organizacionales (ESAN, 2016).

Ante todo, lo expuesto, es necesario analizar la problemática de estudio, donde se parte del crecimiento vertiginoso de las TIC, así como, el uso del internet a nivel mundial, se ha convertido en medios de comunicación relevantes, tanto para las personas, instituciones públicas y privadas y para el sector empresarial. En toda empresa, se maneja grandes cantidades de información, y está hoy en días es considerada como uno de sus principales activos, por esta razón es fundamental que las empresas, se encuentren protegidas frente a cualquier amenaza o peligro.

En la actualidad las empresas, se encuentran expuestas a fraudes y robos de información, en muchas ocasiones, se debe a que las empresas no destinan recursos necesarios que les permita mejorar su plataforma tecnológica y que les permita afrontar amenazas, prevenir riesgos de seguridad, lo que ocasiona en toda empresa la pérdida de información y económica.

Las empresas a nivel de América Latina están inmersas a un contacto de negociaciones digitales y por ende expuestas a un sin número de ciber amenazas, en el estudio realizado por la empresa Deloitte realizado en el año 2016, referente a las

tendencias en gestión de ciber-riesgos y seguridad de la información en Latinoamérica, refiere que de 89 organizaciones de 13 países y 7 industrias diferentes, el 40% sufrieron en algún momento una brecha de seguridad, sin embargo, se considera que este riesgo es mucho más alto que el reportado, debido a que las empresas por su reputación, no siempre reportan este tipo de ataques (Deloitte, 2016).

En el Ecuador, a partir del año 2019, se incrementaron los ataques cibernéticos a los sitios de las organizaciones gubernamentales y empresas privadas, dentro de las instituciones públicas afectadas, se visualizó a la embajada, el banco central, la presidencia, el SRI, esto evidenció la débil preparación y percepción, que se tenía de la ciberseguridad en el país. La principal barrera que enfrentan este tipo de organizaciones es el presupuesto, que se asigna a la inversión en ciberseguridad. Se refleja, también que, las empresas tanto públicas como privadas, no cuentan con procedimiento y políticas formales de seguridad informática, sin embargo, hasta el momento se ha realizado importantes acciones para tratar de combatir los ataques cibernéticos, con la ayuda de organismos como EcuCERT, cuya finalidad es brindar atención ante la presencia de ataques informáticos, bajo el seguimiento de ARCOTEL. Además, existe una red de intercambio y colaboración que contribuye en la defensa gubernamental a través de la implementación de estrategias de ciberseguridad como lo es CSIRT Américas (Morán, 2021).

En el año 2021, en el Ecuador, se perpetúo los ataques financieros y personales a través de malware, de acuerdo al reporte de seguridad de ESET dentro de los cinco códigos maliciosos que más utilizaron los hackers están los virus, troyanos, gusanos, spyware y *ransomware,* desde el año 2020 en Ecuador hubo más de 51 mil registros relacionados con *ryptominers* (malware utilizado para la minería de criptomonedas), alrededor de 140 mil detecciones de *exploits* (código utilizado para aprovechar vulnerabilidades en software), cerca de seis mil detecciones de *ransomware* (malware para el secuestro de información) y casi ocho mil detecciones de spyware (software espía), como datos de algunos tipos de software malicioso. A partir del 2020 el Ecuador

ocupó la sexta posición dentro de los países latinoamericanos con más detecciones de malware, después de Brasil, México, Argentina, Colombia y Perú (Abril, 2021).
Actualmente, la unidad de TI de la EP-EMAPA-A cuenta con una matriz de riesgo obsoleta y con errores por lo que, en constantemente, se tiene inconstancias en Gestión de Calidad- unidad encargada del control de todas las unidades de la empresa. De ahí que es necesario e importante analizar los aspectos de seguridad sobre todo dentro del área de TIC y seguridad física, pues la inadecuada gestión en la seguridad de la información y activos, genera incumplimiento de políticas (en caso de existir), pérdida de conectividad, apagones de energía, fallos del sistema, entre otros riesgos.

La información que maneja la EP-EMAPA-A, es sensible y, por lo tanto, es resguardada, de ahí que las normas ISO 27001 propone la estructuración de un plan de seguridad en el área informática. Se seleccionó esta norma por el alto nivel de aceptación que tiene en relación con la seguridad, dentro de sus principales características es la fácil adaptabilidad a las necesidades de las empresas sin importar el tamaño de esta. La acción principal de la norma es la preservación de confidencialidad, integridad y disponibilidad de información y activos de la empresa.

Debido a la gran conectividad del internet el personal tiene acceso de redes sociales y plataformas de música donde es el principal modo de escape y de ingreso a la información empresarial, por lo que, en los últimos meses, se tuvo un gran fallo en el sistema comercial y en el correo Institucional “Zimbra”, da como resultado varios días sin internet por la falta de seguridad informática en cada una de las computadoras instaladas para los funcionarios.

En cuanto al software implementado en la empresa, esto se ha realizado de manera dispersa y se tiene una base de datos en cada unidad por lo que con lleva una dificultad en la integración de información, provoca un atraso en los tiempos de respuesta a los usuarios y trámites internos.

El no tener una documentación adecuada en la unidad de TI como instructivos técnicos para la gestión de seguridad provoca inconsistencias en la matriz proporcionada por los técnicos que administran la unidad.

Bajo este referente teórico es importante sustentar esta investigación con antecedentes investigativos, en donde se destaque la importancia de la Gestión de Seguridad de la Información, de ahí que se propone el estudio realizado por Alarcón, et al (2016), quienes refieren que la seguridad es importante dentro de las redes y las comunicaciones, porque a través de esto permite obtener soluciones rápidas y eficientes, sobre todo para gestionar de manera eficaz las amenazas informáticas, así como la confidencialidad de los datos. Además, el sistema, que se implemente permite el cumplimiento de estándares.

Todo esto, sobre todo, porque, en las instituciones gubernamentales la seguridad informática es uno de los requerimientos más importante, en la mayoría de las aplicaciones y servicios, que se brindan a la ciudadanía, no se toman en cuenta medidas de seguridad o análisis de posibles puntos débiles. Las instituciones gubernamentales que no cuenten con esquemas de seguridad definidos, se convierten en fácil presa para terceras personas, a las que se las conoce como cibercriminales, que aprovechan la vulnerabilidad de los sistemas con la finalidad de obtener información sensible, crítica y confidencial de los ciudadanos y de las operaciones de la institución. Bajo lo expuesto es necesario que las organizaciones gubernamentales, manejarían un ciclo de mejora continua en los procesos de seguridad.

Con base en la situación problémica planteada, se determina como problema a investigar la siguiente interrogante: ¿Cómo diseñar un plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013?

Al ser esta investigación de tipo cualitativa, se establecen varias preguntas científicas, con las cuales, se pretende ser explícito al momento de responder y sobre todo que tiene correspondencia directa con los objetivos de la investigación:

- ¿Cómo contribuir en la mejora de los procesos internos bajo la norma ISO/IEC 27001: 2013?
- ¿Cuál es la mejor metodología de análisis para el caso de estudio?
- ¿Se puede desarrollar el plan de sistemas de gestión de seguridad en la empresa?

El objetivo general de este estudio, se centra en: Desarrollar un plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013 para el centro de la base de datos (cuarto frio). El camino a seguir en esta investigación está determinado por los objetivos específicos de la misma:

1. Elaborar el estado del arte sobre gestión de riesgos en infraestructuras tecnológicas.
2. Diagnosticar la situación actual de la empresa mediante la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones (MAGERIT).
3. Sustentar la aceptabilidad de riesgos de la empresa.
4. Validar el plan y gestión de seguridad de la información para la EP-EMAPA-A. por criterio de expertos

El fin de esta investigación es generar un plan de gestión de seguridad de la información para EP-EMAPA-A con base en la situación actual, se desarrollaría la planeación SGSI basado en la matriz de riesgos obtenido de la metodología y una guía para la implementación.

La presente investigación destaca la necesidad de contar con un plan de gestión de seguridad de la información (PGSI), desarrollado bajo las Normas ISO 27001:2013, con la finalidad de asegurar la confidencialidad, integridad y sobre todo disponibilidad de información. Desde el punto de vista teórico, se encarga de estudiar el funcionamiento adecuado de este plan en la empresa EP-EMAPA-A.

Metodológicamente, se apoyó en el nivel de investigación descriptivo, se toma en cuenta lineamientos científicos para el establecimiento de la realidad actual de la EP-EMAPA-A, en relación con el manejo de su información, además, los procedimientos, técnicas y métodos, que se empleen en este estudio serían aplicados en investigaciones similares.

Desde el punto de vista diagnóstico - técnico, para la identificación de la problemática y del estado actual del manejo de la información, se utilizó la metodología MARGERIT, la cual, permite el análisis de riegos y está alineada a las normas internacionales ISO 27001, 27002, 27005 y 31000, en la que se realiza un estudio descriptivo de teorías sobre Gestión de Proyectos y Gestión de Riesgos, se revisa las vulnerabilidades y amenazas que están presentes en la empresa, donde se aplicaría las fases de la metodología.

Con base a la utilidad práctica los resultados de esta investigación, que responde a la realidad de la EP-EMAPA-A., serían desarrollados y aplicados en empresas de contextos similares, pues el plan de gestión de seguridad de la información para EP-EMAPA-A, contiene todos las fases y elementos necesario para modernizar el sistema de protección de activos de información en la empresa de estudio.

Los beneficiarios directos son los miembros de la empresa con sus respectivos departamentos, pues a través de la implementación de este plan de seguridad de la información, se cumple con requerimientos legales y normas de seguridad sobre información y sus activos y esto permite tener ventajas comerciales y elevaría el nivel de confianza de sus usuarios.

Este plan de gestión de seguridad de la información para la EP-EMAPA-A., tiene el carácter preventivo, pues su finalidad es generar una cultura de manejo de información tanto en administradores como en usuarios, con la finalidad de mitigar la presencia de riesgos que afecten de manera significativa a la empresa.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Seguridad de la Información

En toda organización la información es un elemento fundamental, esta es utilizada en todas las actividades, que se realizan y la mayor parte de ésta es almacenada de manera digital, pues las organizaciones, no se encuentran alejadas de los diferentes avances tecnológicos y del aporte de estos para el desarrollo y funcionamiento de las mismas. Sin embargo, en la actualidad la información sufre diversos daños, sobre todo en su integridad, de ahí que es importante manejar elementos de seguridad que disminuyan el riesgo de siniestralidad de pérdida de la información.

Como ya se mencionó en la introducción, las organizaciones proveerían estrategias que contribuyan a proteger sus activos ante amenazas, a las que se encuentran expuestas en materia de seguridad de información, para esto es necesario que cuenten con procedimientos adecuados que permitan la implementación de controles de seguridad basados en la evaluación de riesgos, y partir de una medición sistemática de los controles con los que cuente en función de sus necesidades externas e internas.

Dentro de las amenazas a las que están expuestas las organizaciones son externas e internas como incendios, inundaciones, terremotos, fraudes, vandalismos, sabotaje, espionaje, robo de información, entre otras; también, se cuenta con amenazas consideradas como involuntarias que serían causadas por acciones de usuarios como virus, revelación de contraseñas, acciones producidas por falta de conocimientos, entre otras (Arlenys, 2017).

Por lo expuesto, se determina que la seguridad, se convierte en una actividad de gestión, que se transforma en un ciclo y no solo la ejecución de un conjunto de actividades, para esto, es necesario el cumplimiento de normativas existentes para el manejo y seguridad de información. De ahí la necesidad, de que se cuente con un sistema de gestión de Seguridad de la Información, en donde, se determinen políticas,

procedimientos y controles que tengan la finalidad de disminuir los riesgos de la organización y al contrario le brinde ventajas y niveles de resiliencia en relación con el manejo y seguridad de la información.

Por esto, es necesario tener claro referentes teóricos relevantes que fortalezcan el desarrollo de esta investigación, no obstante, López (2016), define a la seguridad de la información como el conjunto de medidas orientadas a la prevención de las organizaciones y de los sistemas tecnológicos, con la finalidad de resguardar y proteger la información, orientadas a garantizar la confidencialidad, disponibilidad y sobre todo integridad de la información. Sin embargo, las ISO 27001, conceptualizan a la seguridad de información como la necesidad de preservar la información en términos de confidencialidad, integridad y disponibilidad, términos claves, sobre los que se cimienta la seguridad de la información donde implica el tratamiento de la misma (Arlenys, 2017).

En correspondencia con lo señalado, Gómez (2018), refiere que es aquella estructura en donde se consideran medidas preventivas que garanticen la confidencialidad, integridad y disponibilidad de la información, basado en las buenas prácticas de los procesos tecnológicos, que se gestiona en una organización y que se enfoquen a la mitigación de los riesgos y amenazas de la información de la empresa. Es importante diferenciar lo que significa los tres pilares de la seguridad de la información:

- Confidencialidad, orientada a la propiedad que tienen las organizaciones para prevenir, que se divulgue la información a que personas que no están autorizadas al manejo de la misma.
- Integridad, refiere a la propiedad que tiene como finalidad la protección de la información, evitar a que los datos sean modificados por personas no autorizadas.
- Disponibilidad, representa aquella característica y propiedad a que la información, se encuentre a disposición de quienes tienen los permisos de acceso.

Como se observa la seguridad de la información, se centra en tres pilares: confidencialidad, integridad y disponibilidad, la finalidad de esta es contribuir al adecuado manejo de la información en donde, se garantice procesos y/o acciones, que se orienten a la mitigación y prevención de riesgos de la información de la empresa, criterio coincidente con Kusumah et al (2014), al indicar que:

> Las dimensiones de la seguridad de la información en el contexto de la confidencialidad, la integridad y la disponibilidad de la información están siempre en el logro de los objetivos comerciales o los objetivos de la empresa / organización. El diseño e implementación del control de riesgos de seguridad de la información evita la filtración de información, la destrucción de información o la falta de disponibilidad de información (p. 10).

La seguridad de la información implica un sistema de gestión y un gobierno efectivo, por esta razón la implementación de estos, se realiza bajo la aplicación de las mejores prácticas y modelos como: ISO *(International Organization for Standardization),* COBIT *(Control Objectives for Information and related Technology),* ITIL *(Information Technology Infrastructure Library),* CMMI *(Capability Maturity Model Integration),* PMBOK *(Project Management Body of Knowledge),* OSSTMM *(Open Source Security Testing Methodology Manual*), entre otros; todas estas normas dan lineamientos claros para la implementación de la gestión de seguridad de la información (GSI), de ahí que es necesario que los problemas de seguridad de información no serían resueltos de manera parcial sino en su totalidad (Setiawan, Syamsudin, & Sastrosubroto, 2017).

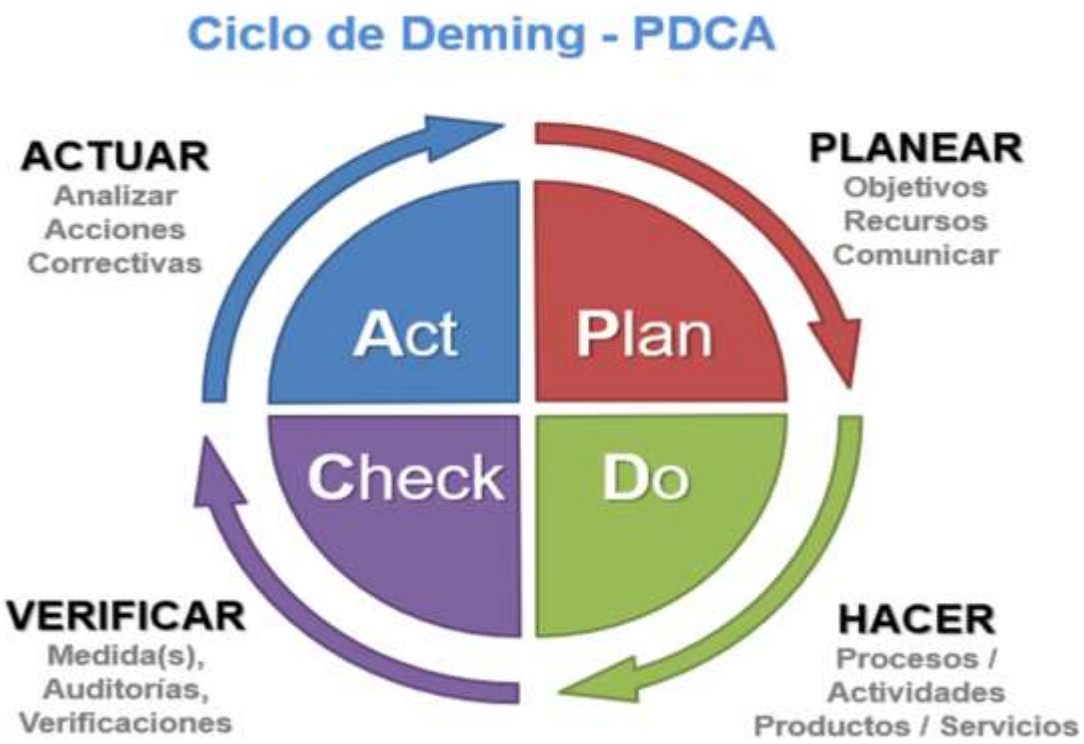
Sistemas de Gestión de Seguridad de la Información

Para que la seguridad de la información cumpla su finalidad, en relación con la protección de su principal activo, es necesario implantar, mantener y mejorar un Sistema de Gestión de Seguridad de Información, el mismo que se desarrolla bajo el

enfoque de mejora continua, que se lo conoce como el Ciclo de Deming, que consta de cuatro pasos:

- Planificar, en esta fase se evalúan los riesgos de seguridad de la información y se determinan los controles adecuados
- Hacer, fase en la que se ejerce la implantación y operaciones de control.
- Verificar, fase que tiene como finalidad la revisión y evaluación el desempeño del SGSI, esto es alcanzar la eficiencia y eficacia.
- Actuar, en esta fase se realizan cambios sistemáticos y periódicos que contribuya a mantener el SGSI al máximo rendimiento (Alvarado, 2019).

