UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

SEGURIDAD EN LA BASE DE DATOS PERSONALES APLICANDO COMPLIANCE DE CIBERSEGURIDAD EN LA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EMAPA

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la información

ÁREA: Seguridad y redes

LÍNEA DE INVESTIGACIÓN: Tecnologías de la información y Sistemas de control

AUTOR: Christian Jonathan Jara Abad

TUTOR: Ing. Franklin Oswaldo Mayorga Mayorga, Mg.

Ambato - Ecuador

febrero - 2024

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: SEGURIDAD EN LA BASE DE DATOS PERSONALES APLICANDO COMPLIANCE DE CIBERSEGURIDAD EN LA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EMAPA, desarrollado bajo la modalidad Proyecto de Investigación por el señor Christian Jonathan Jara Abad, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

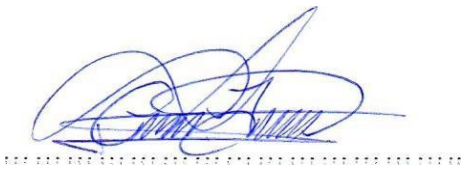
Ambato, febrero 2024.

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: SEGURIDAD EN LA BASE DE DATOS PERSONALES APLICANDO COMPLIANCE DE CIBERSEGURIDAD EN LA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EMAPA es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, febrero del 2024



Christian Jonathan Jara Abad

CC: 180470770-9

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, febrero del 2024

Christian Jonathan Jara Abad ce
180470770-9
AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el señor Christian Jonathan Jara Abad, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado SEGURIDAD EN LA BASE DE DATOS PERSONALES APLICANDO COMPLIANCE DE CIBERSEGURIDAD EN LA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EMAPA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, febrero 2024.


Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL


Firmado electrónicamente por:
EDWIN HERNANDO BUENANO VALENCIA

Ing. Edwin Hernando Buenaño Valencia, Mg
PROFESOR CALIFICADOR


Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Omar Guevara Aulestia, Mg.
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto está dedicado a mis padres como una expresión de profundo agradecimiento por su apoyo constante e incondicional. A lo largo de los altibajos de la vida, han sido mi roca, guiándome con sus consejos francos y honestos. Su fe inquebrantable en mí ha sido fundamental en mi camino hacia el éxito. Aunque el logro es personal, el triunfo es gracias a ustedes.

Para aquel en quien he depositado mi fe, que nunca me ha abandonado, incluso en medio de todas mis equivocaciones, he experimentado su constante presencia a mi lado a lo largo de este extenso trayecto.

A mis amados abuelos, Alcira y Manuel, así como a mi querida madrina Eugenia, quienes han sido los artífices de los momentos más felices en mi vida, y a quienes aspiro seguir llenando de orgullo con mis acciones.

AGRADECIMIENTO

Expreso mi gratitud eterna a mi familia, cuya inspiración y fortaleza han sido la base fundamental para construir mis propios sueños y forjar la persona que.

A mi tutor, el Ing. Mg. Franklin Mayorga por su paciencia y orientación durante todo este proceso.

A mi querida Alma Máter agradezco profundamente por ser el lugar donde me formé, donde he adquirido las lecciones más valiosas y donde se ha sembrado en mí el deseo constante de aprendizaje.

.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

La seguridad cibernética y el cumplimiento normativo son fundamentales en el entorno digital actual. La seguridad en línea protege sistemas, redes y datos contra riesgos informáticos, resguardando la integridad y confidencialidad de la información en un mundo interconectado. El cumplimiento normativo asegura que las organizaciones cumplan regulaciones pertinentes, incluyendo la privacidad de datos y la protección digital. Estos aspectos están vinculados, ya que el cumplimiento normativo establece prácticas seguras y responsables en el ámbito digital, fortaleciendo la resiliencia ante intrusiones digitales.

El presente proyecto busca implementar medidas de seguridad sólidas en la base de datos personal de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, aplicando los principios de compliance de ciberseguridad para proteger la información almacenada en dicha base de datos. El objetivo es establecer un marco de buenas prácticas y cumplimiento normativo que resguarde la confidencialidad, integridad y disponibilidad de los datos personales, mitigando eficazmente posibles riesgos y amenazas cibernéticas.

