UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE CONTABILIDAD Y AUDITORÍA

CARRERA DE CONTABILIDAD Y AUDITORÍA

Análisis de Caso, previo a la obtención del Título de Licenciada en Contabilidad y Auditoría C.P.A.

Tema:

"La seguridad de la información en la EP-EMAPA-A"

Autora: Mayorga Melo, Gabriela Elizabeth

Tutora: Dra. Toscano Morales, Cecilia Catalina

Ambato – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Dra. Cecilia Catalina Toscano Morales con cédula de identidad No. 180262479-9, en mi calidad de Tutora del análisis de caso sobre el tema: **"LA SEGURIDAD DE LA INFORMACIÓN EN LA EP-EMAPA-A"**, desarrollado por Gabriela Elizabeth Mayorga Melo, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, septiembre 2022

TUTORA

.....

Dra. Cecilia Catalina Toscano Morales

C.I. 180262479-9

DECLARACIÓN DE AUTORÍA

Yo, Gabriela Elizabeth Mayorga Melo con cédula de identidad No. 180415221-1, tengo a bien indicar que los criterios emitidos en el análisis de caso, bajo el tema: **"LA SEGURIDAD DE LA INFORMACIÓN EN LA EP-EMAPA-A"**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este análisis de caso.

Ambato, septiembre 2022

AUTORA

.....

Gabriela Elizabeth Mayorga Melo

C.I. 180415221-1

CESIÓN DE DERECHOS

Autorizo a la Universidad Técnica de Ambato, para que haga de este análisis de caso, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi análisis de caso, con fines de difusión pública; además apruebo la reproducción de este análisis de caso, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autora.

Ambato, septiembre 2022

AUTORA

.....

Gabriela Elizabeth Mayorga Melo

C.I. 180415221-1

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el análisis de caso, sobre el tema**: "LA SEGURIDAD DE LA INFORMACIÓN EN LA EP-EMAPA-A"**, elaborado por Gabriela Elizabeth Mayorga Melo, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, septiembre 2022

Dra. Mg. Tatiana Valle
PRESIDENTE

Dr. Edisson Coba
MIEMBRO CALIFICADOR

Dra. Myrian Manjarrés
MIEMBRO CALIFICADOR

DEDICATORIA

Quiero dedicar este trabajo primero a Dios por darme salud y vida para continuar en mi camino y darme la fuerza para no rendirme en los momentos más difíciles.

A mis padres Juan Mayorga y Celia Melo, por siempre darme su apoyo y amor incondicional.

A mi hermano Juan porque siempre desea lo mejor para mí.

Pero en especial le dedico este logro a mi esposo David Peñaloza porque es un ejemplo de superación, humildad y sacrificio y a pesar de las dificultades siempre creyó en mí y nunca me soltó la mano en el camino para lograr mi sueño y me brindó todo su apoyo.

A mis hijos Belén y Jorge porque son mi inspiración para ser una mejor persona cada día y por darme el amor y la comprensión en mis momentos de ausencia por cumplir con mis responsabilidades académicas.

A toda mi familia por siempre darme una voz de aliento.

Gabriela Elizabeth Mayorga Melo

AGRADECIMIENTO

Agradezco a la Universidad Técnica de Ambato por abrirme sus puertas y permitirme preparar como profesional.

A los docentes de la Facultad de Contabilidad y Auditoría que fueron parte de mi formación tanto personal como profesional y por siempre tener un consejo sincero.

A la Empresa Pública-Empresa Municipal de Agua Potable y Alcantarillado de Ambato por la apertura para poder realizar el presente trabajo.

A la Dra. Cecilia Toscano por dedicarme su tiempo y brindarme su apoyo para terminar con éxito este análisis de caso.

Gabriela Elizabeth Mayorga Melo

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: "LA SEGURIDAD DE LA INFORMACIÓN EN LA EP-EMAPA-A"

AUTORA: Gabriela Elizabeth Mayorga Melo
TUTORA: Dra. Cecilia Catalina Toscano Morales
FECHA: Septiembre 2022

RESUMEN EJECUTIVO

El presente análisis de caso acerca de la seguridad de la información en la EP-EMAPA-A consistió en medir la madurez del sistema de seguridad de la información para conocer la situación actual de la empresa para prevenir riesgos y salvaguardar la información que posee la entidad. Para lo cual fue necesario aplicar una entrevista, check list y cuestionarios que fueron muy importantes para poder realizar el modelo de madurez. De tal manera, se obtuvo resultados que permitieron identificar las vulnerabilidades en los procesos de seguridad de la información en la empresa. Además, se detectó que el personal no tenía conocimiento sobre las medidas que deberían tomar en caso de que exista algún tipo de ataque malicioso en el ordenador. En conclusión, la EP-EMAPA-A cumple moderadamente con los procesos de seguridad de la información establecidos en la matriz realizada. De este modo es importante tomar en cuenta los riesgos que presenta la empresa para dar posibles soluciones de acuerdo a las recomendaciones proporcionadas.

PALABRAS DESCRIPTORAS: SEGURIDAD, INFORMACIÓN, PROCESO, MADUREZ, EMPRESA.

TECHNICAL UNIVERSITY OF AMBATO
FACULTY OF ACCOUNTING AND AUDITING
ACCOUNTING AND AUDITING CAREER

TOPIC: "INFORMATION SECURITY IN THE EP-EMAPA-A".

AUTHOR: Gabriela Elizabeth Mayorga Melo
TUTOR: Dra. Cecilia Catalina Toscano Morales
DATE: September 2022

ABSTRACT

The present case analysis about information security in the EP-EMAPA-A consisted of measuring the maturity of the information security system to know the current situation of the company to prevent risks and safeguard the information that the entity possesses. For which it was necessary to apply an interview, check list and questionnaires that were very important to be able to carry out the maturity model. In this way, results were obtained that allowed the identification of vulnerabilities in the company's information security processes. In addition, it was detected that the staff was not aware of the measures they should take in the event of some type of malicious attack on the computer. In conclusion, the EP-EMAPA-A moderately complies with the information security processes established in the matrix carried out. In this way, it is important to take into account the risks that the company presents to give possible solutions according to the recommendations provided.

KEYWORDS: SECURITY, INFORMATION, PROCESS, MATURITY, COMPANY.

ÍNDICE GENERAL

CONTENIDO **PÁGINA**

PÁGINAS PRELIMINARES

PORTADA ……..i

APROBACIÓN DEL TUTOR..... ii

DECLARACIÓN DE AUTORÍA..... iii

CESIÓN DE DERECHOS..... iv

APROBACIÓN DEL TRIBUNAL DE GRADO v

DEDICATORIA vi

AGRADECIMIENTO..... vii

RESUMEN EJECUTIVO viii

ABSTRACT..... ix

ÍNDICE GENERAL..... x

ÍNDICE DE TABLAS xiv

ÍNDICE DE GRÁFICOS xv

CAPÍTULO I 1

1 FORMULACIÓN DEL ANÁLISIS DE CASO 1

1.1 Tema..... 1

1.2 Antecedentes 1

1.2.1 Inseguridad de la información tecnológica 3

1.2.2 Gestión de seguridad de la información en empresas del Ecuador 5

1.2.3 Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos 7

1.2.4 El desarrollo de la EP-EMAPA-A y la aplicación de sistemas de seguridad de la información 10

1.3 Justificación..... 11

1.4 Objetivos 12

1.4.1 Objetivo general 12
1.4.2 Objetivos específicos 12
1.5 Preguntas de reflexión 12
CAPÍTULO II 13
2 FUNDAMENTACIÓN CIENTÍFICA TÉCNICA 13
2.1 Teoría de la información 13
2.2 Seguridad de la información 13
2.2.1 Norma ISO/IEC 27001 16
2.2.2 Norma ISO/IEC 27002 18
2.3 Sistema de gestión de seguridad de la información 20
2.4 Modelo de madurez 21
CAPÍTULO III 23
3 METODOLOGÍA 23
3.1 Metodología e instrumentos de recolección de información 23
3.1.1 Unidad de análisis 23
3.1.2 Fuentes y técnicas de recolección de información 24
3.1.2.1 Fuentes de información primarias 24
3.2 Método de análisis de información 30
CAPÍTULO IV 35
4 DESARROLLO DEL ANÁLISIS DE CASO 35
4.1 Análisis y categorización de la información 35
4.2 Narración del caso 43
4.3 Limitaciones del estudio 48
CAPÍTULO V 49
5 CONCLUSIONES Y RECOMENDACIONES 49
5.1 Conclusiones 49
5.2 Recomendaciones 51

REFERENCIAS BIBLIOGRÁFICAS 52

ANEXOS 59

ÍNDICE DE TABLAS

CONTENIDO **PÁGINA**

Tabla 1. Normas ISO 27000 aplicado en la ciberseguridad 6

Tabla 2. Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos .. 8

Tabla3. Conceptos básicos relacionados con la seguridad dela información 14

Tabla4. Principios de la seguridad de la información 15

Tabla 5. Niveles de madurez y su descripción 22

Tabla 6. Preguntas de la entrevista y sus categorías 25

Tabla 7. Preguntas del check list categorizadas 26

Tabla 8. Personas Encuestadas..... 27

Tabla 9. Preguntas del cuestionario categorizado y escalas..... 28

Tabla 10. Modelo de madurez de cumplimiento..... 29

Tabla 11. Check list categorizado 30

Tabla 12. Tabulación general de la aplicación de encuestas..... 31

Tabla 13. Análisis de datos de la aplicación de encuestas 31

Tabla 14. Análisis de coeficiente de fiabilidad 32

Tabla 15. Modelo de madurez..... 33

Tabla 16. Resumen de madurez de los controles 34

Tabla 17. Análisis del check list..... 35

Tabla 18. Análisis de las encuestas 37

Tabla 19. Análisis de la encuesta por categoría 38

Tabla 20. Análisis de fiabilidad de resultados..... 39

Tabla 21. Resumen de madurez de los procesos 40

Tabla 22. Procesos aprobados y no aprobados..... 42

ÍNDICE DE GRÁFICOS

CONTENIDO **PÁGINA**

Gráfico 1. Consecuencias de los ciberataques en el mundo..... 4

Gráfico 2. Cumplimiento de las EGSI en las instituciones públicas..... 5

Gráfico 3. Ciclo deming o PDCA 7

Gráfico 4. Expresión gráfica teoría de la Información..... 13

Gráfico 5. Modelo PHVA para ISO 27001..... 17

Gráfico 6. Círculo de riesgos..... 21

Gráfico 7. Análisis de datos de las encuestas..... 32

Gráfico 8. Verificación del cumplimiento de actividades del check list..... 36

Gráfico 9. Nivel de madurez por dominios..... 41

CAPÍTULO I

1 FORMULACIÓN DEL ANÁLISIS DE CASO

1.1 Tema

"La Seguridad de la Información en la EP-EMAPA-A."

1.2 Antecedentes

La Empresa Pública- Empresa Municipal de Agua Potable y Alcantarillado de Ambato EP-EMAPA-A, expresa que en el año de 1967 garantizó que la correctagestión, operación y desempeño de los sistemas de agua potable instalados en la ciudad y a pesar de no disponer de muchos recursos esto no fue excusa para no trabajar por elbienestar de la ciudadanía ambateña.Ante la creciente demanda de agua potable paracumplir los objetivos institucionales y mantener competitividad ante otras empresasinició con el desarrollo en el campo de tecnología de la información; debido a esto la EP-EMAPA-A ha adoptado en los últimos años proyectos de tecnología eficaces con orientación hacia los objetivos y estrategiasde la institución.

La creación del Departamento de Informática en el año 1992 sufriómodificaciones en magnitud hasta el año 2000 el Departamento de Informáticarequirió un avance en su infraestructura dado que el espacio departamental no era el apropiado; gracias al cambio domiciliar de la empresa y la realización de lainfraestructura del nuevo edificio un estudio de ubicación de redes, puntos deconexión, ubicaciones de servidores, etc., estas nuevas adecuaciones produjeron lareducción de algunos problemas que se presentaban dentro del departamento.

Desde el cambio de domicilio efectuado en el 2007 se produjeron varios cambiosdentro del departamento como su nombre que pasó de departamento de informáticahacia departamento de Tecnologías de la Información lo que fomento la creación denuevas actividades como: base de datos, mantenimiento, redes, etc. En este mismo año la Unidad de Tecnologías de la Información al igual que el edificio matriz de la EMAPA operaban en el sector de la merced en las calles Bolívar y 5 de

Junio, en los altos del actual almacenes Tía-Laboral, el espacio de operación de Tecnologías de la Información era bastante reducido en el que laboraban el jefe de unidad más 7 ingenieros en sus diferentes áreas de especialidad, el espacio físico del cuarto de servidores era un lugar improvisado pequeño sin las debidas seguridades, sin un sistema de ventilación adecuado, que tampoco contaba con UPS (Uninterruptable Power Supply), también llamado Sistema de Alimentación Ininterrumpida (SAI)), que puedan dar energía de respaldo. Además, la estantería para la ubicación de los servidores también era improvisada y no adecuada para un cuarto de servidores, en aquel tiempo se contaba principalmente con dos servidores tipo torre Pentium III en sus características con 8Gb de RAM (Random Access Memory) y 60gb de espacio en disco duro de almacenamiento, y cada uno contaba con monitores VGA (Video Graphics Array) de 15", el servidor más actual a esa fecha era un servidor de rack HP en el que se encontraba el sistema comercial.

En el año 2008 la empresa inicia funciones en el sector de las calles Antonio Clavijo e Isaías Sánchez, actual ubicación del edificio matriz de la EP-EMAPA-A, este edificio ya contaba con un lugar específico y adecuado para un cuarto de servidores, con la debida seguridad, sistema de ventilación apropiado y un UPS institucional, los equipos se han ido renovando acorde a las necesidades de crecimiento de la empresa, en primera instancia se cambiaron servidores por otros más actuales y que sean apropiados para rack, con mejores características, la última implementación en el año 2016 fue un sistema de virtualización que se compone de un clúster de 3 servidores HP DL380 de iguales características, conectado a un sistema de almacenamiento HP P2000 y comunicados mediante un switch de fibra de alta disponibilidad a una velocidad de 8Gbps, en donde al momento se opera y gestiona la mayor parte de servicios tecnológicos de la EP-EMAPA-A.

El presente Análisis de Caso titulado la seguridad de la información en la EP-EMAPA-A presenta aspectos esenciales base en el campo de la seguridad de la información. Porque permite el análisis de datos, identificar y analizar los riesgos y vulnerabilidades. Del mismo modo, la empresa puede detectar las debilidades de los sistemas informáticos por medio de la ciberseguridad. De tal manera, se puede establecer mecanismos para proteger el sistema de seguridad de la información.

Cabe mencionar que la información de la empresa se maneja de manera interna y externa mediante el internet, el intranet y el correo electrónico. En este sentido, la ciberseguridad es fundamental para los sistemas de información. Así mismo, se procura cumplir con las políticas internas de la empresa para el correcto manejo y protección de la información de los usuarios y de la empresa, todo esto a través de su departamento de Tecnologías de la Información.

1.2.1 Inseguridad de la información tecnológica

En este sentido, Corda (2017) plantea que el riesgo informático es una eventualidad que causa que no se cumpla un objetivo, es decir, es aquello que puede causar daño directamente al funcionamiento o a los resultados que se espera obtener de un sistema informático. Las principales amenazas que son detectadas y que ponen en riesgo a un sistema informático son los actos ocasionados por el hombre, los desastres naturales y acciones maliciosas como robo o fraude (Hernández & Flórez, 2011). Por lo que, es importante diagnosticar oportuna y adecuadamente los riesgos a los que está expuesta la información, ya que han ocurrido una serie de acontecimientos a nivel mundial en cuanto a violación de la información de las empresas.

En términos de Maza (2020) la seguridad internacional y nacional cada vez se encuentra afectada por la aparición de nuevas vulnerabilidades, riesgos y amenazas, debido a los diferentes usos que se les da a las tecnologías exponenciales por los mismos Estados. Así mismo, Ramírez (2021) menciona que la mayor causa de vulnerabilidades y riesgos a los que están expuestas las organizaciones, se debe al mal uso de la tecnología y no solamente a los ataques intencionados. De este modo, las empresas deben contar con personal altamente capacitado para el manejo de información tecnológica ya que comprende una parte fundamental de las mismas.

Los ataques cibernéticos y la pérdida de información han generado impactos muy fuertes en las organizaciones. De este modo, TI (2018) afirma que el acceso a las redes corporativas utilizadas por los hackers es el DNS, utilizándolo como vía para el robo de información confidencial. Así mismo, cabe recalcar que no existe la

seguridad absoluta en un sistema, por lo que siempre se encontrará en riesgo, aunque se tomen medidas para mitigar los mismos (Bustamante, 2014). En este sentido, la protección de información de las organizaciones mediante la seguridad informática es esencial para evitar posibles ataques que las perjudiquen.

En el mismo sentido, el estudio realizado por Alvarado (2018) afirma que por medio de la inteligencia artificial se ha logrado encontrar patrones y asociaciones criminales que eran imposibles de identificar, esto gracias a cientos de denuncias agrupadas. En este sentido, la encuesta realizada por PwC (2018) sobre la seguridad de la información a 9500 directivos y responsables de las Tecnologías de la Información de 122 países, demuestran que las empresas tienen al año un promedio 3,4 percances de seguridad y sobrepasan los 4 millones de dólares en pérdidas económicas. De este modo, las empresas u organizaciones buscan protección para la información de los usuarios mediante programas que les ayuden a minimizar estos incidentes.