Figura 1. Ciclo de Deming PDCA

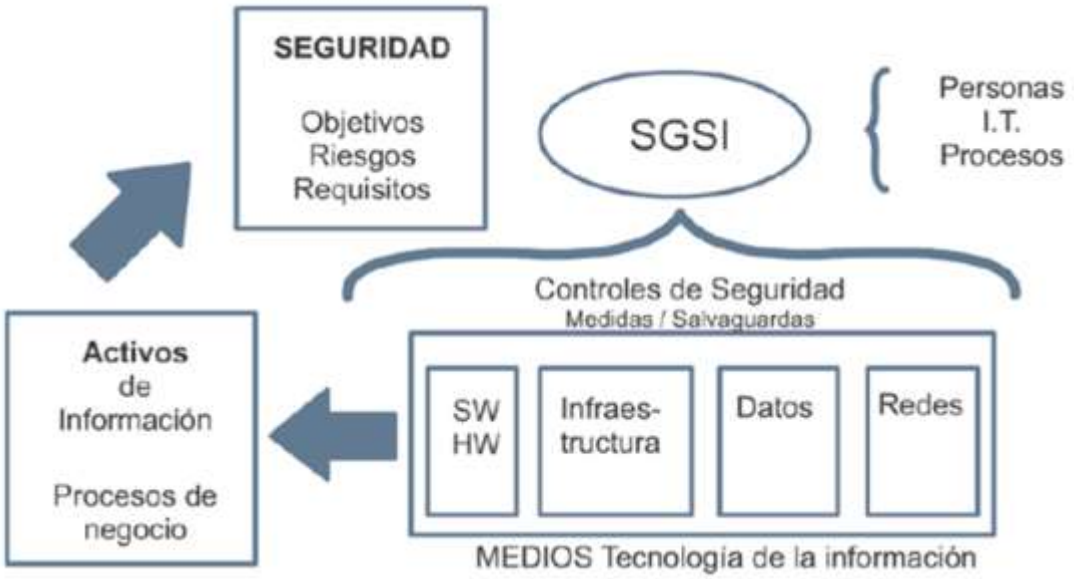


Fuente: Sistema de gestión de seguridad de la información: qué es y sus etapas (Alvarado, 2019)

Lo que es claro que un SGSI, no es un sistema informático, tampoco es una extensión de un sistema de gestión de calidad, ni un conjunto de documentos, que se elaboran

y publican. Contrario a esto los SGSI, constituyen herramientas, que se ponen a disposición de los niveles directivos de las organizaciones, en donde se determinan y se llevan a cabo políticas, objetivos, procesos y procedimientos de seguridad de la información, el mismo que proporciona mecanismos que salvaguarden los activos de la información y de los sistemas, que se procesan en la organización, en correspondencia con las políticas de seguridad y los planes estratégicos de la empresa (Enterprise, 2017). El enfoque principal de los SGSI, se encauza en la mitigación del riesgo empresarial, en la figura 2, se muestra la estructura de un SGSI:

Figura 2. Estructura de un SGSI



Fuente: Sistema de gestión de seguridad de la información (Enterprise, 2017)

Los SGSI proporcionan diferentes beneficios a las organizaciones, entre los principales la reducción del riesgo a la pérdida de la información en las organizaciones; permite la revisión continua de los riegos a los que están expuestas las organizaciones; garantiza una metodología que contribuye a la gestión de la seguridad de la información de forma clara y concisa; se orienta a la implantación de medidas de seguridad, obliga a que se realicen auditorías externas de manera periódica para la identificación de riesgos y que contribuya a la mejora continua; permite que las organizaciones desarrollen estrategias

de resiliencia ante riesgos y amenazas con la información, además, permite que se cumple las legislaciones y normativas existentes; todo lo mencionado favorece la reducción de costos y un mejor funcionamiento de los procesos, con el fin de llevar a las organizaciones a ser cada vez más competitivas (Enterprise, 2017).

La gestión de la seguridad de información se realiza mediante un proceso que sería sistemático, documentado y organizado, en el que se garantice un nivel de protección virtual a la información de toda organización, como ya se mencionó, los SGSI, se orientan a garantizar que los riesgos de seguridad de información sean asumidos, gestionados y minimizados en la organización, además, que la información esté debidamente documentadas, estructurada (Tersek, 2018). Los SGSI, se desarrollan en seis fases, como se observa en la figura 3:

Figura 3. Fases de los SGSI

Fuente: fases del Sistema de gestión de seguridad de la información (Tersek, 2018)

Fase 1 – Situación Actual, en esta fase, se realiza la descripción de la organización, las actividades que realiza, así como la descripción del entorne, en el que se desenvuelve, el tamaño organizacional, su estructura organizacional. La finalidad de

esta fase es la planeación, diseño y definición de recomendaciones para la implementación de un SGSI, enfocado en los procesos de todas las áreas de la organización, por lo que, se define el estado actual de la misma, y, se establecen controles para la mitigación de riesgos, establecer una adecuada brecha de seguridad entre los procesos y el SGSI, permite que se genera cultura en seguridad de la empresa, orientada a la identificación y análisis de riesgos, a través de la sensibilización a los funcionarios y contratistas (Tersek, 2018).

Fase2 – Sistema Gestión Documental, se describe de manera clara y concisa las políticas de seguridad de información, así como se estructura la respectiva documentación del SGSI, entre los más importantes: procedimientos de auditorías externas, gestión de indicadores, procedimientos de revisión por la dirección, gestión de roles y responsabilidades y la metodología de análisis de riesgos; finalmente, se establece la declaración de aplicabilidad (Segovia, 2016).

Fase 3 – Análisis de riesgos, en esta fase se analiza todos los activos, que se encuentran vinculados a la información, además, se define la tabla de valoración de activos, así como sus respectivas escalas de valoración, donde se considera los elementos de criticidad, valor, categoría, servicios y misión; finalmente, se identifican las dimensiones de seguridad bajo cinco dimensiones de seguridad: Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad, sigue una escala de valores con criterios de daño como: muy grave, grave, importante, menor, irrelevante. En base a lo anteriormente ejecutado, se construye la tabla resumen de valoración y, se realiza el análisis de amenazas, para que, con los resultados obtenidos, se valore el riesgo en función de impacto a nivel de operación, financiero, e información de ocurrencia de las amenazas. Posteriormente, se identifica la relación entre las amenazas y los activos. El resultado final de esta fase es la tabla de activos y dimensiones de seguridad (Tersek, 2018).

Fase 4 – Propuesta de proyectos, se establece el plan de tratamiento del riesgo, en donde se establecen las medidas de protección, salvaguarda o contramedidas, que se

implementarían para cada uno de los activos en función del impacto que representa la materialización de una amenaza. Posteriormente, se determina el riesgo residual y se establecen propuestas a través de proyectos (Segovia, 2016).

Fase 5 – Auditoría de cumplimiento*,* para la ejecución de la auditoría, se utiliza el modelo de madurez de la capacidad (CMM) como metodología para el análisis del grado de madurez, posteriormente, se evalúa la madurez, a través del grado cumplimiento y por cada control, se identificaron de acuerdo con los hallazgos positivos y negativos. Finalmente, se determinan los resultados, a través del resumen de hallazgos de la auditoría.

Fase 6 – presentación resultados y entrega de informes*,* a través de la memoria del proyecto, se socializan los resultados y se genera una cultura de seguridad de información con todos los miembros de la organización (Segovia, 2016).

Con base en lo expuesto es claro que los SGSI son herramientas necesarias para toda organización, pues contribuyen a la optimización de los recursos de la misma, así como al ahorro de los costos, pero sobre todo se orienta a la mejora continua en correspondencia con los objetivos y metas planteadas. Este proceso sistemático permite alcanzar niveles de madurez que en ese momento alcanza la organización, los resultados de estos procesos conllevan a cambios de procesos y estructuras que garanticen la integridad, confidencialidad y disponibilidad del principal activo de la organización que es la información.

Los SGSI, se desarrollan bajo la metodología de “mejora continua”, o también, conocida como el ciclo Deming, que desarrolla bajo el círculo PDCA (*Plan – Do-Chechk – Act*), de ahí que es necesario plantear la relación entre el modelo PDCA y las ISO 27001:2013. El ciclo PDCA, es una metodología, que se enfoca en la mejora continua, sin embargo, no sería implantada al 100% de efectividad y precisión, las ISO 27001 incluye dentro de su proceso el mencionado ciclo, en donde:

- *PLAN* (planificar), se define objetivos y procesos necesarios que permitan alcanzar los resultados esperados.
- *DO* (hacer), consiste en la aplicación de los procesos a pequeña escala.
- *CHECK (*verificar), posterior a la aplicación es pertinente realzar el control y analizarlos con la finalidad de validar el cumplimiento de los objetivos y establecer acciones de mejora.
- *ACT* (actuar), se realiza procesos de retroalimentación en correspondencia con las conclusiones del paso anterior y se documenta el proceso.

Para la adaptación del modelo Deming al Sistema de Gestión de Seguridad de Información (SGSI), en la fase de planificación, se crea el SGSI, para el hacer se implementa y opera el SGSI, para la verificación en el SGSI, se supervisa y revisa el sistema; y, finalmente, en el actuar, se mantiene el sistema (Colegio oficial de ingenieros de telecomunicaciones, 2018).

Para la integración del SGSI, dentro de la gestión de una empresa, es un punto importante para que esto, la versión ISO 27001:2013 comparte su estructura con las normas de gestión de calidad ISO 9001, lo que facilita la integración de los diferentes sistemas de gestión en una organización (Sánchez, 2016). Dentro de un sistema de gestión de la seguridad, se encuentran dos tipos de procesos:

- Proceso de gestión, son propios del sistema de gestión y se enfocan en conseguir la revisión y mejora continua del sistema, son comunes a los procesos de gestión de calidad.
- Procesos sobre seguridad de la información, son propios de la seguridad, se integran dentro de los procesos propios de cada actividad de la organización en correspondencia con las demás dimensiones.

Las normas ISO 27001, cuenta con dos cuerpos normativos:

- ISO 27001 Requisitos para un sistema de Gestión (SGSI)

- ISO 27002 Guía de buenas prácticas para la implantación de un SGSI

La primera representa la norma certificable que contiene los requisitos necesarios para la implantación de un sistema de seguridad de información, y la segunda es una guía, en donde se establecen los controles o instrumentos de control, en donde se aborda los problemas o peligros para la seguridad de la información (Colegio oficial de ingenieros de telecomunicaciones, 2018).

Uno de los requisitos importantes en la norma ISO 27001, es el liderazgo, pues refiere el compromiso que tiene toda organización en el proceso de implantación de SGSI, el compromiso de la organización, se valida en la aportación de los recursos sean estos humanos y materiales, dentro de las principales responsabilidades de la dirección de una empresa para esta implantación es la de elaborar una política de seguridad y sus respectivos objetivos; además, comunica estos a toda la organización, para garantizar la participación activa de todos sus integrantes; posteriormente, define las áreas de responsabilidad y los roles correspondientes a la seguridad de información; finalmente, dar el seguimiento de mejora y validar el cumplimiento de los objetivos, con la finalidad de conseguir la mejora continua. Por lo que es fundamental generar una cultura de seguridad dentro de la organización (Gobierno de España, 2017).

Una vez, que se identifique las necesidades de los involucrados de la organización, y se identifique los riesgos, se estructura un plan con actividades orientadas a la mitigación de los mismos, para esto se cumple con los siguientes pasos:

- Identificar las necesidades y expectativas de todos los involucrados
- Analizar los riesgos y oportunidades
- Evaluar los riesgos (a través del análisis de impacto o cálculo de riesgo)
- Estructura el plan de tratamiento de riesgos y,
- Elaborar el plan de tratamiento de riesgo (Colegio oficial de ingenieros de telecomunicaciones, 2018)

Para la planificación, a más de tener el compromiso de la dirección, se considera la gestión de los recursos, la competencia y concienciación personal, la comunicación con todos los involucrados inclusive proveedores externo y tener claro los requisitos de documentación. Para poner en práctica las medidas para la seguridad de la información, se tendría claro el contexto organizacional y el plan de tratamiento de riesgos.

Para la implantación de un SGSI es necesaria una adecuada gestión de riesgo en seguridad de la información, para esto es necesario tener claramente identificados los riesgos existentes. Pues esto permite la aplicación de controles necesarios para su adecuado tratamiento.

Para la evaluación de desempeño, se cuenta con herramientas como: auditorías internas de seguridad de la información y un proceso sistemático para la revisión aplicado por parte de la dirección de la organización (Mantilla, 2018).

Al hablar de mejora continua, no se refiere solamente a la actualización continua del sistema de gestión, sino que también, es la revisión permanente para encontrar oportunidades de mejora y la identificación de los errores cometidos, para su correspondiente retroalimentación oportuna y establecer acciones correctivas y dar un tratamiento a la No Conformidades.

1.2. Plan de gestión de seguridad de la información

Un plan de gestión de datos o de información es un documento, que se elabora al inicio de un proyecto, en este se describe la gestión de los datos, es decir, el procesamiento, que se tiene con la información antes, durante y después. Este documento tiene como propósito analizar y considerar los principales elementos de una política de gestión de datos, además, describe el tratamiento, que se recibe la información, que se recopila o se genera en una organización, es la herramienta que sirve de apoyo para el manejo adecuado del ciclo de vida de la información (CEPAL, 2018).

Uno de los elementos importantes dentro del manejo de la información es considerar la gestión del ciclo de vida de los datos, que se almacenan, pues cualquier activo de la información cumple ciertas fases desde el momento, en que esta se adquiere hasta cuando se la desecha, por lo que es importante asegurar la calidad de los procesos. Considerado que la información cumple un rol vital en el ciclo de producción de toda organización, dentro del este ciclo, se incluyen procesos de generación/ recolección, organización, almacenamiento, recuperación, comunicación, difusión, aprovechamiento, transformación y/o descarte. Existen diferentes modelos que plantean el ciclo de vida de la información Vizcaya (2013), propone un proceso de gestión de información enmarcada en que luego de ser procesada, tenga la finalidad de generar un nuevo conocimiento y, por lo tanto, representa impacto en la toma de decisiones, se constituye como cíclico, es en espiral y tiene un incremento sostenido del valor de la información, como se muestra en la figura 4:

Figura 4. Ciclo de vida de la información

Fuente: (Vizcaya, 2013)

De acuerdo a Ceballos, Cervantes y Fierros (2017), el ciclo de vida de un sistema de información representa un manual que engloba a personas, máquinas y/o métodos

debidamente organizados, con la finalidad de recopilar, procesar y trasmitir los datos que constituyen la información. Un sistema de información está constituido por la infraestructura, la organización, el personal y todos los componentes necesarios para la recopilación, procesamiento, almacenamiento, transmisión, visualización, diseminación y organización de la información.

En este caso, se define que un sistema de información pasa por una serie de fases dentro de las, que se mencionan:

- **Planificación**, en donde se identifican todas las tareas que realicen desde el inicio hasta la finalización de la información;
- **Análisis,** en esta fase se identifica todos los requerimientos para el manejo de la información y para la comprensión adecuada de sistema;
- **Diseño**, se analizan las posibles alternativas necesarias para la implementación del sistema de información y se define la estructura general del sistema;
- **Implementación,** se identifica las herramientas, que se utiliza, así como el entorno en el que se desarrolla y el lenguaje apropiado a usar;
- **Pruebas**, en esta fase se detectan los posibles errores que presentarían, así como también, se realiza la búsqueda de errores para corregirlos en función del contexto y las necesidades;
- **Uso y Mantenimiento,** este consume aproximadamente del 40 al 80% de los recursos, es una de las etapas más importantes, porque en esta fase, se elimina defectos detectados durante la vida útil, se adaptan nuevas necesidades y se le añade funcionalidad a través de características deseables (Ceballos, Cervantes, & Fierros, 2017).

Sin embargo, Coutin (2016), propone el ciclo de vida clásico de la información, este modelo, se lo conoce, también, como modelo en cascada , cumple un orden específico y, no inicia una etapa sin finalizar la anterior, en este modelo se exige una aproximación secuencial, este presenta una desventaja pues a los clientes les resulta difícil

establecer de manera explícita todos los requerimientos y requisitos desde el inicio, otro factor es que no se tiene una versión operativa, mientras no se cumpla con todas las etapas por lo que, que cualquier rectificación relacionada con algún error en las etapas iniciales, este genera un costo adicional en la figura 5, se muestra este modelo:

Figura 5. Ciclo de vida clásico de un sistema de información, modelo en cascada

Fuente: (Coutin, 2016)

También, es importante considerar la arquitectura de la información, que se la considera como la actividad que permite la determinación de los contenidos y la funcionalidad que va a tener esta en la empresa, además, específica la forma en que los usuarios encontrarían la información, a través de su organización, navegación, etiquetado, sistema de búsqueda y mapeo. En la arquitectura, se determina la misión y los objetivos que va a tener la información dentro de la empresa, estos están enfocados en correspondencia con la satisfacción de las necesidades en relación con la organización de la información.

Los procesos, que se toman en cuenta y que son parte de la arquitectura de la información son la selección, organización de la información, diseño de interfase, implementación, posicionamiento, búsqueda y recuperación, y diseminación. Estos procesos pertenecen a un sistema de información, por lo cual, guardan una supuesta

relación con los procesos identificados en el ciclo de vida de la información (Muñoz, 2017).

Un plan de gestión de seguridad de información tiene una estructura específica: alcance, políticas, procedimientos de seguridad de la información, roles y responsabilidades, gestión y clasificación de activos de información, protección de datos personales, clasificación de los activos de la información, gestión documental y gestión de riesgos, mejora continua del SGSI (Ministerio de Minas y Energía, 2020).

- **Alcance**, brinda una explicación clara de la finalidad del documento
- **Políticas**, este elemento es importante porque delinea los criterios, que se cumplen para el manejo adecuado de la seguridad de la información, estas están creadas por una comisión específica, luego ser aprobadas y generar estrategias de actualización. La política tiene un nombre para este caso son: “Políticas de seguridad y privacidad de la información”, los criterios, que se toma de referencia son los establecidos en NTC ISO/IEC 27001:2013. La estructura que tiene es:

    - Número de la política.
    - Título de la política.
    - Norma referente
    - Definición de la política.
    - Objetivo.
    - Alcance/Aplicabilidad.
    - Nivel de cumplimiento.
    - Responsable de la aprobación de política.
    - Responsable de la política.
    - Fecha de vigencia, de actualización y de retiro (Ministerio de Minas y Energía, 2020).

- Las políticas son escritas en forma sencilla y específica, el enunciado es preciso y con lenguaje técnico y explícito

- Todas las personas cubiertas por el alcance y aplicabilidad darían cumplimiento del 100% de la política. El incumplimiento a esta política trae consigo, las consecuencias legales que apliquen a la normativa establecida

- **Procedimientos de seguridad de la información**, indica la forma de actuación y el orden del mismo contribuyen a la preservación de la seguridad y privacidad de la información y se definen en base a lo establecido en la norma a ISO/IEC 27001:2013.

- **Roles y responsabilidades**, Para el adecuado funcionamiento del plan de gestión de seguridad de la información es necesario particularizar roles y responsabilidades de cada persona encargada de establecer y desarrollar cada una de las actividades asignadas (Ministerio de Minas y Energía, 2020).

- **Gestión y clasificación de activos de información**, es necesario contar con un inventario y clasificación de los activos de la información, esta información tendría la siguiente estructura:
  - Número consecutivo único que identifica al activo en el inventario.
  - Proceso al que pertenece el activo.
  - Propietario / Responsable
  - Custodio.
  - Nombre del activo de información.
  - Descripción del activo de información.
  - Categorización del activo de información: por ejemplo, hardware, software, servicio, personas, la cual, se revisaría periódicamente o cuando se presenten cambios en la información o en la estructura que afectaría.
  - Idioma.
  - Medio de conservación.
  - Periodicidad o de generación o actualización en caso de activos expedientes físicos y digitales. Fundamento constitucional o legal.

- Descripción de Condición legitima de la excepción.
- Clasificación del activo de acuerdo a la ley de transparencia.
- Valoración del activo (confidencialidad, integridad y disponibilidad) (Ministerio de Minas y Energía, 2020).