El proyecto fue desarrollado utilizando la metodología Kanban, la cual permite la gestión de proyectos, además se utiliza el software Kanban Flow, aprovechando su eficiencia como tablero Kanban. El proceso fue estructurado en siete etapas distintas, cada una diseñada para abordar aspectos específicos del proyecto. Kanban Flow, al proporcionar una plataforma visual y colaborativa, facilitó la gestión y supervisión de las tareas en cada etapa del proyecto. Como resultado del mismo, se ha conseguido un notable incremento en la capacidad de recuperación de la EMAPA frente a posibles amenazas digitales. La aplicación de acciones de seguridad en la base de datos personal, en cumplimiento con las normativas de ciberseguridad, ha fortalecido de manera eficaz las barreras frente a los riesgos cibernéticos.

Palabras clave: Seguridad cibernética, compliance, metodología Kanban, mitigación de riesgos, compliance de ciberseguridad

ABSTRACT

The Cybersecurity and regulatory compliance are crucial in today's digital environment. Online security safeguards systems, networks, and data against computer risks, preserving the integrity and confidentiality of information of an interconnected world. Normative compliance ensures that organizations adhere to relevant regulations, including data privacy and digital protection. These aspects are linked, the normative compliance establishes secure and responsible practices in the digital realm, enhancing resilience against digital intrusions.

The current project aims to implement robust security measures in the personal database of the Empresa Municipal de Agua Potable y Alcantarillado (EMAPA), applying cybersecurity compliance principles to protect the information stored in the database. The objective is to establish a framework of best practices and normative compliance that safeguards the confidentiality, integrity, and availability of personal data, effectively mitigating potential cyber risks and threats.

The project was developed using the Kanban methodology, which allows project management, and the Kanban Flow software was utilized for its efficiency as a Kanban board. The development process was structured into seven distinct stages, each designed to address specific aspects of the project. Kanban Flow, provides a visual and collaborative platform, facilitated the management and supervision of tasks at each stage of the project. As a result of the project, there has been a notable increase in EMAPA's resilience to potential digital threats. The implementation of security actions in the personal database, in compliance with cybersecurity standards, has effectively strengthened barriers against cyber risks.

Keywords: Cybersecurity, compliance, Kanban methodology, risk mitigation, cybersecurity compliance.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

SEGURIDAD EN LA BASE DE DATOS PERSONALES APLICANDO COMPLIANCE DE CIBERSEGURIDAD EN LA EMPRESA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO EMAPA

1.1.1 Planteamiento del problema

La información es un activo de las organizaciones, que permite la toma de decisiones oportunas a nivel administrativo y, en consecuencia, lograr una alta competitividad en el mercado. Las tecnologías de la información son otro componente clave de la gestión de la información empresarial. La dependencia de una organización en la tecnología, donde las bases de datos son el medio para almacenar y gestionar la información. La seguridad de la información ha tomado un lugar decisivo en la gestión de la información tecnológica y se ha convertido en un elemento clave de todas las estrategias empresariales que tienen como finalidad proteger objetivos importantes a corto, mediano y largo plazo. Teniendo en cuenta las características de disponibilidad, integridad y confidencialidad. En la práctica, los niveles de seguridad se pueden definir de acuerdo con los estándares y los mejores ejercicios que demuestran la reducción de riesgo de una intuición en la base de datos [1].

La seguridad de la base de datos empresarial es un tema de suma importancia en la actualidad, ya que las bases de datos contienen información crítica y confidencial de las empresas y sus clientes. A nivel global, existen diversas situaciones que afectan la seguridad de las bases de datos empresariales, ante estas situaciones, las empresas implantan medidas de seguridad las cuales están influenciadas por una serie de regulaciones y normativas que buscan proteger la privacidad y la integridad de los datos. Vario países que implementan estas normativas de seguridad han experimentado grandes avances significativos en los últimos años, debido a que la normativa de protección de datos ha impulsado a tomar medidas más sólidas para la protección de la información personal [2].