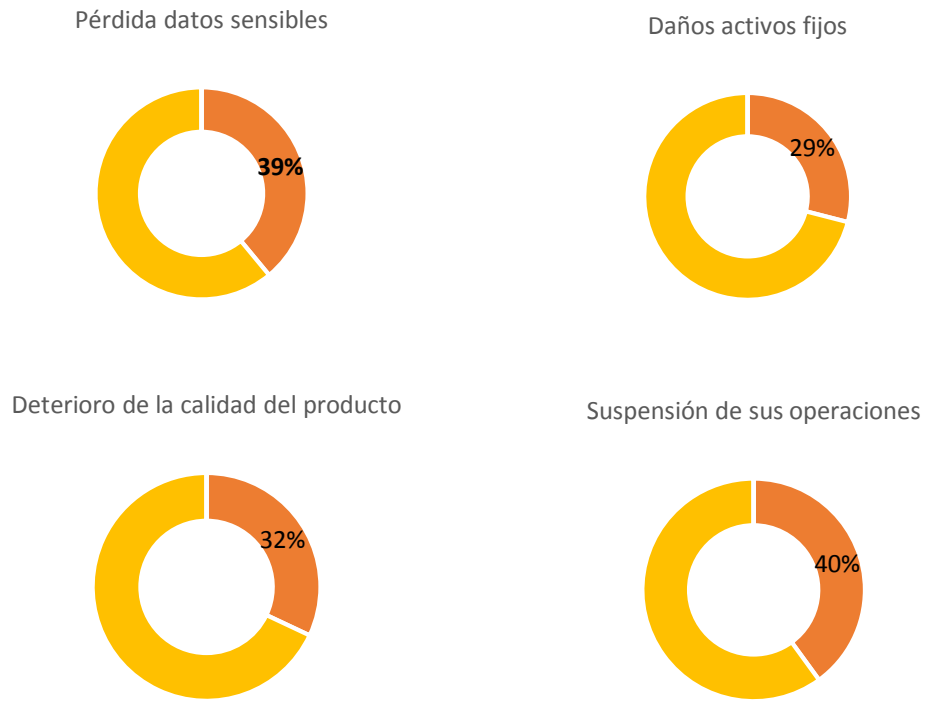


Gráfico 1. Consecuencias de los ciberataques en el mundo
Fuente: PwC (2018)
Elaborado por: Mayorga (2022)

1.2.2 Gestión de seguridad de la información en empresas del Ecuador

La seguridad de la información está relacionada con medidas aplicadas para salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad(Solarte & Enriquez, 2015). De este modo, en la norma ISO 27001 el EGSI es lo más importante porque unifica los criterios con el que se evalúa los riesgos asociados al manejo de la información institucional (EGSI, 2020). Por lo tanto, es necesario tener en cuenta la importancia de la aplicación de la norma ISO para salvaguardar la información para los usuarios.

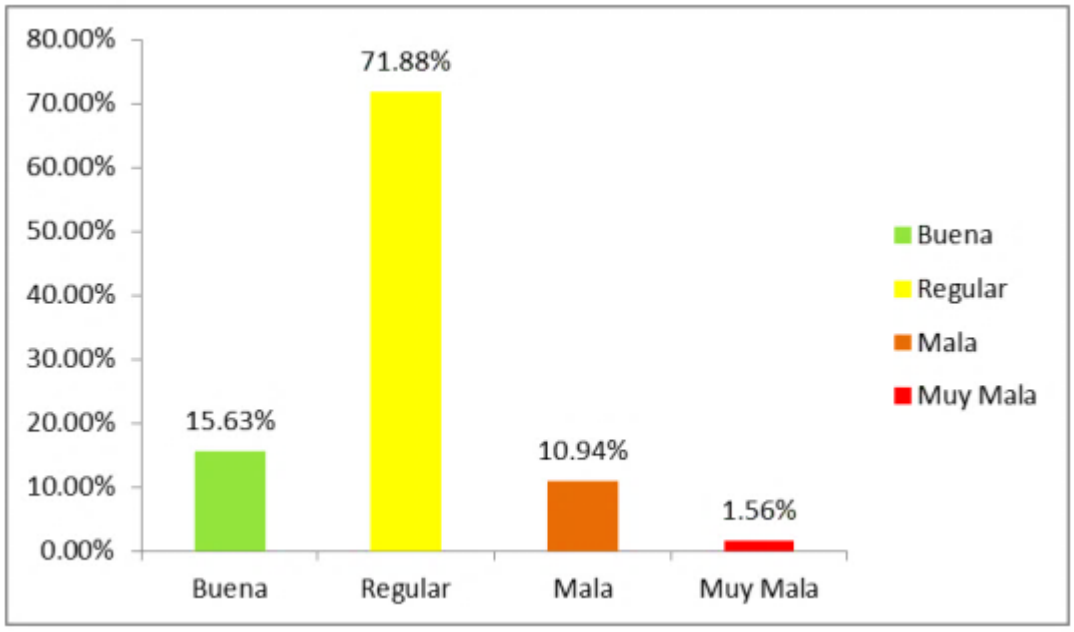


Gráfico 2. Cumplimiento de las EGSI en las instituciones públicas

Fuente: (MINTEL, 2018)

Elaborado por: Mayorga (2022)

Tabla 1. Normas ISO 27000 aplicado en la ciberseguridad

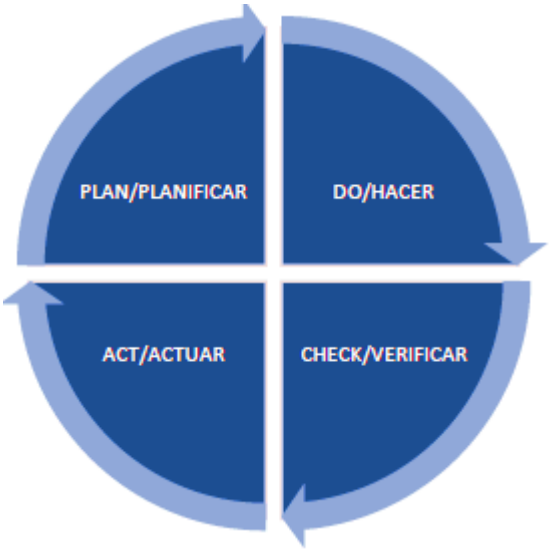
Norma	Detalle
27001	Proporciona establecimiento, implantación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.
27002	Permite controlar la seguridad de información como buena práctica para las organizaciones.
27005	Proporciona directrices para la gestión de riesgos de la seguridad de la información de las empresas.
27007	Permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
27031	Proporciona métodos para mejorar la preparación de las Tecnologías de Información y Comunicación garantizando a continuidad de las empresas.
27701	Administra, gestiona y protege los datos personales de la compañía de acuerdo al Reglamento General de Protección de Datos (RGPD) para que exista confidencialidad en las organizaciones.

Fuente: Murillo et. al (2019)

Elaborado por: Mayorga (2022)

Así mismo, GlobalSUITE (2021) aseguran que las normas ISO 27000 a través del ciclo Deming o PDCA permiten implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Igualmente, una adecuada Gestión de Riesgos en Seguridad de la Información, permitirá una adecuada implantación de un Sistema de Gestión de Seguridad de la Información (EGSI, 2020). De tal manera, esto permite que las organizaciones se mantengan alertas y puedan actuar de acuerdo al riesgo que se les presente.

Gráfico 3. Ciclo deming o PDCA



Fuente: Manay (2019)

Elaborado por: Mayorga (2022)

1.2.3 Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos

El control interno es responsabilidad de cada institución que debe ser aplicado por la máxima autoridad, la dirección y el personal de cada entidad para proporcionar seguridad para lograr los objetivos institucionales y la protección de los recursos públicos. En este sentido, las instituciones públicas deben aplicar las normas de control interno que se enuncian a continuación:

Tabla 2. Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos

410 TECNOLOGÍA DE LA INFORMACIÓN	DETALLE
410-01 Organización informática	Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.
410-02 Segregación de funciones	Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.
410-03 Plan informático estratégico de tecnología	La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.
410-04 Políticas y procedimientos	La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.
410-05 Modelo de información organizacional	La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.
410-06Administración de proyectos tecnológicos	La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que

	conformen dicha unidad.
410-07 Desarrollo y adquisición de software aplicativo	La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos.
410-08 Adquisiciones de infraestructura tecnológica	La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización.
410-09 Mantenimiento y control de la infraestructura tecnológica	La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.
410-10 Seguridad de tecnología de información	La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.
410-11 Plan de contingencias	Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.
410-12 Administración de soporte de tecnología de información	La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.
410-13 Monitoreo y evaluación de los procesos y servicios	Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.
410-14 Sitio web, servicios de internet e intranet	Es responsabilidad de la Unidad de Tecnología de Información 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, de conformidad con las disposiciones legales y considerando los requerimientos de los usuarios externos e internos.
410-15 Capacitación informática	Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.
410-16 Comité informático	Para la creación de un comité informático institucional, se considerarán los siguientes aspectos: el tamaño, la definición y la confirmación.
410-17 Firmas electrónicas	Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos y tecnológicos necesarios.

Fuente: Contraloría General del Estado (2022)
Elaborado por: Mayorga (2022)

1.2.4 El desarrollo de la EP-EMAPA-A y la aplicación de sistemas de seguridad de la información

La empresa cuenta con un departamento de Tecnologías de la Información en el que disponen de personal capacitado para encargarse de la seguridad tecnológica.Según Olmedo & Gavilánez (2018) afirma que los ciberataques ocurren debido a deficiencias en los mecanismos de defensa ante estas amenazas. También, la empresa cuenta con su sistema de seguridad de la información aplicando el esquema gubernamental de seguridad de la información (EGSI).

La empresa aplica sus políticas para controlar la seguridad de la información y así evitar riesgos. Del mismo modo, el EGSI y su implementación está influenciado por los objetivos, requisitos de seguridad, los procesos utilizados y por el tamaño y estructura de la organización (EGSI, 2020). Así mismo, los avances en la tecnología de la información causan que el gobierno de más atención a la protección de sus activos de información para minimizar los riesgos en los sistemas de información

para generar confianza en los usuarios a nivel interno de las instituciones (Pazmiño, 2015).

Según la ISO/IEC (2016), la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. En este sentido, la EP-EMAPA-A busca proteger los datos y recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos.

1.3 Justificación

El presente análisis es fundamental para conocer la situación que vive la empresa internamente y de qué manera manejan el sistema de seguridad de la información. Los beneficiarios de este análisis serán las empresas públicas que prestan servicios y que cuentan con un sistema de información interno y externo, ya que así podrían evitar posibles errores al momento de manejar la información. Así mismo, se pretende aportar datos sobre el manejo de la información pública y el debido proceso para la seguridad de la misma mediante el control interno. En este sentido, el crecimiento acelerado de la tecnología, ha generado graves problemas de vulnerabilidad en las organizaciones con riesgos e inseguridad así como fraudes informáticos, espionaje, sabotaje, virus informático y ataques de intrusión o negación de servicios (Romero & Castillo, 2018).

Este análisis busca beneficiar a la empresa siendo un instrumento para establecer una gestión adecuada de la seguridad de la información. Además, los sistemas informáticos y el uso responsable de la información de la empresa. En este sentido, se entiende por uso responsable el seguimiento de políticas, procedimientos, normas y buenas prácticas que salvaguarden la seguridad de la información tanto impresa como electrónica, sistemas de información y los recursos tecnológicos que posee la institución.

1.4 Objetivos

1.4.1 Objetivo general

Analizar la Seguridad de la Información en la EP-EMAPA-A para la prevención de riesgos y salvaguarda de la información.

1.4.2 Objetivos específicos

- Identificar los procesos de seguridad de la información que posee la EP-EMAPA-A para el resguardo de la información.

- Medir el nivel de madurez delos procesos del sistema de seguridad de la información en la EP-EMAPA-A.

- Relatar los resultados obtenidos del análisis de caso recalcando las recomendaciones de buenas prácticas para el sistema de gestión de seguridad de la información.

1.5 Preguntas de reflexión

1. ¿De qué manera asegura la información actualmente la EP-EMAPA-A?
2. ¿Cuáles son las medidas de seguridad para evitar la filtración de personas no autorizadas?
3. ¿Qué medidas de protección se han implementado dentro de la institución para la seguridad de la información?
4. ¿Cuáles son las buenas prácticas que implementa la empresa para mantener un buen control interno en los procesos de seguridad de la información?
5. ¿De qué manera se podría mejorar la seguridad de la información en la empresa?

CAPÍTULO II

2 FUNDAMENTACIÓN CIENTÍFICA TÉCNICA

2.1 Teoría de la información

Esta teoría es una disciplina mapa que tiene por objetivo orientar el conocimiento en torno a la comunicación, con dirección concreta para investigar la información (Aladro, 2011). Así mismo, Correa (2008) afirma que la teoría de la información se ocupa de aspectos como la evaluación de los métodos y transmisión, conservación, extracción así como de la clasificación y medida de la información. En este sentido, esta teoría sirve para analizar la información y para verificar que los métodos utilizados sean los correctos según las necesidades de la empresa.

De acuerdo a López (1998) la teoría tiene una expresión gráfica sencilla:

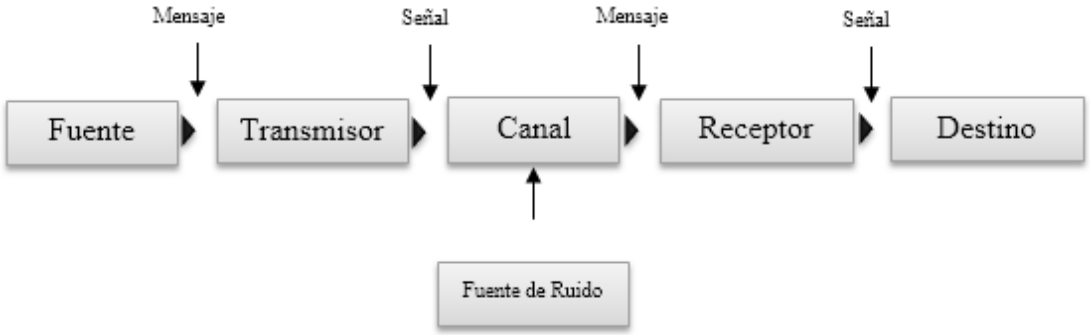


Gráfico 4. Expresión gráfica teoría de la Información
Fuente:López (1998)

2.2 Seguridad de la información

En palabras de Costas (2014), la seguridad está asociada con la contingencia, debido a que dentro de cualquier sistema los principales elementos a proteger son el hardware, que pertenecen a los elementos físicos de un sistema informático; el software que contienen los programas que permiten que el hardware funcione; y los datos que corresponde a la información que maneja el hardware y el software. En este sentido, para Escrivá et al. (2013) son importantes algunos conceptos básicos relacionados con el tema, como:

Tabla3.Conceptos básicos relacionados con la seguridad dela información

Término	Descripción
Activo	Recurso necesario del sistema que tenga valor y sea protegido para que la organización alcance los objetivos propuestos, entre ellos se encuentra el activo de información, que son los elementos que contiene datos almacenados; los activos físicos, relacionada con la infraestructura tecnológica utilizada para gestionar la información; los programas o aplicaciones utilizados y el personal que maneja esta información.
Vulnerabilidad	Debilidad de un activo que pueda implicar en el funcionamiento del sistema informático, los cuales pueden estar relacionados con fallos en las aplicaciones, mal uso de los sistemas, ataques informáticos o virus, por ello es necesario detectar estas situaciones que ponen en peligro la seguridad del sistema.
Amenaza	Una amenaza es cualquier entidad que atente contra el buen funcionamiento de un sistema informático, estas pueden ser pasivas cuando se obtiene información relativa a una comunicación, y activas, en caso de que se realicen cambios no autorizados dentro de los sistemas, por lo que son más peligrosas.
Riesgo	Un riesgo es la probabilidad de que la amenaza se materialice causando daño en algún proceso o sistema, por lo que se debe tratar de manera inmediata a través del análisis de los riesgos para establecer prioridades e implementar procedimientos de seguridad adecuados de acuerdo con las necesidades de la organización.
Información	Todo aquel elemento que contenga datos almacenados en cualquier tipo de soporte. Como por ejemplo, documentos, libros, patentes, correspondencia, estudios de mercado, datos de los empleados, manuales de usuario, etc.

Fuente: Escrivá et. al. (2013)

Elaborado por: Mayorga (2022)

La seguridad de información establece un plan de seguridad para proteger los datos y su integridad dentro de las distintas áreas relacionadas con la gestión informática (Navarro & Díaz, 2014)**.** Así mismo, la ISO 27000 en Colombia son utilizadas en las empresas como estándares de buenas prácticas en las áreas tecnológicas y de esta manera fortalecer los sistemas de seguridad de la información (Ladino & López, 2011). De tal modo, las organizaciones pueden tomar medidas que ayuden a proteger la confidencialidad de la información.

Tabla4.Principios de la seguridad de la información

Principio	Característica	Vulnerabilidad
Confidencialidad	Información accesible únicamente para personas o sistemas autorizados.	Divulgar claves de acceso y violación de protocolos de comunicación.
Integridad	Información que no haya sido alterada y que permita comprobar que no se ha manipulado la información original.	Alterar información sin tener acceso y modificar el mensaje en la red de comunicaciones.
Disponibilidad	Capacidad de un servicio, dato o sistema que este accesible para los usuarios cuando lo requieran.	Presencia de virus y ataques que perjudican al sistema o red.

Fuente: Costas (2014)

Elaborado por: Mayorga (2022)

La seguridad de la información es un catalizador que está unido a la confianza de las partes interesadas tratando los riesgos o creando valor para la empresa como ventaja competitiva (ISACA 2012). Así mismo, Briceño (2021) afirma que la seguridad de la información se involucra con aspectos de la sociedad hiperconectada con la tecnología de información y comunicación. Es decir, hoy en día la seguridad de la información es importante tanto para las empresas como para la sociedad misma.