- **Protección de datos personales**, se protege los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación (tratamiento) por parte de entidades de naturaleza pública y privada:

- **Clasificación de los activos de información**, la información es clasificada de acuerdo a los criterios de confidencialidad:

Cuadro 1.Clasificación de los activos de información

	Disponibilidad	**Integridad**	**Confidencialidad**
1 - Mínimo	La no disponibilidad de la información afectaría la operación normal de la entidad. No tiene implicaciones legales, económicas o de pérdida de imagen	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo	Es la información que ha sido calificada como de conocimiento público. El conocimiento o divulgación no autorizada de la información no tiene ningún impacto negativo en los procesos
2 – Bajo	La no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos	La pérdida posible de en la exactitud de algún dato o estado completo de la información tendría algún impacto negativo en los procesos	Esta información sería entregada o publicada con ciertas restricciones sin que implique daños ni impactos negativos a terceros ni a las actividades y procesos
3 - Medio	La no disponibilidad de la información conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o	Información cuya pérdida de exactitud y completitud conllevaría un impacto negativo de índole legal o económica, retrasar	Es la información que es utilizada por los funcionarios del Ministerio para realizar sus labores en los procesos y que sería conocida por

	generar pérdida de imagen	sus funciones, o generar pérdida de imagen	terceros con la autorización del propietario del activo.
4 – Alto	La falta o no disponibilidad parcial de la información impacta negativamente la prestación de servicios de tecnología y de información	La pérdida en la exactitud de algún dato impacta negativamente la prestación de servicios de tecnología y de información	La divulgación no autorizada de la información impacta negativa y significativamente al proceso evaluado y/u otros procesos
5 - Crítico	La no disponibilidad de la información conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos	Información cuya pérdida de exactitud y completitud conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.	A esta información sólo tendrían acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. La divulgación no autorizada de esta información impacta negativamente

Fuente: (Ministerio de telecomunicaciones y de la sociedad de la información, 2020)

- **Gestión documental,** Para la creación y actualización de la documentación incluiría lo siguiente:

  - Información descriptiva: título, versión, fecha y codificación.
  - Control de cambios entre versiones.
  - Etiquetado y clasificación de la información del documento.
  - Firma de quien elaboró, quien revisó y quien aprobó.

- **Gestión de riesgos,** aquí se plantean los principios y directrices necesarias para la gestión de riesgo, con las cuales, se identificaría y establecería controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información. De acuerdo con la norma ISO 27001:2013 un incidente de seguridad de la información está definido como “un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad

significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información" (ISO27001 Icontec, 2013). Dentro de los posibles eventos, que se presentarían son:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Pérdida o robo de la información.
- Modificación no autorizada.
- Diligenciamiento errado de formatos.
- Perdida o daño de la documentación.

De acuerdo la NTC ISO 27001:2013, se define un evento de seguridad de la información como "la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad." (ISO 27001:2013, ICONTEC, Pág. 11, 2013). Los eventos de seguridad de la información que afectarían son:

Cuadro 2. Eventos de seguridad de la información

Evento	Descripción
Fraude Interno	Está asociado a la intención por parte de un funcionario de la organización de obtener información con fines ajenos a su labor
Fraude Externo	Son actos realizados por personas externas a la organización, que buscan apropiarse indebidamente de la información, por medio de acceso no autorizado, altera o vulnera el procesamiento de la información
Clientes	Según el Anexo A.9.2.2. de la norma ISO 27001:2013 “Se implantaría el suministro de acceso formal de usuarios para asignar o revocar los accesos para todo tipo de usuario”
Fallas Tecnológicas	Pérdida de información asociada a fallas tecnológicas debido a fallas en el procesamiento de la información que vulneran la confidencialidad, integridad y disponibilidad de esta.
Ejecución y administración de procesos	Pérdida de información asociada a errores de administración y ejecución de procesos

Fuente: (Ministerio de Minas y Energía, 2020)

Para la valoración del riesgo, se enumera los posibles riesgos de seguridad de la información, se los identifica con la finalidad de determinar el potencial de riesgo y finalmente, se determina los criterios de impacto y probabilidad, bajo los siguientes criterios:

Tabla 1. Criterios de impacto

Criterio	Valor categoría	Impacto Financiero	Impacto Reputacional	Impacto legal	Impacto operativo
Leve	**1**	Personal	Grupo de funcionarios	Multas	Ajuste a una actividad concreta
Menor	**2**	Grupo de trabajo	Todos los funcionarios	Demandas	Cambios en los procedimientos
Moderado	**3**	Relativo al proceso	Usuarios ciudad	Investigación disciplinaria	Cambios en la interacción de procesos
Alto	**4**	Institucional	Usuarios región	Investigación fiscal	Intermitencia en el servicio
Catastrófico	**5**	Estratégico	Usuario país	Intervención - sanción	Paro total del proceso

Fuente: (Ministerio de Minas y Energía, 2020)

Los criterios de probabilidad de ocurrencia a cada uno de los riesgos se valoran bajo los siguientes parámetros:

Tabla 2. Criterios de probabilidad de ocurrencia

Categoría		Valor categoría	Descripción	Frecuencia
Raro		**1**	El evento ocurriría solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
Improbable		**2**	El evento ocurriría en algún momento	Al menos de una vez en los últimos 5 años.
Posible		**3**	El evento ocurriría en algún momento	Al menos de una vez en los últimos 2 años
Probable		**4**	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año
Casi seguro		**5**	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

Fuente: (Ministerio de Minas y Energía, 2020)

Se valora el riesgo inherente el riesgo, al cual se está expuesto sin ningún tipo de control sobre el activo. Para valorar el riesgo inherente, se asignan las siguientes calificaciones: impacto financiero (IF), impacto reputacional (IR), impacto operativo (IO), impacto legal (IL) y probabilidad (PR). Al asignar las calificaciones al riesgo inherente, se considera que el activo no cuenta con controles para mitigar el impacto o reducir la probabilidad. El valor del riesgo inherente, se obtiene al aplicar la siguiente fórmula:

$$\mathbf{RI = (IF + IR + IO + IL) * PR}$$

- **Mejora continua del SGSI,** en esta fase se realiza la corrección de los errores, y para esto se tiene las siguientes consideraciones: cuando no hay conformidades, se realizan acciones que mitiguen el impacto; se revisan no conformidades para disminuir o eliminar las causas o consecuencias que generaría; si existe otras no conformidades similares, se realizan acciones preventivas (Ministerio de Minas y Energía, 2020).

1.3. Norma ISO/IEC 27001:2013

La ISO 27001 es una norma internacional que contribuye al aseguramiento, la confidencialidad e integridad de los datos y de la información, el estándar ISO 27001:2013, se utiliza para los Sistemas de Gestión de la Seguridad de la Información, permite que las organizaciones realicen la evaluación de riesgo y la aplicación de controles necesarios que fomenten la mitigación de estos. La aplicación de la ISO 27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización (ISOTools, 2017).

En la práctica, se ha demostrado que no es suficiente la implantación de controles y procedimientos de seguridad, que se establecen sin un criterio establecido, por esta razón la Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO / IEC 27000, establece una implementación efectiva de la seguridad de la información empresarial desarrolladas en las normas ISO 27001 / ISO 27002.

A nivel mundial la ISO 27001, se ha convertido en una de las principales normas para la seguridad de la información, su finalidad como ya se ha mencionado es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. La filosofía de esta norma, se basa en la gestión de riesgo y posteriormente en el tratamiento sistemático de este. Las medidas de seguridad, que se implementen en una organización sería bajo una política previamente definida, así como los procedimientos e la implementación de la misma (Kosutic, 2017).

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

Figura 6. Gestión de la seguridad de la información

Fuente: (Kosutic, 2017)

La norma ISO 27001, facilita un SGSI, consistente en medidas orientadas a proteger la información, indistintamente de las medidas, que se utilizan y lo protegen de cualquier amenaza, y que esto garantice la continuidad de las actividades de una empresa. Dentro de los objetivos de los SGSI están la confidencialidad, integridad y la disponibilidad de la información (Normas ISO, 2018). Para la implementación de los SGSI, se cumplirían fases que detallan en la siguiente figura:

Figura 7. Fases para la implementación de un SGSI

Fuente: (Normas ISO, 2018)

Sin embargo, al momento de implantar el SGSI es necesario considerar como elemento fundamental la evaluación de riesgo de la organización, esto permite que la dirección de la organización tenga una visión clara que le orienta para la definición del alcance y ámbito de la aplicación de la norma, así como las políticas y medidas a

implantar, por lo que es necesario que este sistema, se integre a una metodología de mejora continua, que se utiliza en las normas ISO. Por esta razón, es necesario tener clara la metodología de evaluación de riesgo que responda a las necesidades de la empresa, en la siguiente figura se muestra la metodología de evaluación de riesgo:

Figura 8. Metodología de evaluación y tratamiento de riesgo

Fuente: (Normas ISO, 2018)

1. Identificar los activos de la información y cada uno de los responsables, considera un activo a todo lo que representa valor para la organización, en donde se incluye soportes físicos, intelectuales o informativos, así como la marca y reputación, entre otros.

2. Identificar las vulnerabilidades de cada activo, esto es las debilidades propias de cada activo y que genera susceptibilidad para que la organización sufra de ataques o daños

3. Identificar amenazas, son todas aquellas acciones que ocasionarían daño a uno de los activos de la información, como son los desastres naturales, incendios o ataques de virus, entre otros

4. Identificar los requisitos legales y contractuales que la empresa cumple con los diferentes organismos, clientes internos y externos y proveedores.

5. Identificar los riesgos, en esta etapa, se definiría la probabilidad de amenaza o de vulnerabilidad de cada activo y que ocasionaría daño sea total o parcial, en relación con la disponibilidad, confidencialidad e integridad del mismo.

6. Cálculo del riesgo, se determina la probabilidad de ocurrencia de los riesgos, así como del impacto, en función de la prioridad del activo.

7. Plan de tratamiento del riesgo, se define las políticas de tratamiento de los riesgos, así como la política que defina la dirección, se identifica cada uno de los controles para cada riesgo y los que estan encaminados a: asumir, reducir, eliminar y transferir los riesgos (Normas ISO, 2018).

Dentro de todo el proceso de la implementación e implantación del SGSI, bajo ISO 27001, se requiere, que se configure y diseño la siguiente documentación:

- Alcance del SGSI
- Objetivos y política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento de riesgos
- Informe de evaluación de riesgos
- Definición de roles y responsabilidades de seguridad
- Inventario de activos

- Uso aceptable de los activos
- Política de control de acceso
- Procedimientos operativos para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad para proveedores
- Procedimiento para gestión de incidentes
- Procedimientos para continuidad del negocio
- Requisitos legales, normativos y contractuales (Kosutic, 2017)

Y estos son los registros obligatorios:

- Registros de capacitación, habilidades, experiencia y calificaciones
- Monitoreo y resultados de medición
- Programa de auditoría interna
- Resultados de auditorías internas
- Resultados de la revisión por parte de la dirección
- Resultados de medidas correctivas
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (Kosutic, 2017)

Por supuesto que una empresa decidiría confeccionar otros documentos de seguridad adicionales si lo considera necesario.

CAPÍTULO II. METODOLOGIA DE LA INVESTIGACIÓN

2.1. Caracterización de EP-EMAPA-A

La Empresa Pública Empresa Municipal de Agua Potable Ambato (EP-EMAPA-A), se creó mediante registro oficial número 2343, el 4 de julio de 1967 es una institución adscrita al Gobierno Autónomo Descentralizado Municipalidad de Ambato. La finalidad de esta es ser la encargada de la producción, distribución y comercialización del servicio de agua potable y de alcantarillado dentro de la jurisdicción territorial del Cantón Ambato.

La ciudad de Ambato ha crecido de una manera vertiginosa, por lo que para mejorar la atención de la misma la Empresa Municipal de Agua Potable Ambato, dividió su servicio en cinco plataformas:

La plataforma 1, comprende los sectores de Miraflores, la Matriz, San Francisco, la Merced e Ingahurco. Su área es igual a 383,68 ha. La plataforma 2, comprende la ribera occidental del río Ambato y el área de las laderas de Tusaló, Pinllo, Inasipí, Atocha y Ficoa. Su área es igual a 448.90 ha. La plataforma 3, conformada por la altiplanicie más alta de la ciudad, desde el talud de la calle 13 de abril, hacia Huachi Grande y se abre entre las laderas del Casigana y de Pishilata: Su área es igual a 3.711.15 ha. La plataforma 4, se forma por el área comprendida entre las cabeceras parroquiales de Izamba, Martínez y Atahualpa, y los sectores de San Luis, Macasto, El Pisque, Yacupamba y Quillán Loma, la cual, es la de mayor extensión con 3.787.8 Ha. La plataforma 5, que comprende los sectores de la Península y Catiglata Bajo, con un área de 226.7 ha.

Lo descrito anteriormente obliga a que EP EMAPA-A, busque mantener y conservar su calidad de servicios ante la ciudadanía, por lo que busca todas las alternativas para

el mejoramiento de los mismos; se considera el crecimiento poblacional entre el censo 2001 al 2010, en el primero se tuvieron 90.623 viviendas y en el 2010 se registraron 116.470. Hubo un incremento del 28,5%. A nivel del cabildo ambateño, se registró más de 82000 predios urbanos y en la zona rural alrededor de 130000 predios, lo que genera una idea bastante amplia del desarrollo de la ciudad en los próximos años.

En relación con el nivel de atención aproximadamente la EP-EMAPA-A en la oficina matriz, atendió un total de 4060 reclamos, un total de 2454 conexiones de servicio de agua potable factura un total de $4.475.550,51 en el año 2019. Otro problema es que la empresa adolece de una carente planificación de órdenes de trabajo y cumplimiento de las mismas, lo que genera un porcentaje representativo de obras civiles y técnicas sin resolver.

Se considera que EP-EMAPA-A, tiene como misión institucional “prestar un servicio de alto nivel”, sin embargo, en la actualidad se han registrado quejas por ende niveles bajos de eficiencia, lo cual genera descrédito ante la ciudadanía, uno de los problemas fundamentales es justamente el manejo adecuado de los activos de la empresa, por lo que en algunas ocasiones, se refleja la subutilización de estos, lo que influye de manera representativa en el desempeño tanto interno como externo. Esto conllevo a la generación de ocho agencias, que se distribuyeron a nivel de la ciudad, pero según estas fueron creadas sin un estudio técnico en relación al grado de eficiencia y necesidad de las agencias en función del tamaño y crecimiento de la ciudad.

Todo lo expuesto, permite evidenciar que la EP-EMAPA-A, tiene un deficiente manejo y control de sus activos lo que eleva la generación de riesgos para pérdida y manejo inadecuado de la información, por lo que es urgente generar estrategias que contribuya a la mitigación y manejo de la información de manera segura, que contribuya a una mejor diversificación de sus servicios, y responda de manera óptima a la expansión y crecimiento de la ciudad.

2.2. Metodología de investigación

Enfoque de la investigación

El enfoque de esta investigación es cualitativo porque permite establecer la relación de los activos con las posibles vulnerabilidades, que se encuentren en la empresa, así como también, la identificación de las amenazas que produjeran, con lo que se establece el nivel de riesgo, en el que se encuentren los sistemas de información de la EP-EMAPA-A., específicamente del centro de datos.

El método de investigación es inductivo – deductivo, porque el análisis se realizó desde las particularidades de cada uno de los activos de la empresa, se considera los componentes de confidencialidad, integridad y seguridad, para la correspondiente identificación de los riesgos y amenazas, bajo criterios de impacto, probabilidad y riesgo, para la posterior construcción de un plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013

Tipo de Investigación

La presente investigación tuvo una modalidad de campo y, documental - bibliográfica, la primera porque se realizó en el lugar de los hechos. La segunda porque la fundamentación de la información tanto teórica como de análisis, se lo realizó en fuentes primarias y secundarias como libros, artículos, repositorios de información, entre otros; además, se valida la documentación con la que cuenta la empresa, con la finalidad de evidenciar el cumplimiento en relación con la seguridad de la información

El tipo de investigación, se toma en cuenta el nivel de medición y análisis de la información documental, es descriptiva con corte transversal, porque permitió observar y describir como, se desarrollan y manejan los activos y procesos de la EP-EMAPA-A, su manipulación, custodia, confidencialidad, integridad y seguridad de la misma a una determinada fecha, a fin de establecer un estudio del análisis y gestión de riesgos

de los Sistemas de Gestión de Seguridad de la Información a través de la metodología MAGERIT, a partir de la ISO 27001.

Técnicas e instrumentos de recopilación de información

Las técnicas e instrumentos, que se utilizaron permiten la validación y cumplimiento de los objetivos de la investigación, por lo que, para la construcción del estado del arte, se utilizó el análisis de datos como técnica y el instrumento fue la ficha de registro de datos.

Para documentar la aceptabilidad de riesgo de la empresa, se aplicó la entrevista al jefe de la unidad de Tecnologías de la Información de la empresa (anexo 1), como técnica, con su respectivo instrumento que es la guía de entrevistas y a los responsables del centro de la base de datos, se realiza un grupo focal o *focus group* (anexo 2), con la finalidad de sustentar la importancia de la gestión y seguridad de la información y para la recopilación de toda la documentación existente y que respalde este proceso y en caso de no existir sustentar la necesidad de que sea construida oportunamente y acorde las necesidades del departamento.

Población y muestra

La población de estudio representa al jefe de la unidad de tecnologías y los responsables del centro de la base de datos, al ser una población finita e inferior a 100 personas, se trabajó con la totalidad y, no se determinó muestra:

Tabla 3. Población de estudio

CARGO	NUMERO
Jefe TI	1
Analistas Técnicos	4
Total	5

Fuente: Elaboración propia

Análisis de la información recopilada

A continuación, se muestra el resultado de la entrevista empleada al jefe de Tecnologías de la Información de la EP-EMAPA-A, aplicadas con el formato del anexo 1:

Pregunta 1

Respuesta: Si existen políticas para acceso a servidores e información sensible. Sin embargo, fueron implementados por necesidad sin tener un estudio previo de su alcance y la justificación de las políticas y las políticas que ya están implementadas no tienen un correcto mantenimiento y algunas políticas, ya no se utiliza no se procede con el correcto retiro de la política.

Pregunta 2

Respuesta: Se tiene un conocimiento básico sobre la norma y al momento, no se aplica más que políticas simples y no están basadas a ninguna norma. Las únicas normas, que se basan son la ISO 9001 y 17025.

Pregunta 3

Respuesta: Cuando se presenta un riesgo, se analiza ese instante y se intenta solventar el problema, en si se realizan parches momentáneos ante los problemas.

Pregunta 4

Respuesta: Existe una hoja de Excel simple del ingreso de los usuarios creados

Pregunta 5

Respuesta: Si cada área es la encargada de realizar una solicitud por escrito para la creación y modificación de nuevos usuarios. Dirigida a mi persona y por lo consiguiente yo designo a los encargados realizar el trámite.

Pregunta 6

Respuesta: No tiene caducidad únicamente cuando el usuario, se olvida la contraseña, se le resetea y para este procedimiento enviaría un mensaje donde solicite su habilitación.

Pregunta 7

Respuesta: En el correo institucional, no se bloquea, pero en el sistema documental al tercer intento, se bloquea el usuario. De igual manera para desbloquear, se necesita una solicitud por correo para habilitar la cuenta.

Pregunta 8

Respuesta: Si, el que se crea por defecto, pero se les solicita a los usuarios a cambiar la contraseña para seguridad, sin embargo, no todos cambian y se queda de manera genérica.

Pregunta 9

Respuesta: Si se maneja restricciones de acuerdo a perfiles en los sitios web, pero en general las páginas de ocio como YouTube y Spotify, así como redes sociales están permitidas en las computadoras de los usuarios.

Pregunta 10

Respuesta: No en general**,** solo modifican de manera de usuarios donde registran nueva información o modifican algún dato necesario, pero a la modificación de la base de datos que tienen los servidores, no.

Pregunta 11

Respuesta: Simulacros no existen, pero se tiene un entorno de pruebas y desarrollo. Cuando se cae el sistema, se actúa en ese momento, no se tiene una base o modelo de seguimiento cuando, se va el sistema.