En Ecuador, la seguridad de las bases de datos también se encuentra regido por el cumplimiento normativo, la cual ha ganado mucha importancia durante estos años. Es importante destacar que el cumplimiento normativo y la seguridad de las bases de datos en Ecuador aún enfrentan desafíos, muchas organizaciones aún están adaptando sus procesos y tecnologías para cumplir plenamente con las disposiciones de la Ley orgánica de protección de datos personales (LOPD). Además, los ciberataques y las amenazas a la seguridad de los datos son desafíos constantes, por lo que es fundamental que las empresas implementen medidas de seguridad robustas y estén al tanto de las mejores prácticas en protección de datos.

En la ciudad de Ambato, a medida que la tecnología se utiliza en la seguridad, varias empresas están implementado el cumplimiento normativo para garantizar las medidas de seguridad necesarias para la protección de los datos personales.

1.2 Antecedentes investigativos

Después de haber realizado el análisis de fuentes de investigación dentro de los repositorios de las Universidades y además de utilizar Papers se han encontrado información que está siendo usada de apoyo:

M. Alssaf & A. Alkhalifah [3]: Para reducir las amenazas a la seguridad organizacional, varias organizaciones han aplicado varios estándares y pautas de seguridad. Ejemplos de estos estándares son la Organización Internacional de Normalización (ISO,) y la Comisión Electrotécnica Internacional (IEC) (ISO/IEC 27001); y Objetivos de Control para Tecnologías de la Información y Relacionadas (COBIT, Control Objectives for Information and Related Technologies). Estas pautas y estándares brindan las mejores prácticas para la seguridad de SI. Por lo tanto, para ayudar a las personas a mejorar sus actividades de seguridad, las organizaciones están integrando estas normas en un documento denominado Política de Seguridad de la Información (ISP, Internet Service Provide); esta política ayuda a moldear el comportamiento de sus empleados hacia la seguridad.

Según F. Vela [4]: Del estudio realizado se desprende que, la implementación de un SIEM, Security Information and Event Management (Gestión de la Información y

Eventos de Seguridad) para la detección y mitigación de ataques a las bases de datos es un aporte sustancial, para mejorar la seguridad de toda la infraestructura y es un soporte importante para el cumplimiento de la normativa vigente en el Ecuador que aporta al cumplimiento de los Objetivos de Desarrollo Sostenible sugerido en este artículo.

De acuerdo con G. Garzón [1]: El análisis de la información obtenida acerca de las normas o estándares de base de datos nos muestra que no existe una guía especializada en seguridad de base de datos Oracle con parámetros específicos. Los niveles de seguridad obtenidos en este proyecto sirven como referencia para administradores de base de datos que quieran implementar o mejorar sus seguridades.

Según J. Soto & J. Valdivieso [5]: Realizaron una investigación sobre la metodología para transformar registros administrativos en registros estadísticos. Por lo tanto, recomiendan que las instituciones o áreas que manejan registros administrativos con fines estadísticos apliquen procesos que impidan revelar la identidad de un ente (seudonimización), con lo cual se garantiza la vinculación entre varios registros estadísticos con el fin de robustecer el análisis, así también, se evita ocasionar daño o violación de la privacidad, y se genera un ambiente de confianza con los proveedores de datos.

La investigación desarrollada por, A. Quimís [6]: Mediante el modelo de gestión de la información de la estructura de datos se garantiza a las organizaciones públicas el manejo de la información de manera más segura y mejor administrada para los usuarios que monitorean los errores o ataques en las organizaciones.

En la publicación de P. Vaca [7]: Si no se implementa un modelo de gestión de seguridad lógica de la información mediante el uso de políticas aumentará el riesgo de que ocurran pérdidas de información, fallos en la integridad de los datos, así como la denegación de servicios o suspensiones al momento de realizar la recuperación de datos.