Malware.- Según Fuentes (2008) es un término general que se refiere a todos los programas que dañan una computadora. También, actualmente es una de las principales amenazas que afectan a los sistemas informáticos. Así mismo, puede ser un virus, troyano, backdoor, spyware o incluso un

gusano destructivo que puede destruir toda la infraestructura de la red incluso redes nacionales y corporativas.

Debido al malware, aparecen otros ataques como: DDoS (distributed denial of service), distribución de spam, propagación de virus y gusanos a otras redes, sitios de phishing, redes de extensión (redes informáticas en riesgo), pharming y su variante de pharming by driving, entre otras cosas. El malware se está volviendo más sofisticado y muchas soluciones defensivas, como el software antivirus y antispyware, se ven abrumados por los tiempos de respuesta a estas amenazas, porque el virus aprovecha la tecnología para causar daño, rápida y sofisticadamente en su camino para engañara sus víctimas. La prevalencia de este conflicto se deriva de aspectos tales como: no prestar atención a la actualización del sistema operativo; no aplicar programas de actualización central; falta de mecanismos de protección en el dispositivo, como implementar buenas medidas de seguridad: firewalls personales, actualizaciones de antivirus entre otros (Fuentes, 2008).

2.2.1 Norma ISO/IEC 27001

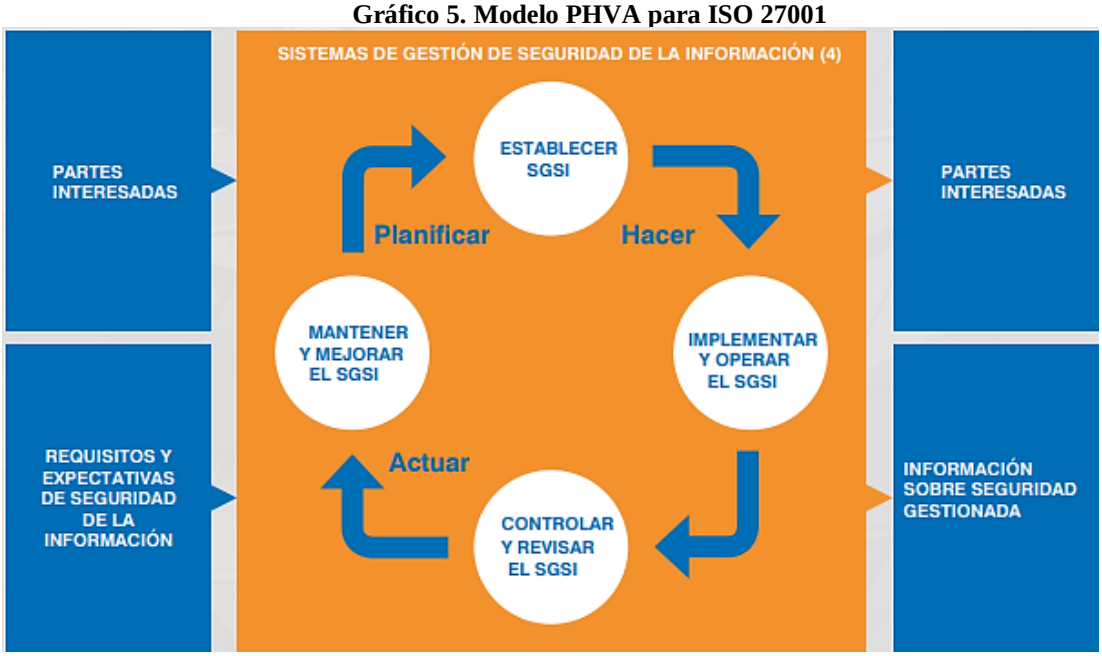
ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013(Advisera, 2022). Es una norma internacional que proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI (Mesquida & Cabestrero, 2010). Así mismo, Calder (2017) afirma que la norma internacional ISO/IEC 27011:2013 gestiona la seguridad de la información en línea con los requisitos reglamentarios de una organización y su apetito de riesgo. De este modo, la seguridad de la información ahora también representa un problema y una responsabilidad que debe ser manejada correctamente.

Del mismo modo, (Ealde, 2020) afirma que ISO 27001 es un estándar internacional para la gestión de la seguridad de la información en las organizaciones tanto para la información física como para la digital. Así también, forma parte de la familia

de normas ISO 27000 que ayuda a las organizaciones a proteger sus activos de información.En este sentido, la implementación de esta regulación que ha sido adoptada por miles de empresas tanto públicas como privadas en todo el mundo, garantiza que la informaciónconfidencial permanezca protegida y disponible. En general, es un estándar amplio que abarca la seguridad técnica, física, humana y de procesos dentro de una empresa.

La ISO 27001 se basa en el ciclo PHVA o ciclo Deming que puede aplicarse no solo al sistema de gestión sino también a cada elemento para proporcionar una mejora continua (Russell, 2022).

Gráfico 5. Modelo PHVA para ISO 27001



Fuente: Russell (2022)

Elaborado por: Mayorga (2022)

ISO 27001 es una norma que permite el aseguramiento, integridad y confidencialidad de la información y de los sistemas que la procesan (ISOTools, 2022). Así mismo, ATICO34 (2022) afirma que la norma ISO 27001 se basa en la gestión de la calidad PDCA o ciclo PDCA.Aunque, en su última actualización no aparece explícitamente, sigue estando muy presente en su estructura:

- **Plan (Planificar):** Es la primera fase de la elaboración del SGSI, en la que se lleva a cabo la identificación de los riesgos que enfrenta la seguridad de la información, realizando para ello un análisis cuantitativo y cualitativo (cuando se requiere) de los riesgos detectados y planificando la respuesta que se les dará, así como los controles necesarios para su mitigación.
- **Do (Hacer):** En esta fase se implementa y pone enmarca el SGSI tal y como se ha definido en la fase anterior.
- **Check (Verificar):** Mientras el plan de seguridad está en funcionamiento, se revisa y evalúa para comprobar su eficacia. Si se detectan carencias o que las medidas y mecanismos resultan insuficientes, se deben analizar las causas tras las mismas y definir posibles mejoras.
- **Act (Actuar):** La estrategia de seguridad siempre debe estar en proceso de mejora continua.

2.2.2 Norma ISO/IEC 27002

Según, ABNT (2005) la seguridad de la información es un tema que se ha vuelto muy conocido en los últimos años, acaparando un amplio espacio mediático y convirtiéndose en un "commodity" en empresas de todos los tamaños y sectores. Por otro lado, es importante señalar que la popularidad del término IS (Seguridad de la Información) ha sido impulsada por el creciente número de incidentes de seguridad que se han producido en el mundo. Las perturbaciones derivadas de estos incidentes son variadas, provocando daños en la imagen de la empresa o fuga de información importante lo que puede derivar en importantes pérdidas económicas.

Es en este contexto que nació la norma internacional ISO/IEC 27002, enfocada en las mejores prácticas para la gestión de la seguridad de la información (ABNT, 2005).

Del mismo modo, PMG (2017) define a la seguridad de la información como el estándar de mantener la confidencialidad, integridad y disponibilidad. Es así que, las empresas pueden mantener una buena práctica de los procesos de seguridad siguiendo las normas establecidas.

En 1995, las organizaciones internacionales ISO (The International Organization for Standardization) e IEC (International Electrotechnical Commission) emitieron un conjunto de estándares que unifican las pautas para el campo de la seguridad de la información, representado por la serie 27000. Esto incluye ISO/IEC 27002 (anteriormente conocido como estándar 17799:2005). Es un estándar internacional que define las mejores prácticas para soportar la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) en las empresas.

Así mismo, esta norma que brinda pautas integrales de implementación describe cómo establecer medidas de control. A su vez, estos controles deben seleccionarse con base en la evaluación de riesgos de los activos comerciales más importantes. Además, ISO 27002 se puede utilizar para respaldar la implementación de SGSI en cualquier tipo de organización, pública o privada, grande o pequeña, con o sin fines de lucro y no solo en las empresas que trabajan con tecnología.

Del mismo modo, Isotools (2022) afirma que la norma ISO 27002 tiene como objetivo que la organizaciónconozca exactamente todos los activos que posee. Además, esta información es una parte muy importante de la gestión de riesgos. Estos son algunos ejemplos de contenido:

Fuentes de información: bases de datos y archivos, documentación del sistema, manuales de usuario, documentos utilizados durante la formación, procedimientos operativos, planes de continuidad y contingencia, etc.

Recursos de software: software de aplicación, sistemas operativos, herramientas utilizadas para realizar el desarrollo, etc.

Bienes físicos: equipos informáticos, equipos de comunicación, mobiliario, etc.

Servicios: Servicios informáticos y de comunicaciones.

En este sentido, los activos de información deben clasificarse de acuerdo con la sensibilidad y la importancia de la información que contienen o reservarse con el fin de determinar cómo se manejará y protegerá la información. Además, las pautas de clasificación que deben esperar que una determinada información sea clasificada y tenida en cuenta no son necesariamente permanentes y pueden modificarse de acuerdo con una política establecida por la propia organización. Es así que, el número de categorías debe tenerse en cuenta al determinar la clasificación completa de acuerdo con esquemas que pueden implementarse de manera compleja dentro de la organización y pueden ser muy poco prácticos.

2.3 Sistema de gestión de seguridad de la información

De acuerdo a Grajales& León (2016) es creado como respuesta a la necesidad de protección de la información en las empresas también es conocido como SGSI (Sistema de Gestión de Seguridad de la Información). Además, tiene como objetivo controlar las consecuencias derivadas de la aparición de riesgos inherentes al acceso de personas no autorizadas y la exposición de la información en diversos procesos de una organización y posibilita el desarrollo de medidas encaminadas a la continuidad de las operaciones.

Del mismo modo, contiene un inventario de activos de información que necesitan ser protegidos dada su criticidad en la operación de los procesos organizacionales, los riesgos y amenazas que enfrentan, y los controles implementados para mitigar y preservar los activos (Grajales & León, 2016).

En este sentido, como base para garantizar que la seguridad de la información se gestione adecuadamente, primero se debe identificar su ciclo de vida y los aspectos relacionados para garantizar la confidencialidad, integridad y disponibilidad.

Lo anterior está documentado, codificado, estructurado y de manera repetible y eficiente donde el riesgo es reconocido, aceptado, gestionado, mitigado y adaptado a los cambios que ocurren en el riesgo, el entorno y la tecnología(ISO 27000, 2022).

Gráfico 6. Círculo de riesgos

Fuente: ISO 27000 (2022)

Elaborado por: Mayorga (2022)

2.4 Modelo de madurez

Un modelo de madurez es una guía para la organización que ofrece un punto de partida para la implementación de buenas prácticas. Además, describe la evolución y mejora de los procesos desde los más inconsistentes hasta los procesos más maduros de la entidad. Así mismo, permite evaluar el desarrollo de los procesos de una organización o negocio y plantear las estrategias para mejorar y alcanzar los objetivos. Del mismo modo, identifica las áreas en las que se debe enfocar la entidad para mejorar (Pérez, 2014).

Así mismo, Grajales & León (2016) afirma Dentro del modelo de seguridad de la información y protección de datos, se tiene en cuenta el nivel de madurez del desarrollo permanente de la seguridad de la información y protección de datos dentro de la organización y estos requisitos se identifican, categorizan y forman parte del proceso de gestión de seguridad de la información.

Del mismo modo, Pérez (2014)afirma que las empresas se percatan que deben hacer varios cambios en sus procesos y sistemas al momento de hacer mejoras. En este

sentido, muchas se encuentran inseguras porque no saben exactamente que deben cambiar, en qué medida y en qué momento deben hacerlo. Por otra parte, Grajales & León (2016) afirman que los modelos de madurez permiten medir los niveles de madurez de los procesos que posee cada empresa. También, identificar las brechas que existen actualmente y crear planes de trabajo que puedan cumplir con los parámetros establecidos en cada nivel.

Tabla 5. Niveles de madurez y su descripción

Nivel	Descripción
Inexistente	La empresa no ha reconocido siquiera que existe un problema a resolver
Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques que tienden a ser aplicados de forma individualo caso por caso
Repetible	La empresa ha documentado procedimientos y si estos se aplican en todos los procesos que interviene en la realización de la actividad. La empresa no tiene establecido un plan de formación, la ejecución del procedimiento es responsabilidad del empleado, por esta razón la probabilidad de errores es alta.
Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida si utilizarlos o no, y es poco probable que se detecten desviaciones
Administrado	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida si utilizarlos o no, y es poco probable que se detecten desviaciones
Optimizado	El desarrollo y ejecución de procesos tienen nivel de madurez alto y se encuentra basado en la mejora continua. El proceso tecnológico o TIC trabaja en la automatización de las actividades, para que el proceso realice las actividades con calidad y efectividad.

Fuente: Sánchez (2018)

Elaborado por: Mayorga (2022)

CAPÍTULO III

3 METODOLOGÍA

3.1 Metodología e instrumentos de recolección de información

3.1.1 Unidad de análisis

Para este caso la unidad de análisis escogida es la EP-EMAPA-A, empresa pública con más de cincuenta años al servicio de Ambatohaciendo llegar el suministro de agua potable a varios sectores de la ciudad. Esta institución maneja gran cantidad de información muy importante para su productividad. De este modo, con la finalidad de salvaguardar y proteger la información requiere del respaldo de los sistemas informáticos.

La empresa maneja una extensa información y utilizan varios sistemas de acuerdo a cada departamento. En este sentido, la seguridad de la información es muy necesaria para evitar el acceso de personas no autorizadas. De este modo, es importante controlar la seguridad informática para evitar ataques maliciosos.

Se efectuó una investigación de campo que determinó que hace algún tiempo atrás la empresa sufrió un secuestro de información a causa de un malware en uno de sus servidores. A pesar de esto, gracias a sus respaldos pudieron reestablecer el servidor y ponerlo a operar normalmente. Por lo tanto, se vio la necesidad de implementar políticas para la seguridad de la información para prevenir nuevos inconvenientes.

Cabe mencionar que la empresa no aplica ninguna norma específica solamente se rigen en sus prácticas y políticas internas establecidas dentro de la unidad de tecnologías de la información. Así mismo, utilizan contraseñas de usuarios, manejo de perfiles, políticas de seguridad en el firewall y reglas de acceso. De este modo, restringen el acceso de terceros protegiendo la seguridad de la información.

Además, la empresa necesita contar con personal calificado en seguridad de la información para tener una mejor guía. De la misma manera, la falta de capacitación

al personal sobre seguridad de la información causa inconvenientes en los equipos por motivo de correos maliciosos que los infectan.

3.1.2 Fuentes y técnicas de recolección de información

3.1.2.1 Fuentes de información primarias

En este caso se aplicó una guía de entrevista para obtener información de forma general sobre varios aspectos de seguridad de la empresa. También, una encuesta para conocer el punto de vista de los trabajadores de cómo se encuentra la protección de la información en la entidad y el check list para verificar la seguridad de la información de la empresa. Cabe mencionar que estos métodos fueron de gran ayuda para medir el nivel de madurez del sistema de seguridad de la información de la empresa.

La entrevista tuvo una duración aproximada de 5 minutos con 22 segundos. La cual fue dirigida al Ing. Alex Acurio, Jefe del departamento de Tecnologías de la Información, cabe mencionar, que esta fue aplicada el día jueves 16 de junio del 2022 a las 15:30pm de manera presencial en el departamento de Tecnologías de la Información.

Tabla 6. Preguntas de la entrevista y sus categorías

Preguntas	Dimensión o categoría
1. ¿Cómo es su sistema de gestión de seguridad de la información?	Seguridad de la información
2. ¿Qué sistemas informáticos se maneja en la empresa?	Sistemas Informáticos
3. ¿Cuáles son los inconvenientes más comunes que ha detectado la empresa en cuanto a tecnología de la información?	Riesgos informáticos
4. ¿Ha existido algún tipo de robo de información o problema similar en la empresa?	Riesgos informáticos
5. ¿Qué tan importante es la seguridad informática para la empresa?	Seguridad informática
6. ¿Qué normas aplica la empresa para gestionar la seguridad de la información?	Seguridad de la información
7. ¿Cuáles son las medidas de seguridad que aplica la empresa para proteger la información interna?	Seguridad de la información
8. ¿Cada qué tiempo se evalúa el sistema de seguridad de la información?	Seguridad de la información

Fuente: Mayorga (2022)

Elaborado por: Mayorga (2021)

Del mismo modo, se aplicó un check list el 16 de junio del 2022 a nivel general de la empresaa través de la evaluación para verificar que haya sido cumplido cada punto en base a la seguridad de la información de acuerdo a las preguntas que se muestran a continuación.

Tabla 7. Preguntas del check list categorizadas

Pregunta	Dimensión o Categoría
1. ¿La institución ha implementado políticas de seguridad de la información?	Políticas de Seguridad de la Información
2. ¿Las políticas de seguridad de la información son aprobadas por la administración?	Políticas de Seguridad de la Información
3. ¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?	Políticas de Seguridad de la Información
4. ¿Se revisa frecuentemente las políticas de seguridad de la información?	Políticas de Seguridad de la Información
5. ¿Se establecen responsabilidades para la revisión y evaluación de las políticas?	Políticas de Seguridad de la Información
6. ¿Disponen de un inventario de activos de información?	Gestión de Activos
7. ¿Existen políticas relacionadas con el uso adecuado de los activos de información?	Gestión de Activos
8. ¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?	Gestión de Activos
9. ¿Los soportes de almacenamiento están en un entorno seguro y protegido?	Gestión de Activos
10. ¿Los datos se almacenan en múltiples copias para reducir el riesgo de daño o pérdida?	Gestión de Activos
11. ¿Existen políticas de control de acceso en función a la seguridad de la información?	Control de Acceso
12. ¿Las políticas se basan en los requerimientos de la institución?	Control de Acceso
13. ¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?	Control de Acceso
14. ¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?	Control de Acceso

Fuente: ISO/IEC 27001 (2013)

Elaborado por: Mayorga (2022)

Del mismo modo, las encuestas fueron aplicadas a varios trabajadores de los departamentos de la EP-EMAPA-A con un total de 20 personas de acuerdo a como se muestra en la siguiente tabla.