Pregunta 12

Respuesta: Si existe y está declarado en el sistema de gestión de calidad, donde se reporta mensualmente el mismo.

Pregunta 13

Respuesta: Solo con pedido expreso, donde se solicite su modificación y solo está encargada una persona para realizar cambios así.

Pregunta 14

Respuesta: No existe ningún registro, que se verifique los accesos de *backups.*

Pregunta 15

Respuesta: Si existe un plan de mantenimiento anual en el hardware en las computadoras, sin embargo, en software, no se tiene por lo que se tiene varios problemas y complicaciones que genera caídas del sistema.

Pregunta 16

Respuesta: Se encuentra bajo llave y solo la persona encargada tiene acceso a la misma.

Pregunta 17

Respuesta: Si se almacenan en base a un secuencial en las facturas y la base de datos esta con tablas específicas, donde se agrupan de manera lógica para su funcionamiento.

Pregunta 18

Respuesta: La unidad no tiene un inventario privado, pero si la unidad de servicios generales cuenta con los activos.

Pregunta 19

Respuesta: En el inventario que tiene servicios generales, sin embargo, no está actualizada el estado de los activos por lo que el estado de mucho de los equipos no

son los correctos. Muchos de ellos son considerados malos, pero no se darían de baja por la actualización del estado.

Análisis: Se presencia que la empresa cuenta con varias políticas de seguridad que permiten el bloqueo de salida de información, sin embargo, se analiza que existen falencias en mucha de los permisos del internet, se toma en cuenta que las redes de ocio son el principal punto de escape de información y de acceso rápido para los atacantes. Así también, como la poca documentación de todos los registros de *backup* como el acceso de los nuevos usuarios es mínima. Una de las partes que más preocupa es la inexistencia de simulacros, es decir, que actúan en el momento que sucede las cosas más, no se mitiga el problema desde la raíz.

Resultados del *Focus Group*

A continuación, se muestra los resultados del *Focus Group* aplicada a los 4 analistas de Tecnologías de la Información de la EP-EMAPA-A, con el formato del anexo 2 y con la hoja de registro el anexo 3:

1. **¿Se aplican actualmente políticas de seguridad para gestionar la información, por favor en caso de respuesta positiva, enúncielas?**

    - Se tiene implementado sistemas de respaldo de información y de copias de seguridad de los servidores
    - Se tiene instalado software antivirus *Firewall*, Antivirus, *Active Directory* en los computadores y servidores con su motor actualizado en los servidores
    - El acceso físico a los centros de cómputo y/o a todos los centros de cableado está únicamente permitido a personal de TI
    - Las políticas de seguridad al momento son básicas como controlar accesos a sistemas por usuario y contraseña y nivel de privilegios mediante definición de perfiles.

2. **¿Están definidas responsabilidades del personal en cuanto al uso**

adecuado de los recursos?

El área de tecnologías de la información cuenta con personal capacitado y con sus funciones definidas acorde al orgánico funcional de la empresa, se clasifica en grupos quienes, se encargan del hardware, el software y soporte técnico

3. **¿Existe un control sobre el acceso no autorizado de personal, con la finalidad de proteger el equipamiento y sistemas que se manejan en la institución?**

   Sí, el área de tecnologías es considerada como área restringida, el acceso se controla por medio de un seguro electromagnético, y el acceso al cuarto de servidores, que se encuentra dentro la unidad de Tecnologías de la Información, se encuentra cerrada bajo llave, limitado el acceso únicamente a personal autorizado.

4. **¿Se realiza un mantenimiento periódico de los equipos de la institución?**

   Actualmente, se cuenta con un Plan de Mantenimiento anual de los equipos y servidores de la Institución.

5. **¿Se realizan tareas de monitoreo a los sistemas de información que se manejan?**

   Por la falta de personal lamentablemente, no se puode realizar un monitoreo preventivo de los sistemas informáticos, se realizan monitoreos diarios al rendimiento de los servidores y sistemas que son utilizados por la EP-EMAPA-A, en caso de detectarse algún inconveniente, se realizan las correcciones necesarias.

6. **¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?**

Por el momento, no se cuenta con personal especializado para realizar esta tarea.

7. **¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?**

   La empresa dispone de sistemas antivirus, firewall perimetral con políticas y niveles de acceso definidos y con reglas para definir niveles de seguridad. Control de puertos, bloqueo de URL.

8. **¿Dispone de un control sobre el inventario de los activos existentes en toda la institución?**

   La empresa dispone de un control de inventarios, pero como tecnologías de la Información, no se tiene un inventario propio de los bienes tecnológicos. La empresa cuenta con la Unidad de Control de Bienes, la cual, se encarga del inventario de todos los bienes de la empresa El control de inventario de todos los bienes de la empresa es llevado por la unidad de servicios generales, los custodios son los responsables de los bienes asignados a cada uno

Análisis: Se presencia que el poco personal especializado en tema de seguridad de la información, no permite, que se realice un correcto monitoreo de las tareas ejecutadas, por lo que se presencia falencias en el ámbito de implementación, control, monitoreo y mantenimiento de seguridad de la información. Simplemente, se manejan con conocimientos básicos de seguridad y actúan al momento de sufrir algún inconveniente.

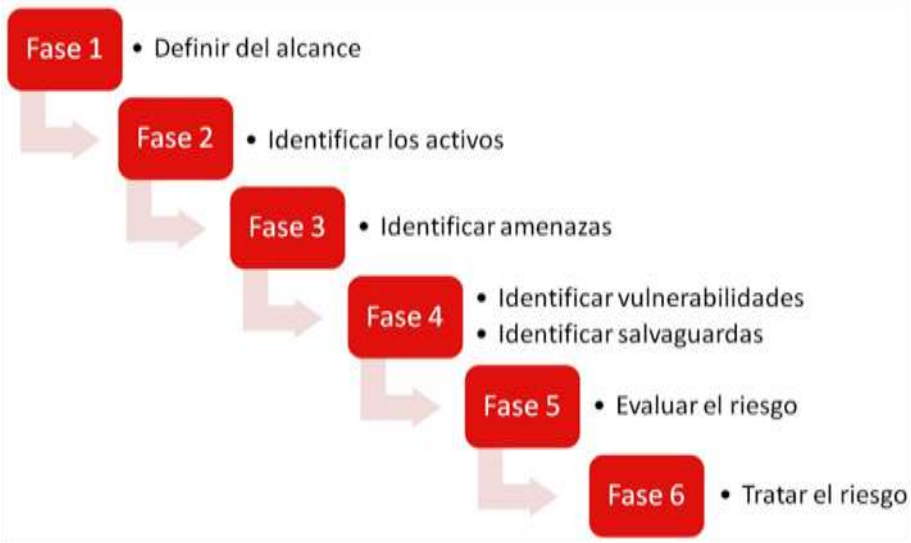
2.3 Metodología de desarrollo

Para el caso del diagnóstico de la situación actual de la empresa, se utilizó la metodología MAGERIT (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2016), esta es una metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, cubre la fase AGR (Análisis y Gestión de Riesgos) y está basada en ISO 27001, se encuentra relacionada sobre todo con la utilización oportuna de los medios electrónicos, informáticos y telemáticos, también, da lugar al análisis de los diferentes riesgos con la finalidad de minimizar medidas de seguridad orientadas a la generación de confianza.

En cuanto a la manipulación y seguridad de la información; para esto la metodología parte de la identificación de activos, la cual, tiene como instrumento una ficha de registro, esta técnica e instrumento son debidamente estructurados, contienen una lista de criterios o desempeños de evaluación previamente establecidos, que se califican mediante una determinada escala, su finalidad es comprobar la presencia y/o ausencia de una serie de características de un determinado tema de estudio, contiene criterios y/o dimensiones, escalas e indicadores (Dirección de Educación media Superior, 2019).

La metodología MAGERIT comprende las siguientes etapas:

Figura 9. Fases de la metodología MARGERIT



Fuente: (Hurtado,2018)

Fase 1: Identificación del alcance

Para el análisis de riesgos la EMAPA estableció como necesidad, la evaluación del Centro de Procesamiento de Datos, puesto que, si bien la empresa es grande y con múltiples áreas, es el centro de datos el que mayor cantidad de activos de información concentra, por lo que es indispensable su análisis.

Cabe indicar que el área establecida para el alcance del presente proyecto es prioritaria en la organización, pues de ella depende el funcionamiento total de la empresa.

Fase 2: Identificación de Activos

La metodología pone a disposición del investigador, algunas herramientas para el análisis y apoyo en las distintas actividades a desarrollar, es así, que está disponible la matriz de identificación de activos, la misma que fue estructurada en base a la

información levantada en el área con el apoyo del personal de tecnología de la empresa.

En la presente matriz, se especifican:

- Los nombres de activos.
- Tipo de activos (hardware o software)
- Proceso que apoya el activo.
- Dependencia a la que pertenece.
- Tipo de información, información pública, información pública clasificada, información pública reservada, no clasificada.
- Si contiene datos personales.
- Tipo de datos personales información, se clasifica en dato personal privado, dato personal público, dato semiprivado y ningún.
- Medios de conservación, se clasifica en sistemas de bases de datos y en ningún lado.
- Y la clasificación de activos de la información que son la disponibilidad, integridad y confidencialidad. Así como, se encuentra en el estado del arte en la ***tabla 1. Clasificación de los activos de información.***

Tabla 4. Identificación de activos del Centro de Datos de la EP-EMAPA-A

n[a].	Nombre del activo	Tipo de activo	Proceso que apoya el activo	Dependencia a la que pertenece	Tipo de información	Tiene datos personales	Tipo de datos personales	Medio de conservación	Disponibilidad	Integridad	Confidencialidad
1	servidor dl 380 g7	hardware	entorno pruebas	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	1	1	3
2	servidor dl 380 g5	hardware	entorno pruebas	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	1	1	3
3	servidor dl 180 g6	hardware	central telefónica	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	4
4	servidor dl 380 g4	hardware	Documental	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	5	4	5
5	servidor dl 380 g8	hardware	gestión de recurso administrativo	unidad de tecnologías de la información	no clasificada	no	n/a	n/a	5	3	4

6	servidor dl 380 g8	hardware	gestión de recurso administrativo	unidad de tecnologías de la información	no clasificada	no	n/a	n/a	5	5	4
7	servidor dl 380 g8	hardware	gestión de recurso administrativo	unidad de tecnologías de la información	no clasificada	no	n/a	n/a	5	5	4
8	servidor hp p 2000	hardware	Documental	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	4	3	5
9	servidor synology d5318xs	hardware	almacenamiento	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	4	5	5
10	Fortinet	hardware	seguridad perimetral	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	5	4	3
11	Fortinet (espejo)	hardware	seguridad perimetral	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	5	4	3

12	switch hp a5500	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	3
13	switch hp a5500	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	3
14	switch de datos	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	3
15	switch de datos	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	3
16	switch de datos	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	3
17	switch de datos	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	3

18	aire acondicionado	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	1	1	1
19	raks 1	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	1	1	1
20	raks 2	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	1	1	1
21	raks 3	hardware	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	1	1	1
22	srv_tomalecturas	software	gestión comercial	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	5	5	5
23	srv_antivirus	software	uso y apropiación de tic	unidad de tecnologías de la información	no clasificada	n/a	n/a	n/a	4	3	4

24	srv_comercial	software	gestión comercial	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	5	4	5
25	srv_facturacion electronica	software	gestión financiera	unidad de tecnologías de la información	publica reservada	si	dato personal publico	sistemas de bases de datos	4	5	5
26	srv_conexcionbancos	software	gestión financiera	unidad de tecnologías de la información	no clasificada	no	n/a	n/a	5	3	3
27	srv_zimbra	software	gestión de recurso administrativo	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	4	5	4
28	srv_erpaplicativo	software	gestión de recurso administrativo	unidad de tecnologías de la información	publica reservada	no	n/a	n/a	4	3	3
29	srv_erpbasededatos	software	gestión de recurso administrativo	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	5	4	4

30	srv_vcenter	software	gestión de recurso administrativo	unidad de tecnologías de la información	no clasificada	no	n/a	n/a	5	5	4
31	srv_sgd	software	gestión de recurso administrativo	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	5	4	4
32	recursos humanos	recursos humanos	gestión de recurso administrativo	unidad de tecnologías de la información	publica reservada	si	dato semiprivado	sistemas de bases de datos	5	3	5

Fuente: Adaptado por el investigador tomado de (ISOTools, 2017)

Análisis: En la tabla 5, se aprecia que la empresa cuenta con 32 activos de información, estos activos son de la Unidad de Tecnologías de la Información (UTI), clasificados en hardware, software y recursos humanos Los procesos a los que apoyan estos activos son el almacenamiento, central telefónica, documental, entorno de pruebas, gestión comercial, gestión de recursos administrativos, gestión financiera y seguridad perimetral. Los activos fueron analizados bajo criterios de: disponibilidad, integridad y confidencialidad; para el primer caso de disponibilidad de los activos, se tiene la siguiente información:

Tabla 5. Disponibilidad de los activos

DISPONIBILIDAD	DESCRIPCIÓN	CANTIDAD ACTIVOS	% ACTIVOS
1. Mínimo	La no disponibilidad de la información afectaría la operación normal de la entidad. No tiene implicaciones legales, económicas o de pérdida de imagen	6	19%
2. Bajo	La no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos	0	0%
3. Medio	La no disponibilidad de la información conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen	0	0%
4. Alto	La falta o no disponibilidad parcial de la información impacta negativamente la prestación de servicios de tecnología y de información	13	41%
5. Crítico	La no disponibilidad de la información conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos	13	41%
Total general		**32**	**100%**

Fuente: Elaboración propia

De los 32 activos que dispone la empresa el 19% de ellos afectan la operación normal de la entidad, pero sin implicaciones legales, económicas o de imagen. Mientras que, el 41% de estos activos el nivel de disponibilidad, se encuentra entre alto y crítico, los primeros impactan de manera negativa la prestación de servicios y de información y los segundos la no existencia de estos produce impactos de índole legal o económica e incluso retrasa las funciones que genera pérdidas de imagen institucional, lo que conlleva a malestar tanto en clientes internos y externos.

Tabla 6. Análisis de la integridad de los activos

INTEGRIDAD	DESCRIPCIÓN	CANTIDAD ACTIVOS	% ACTIVOS
1. Mínimo	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo	6	19%
2. Bajo	La pérdida posible en la exactitud de algún dato o estado completo de la información tener algún impacto negativo en los procesos	0	0%
3. Medio	Información cuya pérdida de exactitud y completitud conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen	13	41%

4. Alto	La pérdida en la exactitud de algún dato impacta negativamente la prestación de servicios de tecnología y de información	6	19%
5. Crítico	Información cuya pérdida de exactitud y completitud conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.	7	22%
Total general		**32**	**100%**

Fuente: Elaboración propia

En relación con la integridad de los activos de la empresa el 19% de estos no posee información significativa, por lo que su nivel de riesgo es mínimo; mientras que, el 41% al perderse conlleva un impacto negativo con repercusiones legales o económicas y retrasa el cumplimiento de las funciones; en el 19% de estos la falta o pérdida impacta en la prestación de servicios de tecnología y de información; finalmente, el 22%, se encuentran en nivel crítico, lo que conlleva a un impacto negativo con pérdida severa de la imagen e impactos legales y económicos.

Tabla 7. Análisis de confidencialidad de los activos

CONFIDENCIALIDAD	DESCRIPCIÓN	CANTIDAD ACTIVOS	% ACTIVOS
1. Mínimo	Es la información que ha sido calificada como de conocimiento público. El conocimiento o divulgación no autorizada de la información no tiene ningún impacto negativo en los procesos	6	19%
2. Bajo	Esta información sería entregada o publicada con ciertas restricciones sin que implique daños ni impactos negativos a terceros ni a las actividades y procesos	0	0%
3. Medio	Es la información que es utilizada por los funcionarios del Ministerio para realizar sus labores en los procesos y que son conocidas por terceros con la autorización del propietario del activo. La divulgación no autorizada de la información impacta negativamente al proceso evaluado y/u otros procesos	10	31%
4. Alto	La divulgación no autorizada de la información impacta negativa y significativamente al proceso evaluado y/u otros procesos	10	31%
5. Crítico	de exactitud y completitud conllevaría un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la	6	19%

	entidad. A esta información sólo tendría acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. La divulgación no autorizada de esta información impacta negativamente		
Total, general		**32**	**100%**

Fuente: Elaboración propia

En correspondencia con la confidencialidad de la información el 19% de estos activos tienen un nivel mínimo, significa que su divulgación no produce impacto a la institución; el 31% el nivel de confidencialidad es medio y alto lo que significa la divulgación no autorizada de la información impacta negativamente al proceso evaluado y/u otros procesos. Finalmente, el 19% presenta un nivel de confidencialidad es crítico lo que refiere que esta información sólo tendría acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. La divulgación no autorizada de esta información impacta negativamente.

Fase 3: Identificación de Amenazas

Se considera que una amenaza representa toda aquella acción que constituye un peligro inminente para la institución, para esta investigación, se consideraron amenazas desde el punto de vista financiero, reputacional, operativo y legal:

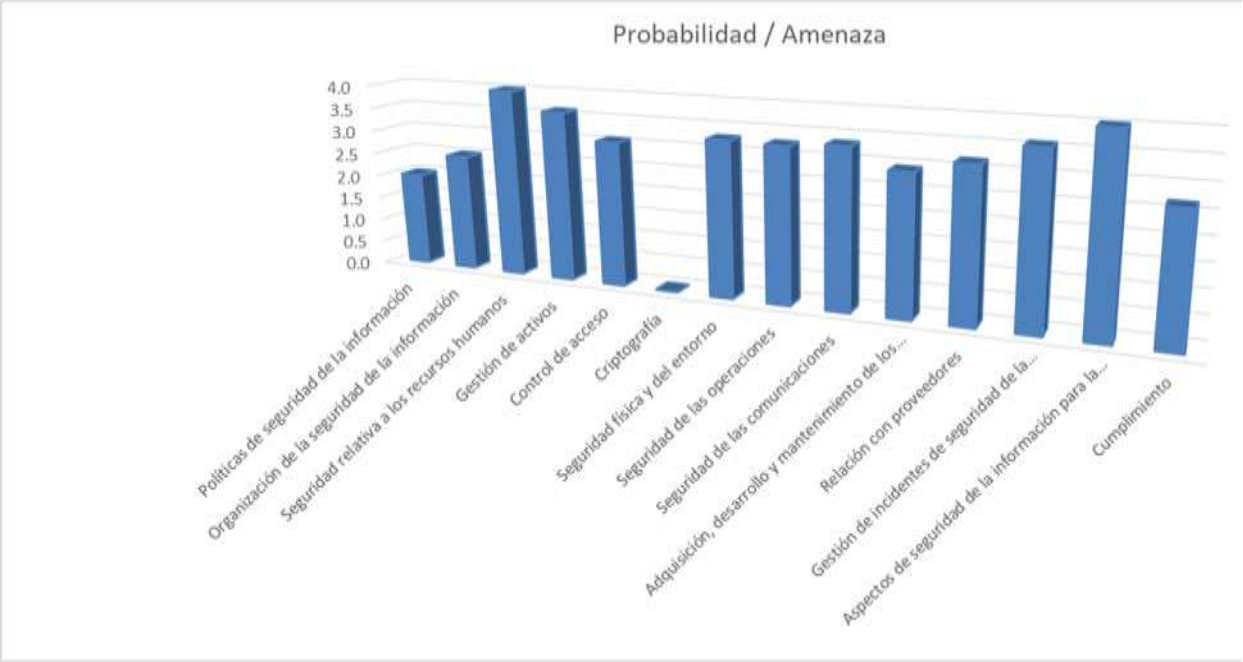
Tabla 8. Análisis de Amenaza

Controles de Seguridad de la Información	**Probabilidad / Amenaza**	**Nivel**
Políticas de seguridad de la información	2.0	Menor
Organización de la seguridad de la información	2.5	Moderado
Seguridad relativa a los recursos humanos	4.0	Alto
Gestión de activos	3.6	Alto
Control de acceso	3.1	Moderado
Criptografía	0.0	Leve
Seguridad física y del entorno	3.3	Moderado
Seguridad de las operaciones	3.3	Moderado
Seguridad de las comunicaciones	3.3	Moderado
Adquisición, desarrollo y mantenimiento de los sistemas de información	2.9	Moderado
Relación con proveedores	3.2	Moderado
Gestión de incidentes de seguridad de la información	3.6	Alto

Aspectos de seguridad de la información para la gestión de la continuidad de negocio	4.0	Alto
Cumplimiento	2.7	Moderado

Fuente: Elaboración propia

Figura 10. Análisis de amenaza



Fuente: Elaboración propia

El nivel de amenaza, que se categoriza como **menor,** en relación con las políticas de seguridad de información, afecta a todo el grupo de trabajo, es decir, a todos los funcionarios, llegaría inclusive a demandas por lo que es necesario cambios en la interacción de los procesos.