Así pues, se tiene una primera alerta sabiendo que no se cuenta con un modelo de gestión de seguridad lógica de la información en el que se incluya las normas y

procedimientos para actuar o reponerse ante un ataque informático o los datos de carácter sensible se vean comprometidos.

Para M. Cordero [8]: Dado que la seguridad de la información tiene un papel muy importante en el apoyo a las actividades de la organización, necesitamos un estándar o punto de referencia que regule la gobernanza sobre la seguridad de la información. Varias organizaciones privadas y gubernamentales desarrollaron organismos de estándares cuya función es establecer puntos de referencia, estándares y, en algunos casos, regulaciones legales sobre seguridad de la información para avalar que se mantenga un nivel adecuado de seguridad, para garantizar que los recursos se usen de la manera correcta y se ejecuten las mejores prácticas de seguridad adoptadas en una organización. Existen varios estándares para el gobierno sobre las Tecnologías de la Información que conducen a la seguridad de la información, como PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL y COBIT.

1.3 Fundamentación teórica

1.3.1 Estructura Empresarial

La estructura empresarial se refiere a la forma en que una organización está instaurada y jerarquizada para llevar a cabo sus actividades comerciales. Está compuesta por los diferentes departamentos, funciones y niveles de autoridad que existen dentro de la empresa.

La estructura empresarial puede variar dependiendo del tamaño de la organización, su industria, su cultura corporativa y sus objetivos estratégicos. Algunos ejemplos comunes de estructuras empresariales incluyen la estructura funcional, la estructura divisional, la estructura matricial y la estructura en red [9].

1.3.2 Gestión empresarial y la administración corporativa

La gestión empresarial se refiere al conjunto de actividades, procesos y decisiones que se llevan a cabo para dirigir y controlar una empresa de manera eficiente y efectiva. Involucra la planificación, organización, dirección y control de los recursos y actividades de la misma con el finde alcanzar los objetivos y metas establecidos. La gestión empresarial abarca áreas como la estrategia empresarial, la gestión financiera, la gestión de recursos humanos, el marketing, la producción, entre otros aspectos clave para el funcionamiento y éxito de una empresa.

Por otro lado, la administración corporativa se centra específicamente en la forma en que una empresa es gobernada y administrada. Implica el establecimiento de estructuras y procesos de toma de decisiones en la empresa, así como el establecimiento de políticas y prácticas para garantizar la transparencia, la responsabilidad y la protección de los intereses de los accionistas y demás partes interesadas. La administración corporativa se ocupa de temas como la junta directiva, el gobierno corporativo, la gestión de riesgos, la ética empresarial y la responsabilidad social corporativa.

La gestión empresarial se enfoca en la gestión general de una empresa, abarcando todas las áreas funcionales y operativas, mientras que la administración corporativa se centra en la gobernanza y las estructuras de toma de decisiones dentro de una empresa para garantizar una gestión efectiva y responsable. Ambos conceptos son fundamentales para el éxito y la sostenibilidad de una organización [10].

1.3.3 Gobernanza Corporativa

La gobernanza corporativa se refiere al conjunto de procesos, políticas, estructuras y normas a través de los cuales una empresa es dirigida, controlada y supervisada con el fin de proteger los intereses de los accionistas y otras partes interesadas. Es un marco de buenas prácticas que busca asegurar la transparencia, la responsabilidad y la toma de decisiones efectiva en la dirección de una empresa.

La gobernanza corporativa establece las reglas y los mecanismos que rigen la relación entre la dirección de la empresa, los accionistas y otros grupos de interés, como empleados, clientes, proveedores y la comunidad en general. También busca alinear los intereses de los distintos actores involucrados en la empresa y salvaguardar los derechos de los accionistas [9].

1.3.4 Aplicación de compliance de Ciberseguridad

La aplicación de compliance se refiere a la implementación y ejecución de programas de cumplimiento normativo en una organización. El compliance, o cumplimiento normativo, se refiere al conjunto de políticas, procedimientos y controles internos que una empresa establece para asegurarse de que sus actividades se realicen de acuerdo con las leyes, regulaciones y estándares éticos aplicables.