Tabla 8. Personas Encuestadas

Nombre	Cargo	Departamento
Ricardo Rivera	Analista Técnico	Tecnologías de la Información
Priscila Aguilar	Asistente Administrativo	Tecnologías de la Información
Darwin Narváez	Analista Técnico	Tecnologías de la Información
Daniel Ipiales	Analista Técnico	Tecnologías de la Información
Alexandra Chávez	Jefe de Atención al Usuario	Dirección Comercial
Blanshy Ortega	Jefe Medición y Facturación	Dirección Comercial
Andrea Jácome	Asistente Administrativo	Dirección Comercial
Elizabeth Chicaisa	Analista Técnico	Dirección Comercial
Milton Salinas	Analista Técnico	Dirección Comercial
Dacy Guerrero	Analista Técnico	Talento Humano/ Administrativo
Pamela Páliz	Asistente Administrativo	Administrativo/Talento Humano
Martín Córdova	Jefe de Talento Humano	Administrativo
María Zurita	Analista de Talento Humano	Talento Humano
David Carrasco	Contador General	Financiero
Lilian Gamboa	Analista Financiero	Financiero
Vanessa Manzano	Analista Técnico	Financiero
Danny Suárez	Inspector de Campo	Dirección Comercial
Gladys Andocilla	Analista Técnico	Dirección Comercial
Mauricio Hidalgo	Inspector de Campo	Dirección Comercial
Ramiro Freire	Inspector de Campo	Dirección Comercial

Fuente: Mayorga (2022**)**

Elaborado por: Mayorga (2022)

En el presente análisis se aplicó también el cuestionario con escalas de tipo Likert de 3 niveles, el 16 de junio del 2022 de forma física para determinar las vulnerabilidades y riesgos que presenta la empresa en base a las siguientes preguntas:

Tabla 9. Preguntas del cuestionario categorizado y escalas

Preguntas	Categoría	Escala
1. ¿Ha firmado un acuerdo de confidencialidad?	Gobierno y Cultura	1. SI 2. NO 3. NO APLICA
2. ¿Se han definido responsabilidades concretas para la seguridad de la información?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
3. ¿Existe una política que define cómo utilizar las tecnologías de la información y los datos de la empresa?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
4. ¿Existe una política para el uso privado de las tecnologías de la información de la empresa?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
5. ¿Está informado regularmente sobre las medidas de seguridad de la información?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
6. ¿Es capaz de identificar un virus o malware?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
7. ¿Gestiona el uso seguro de redes sociales y correo electrónico?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
8. ¿Conoce sobre la normativa pertinente de la seguridad de la información?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
9. ¿Existe una política de la utilización de dispositivos móviles?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
10. ¿Los datos de los dispositivos se encuentran protegidos contra el acceso no autorizado?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
11. ¿En caso de pérdida del dispositivo conoce el procedimiento a seguir?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
12. ¿Conoce cómo actuar en caso de incidente de ciberseguridad?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
13. ¿Posee acceso a los sistemas como administrador?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
14. ¿Se revisan regularmente los perfiles de acceso y usuario de acuerdo a un ciclo definido previamente?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
15. ¿Posee accesos a la infraestructura de las tecnologías de información solamente si son necesarios para el cumplimiento de las funciones?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
16. ¿Se ha capacitado acerca de la utilización de las Tecnologías de información, así como de los datos de la empresa de forma segura?	Alineado con la Estrategia	1. SI 2. NO 3. NO APLICA

Fuente: Cepreven (2022)

Elaborado por: Mayorga (2022)

Del mismo modo se utilizó un modelo de madurez basado en la norma ISO 27002:2013 el cual permitió medir el nivel de madurez del sistema de seguridad de la información de la empresa.

Tabla 10. Modelo de madurez de cumplimiento

Valor	Efectividad	Nivel	Descripción
0	0%	Inexistente	La empresa no ha reconocido siquiera que existe un problema a resolver
1	10%	Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques que tienden a ser aplicados de forma individualo caso por caso
2	50%	Repetible	La empresa ha documentado procedimientos y si estos se aplican en todos los procesos que interviene en la realización de la actividad. La empresa no tiene establecido un plan de formación, la ejecución del procedimiento es responsabilidad del empleado, por esta razón la probabilidad de errores es alta.
3	90%	Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida si utilizarlos o no, y es poco probable que se detecten desviaciones
4	95%	Administrado	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida si utilizarlos o no, y es poco probable que se detecten desviaciones
5	100%	Optimizado	El desarrollo y ejecución de procesos tienen nivel de madurez alto y se encuentra basado en la mejora continua. El proceso tecnológico o TIC trabaja en la automatización de las actividades, para que el proceso realice las actividades con calidad y efectividad.

Fuente: Sánchez (2018)

Elaborado por: Mayorga (2022)

3.2 Método de análisis de información

Para esta investigación fue necesario realizar una entrevista que en este caso fue a una sola persona quien nos permitió conocer algunos aspectos sobre los sistemas de seguridad de la información que se aplicaban y el debido control tecnológico de los datos de la empresa. También, se aplicó el check list para verificar las actividades de seguridad de la información que manejan en la EP-EMAPA-A. De esta manera, se pudo obtener la información necesaria para el respectivo análisis y medición de los niveles de madurez en el sistema de seguridad de la información de la empresa.

De acuerdo a la tabla 4 se fue tabulando las actividades que la empresa iba cumpliendo para su posterior análisis.

Tabla 11. Check list categorizado

CATEGORIA	PORCENTAJE DE CUMPLIMIENTO
Políticas de Seguridad de la Información	
Gestión de Activos	
Control de Acceso	
Seguridad Física y del Entorno	
Seguridad de las Operaciones	
Seguridad en las Comunicaciones	
Gestión de Incidentes	

Fuente:EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Por otra parte, se efectuó el check list el cual analizó los factores que afectan la seguridad física, lógica y la seguridad de la información en base a las normas ISO 27001:2013 y 27002:2013. Para el análisis comprensivo se reflejaron los resultados obtenidos en la presente gráfica de líneas, aquí se pudo observar los porcentajes de cumplimiento de cada categoría. De este modo, se pudo detectar las vulnerabilidades y necesidades de la empresa en sus procesos de seguridad. Este análisis aportó información importante a la empresa.

Tabla 12. Tabulación general de la aplicación de encuestas

PREGUNTA	CATEGORIA	1 (SI)	2 (NO)	3 (NO APLICA)
Pregunta 1	Gobierno y Cultura			
Pregunta 2	Modelo Operativo y de Negocios			
Pregunta 3	Modelo Operativo y de Negocios			
Pregunta 4	Modelo Operativo y de Negocios			
Pregunta 5	Modelo Operativo y de Negocios			
Pregunta 6	Modelo Operativo y de Negocios			
Pregunta 7	Modelo Operativo y de Negocios			
Pregunta 8	Modelo Operativo y de Negocios			
Pregunta 9	Modelo Operativo y de Negocios			
Pregunta 10	Modelo Operativo y de Negocios			
Pregunta 11	Modelo Operativo y de Negocios			
Pregunta 12	Reporte y Tecnología			
Pregunta 13	Reporte y Tecnología			
Pregunta 14	Reporte y Tecnología			
Pregunta 15	Alineado con la Estrategia			
Pregunta 16	Alineado con la Estrategia			
Pregunta 17	Alineado con la Estrategia			

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Para analizar las respuestas de acuerdo al manejo de la seguridad de la información que efectuaba cada departamentose requirió de la tabla 11.

Tabla 13. Análisis de datos de la aplicación de encuestas

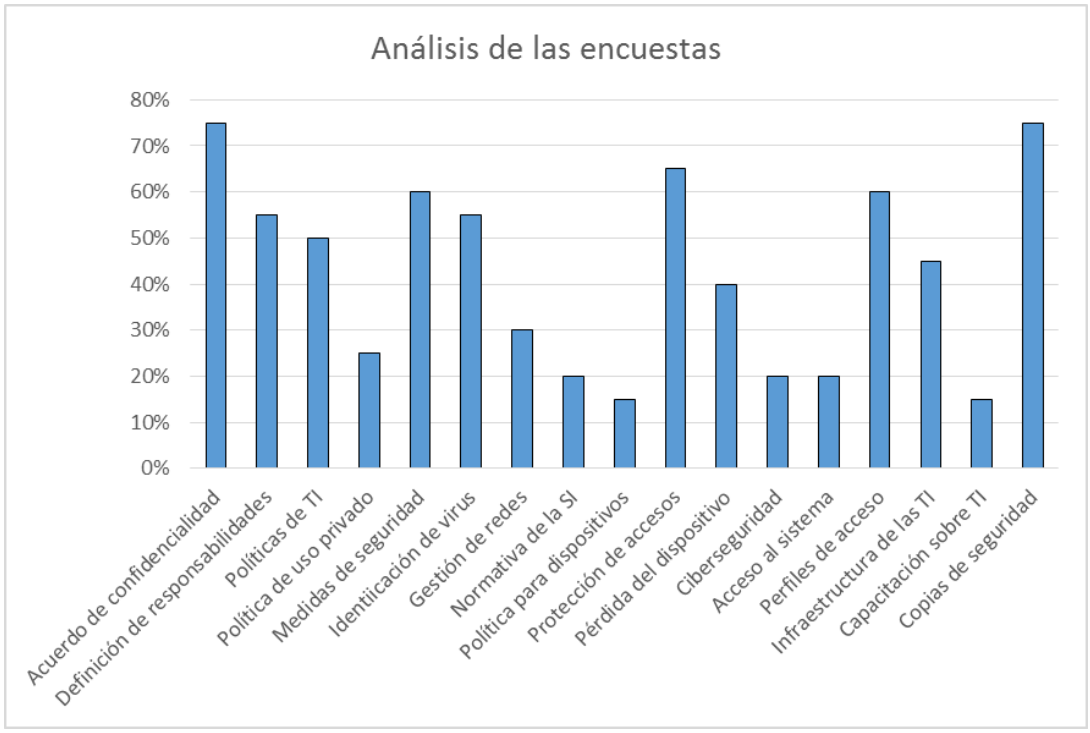
CATEGORIA	PORCENTAJE DE CUMPLIMIENTO
Gobierno y Cultura	
Modelo Operativo y de Negocios	
Reporte y Tecnología	
Alineado con la estrategia	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Se requirió de los datos recopilados en las encuestas y de esta forma se identificaron las vulnerabilidades y fortalezas de la empresa mediante el siguiente gráfico de barras.

Gráfico 7. Análisis de datos de las encuestas



Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

En este caso se utilizó el alfa de Cronbach para mayor fiabilidad de los datos para que el análisis sea correcto y veraz.Así mismo, Yarda (2021) afirma que el alfa de Cronbach es un coeficiente que mide la fiabilidad de una escala de medida. Del mismo modo, el Alfa de Cronbach es un coeficiente que se utiliza para saber cuál es la fiabilidad de una escala o test (Ruiz, 2019).

Tabla 14. Análisis de coeficiente de fiabilidad

ALFA	α =	
NÚMERO DE PREGUNTAS	K=	
VARIANZA DE CADA ITEM	Vi=	
VARIANZA TOTAL	Vt=	

Fuente:EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Con la información obtenida se pudo realizar el modelo de madurez para medir y evaluar cada proceso del sistema de seguridad de la información que se aplica en la entidad como se muestra a continuación.

Tabla 15. Modelo de madurez

PROCESOS				
I. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	**Calificación**	**%**	**Madurez**	**Significado**
Dirección de gestión para la seguridad de la información				
1. ¿La institución ha implementado políticas de seguridad de la información?				
2. ¿Las políticas de seguridad de la información son aprobadas por la administración?				
3. ¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?				
4. ¿Se revisa frecuentemente las políticas de seguridad de la información?				
5. ¿Se establecen responsabilidades para la revisión y evaluación de las políticas?				
II. GESTIÓN DE ACTIVOS				
Responsabilidad por los activos				
6. ¿Disponen de un inventario de activos de información?				
7. ¿Existen políticas relacionadas con el uso adecuado de los activos de información?				
Clasificación de la información				
8. ¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?				
Manejo de medios de almacenamiento				
9. ¿Los soportes de almacenamiento están en un entorno seguro y protegido?				
10. ¿Los datos se almacenan en múltiples copias para reducir el riesgo de daño o pérdida?				
III. CONTROL DE ACCESO				
Requisitos comerciales de control de acceso				
11. ¿Existen políticas de control de acceso en función a la seguridad de la información?				
12. ¿Las políticas se basan en los requerimientos de la institución?				
13. ¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?				
Gestión de acceso de usuarios				
14. ¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?				
15. ¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?				
Control de acceso al sistema y a las aplicaciones				
16. ¿Se controla los datos a los que puede acceder un usuario en particular?				
17. ¿El acceso es protegido contra varios intentos de inicio de sesión?				
18. ¿Las contraseñas de los usuarios se cambian regularmente?				
19. ¿La selección de contraseñas es compleja?				
20. ¿Se restringe el acceso al código fuente del programa de la institución?				

Fuente: Elaboración propia

Del mismo modo, para analizar la efectividad de los 42 controles evaluados en el modelo de madurez se necesitó de la siguiente tabla donde se evidencian los controles que no llegan al nivel de madurez óptimo en la valoración realizada a la EP-EMAPA-A ya que se encuentran entre el 0% y el 50% de efectividad.

Tabla 16. Resumen de madurez de los controles

Valor	Efectividad	Significado	Número	Madurez
0	0%	Inexistente	4	No aprobados
1	10%	Inicial	2	
2	50%	Repetible	1	
3	90%	Definido	6	Aprobados
4	95%	Administrado	5	
5	100%	Optimizado	24	

Fuente: ISO 27002 (2013)

Elaborado por: Mayorga (2022)

CAPÍTULO IV

4 DESARROLLO DEL ANÁLISIS DE CASO

4.1 Análisis y categorización de la información

La EP-EMAPA-A empresa que maneja una gran cantidad de información pública y confidencial de sus actividades almacenadas en su base de datos. La cual es gestionada por el centro de procesamiento informático que no solamente se encarga de dar el soporte técnico necesario sino también vela por la seguridad de dicha información, el análisis efectuado a los procesos de seguridad de la información empleando las normas ISO 27000 han permitido verificar si cumplen los procesos e identificar ciertas vulnerabilidades, amenazas y riesgos en su sistema de seguridad los cuales se presentan a continuación:

Tabla 17. Análisis del check list

CATEGORÍA	PORCENTAJE DE CUMPLIMIENTO
Políticas de Seguridad de la Información	80%
Gestión de Activos	80%
Control de Acceso	100%
Seguridad Física y del Entorno	92%
Seguridad de las Operaciones	100%
Seguridad en las Comunicaciones	100%
Gestión de Incidentes	40%

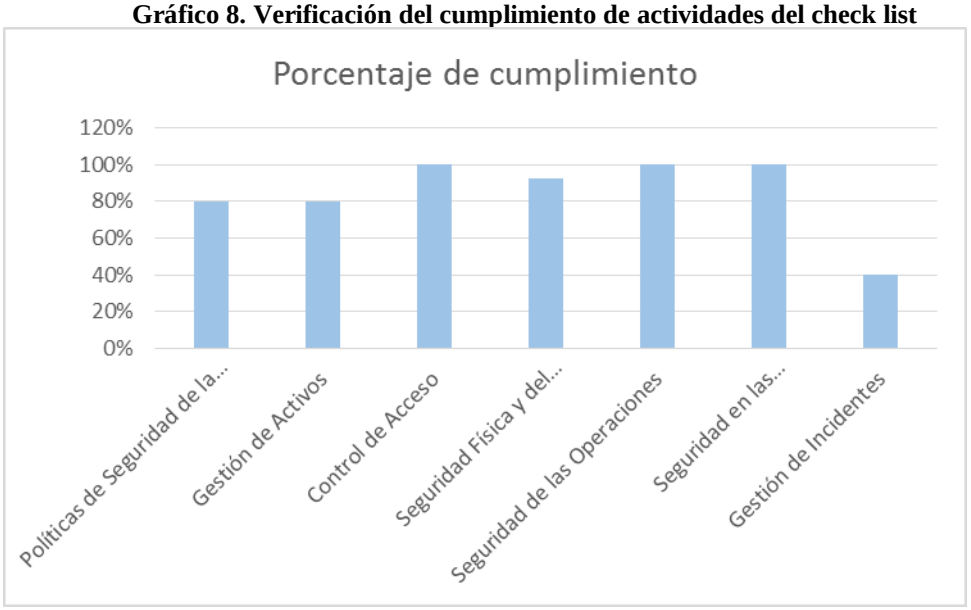
Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

En la categoría de Políticas de Seguridad de la Información cuenta con un 80% de cumplimiento. Pues, no han implementado políticas de seguridad de la información. Del mismo modo, la información noseclasifica entérminosdevalor, criticidad y sensibilidad aladivulgación o modificación noautorizadas. Por otra parte, tampoco se identificaalosusuariosquese lespermitela salidadelosactivosfuerade lainstitución. En este sentido, la Gestión de incidentes es uno de los aspectos que menos se cumple en la

empresa. Puesto que, no se notifican las debilidades de seguridad observadas. Así mismo, no se establece una clasificación de los incidentes de seguridad de la información para identificar su impacto y alcance. Igualmente, los incidentes de seguridad de la información no responden de acuerdo con los procedimientos establecidos.Sin embargo, el departamento de Tecnologías de la Información se encarga de verificar constantemente que no existan ciberdelitos en cada uno de los procesadores de cada departamento para evitar cualquier tipo de ataque.