El nivel de amenaza, que se categoriza como **moderado,** se refiere a la organización de la información, control de acceso, seguridad física - del entorno, de las operaciones y de las comunicaciones, mantenimiento de los sistemas de información, relación con los proveedores y el cumplimiento.

El nivel de amenaza, que se categoriza como **alto,** se refleja en la seguridad relativa de los recursos humanos, gestión de los activos y de los incidentes de seguridad, así como la gestión de la continuidad de la empresa.

Fase 4: Identificar las vulnerabilidades

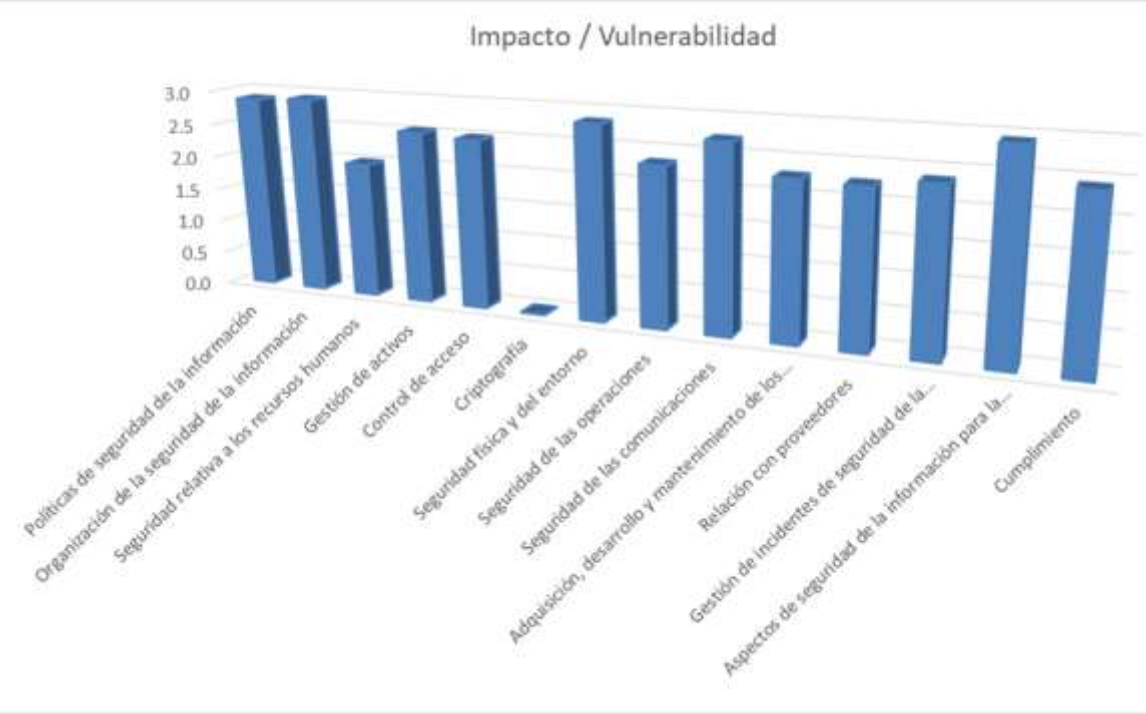
Se considera que una amenaza es la posibilidad de ocurrencia de cualquier tipo o evento que produjera un daño sea este material o inmaterial, para el caso de esta investigación, se determinaron las amenazas en función del criterio de probabilidad de la matriz diagnóstica que determina el estado y aplicabilidad de control de seguridad de la información, como se observa en la tabla 10. Análisis de vulnerabilidad.

Tabla 9. Análisis de vulnerabilidad

Sección	Controles de Seguridad de la Información	Impacto / Vulnerabilidad	Nivel
A5	Políticas de seguridad de la información	2.9	Posible
A6	Organización de la seguridad de la información	2.9	Posible
A7	Seguridad relativa a los recursos humanos	2.0	Improbabilidad
A8	Gestión de activos	2.5	Improbabilidad
A9	Control de acceso	2.5	Improbabilidad
A10	Criptografía	0.0	No se ejecuta
A11	Seguridad física y del entorno	2.8	Posible
A12	Seguridad de las operaciones	2.3	Improbabilidad
A13	Seguridad de las comunicaciones	2.7	Posible
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	2.3	Improbabilidad
A15	Relación con proveedores	2.3	Improbabilidad
A16	Gestión de incidentes de seguridad de la información	2.4	Improbabilidad
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	2.9	Posible
A18	Cumplimiento	2.4	Improbabilidad
Promedio de Vulnerabilidad		**2.4**	**Improbabilidad**

Fuente: Elaboración propia

Figura 11. Análisis de vulnerabilidad



Fuente: Elaboración propia

De acuerdo con los criterios de probabilidad de ocurrencia, se determina que el departamento analizado tiene un nivel de vulnerabilidad de **improbabilidad** (2.4), esto significa que el evento ocurriera en cualquier momento, al menos una vez en los próximos cinco años, los eventos, que se encuentran en este rango son:

Tabla 10. Vulnerabilidad - Improbabilidad

Controles de Seguridad de la Información	**Impacto / Vulnerabilidad**	**Nivel**
Seguridad relativa a los recursos humanos	2.0	Improbabilidad
Gestión de activos	2.5	Improbabilidad
Control de acceso	2.5	Improbabilidad
Seguridad de las operaciones	2.3	Improbabilidad
Adquisición, desarrollo y mantenimiento de los sistemas de información	2.3	Improbabilidad
Relación con proveedores	2.3	Improbabilidad
Gestión de incidentes de seguridad de la información	2.4	Improbabilidad
Cumplimiento	2.4	Improbabilidad

Fuente: Elaboración propia

Mientras que los criterios, que se encuentran en el rango *posible*, es decir, el evento ocurriría en algún momento, al menos de una vez en los próximos 2 años:

Tabla 11. Vulnerabilidad - posible

Controles de Seguridad de la Información	Impacto / Vulnerabilidad	Nivel
Políticas de seguridad de la información	2.9	Posible
Organización de la seguridad de la información	2.9	Posible
Seguridad física y del entorno	2.8	Posible
Seguridad de las comunicaciones	2.7	Posible
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	2.9	Posible

Fuente: Elaboración propia

Sin embargo, el departamento no realiza control de seguridad en relación con la criptografía, es decir, no cuenta con políticas de uso para este tipo de controles, por lo que no hay algún proceso de cifrado para la información almacenada o transferida. Tampoco se realizan procesos de gestión de claves, es decir, no se generan claves diferentes para los sistemas y aplicaciones, o a su vez son débiles; no hay copias de respaldo, ni hay un registro clave de gestión. Esto refleja un nivel de vulnerabilidad significativo para la empresa.

Fase 5: Evaluar el riesgo

Se parte del fundamento teórico el riesgo, se obtiene de la multiplicación entre el impacto y la probabilidad y sus resultados, se determinan sobre 100 puntos, en donde: alto es > 61; medio entre 31-60; y, bajo entre 0 y 30 puntos:

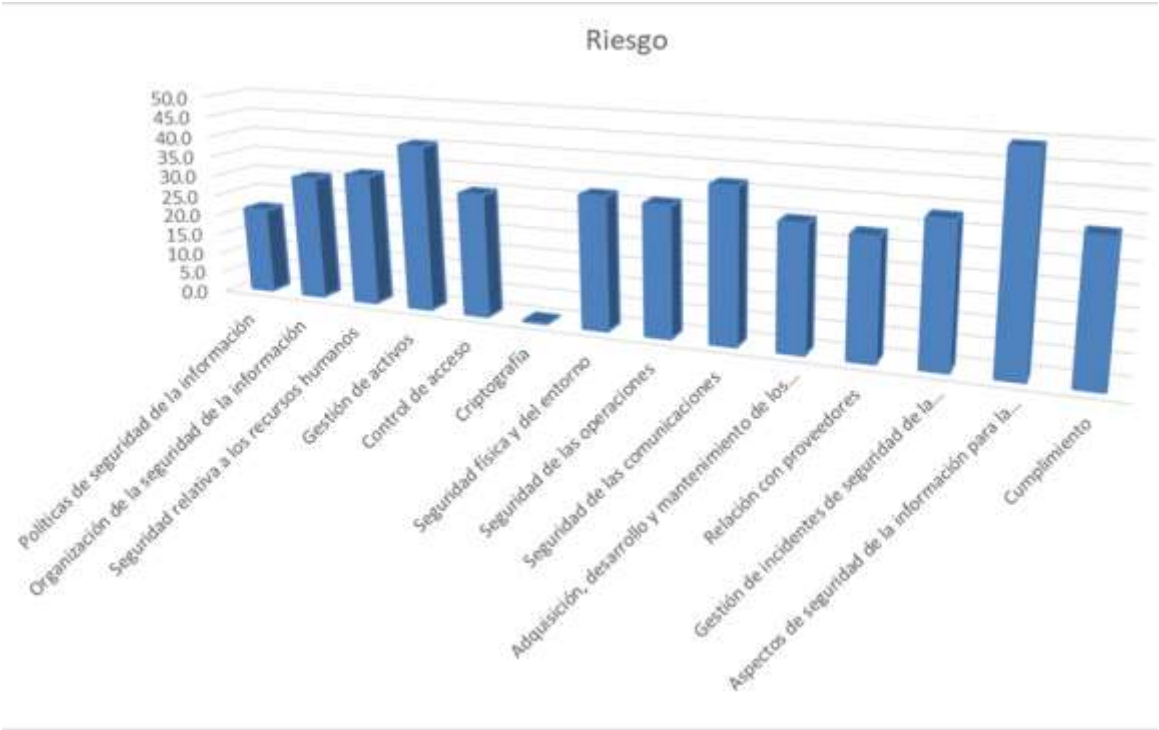
Tabla 12. Evaluación del riesgo

Sección	Controles de Seguridad de la Información	Riesgo	Nivel
A5	Políticas de seguridad de la información	21.0	Bajo
A6	Organización de la seguridad de la información	30.2	Medio
A7	Seguridad relativa a los recursos humanos	32.0	Medio

A8	Gestión de activos	40.3	Medio
A9	Control de acceso	29.8	Medio
A10	Criptografía	0.0	Bajo
A11	Seguridad física y del entorno	31.8	Medio
A12	Seguridad de las operaciones	31.0	Medio
A13	Seguridad de las comunicaciones	36.6	Medio
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	29.6	Medio
A15	Relación con proveedores	28.2	Bajo
A16	Gestión de incidentes de seguridad de la información	33.1	Medio
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	49.0	Medio
A18	Cumplimiento	32.4	Medio
Promedio de Riesgo		**30.5**	

Fuente: Elaboración propia

Figura 12. Evaluación del riesgo



Fuente: Elaboración propia

Como se observa el nivel de riesgo de la empresa en relación con la gestión de la seguridad de la información es de 30.5, lo que se determina como riesgo **medio**. Los controles que más, se encuentran en nivel medio son:

Tabla 13. Riesgo medio

Sección	Controles de Seguridad de la Información	Riesgo	Nivel
A6	Organización de la seguridad de la información	30.2	Medio
A7	Seguridad relativa a los recursos humanos	32.0	Medio
A8	Gestión de activos	40.3	Medio
A9	Control de acceso	29.8	Medio
A11	Seguridad física y del entorno	31.8	Medio
A12	Seguridad de las operaciones	31.0	Medio
A13	Seguridad de las comunicaciones	36.6	Medio
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	29.6	Medio
A16	Gestión de incidentes de seguridad de la información	33.1	Medio
A17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	49.0	Medio
A18	Cumplimiento	32.4	Medio

Fuente: Elaboración propia

Mientras que en riesgo bajo solamente dos controles, que se encuentran en este nivel:

Tabla 14. Riesgo Bajo

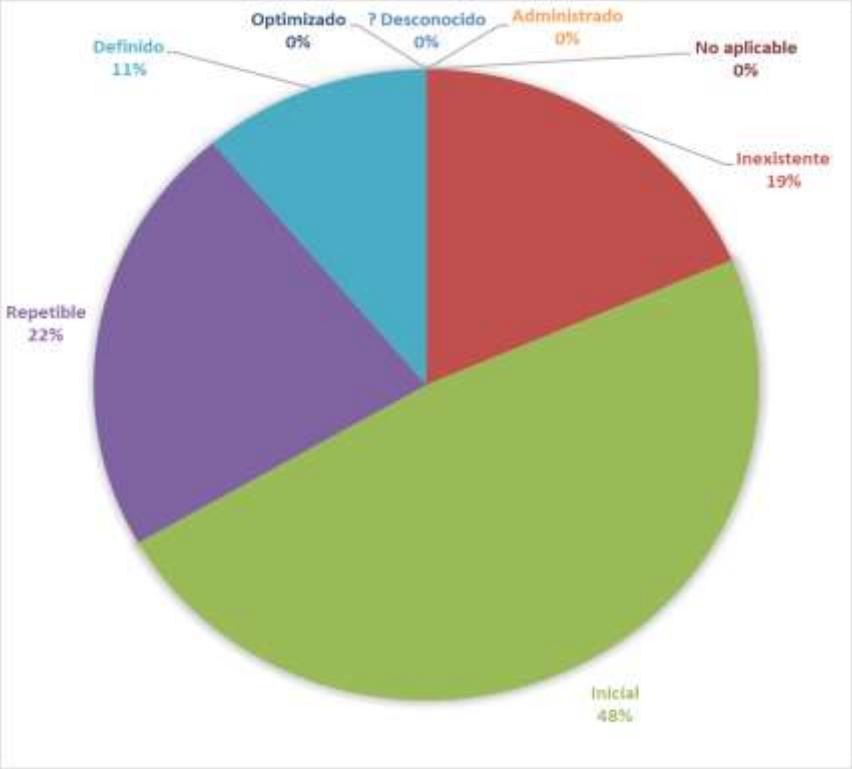
Sección	Controles de Seguridad de la Información	Riesgo	Nivel
A5	Políticas de seguridad de la información	21.0	Bajo
A15	Relación con proveedores	28.2	Bajo

Fuente: Elaboración propia

Fase 6: Tratar el riesgo

Para la fase 6, se realiza el tratamiento de los riesgos identificados, para lo que se considera los resultados obtenidos en la identificación del estado de los diferentes controles de seguridad de información de la empresa, de donde se obtiene:

Figura 13. Estado de los controles de seguridad de la información



Fuente: Elaboración propia

Estos resultados reflejan que el 19% de estos controles, se califican como inexistentes, es decir que, no se lleva a cabo el control de seguridad en los sistemas de información, lo que eleva el nivel de vulnerabilidad y riesgo de la empresa, por lo que es necesario que, a estos, se les identifique tratamiento. El 48%, se encuentran en estado inicial, lo que significa que las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas, su éxito depende de la buena suerte y de tener personal de la alta calidad y también, requieren tratamiento. Sin embargo, hay controles que existen y que de una u otra forma funcionan y hay que establecer tratamiento a los de estado inexistente e inicial.

El 22%, se encuentra en estado repetible, lo que significa que la medida de seguridad, se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación. EL 11%, se

encuentran en estado definido, lo que significa que el control, se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni por el Comité de Dirección. Sin embargo, es claro que ningún control existe ha sido debidamente aprobado y formalizado, por lo que la medición de estos, se dificulta y no se la realiza mediante indicadores.

Para el caso de esta investigación, se da tratamiento a los controles, que se encuentran en estado inexistente e inicial.