El objetivo principal de la aplicación de compliance es prevenir y detectar conductas ilegales, fraudulentas o contrarias a los principios éticos dentro de la organización. Esto implica establecer mecanismos y procesos para garantizar que los empleados y directivos de la empresa actúen de acuerdo con las leyes y regulaciones, evitando así riesgos legales y reputacionales [11].

1.3.5 Tecnologías de la Información

Las Tecnologías de la Información (TI) se refieren al conjunto de herramientas, sistemas y recursos utilizados para adquirir, almacenar, procesar, transmitir y proteger la información en el contexto empresarial y en la sociedad en general. Las TI abarcan una amplia gama de tecnologías y aplicaciones, incluyendo hardware, software, redes de comunicación, sistemas de bases de datos y seguridad de la información.

Las Tecnologías de la Información desempeñan un papel fundamental en las organizaciones, facilitando la automatización de procesos, mejorando la eficiencia operativa, permitiendo la comunicación y colaboración, y brindando acceso a información y recursos en tiempo real. Además, las TI han impulsado la transformación digital en muchos sectores, impactando en la forma en que las

empresas operan, se relacionan con los clientes y desarrollan nuevos modelos de negocio [12].

1.3.6 Seguridad Informática

La seguridad informática se refiere a las medidas y prácticas diseñadas para proteger la información y los sistemas informáticos de amenazas y riesgos, con el objetivo de preservar su confidencialidad, integridad y disponibilidad.

La seguridad informática es esencial para proteger los activos de información crítica de una organización, prevenir pérdidas financieras y reputacionales, y mantener la confianza de los clientes y socios comerciales. La implementación de medidas de seguridad informática debe ser un enfoque integral y en constante evolución, adaptándose a las nuevas amenazas y vulnerabilidades que surgen en un entorno tecnológico en constante cambio [13].

1.3.7 Seguridad de la información

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información en cualquier formato, ya sea electrónico o en papel. Consiste en la implementación de medidas y prácticas destinadas a prevenir el acceso no autorizado, el uso inapropiado, la divulgación o la modificación no autorizada de la información. Es crucial en todas las organizaciones, ya que la información es un activo valioso y vital para el funcionamiento y la toma de decisiones.

La implementación de medidas de seguridad de la información debe ser un enfoque integral y multidisciplinario, considerando tanto aspectos técnicos como organizativos y de concienciación de los empleados. Además, es importante tener en cuenta las regulaciones y normativas específicas que aplican a la protección de la información, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o las leyes de privacidad de datos en diferentes países [14].

1.3.8 Seguridad en la base de datos personal

La seguridad en la base de datos personal se refiere a las medidas y prácticas destinadas a proteger la información personal almacenada en una base de datos contra accesos no autorizados, modificaciones no autorizadas y divulgación indebida. Dado que la información personal puede incluir datos sensibles y privados, es importante garantizar su confidencialidad e integridad.

Se considera esencial la seguridad en la base de datos personal, para proteger la privacidad y confidencialidad de los datos de los individuos. La implementación adecuada de medidas de seguridad ayudará a prevenir fugas de datos, abusos y posibles riesgos legales y reputacionales para las organizaciones que manejan información personal [15].

1.3.9 Metodologías ágiles

Las metodologías ágiles surgieron como una respuesta a las metodologías convencionales, las cuales exhibían rasgos como complejidad, limitada flexibilidad ante cambios, respuesta tardía y una generación excesiva de documentos.

Para considerar eficientemente estas prácticas ágiles como un método de desarrollo aplicado en la industria de aplicaciones móviles, deben exhibir las siguientes características: agilidad, comprensión del mercado, respaldo a la línea de productos de software, desarrollo fundamentado en arquitectura, apoyo a la reutilización, inclusión de sesiones de revisión y aprendizaje, así como una especificación temprana de la arquitectura física [16].