Gráfico 8. Verificación del cumplimiento de actividades del check list



Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga(2022)

De esta manera se identifica que muy pocas de las actividades evaluadas en el check list se cumplen al 100%. Sin embargo, la Gestión de incidentes posee el 40% de cumplimiento siendo así la actividad que menos se cumple. Puesto que, no se notifica cualquier debilidad de seguridad observada en los sistemas o servicios. Por otra parte, tampoco se establece una clasificación de los incidentes de seguridad de la información para identificar el impacto y el alcance del incidente. Del mismo modo, no responden ante los inconvenientes de seguridad de la información de acuerdo con los procedimientos establecidos. Sin embargo, los miembros del departamento de las Tecnologías de la Información se encargan de dar el soporte constante a los equipos.

Para un análisis profundo, las encuestas reflejaron información como soporte de las prácticas de gestión de la seguridad de la información de la empresa. De este modo, se detectó que existen vulnerabilidades en los departamentos en cuanto a políticas, normativas y falta de capacitación acerca del uso de las tecnologías de la información.

A pesar de, que existen políticas internas de la empresa para contrastar algún tipo de ataque pero que muchos de los empleados desconocen.

Tabla 18. Análisis de las encuestas

PREGUNTA	DEFINICIÓN	CATEGORÍA	1 (SI)	2 (NO)	3 (NO APLICA)
1	Acuerdo de confidencialidad	Gobierno y Cultura	15	3	2
2	Definición de responsabilidades		11	9	0
3	Políticas de TI		10	10	0
4	Política de uso privado		5	15	0
5	Medidas de seguridad	Modelo	12	8	0
6	Identificación de virus	Operativo y de	11	9	0
7	Gestión de redes	Negocios	6	13	1
8	Normativa de la S.I		4	16	0
9	Política para dispositivos		3	17	0
10	Protección de accesos		13	6	1
11	Pérdida del dispositivo		8	12	0
12	Ciberseguridad	Reporte y Tecnología	4	16	0
13	Acceso al sistema		4	15	1
14	Perfiles de acceso		12	5	3
15	Infraestructura de las T.I	Alineado con la Estrategia	9	11	0
16	Capacitación sobre T.I		3	17	0
17	Copias de seguridad		15	4	1

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

En el área de uso de la tecnología es fundamental revisar el acceso a los sistemas para un adecuado control del personal que está autorizado a obtener la información de la empresa. En este sentido toma gran importancia la seguridad informática ya que esta protege la privacidad de la información.

En las empresas públicas es común el robo de información y sobre todo cuando no existen suficientes controles. Por lo que, el departamento de tecnologías de la información tiene la tarea de mantener prevenidos a los funcionarios de la empresa en caso de ataques a su software. Del mismo modo, todos protegen a la empresa para mantener la información segura y evitar vulnerabilidades que afecten a la entidad.

El departamento de tecnologías de la información brinda el soporte oportuno a los dispositivos de la empresa y de esta manera crean barreras ante los ciberdelincuentes. Po lo tanto, es importante vigilar que los usuarios no caigan en páginas maliciosas que infecten los procesadores. De igual forma, son fundamentales las copias de seguridad en caso de pérdida de la información.

Tabla 19. Análisis de la encuesta por categoría

CATEGORÍA	PORCENTAJE DE CUMPLIMIENTO
Gobierno y Cultura	75%
Modelo Operativo y de Negocios	42%
Reporte y Tecnología	33%
Alineado con la estrategia	45%

Fuente: EP-EMAPA-A (2022)
Elaborado por: Mayorga (2022)

En la tabla 18 se puede identificar los porcentajes de cumplimiento por categoría. Por otra parte, existen actividades que no se cumplen ni en un 50%. En este sentido, hay la necesidad del análisis donde se muestre concretamente las vulnerabilidades de la empresa.

De este modo, existe un mayor análisis de las vulnerabilidades que tiene la empresa en cuanto a los procesos para la seguridad de la información.

Mediante los resultados de los datos que arrojan las encuestas las actividades no se cumplen moderadamente a excepción de las preguntas 1, 2, 5, 6, 10, 14 y 17 que cumplen con más del 50%. Pues, varios trabajadores han manifestado que no conocen sobre la normativa de seguridad de la información y cómo deben actuar

frente a cualquier incidente relacionado a la misma. En este sentido, el departamento de tecnologías de la información tiene en cuenta las medidas que deberán aplicar en caso de algún incidente.

Como instrumento de investigación se aplicó el alfa de Cronbach para medir la confiabilidad del análisis de los datos obtenidos. De este modo, se obtuvo un 0.60 calificando al análisis como bueno de acuerdo a la siguiente descripción.

Tabla 20. Análisis de fiabilidad de resultados

ALFA	α =	0,60
NÚMERO DE PREGUNTAS	K=	17
VARIANZA DE CADA ITEM	Vi=	4,38
VARIANZA TOTAL	Vt=	9,96

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Este análisis de los datos obtenidos en las encuestas presentó un coeficiente de fiabilidad bueno en esta investigación. Debido a que, las preguntas fueron planteadas de acuerdo a investigaciones realizadas por otros autores. También, las fuentes fueron confiables haciendo que la investigación sea veraz y seria. En este sentido, este análisis es importante para fortalecer aspectos importantes de la empresa para la seguridad de la información.

Una vez evaluados los procesos del sistema de seguridad de la información se procedió a obtener la calificación, porcentaje y en qué nivel de madurez se encuentra cada uno de ellos como se muestra en la siguiente tabla.

Tabla 21. Resumen de madurez de los procesos

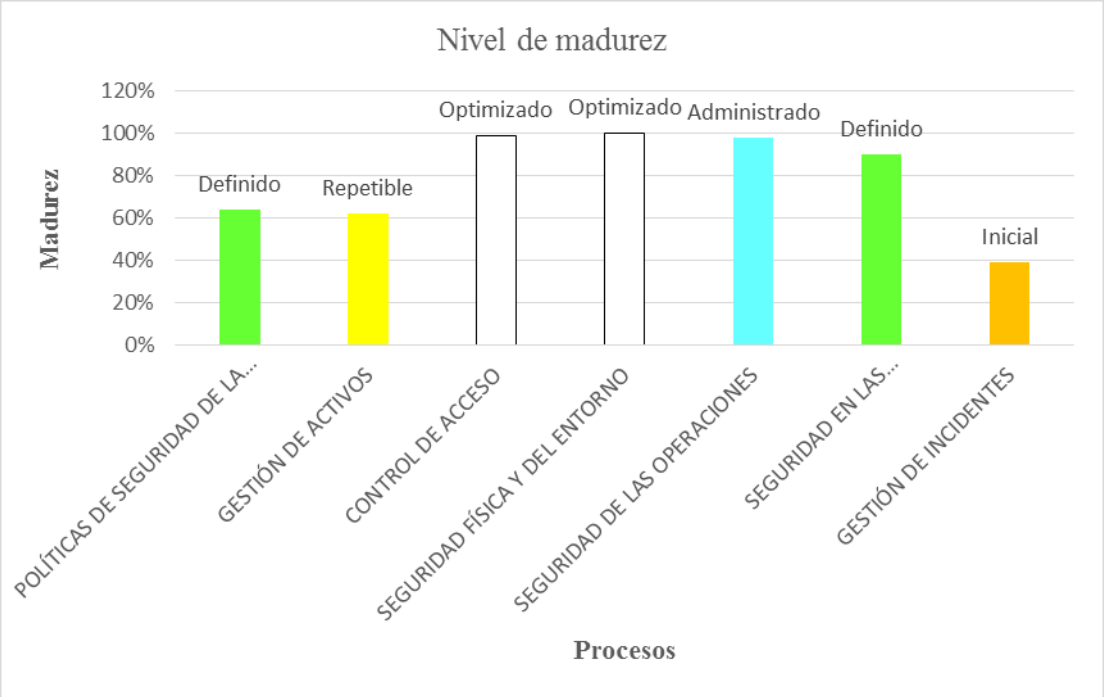
PROCESOS				
I. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	**Calificación**	**%**	**Madurez**	**Significado**
Dirección de gestión para la seguridad de la información			64%	Definido
1. ¿La institución ha implementado políticas de seguridad de la información?	0	0%		
2. ¿Las políticas de seguridad de la información son aprobadas por la administración?	2	50%		
3. ¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?	3	90%		
4. ¿Se revisa frecuentemente las políticas de seguridad de la información?	3	90%		
5. ¿Se establecen responsabilidades para la revisión y evaluación de las políticas?	3	90%		
II. GESTIÓN DE ACTIVOS				
Responsabilidad por los activos			62%	Repetible
6. ¿Disponen de un inventario de activos de información?	1	10%		
7. ¿Existen políticas relacionadas con el uso adecuado de los activos de información?	3	90%		
Clasificación de la información				
8. ¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?	1	10%		
Manejo de medios de almacenamiento				
9. ¿Los soportes de almacenamiento están en un entorno seguro y protegido?	5	100%		
10. ¿Los datos se almacenan en múltiples copias para reducir el riesgo de daño o pérdida?	5	100%		
III. CONTROL DE ACCESO				
Requisitos comerciales de control de acceso			99%	Optimizado
11. ¿Existen políticas de control de acceso en función a la seguridad de la información?	5	100%		
12. ¿Las políticas se basan en los requerimientos de la institución?	4	95%		
13. ¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?	5	100%		
Gestión de acceso de usuarios				
14. ¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?	5	100%		
15. ¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?	5	100%		
Control de acceso al sistema y a las aplicaciones				
16. ¿Se controla los datos a los que puede acceder un usuario en particular?	4	95%		
17. ¿El acceso es protegido contra varios intentos de inicio de sesión?	5	100%		
18. ¿Las contraseñas de los usuarios se cambian regularmente?	5	100%		
19. ¿La selección de contraseñas es compleja?	5	100%		
20. ¿Se restringe el acceso al código fuente del programa de la institución?	5	100%		

Fuente:EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Con los resultados obtenidos de la tabla 20 se puede evidenciar cuales son los procesos que más se cumplen dentro del sistema de seguridad de la información. Es así que, realizados los cálculos se pudo evidenciar que la EP-EMAPA-A tiene un 79% de madurez en los procesos evaluados de su sistema de seguridad de la información. En este sentido, la empresa cumple moderadamente con las buenas prácticas de control para la seguridad de la información.

Gráfico 9. Nivel de madurez por dominios



Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

A continuación se muestra el porcentaje de efectividad para los 42 procesos evaluados donde se puede evidenciar que 7 de ellos no están aprobados en la valoración realizada, esto equivale a un 17% de los procesos entre un 0% y 50% de efectividad. En este sentido, la empresa carece de algunos procesos estándar y en su lugar existen enfoques que tienden a ser aplicados de forma individual o caso por caso. El 83% restante se valora como aprobados ya que la mayor parte de los procesos se encuentran entre el 90% y 100% en la valoración de efectividad. Es así

que, la empresa implementa en mayor porcentaje los procesos en general, todo esto basado en la norma ISO/IEC 27002:2013.

Tabla 22. Procesos aprobados y no aprobados

Valor	Efectividad	Significado	Número	Madurez	Total
0	0%	Inexistente	4	No aprobados	17%
1	10%	Inicial	2		
2	50%	Repetible	1		
3	90%	Definido	6	Aprobados	83%
4	95%	Administrado	5		
5	100%	Optimizado	24		

Fuente: Elaboración propia

4.2 Narración del caso

1. ¿De qué manera asegura la información actualmente la EP-EMAPA-A?

El departamento de tecnologías de la información se encarga de mantener cada dispositivo funcional. Además, vela por la seguridad de la información manteniendo actualizados los antivirus de los dispositivos de cada departamento. También, dando mantenimiento constante a los servidores para evitar cualquier tipo de riesgo.

Por otra parte, garantizan la seguridad de la red ya que mantienen un control de registro de los dispositivos conectados. Además, no tienen acceso a la red todos los dispositivos sino solamente los que cuenten con el permiso correspondiente. Del mismo modo, cada área cuenta con su propio sistema operativo, por ejemplo, el área financiera maneja su sistema contable, el área comercial tiene un sistema diseñado para la misma. Pero la idea es que entre a trabajar ya un ERP que integre todos estos sistemas en un solo entrono y les permita trabajar ya en una misma base de datos.

Así mismo, se establecieron medios de comunicación internos entre el personal de la institución para facilitar la información requerida. Pues mencionan, que dan prioridad o establecen como métodos de comunicación el correo institucional Zimbra.

Todo funcionario de la EP-EMAPA-A debe manejar de manera confidencial la información interna de la empresa así no haya firmado ningún acuerdo hasta cuando deje de prestar sus servicios en la entidad. Además, los sistemas operativos que manejan deben ser utilizados solamente para fines de trabajo dentro de la empresa.

2. ¿Cuáles son las medidas de seguridad para evitar la filtración de personas no autorizadas?

Hasta el momento no han detectado algún tipo de filtración por personas no autorizadas. Tampoco, se ha detectado ningún tipo de ataque a sus sistemas y ningún intento de acceso a la información sin previa autorización.

Las medidas de seguridad para evitar la filtración de personas no autorizadas son en la parte física,primero su centro de datos está bastante protegido, se controla bastante el acceso a esa área, de hecho nadie puede tener acceso más que personal específicamente que pertenezca a ese departamento. Además a nivel lógico también se rigen en cuestión de reglas de acceso y permisos en el firewall. En este sentido, todo ese tipo de controles les permiten proteger la información ante personas no autorizadas.

También, se manejan bajo contraseñas y perfiles de usuario que ayudan a mantener controlado quién maneja la información. Así mismo, existe un control de los usuarios que acceden a la información constantemente.

La empresa utiliza medidas de proteccióncomo es la aplicación de copias de seguridad de la información importante de la entidad. Puesto que, los sistemas que manejan son utilizados por varios usuarios por esta razón efectúan controles en los accesos. Igualmente, para una mayor eficiencia yprotección del software se manejan con antivirus licenciados y que son renovados constantemente. Del mismo modo, como medida de control cuidan los puertos de entradaexterna como es en el caso de la utilización de USB en los dispositivos.

3. ¿Qué medidas de protección se han implementado dentro de la institución para la seguridad de la información?

La empresa implementa las Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, en este caso se puede mencionar la 410 de Tecnologías de la información como son:

410-01 Organización informática
410-02 Segregación de funciones
410-03 Plan informático estratégico de tecnología
410-04 Políticas y procedimientos
410-05 Modelo de información organizacional
410-06 Administración de proyectos tecnológicos
410-07 Desarrollo y adquisición de software aplicativo
410-08 Adquisiciones de infraestructura tecnológica
410-09 Mantenimiento y control de la infraestructura tecnológica
410-10 Seguridad de tecnología de información
410-11 Plan de contingencias
410-12 Administración de soporte de tecnología de información
410-13 Monitoreo y evaluación de los procesos y servicios
410-14 Sitio web, servicios de internet e intranet
410-15 Capacitación informática
410-16 Comité informático
410-17 Firmas electrónicas

Además, la empresa cuenta con bases respaldadas y guardadas dentro de medios físicos y digitales también debidamente protegidos.Las medidas de protección dentro de la institución para la seguridad de la información son básicamente en el tema de usuarios, contraseñas, manejo de perfiles. Es así que, mediante esos protocolos restringen el acceso de muchas personas.

Para mantener las medidas de protección que permitan desempeñar las actividades normalmente, en lo referente a la seguridad física de la institución se han implementado

varias medidas de seguridad a las zonas que contienen información confidencial o recursos de suma importancia como son accesos con claves.

4. ¿Cuáles son las buenas prácticas que implementa la empresa para mantener un buen control interno en los procesos de seguridad de la información?

Para mantener un buen manejo de los sistemas operativos que contienen la información la empresa implementa las buenas prácticas. Es así que, para mantener un buen control interno en los procesos de seguridad de la información principalmente se utiliza el manejo de contraseñas verificando que estas no sean muy débiles. Además el manejo de perfiles que cada persona tiene asignado, solamente su parte a la que debe acceder dentro de cada sistema. Entonces, no pueden acceder a toda la información ni los usuarios de la empresa y mucho menos personas externas.

Por otra parte, la empresa aplica acuerdos de confidencialidad solo en ciertos departamentos lo que ocasiona que no exista responsabilidad de la información que maneja cada uno de los usuarios. De esta manera, se demuestra la falta de seguridades al momento de entregar un dispositivo y un usuario.

La información de la empresa se maneja en diferentes sistemas operativos dependiendo de cada departamento. Además, los sistemas están habilitados de acuerdo a las necesidades de los funcionarios para evitar el acceso a toda la información de la empresa.

5. ¿De qué manera se podría mejorar la seguridad de la información en la empresa?

La EP-EMAPA-A no se rige a ninguna norma de seguridad de la información sino únicamente tienen certificación de la norma de calidad ISO 9001:2005. A pesar de esto se manejan bajo prácticas y políticas internas, dada la importancia de mantener segura la información. Ya que, si los sistemas de información internos son utilizados de manera incorrecta pueden causar problemas que afecten a la productividad y desarrollo.

Creo que sería bueno que en el área de tecnologías de la información cuenten con una persona certificada o especializada dentro de lo que es el tema de seguridad informática para que les sirva de apoyo para definir mejores políticas y a documentar ese tema. También sería bueno una capacitación para todo el personal de la empresa para que tenga conciencia sobre lo que es la seguridad informática y de la información.

El personal no conoce las medidas a seguir en caso de incidente de ciberseguridad lo que provoca un riesgo alto. Puesto que, los malware avanzan hasta provocar severos daños en los sistemas y procesadores ya sea por virus o dependiendo la situación en la que se vea comprometido el usuario.