Tabla 15. Tratamiento del riesgo

Sección	Controles de Seguridad de la Información	Estado	Tratamiento del riesgo
A5.1.2	Revisión de las políticas para la seguridad de la información	Inexistente	Establecer las políticas de seguridad para el manejo y control de los activos, que serían aprobadas y socializadas
A6.1.4	Contacto con grupos de interés especial	Inexistente	Es necesario una hoja de registro, que se especifique la ejecución de parches y amenazas de cada día, que se realizan en los sistemas.
A7.2.3	Proceso disciplinario	Inexistente	Se difundiría la información sobre las políticas, que se realice para conocimientos de los funcionarios
A8.3.1	Gestión de soportes extraíbles	Inexistente	Crear un registro, que se especifique y actualice los activos, este estaría bajo llave los datos almacenados que estos requieran
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inexistente	Construir la política y los controles para solucionar los problemas en los ataques maliciosos en el correo institucional
A12.1.2	Gestión de cambios	Inexistente	Definir los roles y responsabilidades del personal, así como los procedimientos a seguir para documentar los cambios, que se realizan
A12.7.1	Controles de auditoría de sistemas de información	Inexistente	Realizar periódicamente auditorias en base a la seguridad de la información solo auditorias de la norma ISO 9001. Se pude utilizar el instrumento de evaluación ya definido
A13.2.2	Acuerdos de intercambio de información	Inexistente	Establecer niveles de restricciones al respecto de transferencia de información
A16.1.3	Notificación de puntos débiles de la seguridad	Inexistente	Se les recomienda no ingresar ningún tipo de información en páginas no verificadas, sin embargo, no es una obligación
A16.1.7	Recopilación de evidencias	Inexistente	Realizar seguimientos ante el impacto generado por los diferentes incidentes
A18.1.4	Protección y privacidad de la información de carácter personal	Inexistente	Establecer políticas y controles el manejo, protección y privacidad de la información
A5.1.1	Políticas para la seguridad de la información	Inicial	Crear un documento donde, se especifique las políticas de seguridad (objetivo, alcance,

			importancia) mediante reuniones periódicas. Obtener asesoría sobre la seguridad de información para que todos los usuarios entiendan la importancia de su utilización
A6.1.5	Seguridad de la información en la gestión de proyectos	Inicial	Se necesita una matriz de riego para conocer su criticidad y mitigar los mismos
A7.1.1	Investigación de antecedentes	Inicial	Se realizaría un análisis en el área de Talento Humano, política netamente de esa área
A7.1.2	Términos y condiciones del empleo	Inicial	
A7.2.1	Responsabilidades de gestión	Inicial	Difundir la información sobre las políticas, que se realice para conocimientos de los funcionarios
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Inicial	
A8.2.1	Clasificación de la información	Inicial	Se tendría registros de políticas donde, se clasifique la información, y estas estarían registradas en el sistema de gestión de calidad.
A8.2.2	Etiquetado de la información	Inicial	
A8.2.3	Manipulado de la información	Inicial	
A9.3.1	Uso de la información secreta de autenticación	Inicial	Solo se entrega de manera verbal por lo que incurría a ingeniería social, la cual, pone en riesgo la información
A11.2.5	Retirada de materiales propiedad de la empresa	Inicial	Se extraería información sin ningún control solo queda la ética de no divulgación firmada en el contrato inicial del funcionario.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inicial	Solo se menciona que es recomendable tener limpia la pantalla, sin embargo, no se cumple con certeza. Falta de verificación
A12.1.3	Gestión de capacidades	Inicial	Solo se actua mediante las necesidades, que se presente no hay estudio de capacidad, por lo que, no se tiene un análisis de riesgo
A12.6.1	Gestión de las vulnerabilidades técnicas	Inicial	Las amenazas y los riesgos, se intentan mitigar al momento que sucede, no hay un plan que permita seguir un proceso para solventar los problemas. Crear un plan de mitigación de riesgo
A14.2.5	Principios de ingeniería de sistemas seguros	Inicial	Solo se conoce de ingeniería como conceptos básicos, se necesita actualización de los funcionarios que están a cargo del cuarto de datos

A14.3.1	Protección de los datos de prueba	Inicial	Se tienen software para entorno de prueba, sin embargo, no se realiza ningún registro de esto. Realizar un registro de protección de datos
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inicial	Realiza el seguimiento ante el impacto generado al incidente
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inicial	Se conoce cuales son los principios, sin embargo, muchos de ellos, no se aplican y solo se actúa n el momento del desastre
A18.2.1	Revisión independiente de la seguridad de la información	Inicial	Se tiene una matriz de riesgo obsoleta por lo que no es de garantía para una auditoria y no se registra ningún valor. Actualizar la matriz
A18.2.3	Comprobación del cumplimiento técnico	Inicial	Al no tener bien definidos los riesgos, no se trataría los riesgos

Fuente: Elaboración propia

Los resultados de la investigación demostraron los riesgos potenciales contra los activos de seguridad, la falta de procedimientos de seguridad y la poca importancia de capacitación en temas de ciberseguridad a los servidores que laboran en la organización, por lo que es fundamental desarrollar políticas de seguridad de la información, enfocar sus esfuerzos en el área de la ciberseguridad, precisamente en esta era en la que todas las empresas buscan la innovación tecnológica y por ende el crecimiento de los sistemas de información y servicios a través de internet.

CAPÍTULO III ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Plan de Gestión de Seguridad de la Información

Con base en la metodología desarrollada que implica el análisis por fases desde la definición del alcance, identificación de activos, identificación de amenazas, identificación de salvaguardas, evaluación de riegos y tratamiento de riesgos; el resultado de la investigación se resume en un plan de gestión de seguridad de la información que responde a la estructura planteada por el Gobierno de Colombia (2018), el cual, se describe a continuación:

Plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013

Introducción

En la actualidad el manejo de la gestión y seguridad de la información cobra importancia en todas las empresas, pues de esta manera, se aseguran los medios de almacenamiento, para esto, se establecen políticas y controles necesarios que permita que esta información sea gestionada de manera eficiente con la finalidad de asegurar su integridad, confidencialidad y disponibilidad.

Con base en los resultados obtenidos, se determina como debilidad, la inexistencia de políticas centradas en el manejo de seguridad de la información. El área de tecnologías de información de la empresa cuenta con un instructivo de contingencias, sin embargo, en este no se exponen controles para la seguridad de la información, lo que se enfatiza es el accionar frente a los diferentes desastres, más no existe nada con relación a la seguridad de la información. Por esta razón es fundamental estructurar este plan con la finalidad de establecer parámetros que contribuyan a asegurar la integridad, confidencialidad y disponibilidad de los datos.

La Empresa Municipal de Agua Potable y Alcantarillado de Ambato (EMAPA) fue suscrita el 30 de junio de 1967, y el 3 de junio de 2010, se constituye como Empresa Pública, Empresa de Agua potable y Alcantarillado de Ambato (EP-EMAPA-A).

Objetivos

Objetivo General

Presentar el Plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013 para el centro de datos.

Objetivo Específicos

- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

Alcance

El Plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013 para el centro de datos, se realiza con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para la EP-EMAPA-A.

Marco Legal

El Plan de plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013 para el centro de datos, se ampara bajo el siguiente marco legal:

Tabla 16. Marco legal ISO/IEC 27001:2013

Norma	Descripción
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

Fuente: Elaboración propia

Misión de EP-EMAPA-A

Desarrollar, mantener y operar la infraestructura instalada para la dotación de servicios básicos de agua potable y alcantarillado de manera eficiente para contribuir a la salud y bienestar de la ciudadanía ambateña, garantizando el mantenimiento y conservación de las fuentes de agua, apoyando en el cuidado ambiental de la zona de influencia, implementando tecnología adecuada y altos estándares de calidad

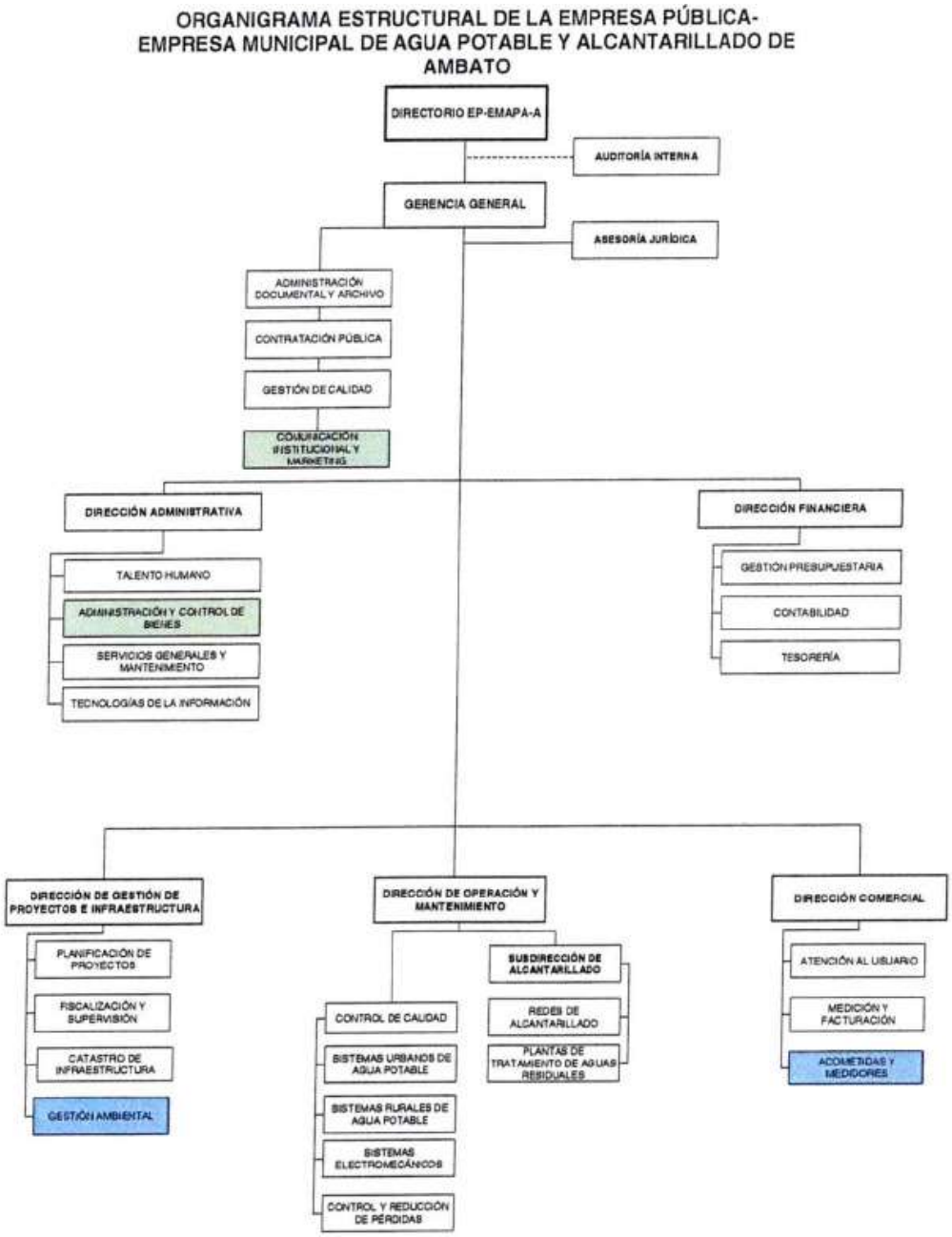
Visión de EP-EMAPA-A

Ser reconocida en el año 2022, como una empresa eficiente, rentable e innovadora en la dotación de servicios de agua potable y alcantarillado, con responsabilidad social y ambiental en el desarrollo de obras y proyectos de agua potable y alcantarillado

Política de calidad de EP-EMAPA-A

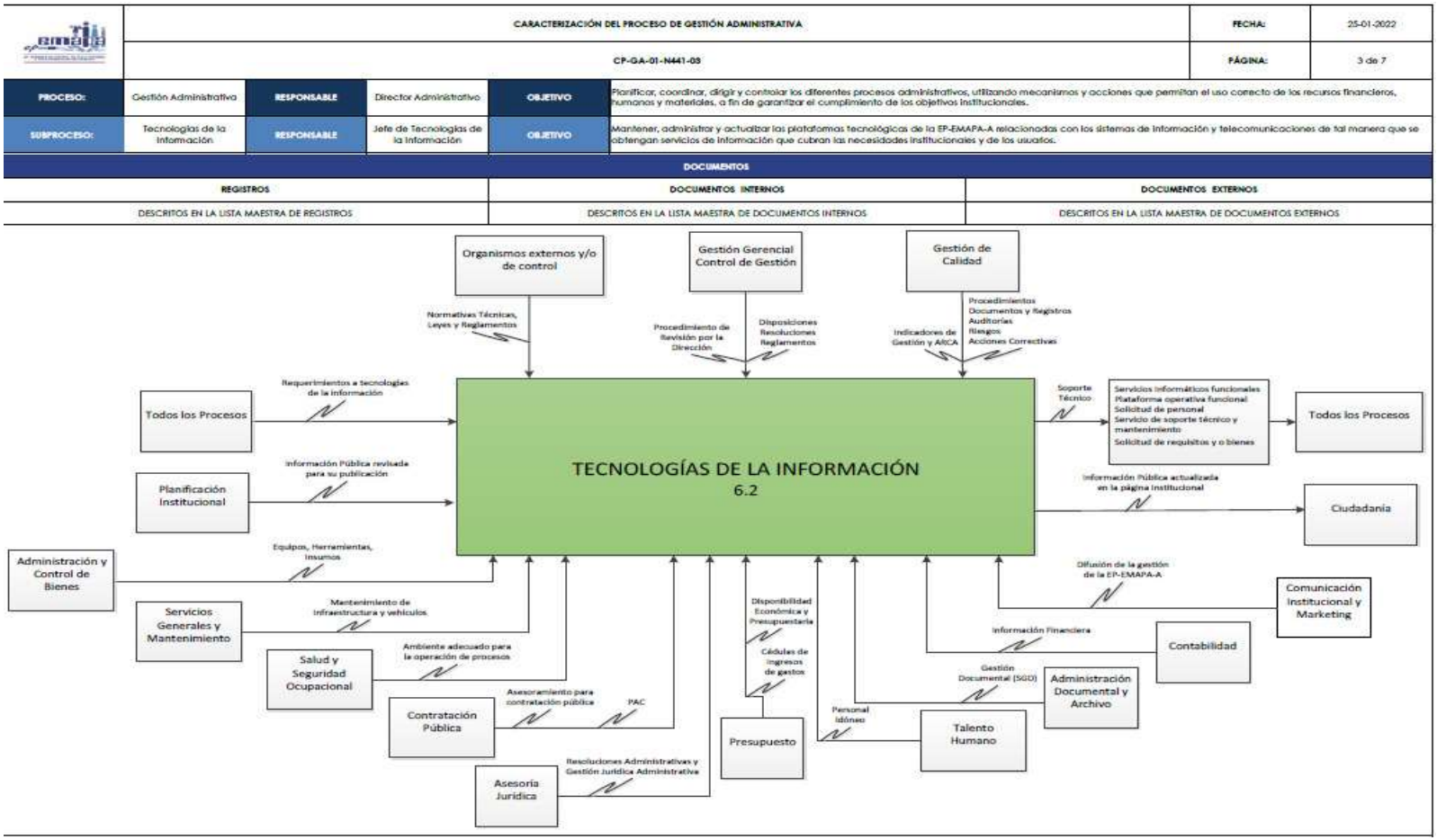
La EP-EMAPA-A suministra servicios de agua potable y alcantarillado cumpliendo normas técnicas y registro legales aplicables, mejorando continuamente sus procesos para satisfacer a sus usuarios

Figura 14. Estructura Orgánica de EP-EMAPA-A



Fuente: EP-EMAPA-A (2022)

Figura 15. Estructura Orgánica del departamento de Tecnología de Información



Fuente: EP-EMAPA-A (2022)

Arquitectura de las políticas del sistema de seguridad de la información

Es evidente de acuerdo con la literatura revisada, que, no existe una arquitectura estándar para la definición de políticas de seguridad, sin embargo, es importante contar con una buena estructuración de las mismas, apoyada en dimensiones de seguridad de la información, Fintes (2017), plantea la siguiente estructura, que es adoptada en esta propuesta:

Figura 16. Arquitectura de las políticas del sistema de seguridad de la información

Fuente: Fintes (2017)

En base a este esquema, se desarrolla las funciones y controles del sistema de seguridad de información, planteado, como propuesta. Toda esta información sería divulgada y actualizada de manera permanente, en correspondencia con las necesidades de la institución y las exigencias de control de información internas y externas.

Funciones del Departamento de Tecnologías de Información de EP-EMAPA-A

Art. 19.- UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN. - Su objetivo es crear, mantener, administrar y actualizar las plataformas tecnológicas de la EP-EMAPA-A relacionadas con los sistemas de información y telecomunicaciones de

tal manera, que se obtengan servicios de información que cubran las necesidades institucionales y de los usuarios.

Relación de Dependencia. - Depende de la Dirección Administrativa.

Unidades Dependientes: Ninguna.

Atribuciones y/o Funciones de Tecnologías de la Información: Son atribuciones y/o funciones de la Unidad las siguientes:

1. Coordinar la generación, disponibilidad y uso apropiado de la información con las direcciones, unidades y áreas de la Institución;
2. Elaborar e implementar un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos de la empresa;
3. Proponer las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y la infraestructura tecnológica necesaria;
4. Definir, documentar y difundir las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y telecomunicaciones;
5. Incorporar controles y sistemas de aseguramiento de la información;
6. Gestionar convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con tecnología de información;
7. Definir el modelo de información de la Institución a fin de, que se facilite la creación y uso de la misma;
8. Definir, implantar y actualizar las adquisiciones de infraestructura tecnológica y software de la Institución;

9. Regular y ejecutar los mecanismos, procedimientos y planes que garanticen el mantenimiento y uso adecuado la infraestructura tecnológica y telecomunicaciones de la institución;
10. Establecer mecanismos que protejan y salvaguarden la información y operación, que se procesa mediante Sistemas informáticos de acuerdo a la Normativa vigente;
11. Implementar un plan de contingencias para el área;
12. Elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web de la entidad, a base de disposiciones legales, normativas y los requerimientos de los usuarios internos y externos;
13. Proponer el plan Operativo Anual de Unidad;
14. Gestionar y garantizar la vigencia de los permisos de operación para telecomunicaciones;

Identificación de Activos de EP-EMAPA-A

La EP-EMAPA-cuenta con activos, que se identificaron de manera oportuna en el diagnóstico de esta investigación y se encuentran en la tabla 5 de este trabajo.

Controles de seguridad de información

Este plan de seguridad de información se orienta al aseguramiento de la confidencialidad, integridad y disponibilidad de la información, por lo que se establecen políticas, normas, y controles de los siguientes dominios de la empresa:

- Organización de la Información
- Seguridad de personal
- Seguridad de comunicaciones y operaciones
- Control de accesos
- Mantenimiento de sistemas de información
- Gestión de continuidad de la empresa
- Organización de la información

Para la organización de la información, es importante que los responsables del proceso respondan las siguientes interrogantes: ¿Qué, hay que proteger?, ¿Contra qué o quién?, y, ¿Cuál es la importancia de cada recurso?, ¿Cuál es el grado de protección?, ¿Requisitos de protección?, ¿Expectativas de los directivos, clientes y usuarios?, y, ¿qué se espera de la seguridad de la información?