4.3 Limitaciones del estudio

El presente análisis de caso ha tenido algunas limitaciones con respecto al tiempo de ejecución y recolección de información debido a la documentación que se debe hacer para poder obtener la colaboración de la empresa en cuanto a entrega de información, esto a causa de falta de tiempo por parte del señor gerente para revisar los documentos que fueron requeridos, debido a sus ocupaciones y compromisos fuera de la empresa. Esto causó un retraso considerable en el desarrollo de la investigación. Además, resultó complicado obtener la información necesaria porque el departamento de Tecnologías de la información no tenía documentada varia información que resulta importante y útil. En este sentido se encuentran anexados los únicos documentos que fueron proporcionados por la empresa de manera física.

CAPÍTULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- De acuerdo a la norma ISO/IEC 27002:2013 la empresa presenta un nivel moderado en su sistema de seguridad de la información que representa el 83% de cumplimiento de todos los procesos, sin embargo aún existen algunas falencias en sus procesos que no les permite llegar al 100% de efectividad. Además, la falta de conocimiento por parte del personal sobre seguridad de la información, hace que se convierta en una debilidad para la empresa y que el sistema de seguridad de la información no mejore

  Del mismo modo, la entidad no cuenta con registros de auditorías en tema de seguridad de la información así como tampoco cuentan con un profesional calificado en este tema que los pueda guiar y ayudar a estructurar un buen SGSI y que puedan calificar para obtener una certificación en seguridad de la información sino únicamente poseen la Norma de Calidad ISO 9001:2005. Además, la ausencia o desconocimiento por parte del personal de las normativas y políticas de seguridad hacen que la empresa sea más vulnerable ante cualquier ataque malicioso.

- El modelo de madurez basado en la norma ISO/IEC 27002:2013 aplicado para medir el nivel de madurez del sistema de seguridad de la información, permite conocer el estado real de la empresa frente a cualquier eventualidad. De este modo, se refleja que a pesar de no regirse a ninguna norma de seguridad vigente, cumplen moderadamente con los procesos de seguridad. Además, a partir de los resultados la empresa puede corregir y mejorar su sistema de seguridad de la información haciendo énfasis en los procesos que les falta aplicar.

Existe un porcentaje del 17% de procesos no aprobados que pueden ser corregidos si se establece un mejor control y uso de las buenas prácticas y políticas de seguridad de la información caso contrario seguirá existiendo esa brecha que no les permite a la empresa avanzar al nivel óptimo que requiere para salvaguardar por completo la información.

- Mediante los resultados obtenidos se puede recalcar que la empresa maneja una gran cantidad de información importante, pero debido a la falta de implementación de una norma que controle el sistema de seguridad de la información y el desconocimiento de las buenas prácticas sobre seguridad, los errores y las falencias van a seguir existiendo.

  Del mismo modo, la empresa no tiene la información de importancia, como políticas, inventario de activos o controles, debidamente documentados y archivados hacen que se les haga más difícil darse cuenta de los errores y falencias que tiene su sistema de seguridad, esto hace que actúen en el momento que tienen un problema en lugar de prevenirlo.

  Sin embargo, la empresa tiene un nivel optimizadodel control de acceso a los diferentes sistemas que manejan dentro de la entidad así como también cuentan con una óptima seguridad física y del entorno convirtiéndose esto en una fortaleza para la empresa.

5.2 Recomendaciones

- Implementar un mayor control sobre los procesos de manera adecuada y debidamente respaldada con relación al sistema de seguridad de la información de la empresa para alcanzar el nivel óptimo de madurez en todos los dominios y realizar evaluaciones continuamente para detectar las debilidades e implementar mejoras. Del mismo modo, capacitar al personal sobre seguridad de la información y sobre la responsabilidad que tienen al manejar cualquier recurso para el procesamiento de la información.

- Asesorar a todos los funcionarios sobre el riesgo que corre la empresa al divulgar información confidencial y con el mal manejo de los sistemas tecnológicos. Así mismo, documentar toda clase de control que se haga dentro del departamento de tecnologías de la información, ya que esto servirá para futuras comparaciones y seguir mejorando las buenas prácticas.

- En definitiva, es de vital importancia contar con un profesional especializado en seguridad de la información para mejorar el proceso de control de incidentes. También, es necesario realizar un inventario de activos ya que son de gran utilidad al momento de entregar a cada usuario. Así mismo, es muy importante implementar normas y políticas vigentes, que se encuentren debidamente aprobadas y documentadas, pero sobre todo que estas sean divulgadas para el conocimiento de todo el personal de la empresa y así podrán saber cómo actuar ante posibles amenazas que pueden ocurrir de manera intencional o no.

REFERENCIAS BIBLIOGRÁFICAS

ABNT, A. B. (2005). *Ostec seguro digital de resultados*. Obtenido de https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/

Advisera, E. S. (2022). *Advisera*. Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Aladro, V. E. (2011). La Teoría de la Información ante las nuevas tecnologías de la comunicación. *CIC, Cuadernos de Información y Comunicación, 16*, 83-93.

Alvarado, N. (28 de noviembre de 2018). *Tecnología contra el crimen: Entusiasmo con cautela y criterio*. Obtenido de https://blogs.iadb.org/seguridad-ciudadana/es/tecnologia-contra-el-crimen-entusiasmo-con-criterio/

ATICO34. (2022). *Norma ISO 27001 sobre Seguridad y Privacidad de la Información*. Obtenido de https://protecciondatos-lopd.com/empresas/norma-iso-27001/

Briceño, E. V. (2021). *Seguridad de la Información.* Área de Innovación y Desarrollo. doi:https://doi.org/10.17993/tics.2021.4

Bustamante, G. &. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*(6), 71-76. Obtenido de https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206

Calder, A. (2017). *Nueve pasos para el éxito. Una visión de conjunto para la aplicación de la Iso 27001:2013.* Reino Unido: IT Governance Publishing.

Cañedo, R. R. (2005). *La Informática, la Computación y la Ciencia de la Información: Una Alianza para el Desarrollo.* Acimed, 13(5) 1-1.

Castromán, J., & Porto, N. (2005). Responsabilidad Social y Control Interno. *Revista Universo Contábil, 1*(2), 86-101.

Cepreven. (2022). *Seguridad Informática. Ciberseguridad Empresas*. Obtenido de https://www.cepreven.com/cuestionario-ciberseguridad/

Corda, M. C. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave, 7*(nº. 1). doi: https://doi.org/10.24215/18539912e032

Correa, V. M. (2008). *Fundamentos de la Teoría de la Información.* Medellín: ITM.

Costas, S. J. (2014). *Seguridad Informática.* Madrid: RA-MA, S.A. Obtenido de https://elibro.net/es/ereader/uta/62452

Díaz Durán, M., Gil, J., & Vílchez Olivares, P. (Julio de 2010). Hacia la convergencia mundial del marco conceptual para la preparación de los estados financieros. *Contabilidad y Negocios, 5*(9).

Ealde. (17 de diciembre de 2020). Obtenido de https://www.ealde.es/iso-27001-para-que-sirve/

EGSI. (2020). Guía para la Implementación del Esquema Gubernamental de Seguridad de la Información.

Escrivá, G. R. (2013). *Seguridad Informática.* Obtenido de https://elibro.net/es/ereader/uta/43260

Excellence, I. (15 de abril de 2021). *SGSI* . Obtenido de SGSI Blog especializado en Sistemas de Gestión de Seguridad Informática: https://www.pmg-ssi.com/2021/04/aspectos-a-tener-en-cuenta-antes-de-implantar-un-sistema-de-seguridad-de-la-informacion/

Fuentes, L. F. (10 de abril de 2008). Malware, una amenaza de internet. *Revista digital universitaria, 9*(4), 1-9. Obtenido de https://www.ru.tic.unam.mx/bitstream/handle/123456789/1368/art22_2008.pdf?sequence=1&isAllowed=y

Galaz, Y. (2015). Marco de Referencia para la Implementación, Gestión y Control Interno. *Deloitte*.

GlobalSUITE. (3 de septiembre de 2021). *Estándares y Normas ISO para Mejorar la Ciberseguridad. GlobalSUITESolution*. Obtenido de https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-laciberseguridad/

Grajales, L., & León, M. (2016). Diagnóstico del grado de madurez de los controles de seguridad establecidos en la norma NTC ISO/IEC 27001:2013 para asegurar la confidencialidad, integridad, disponibilidad y control de la información en instituciones públicas de educación preescolar. *Tesis de Grado.* Universidad Católica de Pereira, Pereira. Obtenido de https://repositorio.ucp.edu.co/bitstream/10785/3871/1/DDMIST3.pdf

Hernández, Z. J., & Flórez, S. J. (2011). Seguridad física y lógica en el manejo de la información policial. *Revista Logos, Ciencia & Tecnología, 3*(1), 222-223. Obtenido de http://www.redalyc.org/articulo.oa?id=517751801016

ISO 27000, E. (13 de 08 de 2022). *Portal ISO 27001 en Español*. Obtenido de https://www.iso27000.es/sgsi.html

ISOTools. (13 de abril de 2015). *SGSI*. Obtenido de SGSI Blog especializado en Ssitemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/

ISOTOOLS. (7 de febrero de 2018). *¿Cómo ha Cambiado el Nuevo COSO ERM 2017?* Obtenido de https://www.isotools.org/2018/02/07/ha-cambiado-nuevo-cosoerm-

ISOTools. (2022). Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Isotools. (2022). *Plataforma tecnológica para la gestión de la excelencia*. Obtenido de https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

Izaguirre Olmedo, J. &. (2018). Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal, 3*(9), 172-181. doi:https://doi.org/10.33890/innova.v3.n9.2018.837

Izquierdo, F. F. (2000). La Historia Moderna y Nuevas Tecnologías de la Información y las Comunicaciones. *Cuaderno de Historia Moderna*(24, 11-31).

Jiménez, R. A. (2013). Desarollo tecnológico y su impacto en el proceso de globalización económica: Retos y oportunidades para los países en desarrollo en el marco de la era del acceso. *Visión Gerencial, 1*, 123-150.

Ladino, M. V., & López, A. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. *Scientia Et Technica, XVII*(47), 334-339.

Laski, J. P. (julio-diciembre de 2006). El control interno como estrategia de aprendizaje organizacional: El modelo COSO y sus alcances en América Latina. *Revista Gestión y Estrategia*(30), 9-24. Obtenido de https://doi.org/10.24275/uam/azc/dcsh/gye/2006n30/Laski (Original work published 1 de diciembre de 2006)

López, R. (1998). Crítica de la Teoría de la Información: Integración y Fragmentación en el Estudio de la Comunicación. *inta moebio, 3*, 24-30.

Maza. (7 de septiembre de 2020). *El Impacto de las Tecnologías Exponenciales a la Seguridad Nacional e Internacional/Foreign Affairs Latinoamérica*. Obtenido de https://revistafal.com/el-impacto-de-las-tecnologias-exponenciales-a-la-

Mesquida, A. L., & Cabestrero, I. (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. *REICIS. Revista Española de Innovación, 6*(3), 25-34. Obtenido de https://www.redalyc.org/articulo.oa?id=92218768002

MINTEL. (2018). *Libro Blanco de Territorios Digitiales en Ecuador.*

Morán, G. L., & Castro, M. I. (2017). *Modelo de plan estratégico de sistemas para la gestión y organización a través de una plataforma informática* (Vol. 1). 3Ciencias.

Murillo, L. N., & Erazo, J. (2019). Sistema de Control Interno con Enfoque. *Revista Arbitrada Interdisciplinaria Koinoníia, 4*(2), 241.

Navarro, M., & Díaz, L. (2014). *Sistemas de información en la empresa.*

Oberheide, J. C., & Jahanian, F. (2008). CloudAV: N-Version Antivirus in. *USENIX Security Symposium*, 91-106.

Ordoñez, L. (2007). El desarrollo tecnológico en la historia. *Areté, XIX*(2), 187-209.

Pazmiño, V. L. (2015). *Calidad de la Gestión en la Seguridad de la Información basada en la Norma ISO/IEC 27001, EN.* Quito.

Pérez, E. M. (Mayo de 2014). Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. *Ingeniería Industrial, 35*(2), 146-158. Obtenido de http://scielo.sld.cu/pdf/rii/v35n2/rii04214.pdf

PMG, S. (3 de agosto de 2017). *Seguridad de la Información*. Obtenido de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

PwC. (2018). *Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018.* Obtenido de https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html

Quevedo, V. C. (2002). Midiendo el impacto. *Ciencia, Innovación y Desarrollo, 7(1), 1-10*.

Ramírez, A. C. (2021). *Riesgo Tecnológico y su Impacto para las Organizaciones parte I/ Revista Seguridad.* Obtenido de https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-

Rivas, M. G. (julio-diciembre de 2011). Modelos contemporáneos de control interno. Fundamentos teóricos. *Observatorio Laboral*, *4*(8), 115136.

Rodríguez, I. (31 de 10 de 2020). *Auditool.* Obtenido de https://www.auditool.org/blog2/auditoria-de-ti/7469-medidas-de-ciberseguridad-que-todo-auditor-debe-verificar

Romero, C. M., & Castillo, M. M. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades* (primera ed.). Manabí: 3 Ciencias Editorial Área de Innovación y Desarrollo, S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Ruiz, M. L. (22 de mayo de 2019). *Psicología y mente*. Obtenido de https://psicologiaymente.com/miscelanea/alfa-de-cronbach

Russell, J. (2022). *NQA Organismo de certificación global.* Recuperado el 2022, de https://www.nqa.com/es-mx/certification/standards/iso-27001#:~:text=La%20ISO%2027001%3A2013%20es%20la%20norma%20internacional%20que%20proporciona,informaci%C3%B3n%2C%20as%C3%AD%20como%20cumplimiento%20legal.

Sánchez, A. F. (2018). Plan de implementación de la ISO/IEC 27001:2013, en la fundación universitaria San Mateo. *Trabajo final de máster (MISTIC).* Universidad Oberta de Catalunya, Catalunya.

Solarte, F. N., & Enriquez, E. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL-RTE, 28*(5), 492-507.

TI, R. B. (2018). *Un 39% de las Empresas de la UE Sufre Robo de Datos. Revista Byte*. Obtenido de https://revistabyte.es/actualidad-it/empresas-sufre-robo-de-

Yirda, A. (7 de febrero de 2021). *ConceptoDefinición*. Obtenido de https://conceptodefinicion.de/alfa-de-cronbach/.

ANEXOS

Anexo 1

Entrevista

Persona: Ing. Alex Acurio **Cargo:** Jefe de Departamento de Tecnologías de la Información

1. ¿Cómo es su sistema de gestión de seguridad de la información?

Bueno nosotros gestionamos la seguridad mediante políticas, mediante establecer reglas de acceso, usuarios, contraseñas, manejo de perfiles entonces nos basamos en una serie de actividades y acciones que nos permiten proteger la información de acá.

2. ¿Qué sistemas informáticos se maneja en la empresa?

Actualmente manejamos varios sistemas informáticos cada área ehh… tiene su propio sistema, por ejemplo dentro del área comercial manejan lo que es el sistema diseñado o designado para esa área específicamente igual lo que es el sistema financiero por ejemplo pero la idea es que entre a trabajar ya un ERP que integre ya todos estos sistemas dentro de un solo entorno y nos permita trabajar dentro de una misma base de datos.

3. ¿Cuáles son los inconvenientes más comunes que ha detectado la empresa en cuanto a tecnología de la información?

Bueno uno de nuestros inconvenientes más comunes últimamente han sido nuestros compañeros osea el personal interno de acá de la empresa que a veces les llega correos maliciosos y ellos dan clic y por ahí se nos infecta algunas máquinas, creo que eso es en lo principal que tenemos que trabajar no, capacitar a los usuarios para que eso no pase.

4. ¿Ha existido algún tipo de robo de información o problema similar en la empresa?

Tuvimos un problema con un servidor en el que nos cayó un malware ehhm… nos secuestró la información pero gracias a que tenemos respaldos pudimos reestablecer ese servidor y ponerlo a operar nuevamente.

5. ¿Qué tan importante es la seguridad informática para la empresa?

La información es vital para nosotros porque tenemos información de los usuarios de las personas de aquí de la ciudad de Ambato los cuales deben tener sus datos protegidos para que no vaya a caer en manos de terceros y puedan hacer mal uso de la misma, por eso protegemos nuestros servidores para mantener segura la información.

6. ¿Qué normas o leyes aplica la empresa para gestionar la seguridad de la información?

Bueno de momento no estamos aplicando ninguna norma específica nos guiamos más en las prácticas o políticas que las tenemos establecidas aquí dentro de la unidad para lo que es la seguridad de la información.

7. ¿Cuáles son las medidas de seguridad que aplica la empresa para proteger la información interna?

Las medidas son básicamente lo que son usuarios, contraseñas, manejo de perfiles, políticas de seguridad en nuestro firewall, reglas de acceso entonces todo eso restringe el acceso de terceros hacia acá hacia nuestra empresa, entonces podemos proteger la información.

8. ¿Cada qué tiempo se evalúa el sistema de seguridad de la información?

Bueno no tenemos determinado o definido una periodicidad específica pero si constantemente estamos preocupados por lo que es el tema de seguridad y evaluando las reglas de acceso y los perfiles que tienen los usuarios y ese tipo de cosas.

9. ¿Cuáles son los problemas o necesidades que tiene la empresa en cuanto a seguridad de la información?

Justamente yo creo que una falta de capacitación y de conciencia del personal de acá acerca de los temas de seguridad y los datos que estamos acá manejando, además de que sería bueno contar con una persona certificada o especializada en el tema de seguridad informática para que nos guíe en ese tema.

Anexo

Tabla check list

PREGUNTAS	SI	NO	OBSERVACIÓN
I. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
Dirección de gestión para la seguridad de la información			
1. ¿La institución ha implementado políticas de seguridad de la información?		X	
2. ¿Las políticas de seguridad de la información son aprobadas por la administración?	X		
3. ¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?	X		
4. ¿Se revisa frecuentemente las políticas de seguridad de la información?	X		
5. ¿Se establecen responsabilidades para la revisión y evaluación de las políticas?	X		
II. GESTIÓN DE ACTIVOS			
Responsabilidad por los activos			
6. ¿Disponen de un inventario de activos de información?	X		
7. ¿Existen políticas relacionadas con el uso adecuado de los activos de información?	X		
Clasificación de la información			
8. ¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?		X	
Manejo de medios de almacenamiento			
9. ¿Los soportes de almacenamiento están en un entorno seguro y protegido?	X		
10. ¿Los datos se almacenan en múltiples copias para reducir el riesgo de daño o pérdida?	X		
III. CONTROL DE ACCESO			
Requisitos comerciales de control de acceso			
11. ¿Existen políticas de control de acceso en función a la seguridad de la información?	X		

12. ¿Las políticas se basan en los requerimientos de la institución?	X		
13. ¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la	X		
Gestión de acceso de usuarios			
14. ¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?	X		
15. ¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?	X		
Control de acceso al sistema y a las aplicaciones			
16. ¿Se controla los datos a los que puede acceder un usuario en particular?	X		
17. ¿El acceso es protegido contra varios intentos de inicio de sesión?	X		
18. ¿Las contraseñas de los usuarios se cambian regularmente?	X		
19. ¿La selección de contraseñas es compleja?	X		
20. ¿Se restringe el acceso al código fuente del programa de la institución?	X		
IV. SEGURIDAD FÍSICA Y DEL ENTORNO			
Áreas Seguras			
21. ¿Los perímetros del edificio de la institución son físicamente sólidos?	X		
22. ¿Existe un área de recepción para controlar el acceso físico al edificio?	X		
23. ¿Implementan controles de acceso a áreas donde se almacena información confidencial de la institución?	X		
24. ¿Mantienen seguridad en puertas, escritorios y archivadores de la institución?	X		
25. ¿Cuentan con un plan de seguridad para evitar daños por desastres naturales o ataques maliciosos a la institución?	X		
26. ¿Las áreas donde el personal desarrolla sus actividades son seguras?	X		
Equipo			
27. ¿Los equipos están ubicados en sitios adecuados para reducir el acceso innecesario a las áreas de trabajo?	X		

28. ¿Las instalaciones de almacenamiento están protegidas para evitar accesos no autorizados?	X		
29. ¿Los equipos están protegidos contra interrupciones causadas por fallas en los servicios públicos (electricidad, telecomunicaciones, agua)?	X		
30. ¿El cableado está protegido contra interceptaciones, interferencias o daños?	X		
31. ¿Cuentan con una programación de mantenimiento de los equipos informáticos?	X		
32. ¿Se identifica a los usuarios que se les permite la salida de los activos fuera de la institución?		X	
33. ¿Se mantiene un control a los activos que están fuera de las instalaciones?	X		
V. SEGURIDAD DE LAS OPERACIONES			
Protección contra malware			
34. ¿Se implementan controles para evitar el uso de sitios web maliciosos o sospechosos?	X		
Copia de seguridad			
35. ¿Las copias de seguridad se almacenan en un lugar seguro?	X		
VI. SEGURIDAD EN LAS COMUNICACIONES			
Gestión de la seguridad de la red			
36. ¿Las redes son administradas y controladas para proteger la información de la institución?	X		
37. ¿Se monitorea periódicamente la capacidad del proveedor de servicios de red?	X		
VII. GESTIÓN DE INCIDENTES			
Gestión de incidentes y mejoras de seguridad de la información			
38. ¿Se establecen responsabilidades para desarrollar los procedimientos establecidos en la institución?	X		
39. ¿Se reportan eventos o incidentes de seguridad de la información?	X		
40. ¿Se notifica cualquier debilidad de seguridad observada en los sistemas o servicios?		X	
41. ¿Se establece una clasificación de los incidentes de seguridad de la información para identificar el impacto y el alcance del incidente?		X	
42. ¿Los incidentes de seguridad de la información se responden de acuerdo con los procedimientos establecidos?		X	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 3

Tabla. Preguntas del check list categorizadas

Pregunta	Dimensión o Categoría
1. ¿La institución ha implementado políticas de seguridad de la información?	Políticas de Seguridad de la Información
2. ¿Las políticas de seguridad de la información son aprobadas por la administración?	Políticas de Seguridad de la Información
3. ¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?	Políticas de Seguridad de la Información
4. ¿Se revisa frecuentemente las políticas de seguridad de la información?	Políticas de Seguridad de la Información
5. ¿Se establecen responsabilidades para la revisión y evaluación de las políticas?	Políticas de Seguridad de la Información
6. ¿Disponen de un inventario de activos de información?	Gestión de Activos
7. ¿Existen políticas relacionadas con el uso adecuado de los activos de información?	Gestión de Activos
8. ¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?	Gestión de Activos
9. ¿Los soportes de almacenamiento están en un entorno seguro y protegido?	Gestión de Activos
10. ¿Los datos se almacenan en múltiples copias para reducir el riesgo de daño o pérdida?	Gestión de Activos
11. ¿Existen políticas de control de acceso en función a la seguridad de la información?	Control de Acceso
12. ¿Las políticas se basan en los requerimientos de la institución?	Control de Acceso
13. ¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?	Control de Acceso
14. ¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?	Control de Acceso
15. ¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?	Control de Acceso
16. ¿Se controla los datos a los que puede acceder un usuario en particular?	Control de Acceso

17. ¿El acceso es protegido contra varios intentos de inicio de sesión?	Control de Acceso
18. ¿Las contraseñas de los usuarios se cambian regularmente?	Control de Acceso
19. ¿La selección de contraseñas es compleja?	Control de Acceso
20. ¿Se restringe el acceso al código fuente del programa de la institución?	Control de Acceso
21. ¿Los perímetros del edificio de la institución son físicamente sólidos?	Seguridad Física y del Entorno
22. ¿Existe un área de recepción para controlar el acceso físico al edificio?	Seguridad Física y del Entorno
23. ¿Implementan controles de acceso a áreas donde se almacena información confidencial de la institución?	Seguridad Física y del Entorno
24. ¿Mantienen seguridad en puertas, escritorios y archivadores de la institución?	Seguridad Física y del Entorno
25. ¿Cuentan con un plan de seguridad para evitar daños por desastres naturales o ataques maliciosos a la institución?	Seguridad Física y del Entorno
26. ¿Las áreas donde el personal desarrolla sus actividades son seguras?	Seguridad Física y del Entorno
27. ¿Los equipos están ubicados en sitios adecuados para reducir el acceso innecesario a las áreas de trabajo?	Seguridad Física y del Entorno
28. ¿Las instalaciones de almacenamiento están protegidas para evitar accesos no autorizados?	Seguridad Física y del Entorno
29. ¿Los equipos están protegidos contra interrupciones causadas por fallas en los servicios públicos (electricidad, telecomunicaciones, agua)?	Seguridad Física y del Entorno
30. ¿El cableado está protegido contra interceptaciones, interferencias o daños?	Seguridad Física y del Entorno
31. ¿Cuentan con una programación de mantenimiento de los equipos informáticos?	Seguridad Física y del Entorno
32. ¿Se identifica a los usuarios que se les permite la salida de los activos fuera de la institución?	Seguridad Física y del Entorno
33. ¿Se mantiene un control a los activos que están fuera de las instalaciones?	Seguridad Física y del Entorno
34. ¿Se implementan controles para evitar el uso de sitios web maliciosos o sospechosos?	Seguridad de las Operaciones
35. ¿Las copias de seguridad se almacenan en un lugar	Seguridad de las Operaciones

seguro?	
36. ¿Las redes son administradas y controladas para proteger la información de la institución?	Seguridad de las Comunicaciones
37. ¿Se monitorea periódicamente la capacidad del proveedor de servicios de red?	Seguridad de las Comunicaciones
38. ¿Se establecen responsabilidades para desarrollar los procedimientos establecidos en la institución?	Gestión de Incidentes
39. ¿Se reportan eventos o incidentes de seguridad de la información?	Gestión de Incidentes
40. ¿Se notifica cualquier debilidad de seguridad observada en los sistemas o servicios?	Gestión de Incidentes
41. ¿Se establece una clasificación de los incidentes de seguridad de la información para identificar el impacto y el alcance del incidente?	Gestión de Incidentes
42. ¿Los incidentes de seguridad de la información se responden de acuerdo con los procedimientos establecidos?	Gestión de Incidentes

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 4

Tabla. Detalle de análisis check List

CATEGORÍA	PREGUNTA	CUMPLE
Políticas de Seguridad de la Información	1	2
Políticas de Seguridad de la Información	2	1
Políticas de Seguridad de la Información	3	1
Políticas de Seguridad de la Información	4	1
Políticas de Seguridad de la Información	5	1
Gestión de Activos	6	1
Gestión de Activos	7	1
Gestión de Activos	8	2
Gestión de Activos	9	1
Gestión de Activos	10	1
Control de Acceso	11	1
Control de Acceso	12	1
Control de Acceso	13	1
Control de Acceso	14	1
Control de Acceso	15	1
Control de Acceso	16	1
Control de Acceso	17	1
Control de Acceso	18	1
Control de Acceso	19	1
Control de Acceso	20	1
Seguridad Física y del Entorno	21	1
Seguridad Física y del Entorno	22	1
Seguridad Física y del Entorno	23	1
Seguridad Física y del Entorno	24	1
Seguridad Física y del Entorno	25	1
Seguridad Física y del Entorno	26	1
Seguridad Física y del Entorno	27	1
Seguridad Física y del Entorno	28	1
Seguridad Física y del Entorno	29	1
Seguridad Física y del Entorno	30	1
Seguridad Física y del Entorno	31	1
Seguridad Física y del Entorno	32	2
Seguridad Física y del Entorno	33	1
Seguridad de las Operaciones	34	1
Seguridad de las Operaciones	35	1
Seguridad en las Comunicaciones	36	1
Seguridad en las Comunicaciones	37	1
Gestión de Incidentes	38	1
Gestión de Incidentes	39	1
Gestión de Incidentes	40	2
Gestión de Incidentes	41	2
Gestión de Incidentes	42	2

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 5

Tabla Tabulación check list categoría políticas de seguridad de la información

	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
	X	F	FR	%	F
SI	1	4	0,8	80	4
NO	2	1		0	5
TOTAL		5	0,8	80	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 6

Tabla Tabulación check list categoría gestión de activos

	GESTIÓN DE ACTIVOS				
	X	F	FR	%	F
SI	1	4	0,8	80	4
NO	2	1		0	5
TOTAL		5	0,8	80	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 7

Tabla Tabulación check list categoría control de acceso

	CONTROL DE ACCESO				
	X	F	FR	%	F
SI	1	10	1	100	10
NO	2			0	10
TOTAL		10	1	100	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 8

Tabla Tabulación check list categoría seguridad física y del entorno

	SEGURIDAD FÍSICA Y DEL ENTORNO				
	X	F	FR	%	F
SI	1	12	0,92	92	12
NO	2	1		0	13
TOTAL		13	0,92	92	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 9

Tabla Tabulación check list categoría seguridad de las operaciones

	SEGURIDAD DE LAS OPERACIONES				
	X	**F**	**FR**	**%**	**F**
SI	1	2	1,00	100	2
NO	2			0	2
TOTAL		2	1,00	100	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 10

Tabla Tabulación check list categoría seguridad de las comunicaciones

	SEGURIDAD EN LAS COMUNICACIONES				
	X	**F**	**FR**	**%**	**F**
SI	1	2	1,00	100	2
NO	2			0	2
TOTAL		2	1,00	100	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 11

Tabla Tabulación check list categoría gestión de incidentes

	GESTIÓN DE INCIDENTES				
	X	**F**	**FR**	**%**	**F**
SI	1	2	0,40	40	2
NO	2	3		0	5
TOTAL		5	0,40	40	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 12

Tabla Detalle análisis aplicación de encuestas

Nº	ENCUESTADOS	CARGO	PREGUNTA 1	PREGUNTA 2	PREGUNTA 3	PREGUNTA 4	PREGUNTA 5	PREGUNTA 6	PREGUNTA 7	PREGUNTA 8	PREGUNTA 9	PREGUNTA 10	PREGUNTA 11	PREGUNTA 12	PREGUNTA 13	PREGUNTA 14	PREGUNTA 15	PREGUNTA 16	PREGUNTA 17	SUMA
1	Ricardo Rivera	Analista Técnico	1	2	2	2	1	1	2	2	2	1	1	1	1	1	1	2	1	24
2	Priscila Aguilar	Asistente Administrativo	1	2	2	2	2	1	2	1	2	1	2	1	2	1	2	1	1	26
3	Darwin Narváez	Analista Técnico	1	2	1	2	2	1	2	2	2	1	2	2	1	1	2	2	1	27
4	Daniel Ipiales	Analista de TIC	2	2	2	2	2	1	1	1	2	2	2	2	1	1	1	2	1	27
5	Alexandra Chávez	Jefe de atención al usuario	1	1	1	2	1	2	2	2	2	3	1	2	2	1	1	2	1	27
6	Blanshy Ortega	Jefe Medición y facturación	1	1	1	2	1	2	2	2	2	1	1	2	2	1	1	2	1	25
7	Andrea Jácome	Asistente comercial	1	1	1	2	2	2	2	2	2	1	1	2	2	1	2	2	1	27
8	Elizabeth Chicaiza	Analista Técnico	1	2	2	2	2	2	1	2	2	2	2	2	2	3	1	2	1	31
9	Milton Salinas	Analista Técnico	2	2	1	1	1	2	2	2	2	1	2	2	2	2	2	2	1	29
10	Dacy Guerrero	Analista Técnico	1	1	2	2	1	2	2	2	2	1	2	2	2	2	2	2	2	30
11	Pamela Páliz	Asistente Administrativo	1	1	1	2	1	1	1	1	2	2	2	2	3	3	1	1	1	26
12	Martín Córdova	Jefe de Talento Humano	1	2	2	2	1	1	3	2	2	2	2	1	2	3	2	2	2	32
13	María Zurita	Analista de Talento Humano	1	2	2	2	2	1	1	2	2	2	2	2	2	1	1	2	1	28
14	David Carrasco	Contador General	1	1	1	1	1	1	2	2	2	1	1	2	2	2	2	2	1	25
15	Lilian Gamboa	Analista Financiero	2	2	2	2	1	2	1	2	2	1	2	2	2	2	2	2	1	30
16	Vanessa Manzano	Analista Técnico	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17
17	Danny Suárez	Inspector de Campo	1	1	2	2	2	1	2	2	1	1	1	2	2	1	1	2	3	27
18	Gladys Andocilla	Analista Técnico	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	31
19	Mauricio Hidalgo	Inspector de Campo	3	1	1	1	1	1	2	2	2	1	1	2	2	1	2	2	2	27
20	Ramiro Freire	Inspector de Campo	3	1	1	1	1	2	2	2	1	1	2	2	2	1	2	2	2	28
	ANÁLISIS DE DATOS		15	11	10	5	12	11	6	4	3	13	8	4	4	12	9	3	15	
	PORCENTAJE DE ANÁLISIS		75%	55%	50%	25%	60%	55%	30%	20%	15%	65%	40%	20%	20%	60%	45%	15%	75%	

Fuente: EP-EMAPA-A (2022)

Elaborado por: Mayorga (2022)

Anexo 13

Tabla. Resumen de madurez de los procesos

PROCESOS				
I. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	**Calificación**	**%**	**Madurez**	**Significado**
Dirección de gestión para la seguridad de la información			64%	Definido
1. ¿La institución ha implementado políticas de seguridad de la información?	0	0%		
2. ¿Las políticas de seguridad de la información son aprobadas por la administración?	2	50%		
3. ¿Las políticas de seguridad de la información son comunicadas oportunamente a los empleados de la institución?	3	90%		
4. ¿Se revisa frecuentemente las políticas de seguridad de la información?	3	90%		
5. ¿Se establecen responsabilidades para la revisión y evaluación de las políticas?	3	90%		
II. GESTIÓN DE ACTIVOS				
Responsabilidad por los activos			62%	Repetible
6. ¿Disponen de un inventario de activos de información?	1	10%		
7. ¿Existen políticas relacionadas con el uso adecuado de los activos de información?	3	90%		
Clasificación de la información				
8. ¿La información se clasifica en términos de valor, criticidad y sensibilidad a la divulgación o modificación no autorizadas?	1	10%		
Manejo de medios de almacenamiento				
9. ¿Los soportes de almacenamiento están en un entorno seguro y protegido?	5	100%		
10. ¿Los datos se almacenan en múltiples copias para reducir el riesgo de daño o pérdida?	5	100%		
III. CONTROL DE ACCESO				
Requisitos comerciales de control de acceso			99%	Optimizado
11. ¿Existen políticas de control de acceso en función a la seguridad de la información?	5	100%		
12. ¿Las políticas se basan en los requerimientos de la institución?	4	95%		
13. ¿Se han delimitado perfiles de acceso a los usuarios para el acceso a los sistemas que maneja la empresa?	5	100%		
Gestión de acceso de usuarios				
14. ¿Existe un proceso de registro y cancelación de registro de usuario para permitir la asignación de derechos de acceso?	5	100%		
15. ¿Mantienen un registro de los accesos otorgados al usuario para acceder a los sistemas?	5	100%		
Control de acceso al sistema y a las aplicaciones				
16. ¿Se controla los datos a los que puede acceder un usuario en particular?	4	95%		
17. ¿El acceso es protegido contra varios intentos de inicio de sesión?	5	100%		
18. ¿Las contraseñas de los usuarios se cambian regularmente?	5	100%		
19. ¿La selección de contraseñas es compleja?	5	100%		
20. ¿Se restringe el acceso al código fuente del programa de la institución?	5	100%		