Lo elementos, que se tomarían en cuenta en los resultados del análisis de los riesgos, en correspondencia con los objetivos de EP-EMAPA, las vulnerabilidades y amenazas de los activos, así como la probabilidad de ocurrencia de estas. Otro componente importante es la normativa vigente y los requisitos de EP-EMAPA, para el soporte de sus operaciones. En base a lo expuesto, se plantea los objetivos, políticas y controles necesarios para este control:

Cuadro 3. Organización de la información

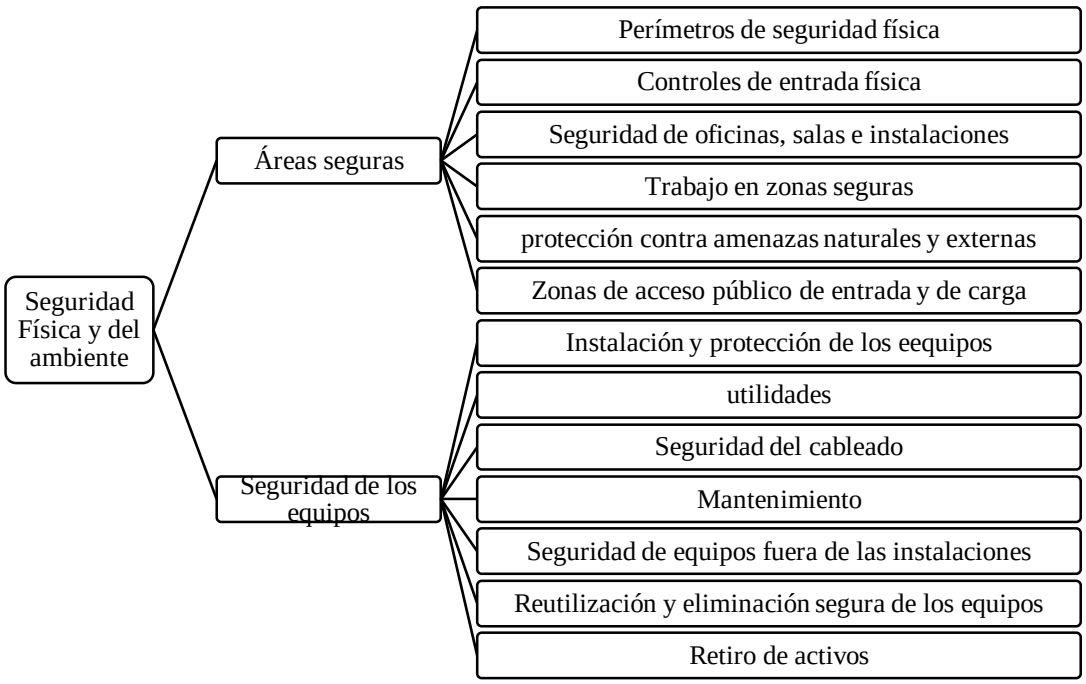
Organización de la Información
Descripción. Este dominio es el encargado de proponer los controles de seguridad de información y que permita la reducción de riesgo de eventos perjudiciales para la empresa Es la comisión que esta constituida por: Gerente General, jefe de Talento Humano, el Oficial de Seguridad y el jefe de TI
Objetivo. Gestionar la seguridad de la información dentro de la empresa
Política. Velar por el cumplimiento de los controles de seguridad de la información
Controles. • Promover la seguridad de información dentro de la empresa. • Establecer las políticas de seguridad de información de la organización • Recibir los requerimientos de la Comisión de Seguridad de Información, evaluarlos y determinar su aprobación y asignación de recursos de ser el caso. • Elevar los requerimientos para el cumplimiento y mejora del SGSI • Coordinar las revisiones a las normas de seguridad de información implementadas. • Comunicar cualquier brecha, incidencia o evento de seguridad de información de manera oportuna

Fuente: Elaboración propia

- **Seguridad de la información**

La seguridad de información es un componente fundamental, se considera el tratamiento de la seguridad física y del ambiente, para esto se consideran dos áreas la segura y la de seguridad de los equipos, en donde, se cumpliría una serie de actividades, que se enlistan en el siguiente esquema:

Figura 17. Seguridad Física y del Ambiente



Fuente: Elaboración propia

En base al esquema propuesto, que establece las necesidades de seguridad de acceso físico a las instalaciones, así como de su perímetro, áreas y usuarios internos y externos, se plantean los siguientes objetivos, políticas y controles para la seguridad del personal, y, la seguridad de comunicación y operaciones

Cuadro 4. Seguridad personal

Seguridad personal
Descripción. El proceso de selección de personal y de proveedores permite reducir el riesgo de su contratación que dañaría a la empresa

Objetivo. Reducir los riesgos que serían generados por error humano o por el uso inadecuado de los activos de información
Política. Velar por el cumplimiento de los controles de seguridad de la información En relación con la Base de datos, se inserta una alerta dentro del sistema, lo que permite identificar los clientes, que se encuentran registrados en la lista negra internacional
Controles. • Inclusión de la seguridad en las responsabilidades y funciones laborales • Selección y política de personal • Hacer acuerdos de Confidencialidad. • Realizar acciones concientización, educación y entrenamiento en seguridad de la información • Implementar un proceso disciplinario en caso de incumplimiento • El ingreso a áreas de acceso interno, limitado y restringido es explícitamente autorizado y con algún elemento físico visible de identificación, que distinga la condición de personal, proveedor o visitan • Todas las visitas al personal de la Oficina Administrativa son registradas por el agente de seguridad de turno. • Las visitas programadas son anunciadas al agente de seguridad de turno para que sean rápidamente identificadas. • El ingreso a áreas de acceso limitado y restringido cuenta con algún elemento de identificación adicional. • Las oficinas quedan cerradas cuando no hay personas en su interior. • Existen medios e información de respaldo ubicados a una distancia conveniente, en ubicaciones diferentes de los equipos principales. • Se cuenta con extintores convencionales en oficinas administrativas y con extintores de en el Data Center.

Fuente: Elaboración propia

Cuadro 5. Seguridad de comunicacion y operaciones

Seguridad de comunicación y operaciones
Descripción. Responsable de establecer los procedimientos debidamente documentados para realizar las actividades relacionadas con el procesamiento e intercambio de la información y de todos los recursos de comunicaciones. Las seguridades de las bases de datos (BD) tratan y protegen los datos de la base de datos, el sistema de gestión de BD, cualquier aplicación asociada, el servidor de BD físico y/o el servidor de BD, y, la infraestructura informática y/o red utilizada para acceder a la BD
Objetivo. Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación
Política. Se cuenta con mecanismos de protección, detección y eliminación de código malicioso e intrusos en la red interna, así como de recuperación y respaldo automático de la información y procesos críticos. Se planifica la capacidad de los sistemas de información y monitorear el uso de los mismos por parte del personal y de proveedores, para evitar problemas de procesamiento de información, se considera ambientes de desarrollo, prueba y producción separados La seguridad física de la BD, tomaría en cuenta si el servidor es local o se encuentra en un centro de datos *cloud*, para en función de esto ubicarlo dentro de un entorno seguro y con control de climatización
Controles. • Se elabora y se mantiene los procedimientos y las guías de usuarios finales, de configuración, de sistemas de información y recursos de comunicación.

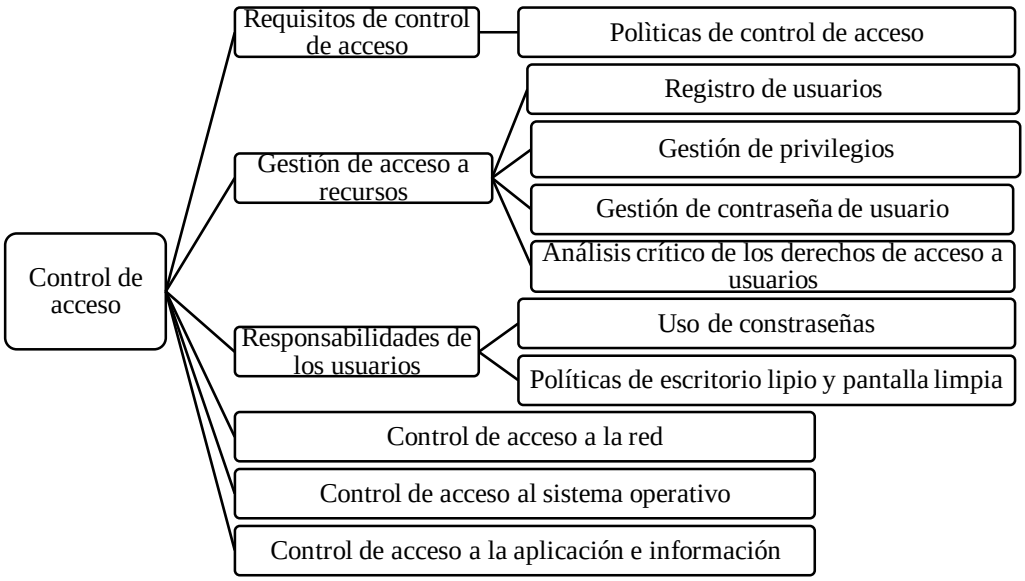
• Se cuenta con los procedimientos documentados de los procesos de contingencia y respaldo por cada sistema o proceso de información crítico. • Se tiene identificado a los responsables de la operatividad de cada sistema de información, así como a los contactos de emergencia respectivos. • La aceptación de nuevos sistemas de información considera parámetros de seguridad de información tales como: rendimiento y capacidad de los equipos informáticos; procedimientos de recuperación ante errores y reinicio; procedimientos de pruebas; procedimiento de Contingencia y Respaldo; usabilidad y capacitación a usuarios; documentación y manuales; y, otras medidas de seguridad de información adoptadas. • No descarga o instalar software no autorizado en los equipos. • En caso un usuario detecte código malicioso en un equipo, informar inmediatamente a la Jefatura de sistemas para que ejecuten el procedimiento respectivo. • Se cuenta con las herramientas necesarias y actualizadas que permitan la detección y eliminación de código malicioso de manera automática. • Se cuenta con procedimientos que permitan la recuperación ante una contingencia causada por código malicioso.

Fuente: Elaboración propia

- **Control de accesos**

En relación al control de accesos es necesario tomar en cuenta los controles de acceso lógico, en correspondencia con los privilegios de acceso, contraseñas, acceso a la res, entre otros, para lo cual, se considera algunas categorías de seguridad, como los requisitos del negocio, control de usuarios, responsabilidades de usuarios, control de acceso a la red, a los sistemas operativos y el acceso a la información. En función de lo expuesto, se establecen las necesidades y las acciones a realizar:

Figura 18. Control de acceso



Fuente: Elaboración propia

En base a las acciones propuestas, se plantean los objetivos, políticas y controles necesarios para esta área:

Cuadro 6. Control de accesos

Control de accesos
Descripción. Son los responsables de identificar a un usuario y/o grupo de usuarios, con un usuario y contraseña, con los que tienen acceso a los sistemas de información autorizados, de acuerdo al perfil asignado.
Objetivo. Gestionar y administrar el acceso lógico a los equipos informáticos, así como a la información y aplicaciones, según autorizaciones preestablecidas.
Política. Generar acceso a los sistemas y/o información de acuerdo a: tipo de información, funciones del usuario, perfiles de acceso. Establecer una normativa para la generación de accesos lógicos. Proponer un proceso de gestión de acceso a usuarios, que incluya la administración de privilegios, contraseña de usuarios. En el caso de contraseñas temporales estas, se envia a los usuarios de manera segura y se cambian inmediatamente por los mismos una vez recibidas y verificadas. Los controles de acceso administrativo y de red, tendría un número mínimo y práctico de usuarios debidamente autorizados a la BD y tener limitado los niveles de acceso. El cifrado de los datos, incluiría los datos de la BD y los datos credenciales, poseería un cifrado seguro mientras estos, se encuentren en reposo y en tránsito. Toda clave de cifrado, se manejaría en función de directrices de mejores prácticas.
Controles. • El identificador es único para cada usuario. • Las contraseñas serían seguras, que no sean fácilmente deducibles. • Activar el bloqueo de pantalla cuando el equipo, se encuentre desatendido temporalmente.

- Al terminar la jornada de trabajo, se cancelan las sesiones de usuario dentro de las aplicaciones, además, de que se activa el bloqueo de pantalla.
- La sesión de administrador del servidor se cierra al concluir la jornada de trabajo.
- Se implementa mecanismos de identificación de un usuario, que se conecta remotamente a la red de la organización, así como la identificación del punto de conexión remota.
- Se implementa dominios o grupos de red necesarios para controlar los accesos lógicos a la red y flujos de información, se toma en cuenta el impacto en el rendimiento de la red.
- Los sistemas de información, según su criticidad y uso, desconectar automáticamente las sesiones de conexión tras un periodo definido de inactividad que sea configurable por cada sistema.

Fuente: Elaboración propia

- **Mantenimiento de sistemas de información**

En relación con el mantenimiento de los sistemas de información, en esta sección, se orienta al desarrollo de la seguridad de la información en las aplicaciones de EP-EMAPA, en base a los requisitos de seguridad de los sistemas de información, así como el procesamiento correcto de las aplicaciones, los controles criptográficos, la seguridad de los archivos y de los procesos de desarrollo y soporte, enmarcados en principios de gestión de vulnerabilidad técnica:

Figura 19. Control de acceso

Fuente: Elaboración propia

En base al esquema planteado en el control de mantenimiento de sistemas de información, se plantean los siguientes objetivos, políticas y controles:

Cuadro 7. Mantenimiento de sistemas de información

Mantenimiento de sistemas de información
Descripción. Establecer niveles de servicio, así como el alineamiento a las normativas de Desarrollo y Mantenimiento de Sistemas respectivas.
Objetivo. Garantizar un adecuado nivel de seguridad de información a todos los sistemas y aplicaciones, desde su desarrollo y durante todo su ciclo de vida
Política. Validar los datos de entrada. Establecer procedimientos y/o mecanismos de comprobación para detectar cualquier tipo de corrupción de información por consecuencia de errores del proceso o por actos deliberados. Las auditorías de base de datos, se realizarían con regularidad. Registrar todos los inicios de sesión en el servidor de BD y el sistema operativo, así como también, todas las operaciones, que se realicen con datos confidenciales en la BD. Las contraseñas, los códigos o números de identificación de las BD y de las terminales de acceso remoto, encontrarse debidamente encriptados.
• **Controles.** Implementación de restricciones que minimicen el riesgo de fallas en los sistemas de información. • Generación de un reporte de todos los cambios, que se generen en los sistemas. • Establecimiento de un registro de copias y uso de la información. • Los cambios, que se realicen no comprometerían los controles de seguridad de información, que se hayan implementado. • Los cambios serían previamente planificados, sin que afecte la operatividad del sistema. • Establecimiento de la asignación de recursos necesarios para mantenimientos, revisiones, pruebas y cambios en el sistema operativo.

Fuente: Elaboración propia

- **Gestión de continuidad de la empresa**

La gestión de continuidad, se relaciona con la gestión de incidentes de seguridad de la información, las responsabilidades y el proceso de recolección de la evidencia, y este se caracteriza en dos categorías fundamentales la de reporte de eventos y debilidades y la gestión de incidentes y mejoras; así como, los aspectos de seguridad de la información:

Figura 20. Gestión de continuidad

Fuente: Elaboración propia

En base al esquema planteado en la gestión de continuidad, se plantean los siguientes objetivos, políticas y controles:

Cuadro 8. Gestión de continuidad de la empresa

Gestión de continuidad de la empresa
Descripción. Son los responsables de implementar la gestión de continuidad del negocio con la finalidad de reducir a niveles aceptables las interrupciones que serían generadas por desastres o fallas de procesos críticos.
Objetivo. Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos de los efectos de fallas significativas o desastres.
Política. Implementar un plan de continuidad que responde a los resultados de la evaluación de riesgos y a los eventos identificados. Implementar planes de mantenimiento y recuperación de operaciones, que garanticen la disponibilidad de la información.
Controles. • El plan de continuidad contendría: identificación de vulnerabilidades, riesgos e impacto, donde, se prioriza los procesos críticos de negocio; identificación de activos implicados en los procesos críticos del negocio; asignación de recursos financieros, humanos, técnicos y ambientales; adquisición de seguros adecuados; asignación de responsabilidades; mantenimiento del plan. • Para la continuidad y evaluación de riegos, se considera lo siguiente: eventos que causarían interrupciones a los procesos de negocio, su probabilidad e impacto para la organización y para la seguridad de información. El plan de continuidad de negocio es implementado de acuerdo con los resultados de la evaluación de riesgos y a los eventos identificados.

Fuente: Elaboración propia

2.3. Validación del Plan

Para el cumplimiento del último objetivo, se validó el plan y gestión de seguridad de la información para la EP-EMAPA-A., a través del criterio de expertos, bajo el Método Delphi, en donde, primero se seleccionó a los expertos, se les envía el plan a ser valorado, se analizan las respuestas y se identifican las áreas en las que están de acuerdo o en las que difieren. Para realizar la valoración del nivel de experiencia de los expertos, para lo que se autoevalúa los niveles de información y argumentación que tienen sobre el tema, pero primero, se levanta un perfil breve de este:

Cuadro 9. Valoración de la experiencia de los expertos

Valoración de la Experiencia de los Expertos	
Nombre del Experto	
Título de tercer nivel	
Título de cuarto nivel	
Lugar de Trabajo	
Cargo que desempeña	
Años de experiencia profesional	

Fuente: Elaboración propia

Tabla 17. Coeficiente de conocimiento de información

Coeficiente de Conocimiento o Información (Kc)										
Nivel de Conocimiento sobre el tema de estudio										
Expertos	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Fuente: Elaboración propia

Con esta información, se calcula el Coeficiente de Conocimiento o Información (Kc), con la fórmula:

$$\mathbf{Kc= n\ (0,1)}$$

Kc: Coeficiente de Conocimiento o Información

n: Rango seleccionado por el experto

Posteriormente, se determina el nivel de argumentación de los expertos, bajo la siguiente tabla patrón:

Tabla 18. Coeficiente de argumentación

Coeficiente de Argumentación (Ka)			
Dimensiones	**Alto**	**Medio**	**Bajo**
Análisis teóricos realizados por usted	0.3	0.2	0.1
Su experiencia obtenida	0.5	0.4	0.2
Trabajos de autores nacionales	0.05	0.05	0.05
Trabajos de autores extranjeros	0.05	0.05	0.05
Su conocimiento del estado del problema en el extranjero	0.05	0.05	0.05
Su intuición	0.05	0.05	0.05

Fuente: Elaboración propia

Posteriormente, se calcula el Ka bajo la siguiente fórmula:

$$\mathbf{Ka = a\ ni = (n1 + n2 + n3 + n4 + n5 + n6)}$$

Ka: Coeficiente de Argumentación

ni: Valor correspondiente a la fuente de argumentación i (1 hasta 6)

Una vez identificados los dos Coeficientes, se procede a la obtención del Coeficiente de Competencia (K):

$$\mathbf{K = 0{,}5\ (Kc + Ka)}$$

K: Coeficiente de Competencia

Kc: Coeficiente de Conocimiento

Ka: Coeficiente de Argumentación

Posteriormente obtenido los resultados, se valoran de la manera siguiente:

$0{,}8 < K < 1{,}0$ Coeficiente de Competencia Alto

$0{,}5 < K < 0{,}8$ Coeficiente de Competencia Medio

$K < 0{,}5$ Coeficiente de Competencia Bajo

Una vez calificado y seleccionado a los expertos, se procede a la valoración de la respectiva propuesta por parte de los expertos (anexo 4).

3.2. Análisis de los resultados de la validación

Con base en la explicación anterior, se obtuvieron los siguientes resultados:

Tabla 19. Valoración de la experiencia de los expertos

Valoración de la Experiencia de los Expertos					
	E1 - Mauricio Rodrigo Cando Segovia	**E2 - Galo Xavier Robayo Laz**	**E3 - Xavier Francisco lópez Andrade**	**E4 - Daniel Alejandro Ipiales Paredes**	**E5 - Eddy Alejandro Torres Constante**
Título de tercer nivel	Ingeniero en Sistemas	Ingeniero en Sistemas	Ingeniero en Sistemas de computación	Ingeniero en Sistemas	Ingeniero en Ciencias de la Computación - Magna Cum Laude
Título de cuarto nivel	Maestría en Ciberseguridad	Maestría en Sistemas de Información Gerencial	Maestría en gerencia Informática con mención en redes y desarrollo de Software	Maestría en Gerencia Informática	
Lugar de Trabajo	Instituto Nacional de Estadística y Censos	Gobierno Provincial de Tungurahua	Municipalidad de Ambato	EP-EMAPA-A	CAPMATION INC.
Cargo que desempeña	Analista de Tecnologías de la Información	Jefe de Tecnologías de la Información	Jefe de Tecnologías de la Información	Jefe de Tecnologías de la Información (encargado)	Ingeniero de Software en desarrollo web.
Años de experiencia profesional	11 años	12 años	28 años	23 años	3 años
Grado de conocimiento /10 (X)	8	8	9	9	**5**
Kc = X(0.1)	0.8	0.8	0.9	0.9	**0.6**

Fuente: Elaboración propia

Tabla 20. Coeficiente de argumentación de los expertos

Coeficiente de Argumentación (Ka)								
Dimensiones	**Alto**	**Medio**	**Bajo**	**E1**	**E2**	**E3**	**E4**	**E5**
Análisis teóricos realizados por usted	0.3	0.2	0.1	0.2	1.3	0.3	0.3	0.1
Su experiencia obtenida	0.5	0.4	0.2	0.2	0.3	0.4	0.3	0.1
Trabajos de autores nacionales	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
Trabajos de autores extranjeros	0.05	0.05	0.05	0.03	0.01	0.03	0.03	0.03
Su conocimiento del estado del problema en el extranjero	0.05	0.05	0.05	0.01	0.03	0.01	0.03	0.01
Su intuición	0.05	0.05	0.05	0.05	0.03	0.04	0.05	0.04
Ka				**0.54**	**1.72**	**0.83**	**0.76**	**0.33**
K = 0.5 (Kc + Ka)				**0.72**	**2.14**	**1.36**	**1.22**	**0.56**
Interpretación				**Medio**	**Alto**	**Alto**	**Alto**	**Bajo**

Fuente: Elaboración propia

En correspondencia, con los resultados, se trabaja para esta investigación con los expertos 1,2,3,4, y no se trabaja con el experto 5.