IV. SEGURIDAD FÍSICA Y DEL ENTORNO				
Áreas Seguras			100%	Optimizado
21. ¿Los perímetros del edificio de la institución son físicamente sólidos?	5	100%		
22. ¿Existe un área de recepción para controlar el acceso físico al edificio?	5	100%		
23. ¿Implementan controles de acceso a áreas donde se almacena información confidencial de la institución?	5	100%		
24. ¿Mantienen seguridad en puertas, escritorios y archivadores de la institución?	5	100%		
25. ¿Cuentan con un plan de seguridad para evitar daños por desastres naturales o ataques maliciosos a la institución?	5	100%		
26. ¿Las áreas donde el personal desarrolla sus actividades son seguras?	5	100%		
Equipo				
27. ¿Los equipos están ubicados en sitios adecuados para reducir el acceso innecesario a las áreas de trabajo?	5	100%		
28. ¿Las instalaciones de almacenamiento están protegidas para evitar accesos no autorizados?	5	100%		
29. ¿Los equipos están protegidos contra interrupciones causadas por fallas en los servicios públicos (electricidad, telecomunicaciones, agua)?	5	100%		
30. ¿El cableado está protegido contra interceptaciones, interferencias o daños?	5	100%		
31. ¿Cuentan con una programación de mantenimiento de los equipos informáticos?	4	95%		
32. ¿Se identifica a los usuarios que se les permite la salida de los activos fuera de la institución?	5	100%		
33. ¿Se mantiene un control a los activos que están fuera de las instalaciones?	5	100%		
V. SEGURIDAD DE LAS OPERACIONES				
Protección contra malware			98%	Administrado
34. ¿Se implementan controles para evitar el uso de sitios web maliciosos o sospechosos?	3	95%		
Copia de seguridad				
35. ¿Las copias de seguridad se almacenan en un lugar seguro?	5	100%		
VI. SEGURIDAD EN LAS COMUNICACIONES				
Gestión de la seguridad de la red			90%	Definido
36. ¿Las redes son administradas y controladas para proteger la información de la institución?	3	90%		
37. ¿Se monitorea periódicamente la capacidad del proveedor de servicios de red?	3	90%		
VII. GESTIÓN DE INCIDENTES				
Gestión de incidentes y mejoras de seguridad de la información			39%	Inicial
38. ¿Se establecen responsabilidades para desarrollar los procedimientos establecidos en la institución?	5	100%		
39. ¿Se reportan eventos o incidentes de seguridad de la información?	4	95%		
40. ¿Se notifica cualquier debilidad de seguridad observada en los sistemas o servicios?	0	0%		
41. ¿Se establece una clasificación de los incidentes de seguridad de la información para identificar el impacto y el alcance del incidente?	0	0%		
42. ¿Los incidentes de seguridad de la información se responden de acuerdo con los procedimientos establecidos?	0	0%		

Fuente: ISO 27002 (2013)

Elaborado por: Mayorga (2022)

Anexo 14

Tabla Cálculo nivel de madurez

PROCESOS	Madurez	Significado
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	64%	Definido
GESTIÓN DE ACTIVOS	62%	Repetible
CONTROL DE ACCESO	99%	Optimizado
SEGURIDAD FÍSICA Y DEL ENTORNO	100%	Optimizado
SEGURIDAD DE LAS OPERACIONES	98%	Administrado
SEGURIDAD EN LAS COMUNICACIONES	90%	Definido
GESTIÓN DE INCIDENTES	39%	Inicial
	79%	

Fuente: Elaboración propia

Anexo 15

emapa ep	**INSTRUCTIVO PARA CREACIÓN DE USUARIOS DE LA EP-EMAPA-A**	**FECHA:** 19-12-2019
	IT-TIC-07-N753-00	**PÁGINA:** 1 de 3

CONTROL DE CAMBIOS Y ACTUALIZACIONES		
No. VERSIÓN	**FECHA**	**DETALLE DE LA ACTUALIZACIÓN**
00	19-12-2019	Versión Inicial
SE PROHIBE LA REPRODUCCION Y/O DISTRIBUCION DEL PRESENTE DOCUMENTO SIN PREVIA AUTORIZACION DE EP-EMAPA-A		

Elaborado por:	**Revisado por:**	**Aprobado por:**
Responsable del Proceso de Tecnologías de la Información	Directora Administrativa	Directora Administrativa

1. OBJETIVO

Establecer el método para gestionar los roles, privilegios, ingresos, actualizaciones y desactivaciones en los accesos a la información de los sistemas informáticos por parte de los usuarios de la EP-EMAPA-A

2. ALCANCE

Aplica a todos los usuarios (funcionarios o trabajadores) que de alguna manera tengan el manejo de los sistemas informáticos de la EP-EMAPA-A

2. DEFINICIONES

Usuario funcionario o trabajador de la EP-EMAPA-A al cual se le asigna un seudónimo, por el equipo de trabajo de Tecnologías de la Información, para manejar los accesos a los distintos Sistemas informáticos de la Institución.

Director funcionario quien dirige y coordina las actividades de una Dirección de la EP-EMAPA-A

Jefe de Tecnologías de la Información Funcionario quien dirige y coordina las actividades de la Unidad de Tecnologías de la Información

Funcionario de la Unidad de Tecnologías de la Información Funcionario quien está a cargo de la administración de los sistemas informáticos de la EP-EMAPA-A

Correo Institucional es el sistema de correo electrónico que posee la EP-EMAPA-A para comunicación con usuarios internos y externos

3. DESCRIPCIÓN DE ACTIVIDADES

3.1. Metodología

1. Talento Humano elabora un documento indicando la información del usuario referente a ingresos, roles, privilegios y desactivaciones de los sistemas informáticos de la EP-EMAPA-A.
2. El documento debe ser firmado por el usuario y debe ser revisado y aprobado por la Dirección donde va a laborar el dicho usuario
3. El documento debe ser enviado a la Unidad de Tecnologías de la Información, a través del Sistema de Gestión Documental o del Correo Institucional (correo del Director o Jefe de la Unidad).
4. El Jefe de Tecnologías de la Información revisa que los accesos solicitados en los sistemas sean coherentes con las funciones y actividades asignadas al usuario y dispone a los funcionarios de la Unidad de Tecnologías de la Información proceder con las actividades relacionadas.

5. El o los funcionarios de Tecnologías de la Información ingresan la información del usuario en los sistemas solicitados y aprobados de acuerdo con las políticas y estándares.

6. El Jefe de Tecnologías de la Información o un funcionario designado de la misma Unidad notifica mediante Correo Electrónico Institucional al Director requirente y al Usuario la información relativa a datos, claves etc. Para que el usuario pueda ingresar a los sistemas

4. REFERENCIAS A OTROS DOCUMENTOS

N/A

5. REGISTROS ASOCIADOS

CÓDIGO	IDENTIFICACIÓN/NOMBRE
RG-TIC-11-N753-XX	CREACIÓN, MODIFICACIÓN, DESACTIVACIÓN USUARIOS EP-EMAPA-A

6. LISTA DE DISTRIBUCIÓN

PROCESO
TODOS LOS PROCESOS

Anexo 16

	INSTRUCTIVO DE CONTROL, RESPALDO, ARCHIVO Y CUSTODIA DE LA INFORMACIÓN ELECTRÓNICA	**FECHA:** 01-12-2021
	IT-GA-TIC-05-N753-09	**PÁGINA:** 1 de 5

CONTROL DE CAMBIOS Y ACTUALIZACIONES		
No. VERSIÓN	**FECHA**	**DETALLE DE LA ACTUALIZACIÓN**
08	07-08-2019	• Cambio de codificación por reestructura del SGC 9001. El subproceso de Gestión de Calidad es parte del proceso de Gestión Gerencial y subproceso Tecnologías de la Información es parte del proceso de Gestión Administrativa. • Cambio servidor (SGC) storage.emapa.gob.ec. • Cambio de nombre genérico a los sistemas informáticos.

Elaborado por:	**Revisado por:**	**Aprobado por:**
Firmado electrónicamente por: MARCELO PATRICIO TOALOMBO MONTERO Ing. Marcelo Patricio Toalombo Montero	Firmado electrónicamente por: CESAR FILIBERTO MEDINA LLERENA Ing. César Filiberto Medina Llerena	Firmado electrónicamente por: CESAR FILIBERTO MEDINA LLERENA Ing. César Filiberto Medina Llerena
Jefe de Tecnologías de la Información (Enc.)	Director Administrativo	Director Administrativo

1. OBJETIVO.

Proteger, controlar, asegurar la información generada en la EP-EMAPA-A definida como importante y que se encuentra bajo custodia Unidad de Tecnologías de la Información.

2. ALCANCE.

Desde el respaldo de cada funcionario hasta el respaldo de los sistemas informáticos de la EP-EMAPA-A, su archivo y custodia, aplica para los Sistemas de Gestión de Calidad ISO 9001 e ISO/IEC 17025.

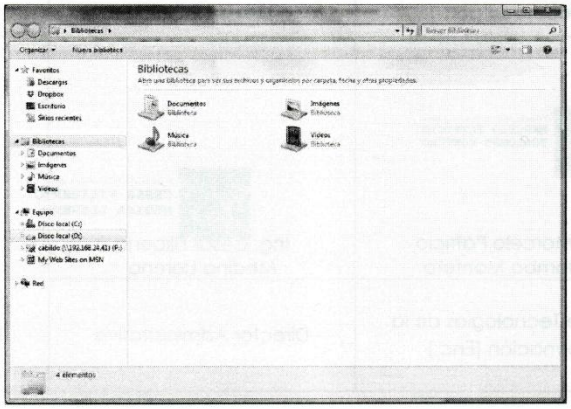
3. DESCRIPCIÓN DE ACTIVIDADES.

3.1. RESPALDO DE LA INFORMACIÓN

Los funcionarios serán los responsables de crear una carpeta en su máquina en la unidad D, donde se alojarán los documentos que se desee respaldar. La unidad D es la unidad que se crea conjuntamente con la unidad C.

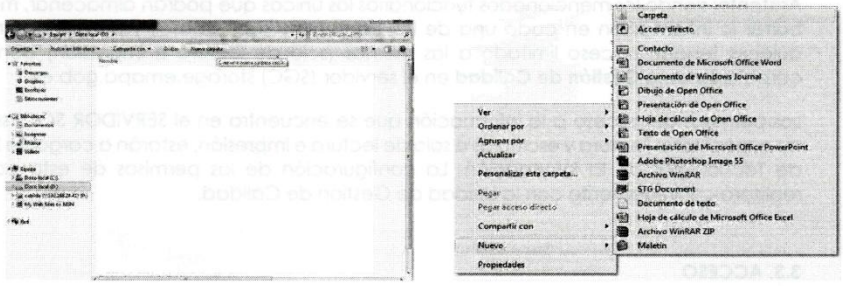
La Unidad C es donde se almacenan toda la información del sistema operativo y es la unidad que con mayor frecuencia se daña, mientras que la Unidad D queda intacta y se evita que los documentos no se dañen o pierdan.

SELECCIONE LA UNIDAD D



Cada funcionario deberá respaldar la información generada en la UNIDAD D, donde podrá crear las carpetas que contengan la información relevante y organizarla según su necesidad.

CREE DENTRO DE LA UNIDAD D SUS CARPETAS Y ORGANICE SU INFORMACIÓN



La información a respaldar en la UNIDAD D dentro de las carpetas podrá ser: documentos de texto, hojas de cálculo, reportes con valor agregado, planillas, mapas, planos (menos los *.bak o de respaldo), dibujos, etc.; archivos que contengan información de la Empresa. No se guardarán respaldos de documentos o archivos personales de los funcionarios, fotos, música, video, etc.

En el caso de que el funcionario desee tener un Respaldo externo de la información alojada en la UNIDAD D, tiene dos opciones:

- Utilizar dispositivos externos propios o institucionales, el archivo y custodia será responsabilidad del funcionario es recomendable sacar respaldos en unidades externas, sean estos discos duros externos, blu-ray, flash memory, etc. La Unidad de Tecnologías de la Información brindará asesoramiento para realizar este procedimiento de respaldo de información a los dispositivos antes mencionados, la unidad requirente deberá proporcionar los dispositivos externos.

- Solicitar el respaldo y custodia de la información a la Unidad de Tecnologías de la Información. En éste último caso, la Unidad de Tecnologías de la Información, evaluará la información y sólo se realizará el Respaldo y custodia de la información relevante de la Empresa. Se llevará el registro Respaldo, Archivo y Custodia de la Información (**RG-TIC-07-N7531-XX**) como evidencia de que se ha realizado el respaldo y se custodiará la información.

Los funcionarios no respaldarán reportes disponibles de los sistemas informáticos: Documental y Archivo, Comercial, Financiero, DOM, etc.) actividad que corresponderá al personal de la Unidad de Tecnologías de la Información.

3.2. SERVIDOR DEL SGC

Tecnologías de la Información brindará alojamiento de la información que el responsable del proceso de Gestión de Calidad solicite en el servidor (SGC) storage.emapa.gob.ec, donde está creada una carpeta con el nombre **Sistema Gestión de Calidad**, dentro de esa carpeta estarán otras carpetas referentes a cada uno de los sistemas y procesos de Gestión de Calidad, con el fin de controlar la documentación, como lo indica el Procedimiento de elaboración y control de documentos y registros (**PR-GG-SGC-01-N75-XX**). A estas carpetas tendrá control total (lectura y escritura) únicamente el Jefe de Gestión de Calidad o su

Asistente; siendo los mencionados funcionarios los únicos que podrán almacenar, modificar o borrar la información en cada una de las carpetas y subcarpetas y determinarán quién o quienes tengan acceso limitado a las mismas (solo de lectura e impresión) dentro de la carpeta **Sistema Gestión de Calidad** en el servidor (SGC) storage.emapa.gob.ec.

Los permisos de acceso a la información que se encuentra en el SERVIDOR SGC, sean estos de control total (lectura y escritura) o solo de lectura e impresión, estarán a cargo de la Unidad de Tecnologías de la información. La configuración de los permisos de esta carpeta se realizará conjuntamente con la Unidad de Gestión de Calidad.

3.3. ACCESO

Con el fin de proteger la información generada e impedir el acceso no autorizado de la misma, manipulación indebida o pérdida de la información, el acceso a los equipos se realizará conforme se describe en el Procedimiento de Elaboración y Control de documentos y registros (**PR-GG-SGC-01-N75-XX**). En el caso de que se requiera información que se encuentra bajo custodia de TIC, se realizará el requerimiento de la misma para su entrega.

3.3. FRECUENCIA

La Unidad de Tecnologías de la Información (TIC) determina la frecuencia del respaldo de la información. Se procurará sacar respaldos diarios de los sistemas que son críticos para el normal funcionamiento de la Institución: Sistema Comercial, Sistema Financiero, Documental, Correo, DOM-Ingreso de Reportes.

Una vez al mes, por motivos de control, se llenará el Registro Respaldo, Archivo y Custodia de la Información (**RG-TIC-07-N7531-XX**), previo la verificación de los archivos respaldados, de las bases de datos (Comercial, Financiero y DOM Ingreso de Reportes).

Los respaldos del Servidor del SGC se realizarán trimestralmente por parte de TIC, de forma similar en el Laboratorio de Control de Calidad de la EP-EMAPA-A se realizará respaldos de la información referente a la Norma ISO 17025 al menos una vez por semestre. No se requiere el pedido de respaldo por parte de las unidades y se llenará el Registro Respaldo, Archivo y Custodia de la Información (**RG-TIC-07-N7531-XX**).

Los sistemas (Documental, Correo, Financiero y DOM Ingreso de Reportes), se realiza el respaldo diariamente; los mismos que se sobrescriben al obtener el nuevo respaldo de los servidores virtualizados.

3.4. CUSTODIA

Como se señaló en el numeral 3.1 los respaldos que lleve cada funcionario en medios externos, serán responsabilidad de los mismos. Los respaldos realizados por la Unidad de Tecnologías de la Información serán custodiados en el data storage y discos externos.

Se garantizará que la información respaldada permanezca por al menos 15 años bajo custodia de la Unidad de Tecnologías de la Información.

Posterior a ello, se revisará conjuntamente con personal de Archivo y los Responsables de las Unidades que apliquen la necesidad de mantener la información digital por más de 15 años

y se decidirá el destino final de los archivos considerando las disposiciones legales y/o reglamentarias que apliquen, así como las necesidades institucionales.

3.5 CONTROL DE DATOS Y GESTIÓN DE LA INFORMACIÓN

Para el Sistema de Gestión ISO/IEC 17025, el control de datos y gestión de la información relacionada al manejo de los sistemas informáticos, se realizará conforme se describe en el Procedimiento de Elaboración y Control de documentos y registros (**PR-GG-SGC-01-N75-XX**). Los funcionarios de la Unidad de Tecnologías de la Información han suscrito el **17025-RG-CC-01-XX** Acuerdo Legal de Imparcialidad y Confidencialidad.

4. REGISTROS ASOCIADOS.

CÓDIGO	IDENTIFICACIÓN/NOMBRE
RG-TIC-07-N7531-XX	REGISTRO RESPALDO, ARCHIVO Y CUSTODIA DE LA INFORMACIÓN

5. REFERENCIA A OTROS DOCUMENTOS

Documentos Internos y documentos Externos

CÓDIGO	IDENTIFICACIÓN/NOMBRE
PR-GG-SGC-01-N75-XX	PROCEDIMIENTO DE ELABORACIÓN Y CONTROL DE DOCUMENTOS Y REGISTROS
DE-GG-SGC-01-XX	NORMA INTERNACIONAL -ISO 9001 SISTEMA DE GESTIÓN DE CALIDAD REQUISITOS
17025-DE-SGC-02-XX	NORMA TÉCNICA ECUATORIANA NTE INEN ISO IEC 17025

6. LISTA DE DISTRIBUCIÓN DEL DOCUMENTO:

Proceso
Todos los Procesos