Tabla 21. Calificación de criterios por expertos

Criterios	E1 - Mauricio Rodrigo Cando Segovia	E2 - Galo Xavier Robayo Laz	E3 - Xavier Francisco López Andrade	E4 - Daniel Alejandro Ipiales Paredes
Claridad				
La propuesta esta formulada con el lenguaje apropiado y comprensible	4	3	5	5
Objetividad				
La propuesta permite medir los hechos observables	4	3	4	5
Actualidad				
Adecuado al avance de la ciencia y tecnología	5	4	5	5
Organización				
Presentación ordenada	4	3	4	4
Suficiencia				
Comprende los aspectos en cantidad y claridad	4	3	5	4
Pertinencia				
Permite conseguir datos de acuerdo a los objetivos	4	3	5	5
Consistencia				
Permite conseguir datos basados en los modelos teóricos	4	4	5	5
Coherencia				
Hay coherencia entre todos los elementos de la propuesta	4	3	5	5
Metodología				
La propuesta responde al propósito de la investigación	4	3	5	5
Aplicación				
La propuesta responde a las necesidades de la empresa y se orienta a la solución del problema	4	3	5	5
PROMEDIO	4.1	3.2	4.8	4.8

Fuente: Elaboración propia

En correspondencia, con los resultados obtenido la propuesta, se valora 4.2/5, por lo que se válida y sería aplicada

CONCLUSIONES

- La elaboración del estado del arte sobre gestión de riesgos en infraestructuras tecnológicas, que se realizó a partir de la investigación en diferentes repositorios de alto impacto sobre los Sistemas de Gestión de Seguridad de la Información y su impacto en las empresas que son hoy por hoy un elemento esencial para el funcionamiento de la infraestructura tecnológica; así también, se investigó la norma ISO/IEC 27001:2013 Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información, que permiten analizar los controles de una institución para alcanzar los requisitos que sugiere la norma.

- El diagnóstico de la situación actual de la empresa mediante la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones (MAGERIT), en base a los resultados obtenidos al aplicar la metodología MAGERIT, se determinó, que se cuenta con 32 activos, los mismo que son debidamente identificados y categorizados en función de disponibilidad, integridad y confidencialidad, para el primer caso el 41% son considerados como críticos, para el segundo caso el 22% son críticos y finalmente, el 19% de los activos son valorados como críticos.

- Dentro de las principales amenazas, que se identifican y que representan un nivel alto de amenazas, se enfoca en la seguridad relativa a los RRHH, así como, la organización de la seguridad de información, la gestión de incidentes de seguridad de información, y los relacionado con los aspectos de seguridad de la información para la adecuada gestión de continuidad del negocio.

- Las vulnerabilidades identificadas que generan un alto impacto a la empresa, se tienen en la gestión y control de los activos, así como, la seguridad de operaciones, y la gestión de incidente de seguridad de la información. Sin embargo, el departamento no realiza control de seguridad en relación con la

criptografía, es decir, no cuenta con políticas de uso para este tipo de controles, por lo que no hay cifrado para la información almacenada o transferida.

- La sustentación de la aceptabilidad de los riesgos, que se presentan en el manejo de seguridad de la información de la empresa, se tiene en la revisión de políticas para la seguridad de la información, la falta de procesos disciplinarios, la gestión de soportes extraíbles y de cambios, la falta de controles de auditoría de sistemas de información, la notificación de los puntos débiles de seguridad y la debida recopilación de evidencias.

- Para la validación del plan de gestión de seguridad preventivo de la información para la EP-EMAPA-A. por criterio de expertos, se identificaron 4 expertos con un coeficiente de argumentación alto, estos validan la propuesta en relación de claridad, objetividad, actualidad, organización, suficiencia, pertinencia, consistencia, coherencia, metodología y aplicación, se considera como debilidad con un promedio de 3.75 la organización del plan; sin embargo, la valoración promedio total es de 4.2/5, lo que se valida como alto, esto significa que la propuesta es factible.

RECOMENDACIONES

- Al ser el tema de gestión de riesgo de la información es algo relevante para las empresas, es importante generar una cultura de manejo y control de la información, con la finalidad mitigar la incidencia de riegos que afecten de manera significativa a la empresa.

- Generar políticas de manejo de activos que contribuya a tener claramente identificados los mismos, así como registros del manejo, riegos e incidentes generados, sobre todo del centro de base de datos.

- Realizar seguimiento a la aplicación del plan de gestión de seguridad de la información preventivo para la EP-EMAPA-A. a través de auditoría internas de la información, cuyos resultados permiten procesos de retroalimentación que contribuye al planteamiento de acciones correctivas.

BIBLIOGRAFÍA

Abril, L. (2021). *Ecuador está entre los países con más ciberataques en América Latina.* Quito: El Comercio. Obtenido de https://www.eco m/te nden cias/tecnologia/ecuador-ciberataques-america-latina-hacker.html

Agesic. (2016). *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento*. Colombia. Obtenido de https://www.agesic.gub.uy/

Alarcón, P., Barriga, R., Picón, C., & Alarcón, J. (2016). *La importancia de la seguridad informática en las instituciones gubernamentales* (Ecuador. Revista Caribeña de Ciencias Sociales, 141-212. Obtenido de http s:// ww w.e umed.net/rev/caribe/2016/11/seguridad.html

Alvarado, C. (12 de julio de 2019). *Sistema de gestión de seguridad de la información: qué es y sus etapas.* Recuperado el 10 de marzo de 2022, de https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la info rm acion-que-es-etapas

Araya, S., & Orero , A. (2016). *Los sistemas de información y su intyeracción con la dimensión culturakl de las organizaciones*. *Revista Ingeniería Industrial, 3*(1), 74-88. Obtenido de http://rev istas.ubi obio.cl/in dex.php/ RI/article /view/13 9/3363

Arlenys, C. (2017). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basada en la norma ISO/IEC 27001:2013. Tesis*. Colombia: Institución universitaria politécnico Grancolombiano. Obtenido de https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Fi nal.pdf?sequence=1&isAllowed=y

Ceballos, M., Cervantes, A., & Fierros, S. (12 de julio de 2017). *Ciclo de vida de un sistema de información*. Recuperado el 11 de marzo de 2022, de https://www.gestiopolis.com/ciclo-de-vida-de-un-sistema-de-informacion/

CEPAL. (12 de mayo de 2018). *¿Qué es la Gestión de Datos de Investigación?* Recuperado el 14 de marzo de 2022, de https://biblioguias.cepal.org/gestion-de-datos-de-investigacion/definicion

Chiavenato, i. (2006). *Introducción a la Teoría General de la Administración* (Séptima Edición ed.). MAdrid: McGraw-Hill Interamericana.

Colegio oficial de ingenieros de telecomunicaciones. (2018). *Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001.* España: Grupo de nue vas actividades profesionales. Obtenido de https://w ww. coit.e s/sites /default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seg uridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Coutin, A. (2016). *Arquitectura de información para sitios web. Guía práctica para usuarios.* Madrid: Editorialñ Anaya Multimedia.

Cuervo, j., Gómez, L., & Giraldo, H. (2016). *Actualidad y perspectivas de los sistemas de información contable en las empresas de servicios públicos domiciliarios. Revista UDEA, 38*(2), 210-221. Obtenido de http s://r evis tas. udea.edu.co/index.php/cont/article/view/25578

Deloitte. (2016). *El delito informático, otra inquietud de las empresas.* Ecuador: Revista lideres. Obtenido de https://www.revistalideres.ec/lideres/delito-tecnologia-internet-empresas-fraude.html

Enterprise. (14 de marzo de 2017). *Sistema de gestión de Seguridad de Información.* Recuperado el 10 de marzo de 2022, de https:// .cl/conoces-lo-que-es-un-sistema-de-gestion-de-seguir dad-d e-la-informacion/

ESAN. (13 de mayo de 2016). *La norma ISO 27001 y la mejora continua en la gestión de seguridad de la información.* Recuperado el 1 de marzo de 2022, de https://www.esan.edu.pe/conexion-esan/norma-iso-27001-mejora-continua-en-la-gestion-de-seguridad-informacion

Gobierno de España. (20 de julio de 2017). *ISO/IRC 27001: PDCA.* Recuperado el 2 de marzo de 2022, de http: //des carg as.p ntic. me c.e s/m ent or/v isita s/d em oSeguridadInformatica/isoirc_27001_pdca.html

Gómez, A. (2018). *Seguridad en equipos informáticos*. España: ProQuest Ebook Central.

Hurtado Cruz, M. L. (2018). *Gestión de riesgo, metodologías Octave y Ma ger it (B a c helor's thesis*, Universidad Piloto de Colombia).

Inteco. (2014). *Implantación de un SGSI en la empresa.* España: Instituto Nacional de Tecnologías de la Comunicación. Obtenido de https ://ww w.in cibe es/e xtfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISOTools. (14 de julio de 2017). *Sistemas de Gestión de Riesgos y Seguridad.* Recuperado el 20 de marzo de 2022, de https: //www .isoto ols.or g/normas/riesgos-y-seguridad/iso-27001/

Kosutic, D. (14 de enero de 2017). *Una introducción simple a los aspectos básicos.* Recuperado el 20 de marzo de 2022, de https:// adviser a.com/ 27001ª cademy/es/que-es-iso-27001/

Kusumah, P., Sutikno, S., & Rosmansyah, Y. (2014). *Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL* (case study: INTRAC). *International Conference on ICT For Smart iety (ICISS*, (págs. 1-6). Indonesia. doi:DOI: 10.1109/ICTSS.2014.7013193

López, P. (2016). *Seguridad Informática.* España: Editex.

Mantilla, A. (2018). *Gestión de seguridad de la información con la norma ISO 27001:2013*. *Revista espacios, 7*(3), 74-88. Obtenido de https://w ww.revist aespacio s.com/a18v39n18/18391805.html

Matheron, J. (1990). *Merise metosología de desarrollo de sistemas. Teoría aplicada.* Madrid: Editorial Parainfo.

Ministerio de Minas y Energía. (2020). *Plan de seguridad y privacidad de la información .* Colombia: Minenergía . Obtenido de https:// www.m inenerg ia.gov.co/documents/10192/24170291/Plan+de+Seguridad+y+Privacidad+d e+la+Informaci%C3%B3n+2020.pdf

Ministerio de telecomunicaciones y de la sociedad de la información. (2020). *Guía para la implementación del esquema gubernamental del seguridad de la información.* Quito: Subsecretaría de Estado-Gobierno Electrónico. Obtenido dehttps://www.gobiernoelectronico.gob.ec/wpcontent/uploads/2020/04/GU%C3%8DA-PARA-LA-IMPLEMENTACI%C3%93N-DEL-EGSI-ABRIL2020.pdf

Morán, N. (2021). E*stado de la ciberseguridad en las empresas del sector público del ecuador: una revisión sistemática. Tesis*. Guayaquil: Universidad Politécnica Salesiana. Obtenido de https:// dspace .ups.ed u.ec/bi tstream /123456789/20243/1/UPSGT003204.pdf

Muñoz, C. (2017). *Sistemas de información: principios y aplicaciones.* La Habana: Editorial Felix varela.

Normas ISO. (14 de agosto de 2018). *ISO 27001 gestión de la seguridad de la información.* Recuperado el 21 de marzo de 2022, de https://www.normas-iso.com/iso-27001/

O´Brien, J., & Marakas, G. (2006). *Sistemas de información gerencial* (Séptima Edición ed.). Bolivia: Editorial MsGrae-Hill. Obtenido de http: //cot ana. infor matica.edu.bo/downloads/ld-Sistema s%20de %20Info rmac ion %20 Gere ncial -J%20Obrien.pdf

Pérez, D. (2017). *Contribución de las tecnologías de la información a la generación de valor en las organizaciones: Un modelo de análisis y valorización desde la gestión del conocimiento, la productividad y la excelencia en la gestión. Tesis doctoral*. Cantabria: Universidad de Cantabria. Obtenido de https ://www.tdx.cat/bitstream/handle/10803/10587/2de8.DPG_capt2.pdf?sequen ce=3

Sánchez, J. (2016). *Análisis y Gestión de Riesgos en los Sistemas de Información.* España: Departamento de Publicaciones, EUI-UPM.

Sarabia, J. (2017). *Sistemas de información y nuervas tecnologías: influencias de las nuevas tecnologíasd en la estructura organizativa de la empresa Narabra*. *tesis doctoral*. España: Universidad de Canrabria. Obtenido de https ://www.tesisenred.net/bitstream/handle/10803/10586/3de7.MEGR_capt3.pdf?sequence=4&isAllowed=y

Segovia, A. (2016). *Plan de implementación del SGSI basado en la norma ISO 27001:2013.* España: Universitat Oberta de Catalunya. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53466/9/pmayaaTFM0616presentaci%C3%B3n.pdf

Setiawan, A., Syamsudin, A., & Sastrosubroto, A. (2017). *Information security governance on national cyber physical systems.* International Conference on Information Technology Systems and Innovation *(ICITSI)* (págs. 1-6). Indonesia: IEEE. doi:DOI: 10.1109/ICITSI.2016.7858210

Tersek, I. (25 de agosto de 2018). *Sistema de Gestión de la Seguridad de la Información (SGSI).* Recuperado el 10 de marzo de 2022, de http:/ /sifor ense.blogspot.com/2016/05/sistema-de-gestion-de-la-seguridad-de.html

Vizcaya, A. (2013). *Información: procesamiento de contenido.* Argentina: Ediciones Paradigms.

ANEXOS

Anexo 1. Entrevista

Entrevista aplicada al jefe de Tecnologías de la Información

Pontificia Universidad Católica del Ecuador | Sede Ambato

Modelo de entrevista para obtener información sobre la aceptabilidad de riesgos de la empresa

Objetivo	Sustentar la aceptabilidad de riesgos de la empresa EP-EMAPA
Investigador	Priscilla Lizbeth Aguilar Molina Estudiante de la Escuela de Ingeniería de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ambato

Consideraciones Generales

1. Se le solicita muy amablemente responder de forma abierta pero objetiva
2. La información aquí recolectada tiene fines investigativos

Desarrollo

1. ¿Existen políticas de seguridad de la información?

_____

2. ¿Tiene conocimientos acerca de la norma 27001?

_____

3. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?

_____

4. ¿Existe algún registro de los usuarios creados?

_____

5. ¿Se debe solicitar permisos para la creación de usuarios?

_____

6. ¿Las claves creadas tienen caducidad?

_____

7. ¿Se bloquea el usuario al digitar mal la contraseña?

_____

8. ¿Las contraseñas de los sistemas para los usuarios son genéricos?

_____

9. ¿Está permitido el acceso a páginas web diferentes a las páginas institucionales de la empresa?

10. ¿Los usuarios tienen acceso a la configuración (modificar, eliminar, crear) en la base de datos?
11. ¿Existen simulacros en el caso de caída del sistema?
12. ¿Existe un registro del personal que hace respaldos?
13. ¿El administrador puede realizar cambios en la base de datos?
14. ¿Existe registro de control para el acceso de los Backus?
15. ¿Hay mantenimientos periódicamente en los equipos de la empresa?
16. ¿Existe control sobre el acceso físico de las copias de seguridad?
17. ¿Existe un orden lógico para el almacenamiento de los datos?
18. ¿Existe un inventario de los recursos informáticos de la empresa?
19. ¿Existe un inventario de los activos fijos para conocer de su existencia y su estado?

Gracias por su colaboración

Anexo 2. *Focus Group*

Focus Group aplicada a los responsables del centro de la base de datos, es decir, el cuarto frío

Modelo de *Focus Group* para obtener información sobre la aceptabilidad de riesgos de la empresa

Objetivo	Sustentar la aceptabilidad de riesgos de la empresa EP-EMAPA
Investigador	Priscilla Lizbeth Aguilar Molina Estudiante de la Escuela de Ingeniería de Sistemas de la Pontificia Universidad Católica del EcuadorSede Ambato

Consideraciones Generales

1. Se le solicita muy amablemente responder de forma abierta pero objetiva
2. La información aquí recolectada tiene fines investigativos

Desarrollo

1. ¿Se aplican actualmente políticas de seguridad para gestionar la información, por favor en caso de respuesta positiva, enúncielas?
   _____
2. ¿Están definidas responsabilidades del personal en cuanto al uso adecuado de los recursos?
   _____
3. ¿Existe un control sobre el acceso no autorizado de personal, con la finalidad de proteger el equipamiento y sistemas, que se manejan en la institución?
   _____
4. ¿Se realiza un mantenimiento periódico de los equipos de la institución?
   _____
5. ¿Se realizan tareas de monitoreo a los sistemas de información, que se manejan?
   _____
6. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?
   _____
7. ¿Qué mecanismo, técnicas y/o herramientas de seguridad, se aplican en los sistemas de información y de comunicación?
   _____
8. ¿Dispone de un control sobre el inventario de los activos existentes en toda la institución?
   _____

Gracias por su colaboración

Anexo 3. Hoja de asistencia al *Focus Group*

Hoja de Asistencia a ***Focus Group***

Pontificia Universidad Católica del Ecuador | Sede Ambato

Hoja de Asistencia: Reunion de *Focus Group* **para obtener información sobre la aceptabilidad de riesgos de la empresa. Realizada el 12 de abril de 2022**

Nombre	Cargo	Firma
Ricardo Rivera	Analista Técnico de TI de la EP-EMAPA-A	
Darwin Narváez	Analista Técnico de TI de la EP-EMAPA-A	
Jonathan Zapata	Analista Técnico de TI de la EP-EMAPA-A	
Daniel Ipiales	Analista Técnico de TI de la EP-EMAPA-A	

Anexo 4. Ficha de valoración de la propuesta por expertos

Ficha de valoración de la propuesta por Expertos

Objetivo	Validar el Plan de Gestión de seguridad de la Información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013
Investigador	Priscilla Lizbeth Aguilar Molina Estudiante de la Escuela de Ingeniería de Sistemas de la Pontificia Universidad Católica del Ecuador Sede Ambato

Consideraciones Generales

1. Se le solicita muy amablemente responder de forma más sincera.
2. La información aquí recolectada tiene fines investigativos

Criterios	**Muy malo (1)**	**Malo (2)**	**Regular (3)**	**Bueno (4)**	**Muy bueno (5)**
Claridad La propuesta esta formulada con el lenguaje apropiado y comprensible					
Objetividad La propuesta permite medir los hechos observables					
Actualidad Adecuado al avance de la ciencia y tecnología					
Organización Presentación ordenada					
Suficiencia Comprende los aspectos en cantidad y claridad					
Pertinencia Permite conseguir datos de acuerdo con los objetivos					
Consistencia Permite conseguir datos basados en los modelos teóricos					
Coherencia Hay coherencia entre todos los elementos de la propuesta					
Metodología La propuesta responde al propósito de la investigación					

Aplicación La propuesta responde a las necesidades de la empresa y se orienta a la solución del problema					