1.3.10 Lean

La metodología Lean, que se originó en el sistema de producción de Toyota, se ha expandido más allá de la manufactura y se utiliza en diversas industrias para optimizar procesos y reducir desperdicios. Su enfoque principal es maximizar el valor para el cliente mientras se minimizan los recursos utilizados. Se aplica en sectores como la producción, servicios, desarrollo de software y gestión empresarial

con el objetivo de mejorar la eficiencia y la calidad. Esta metodología se basa en principios como la eliminación de desperdicios, la mejora continua y la participación activa de los empleados en la toma de decisiones.

La metodología Lean había alcanzado una extensa aprobación en la industria y seguía siendo adoptada por organizaciones con el objetivo de mejorar la agilidad y eficiencia. Su enfoque en suprimir procesos superfluos y su capacidad de adaptación la posicionan como una herramienta valiosa en entornos empresariales dinámicos y cambiantes [17].

1.3.11 Scrum

Scrum es una metodología ágil que se usa para administrar proyectos complejos. Se fundamenta en valores de trasparencia, inspección y adaptación, con una orientación iterativa e incremental en el desarrollo. Scrum se utiliza frecuentemente en la industria de desarrollo de software, pero también se ha implementado con éxito en diferentes campos como marketing, investigación y desarrollo de productos.

La metodología Scrum se puede aplicar a cualquier tipo de proyecto de desarrollo de software, sin importar su tamaño o complejidad. Además, también se puede utilizar en otros tipos de proyectos, como el desarrollo de productos, el diseño de servicios o la investigación y desarrollo. Scrum se basa en principios ágiles y se enfoca en la colaboración, la entrega iterativa e incremental, y la adaptabilidad a los cambios. Al utilizar Scrum, los equipos pueden mejorar la eficiencia, la calidad y la satisfacción del cliente [18].

1.3.12 Kanban

La metodología Kanban es un enfoque visual de gestión que se utiliza para optimizar el flujo de trabajo y mejorar la eficiencia en diferentes contextos. Se originó en el sistema de producción de Toyota y se ha extendido a industrias como la manufactura, el desarrollo de software y la gestión de proyectos. Kanban se utiliza para visualizar y controlar el flujo de trabajo, limitar la cantidad de trabajo en progreso y fomentar la colaboración y la mejora continua. Su objetivo principal es maximizar la eficiencia

y la calidad al eliminar los cuellos de botella y minimizar los tiempos de espera. Al implementar Kanban, los equipos pueden mejorar la productividad, la transparencia y la satisfacción del cliente [19].

1.3.13 Kanban Flow

Kanban Flow es una metodología de gestión del flujo de trabajo que se enfoca en la visualización del trabajo, la limitación de las funciones en progreso y la mejora continua. Su objetivo es mejorar la eficiencia y la productividad de los procesos de trabajo, reduciendo el desperdicio y mejorando la calidad.

Al limitar la cantidad de trabajo en progreso, Kanban Flow ayuda a evitar la sobrecarga y la acumulación de tareas, lo que puede llevar a retrasos y baja calidad en el trabajo. Al visualizar el trabajo, los equipos pueden identificar cuellos de botella y áreas de mejora, lo que les permite tomar medidas para optimizar el flujo de trabajo.

En contraste con otras metodologías de gestión del flujo de trabajo, Kanban Flow destaca por su sencillez y flexibilidad. Este enfoque no demanda una cantidad significativa de documentación o formación, lo que lo convierte en una elección atractiva para aquellas organizaciones que buscan implementar una nueva metodología de gestión del flujo de trabajo de manera rápida y sin complicaciones [20].

1.4 Objetivos

1.4.1 Objetivo general

Implementar medidas de seguridad en la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, aplicando compliance de Ciberseguridad.

1.4.2 Objetivos específicos

- Evaluar la seguridad de la base de datos personal de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.
- Investigar la importancia del compliance en la ciberseguridad.
- Optimizar la seguridad en la base de datos personales aplicando compliance de Ciberseguridad en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

En el presente proyecto de investigación se realizó una encuesta al personal del departamento de tecnologías de la intimación TI. La cual tiene como objetivo recopilar información sobre las expectativas, necesidades y prioridades con respecto a la seguridad de la base de datos personal de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.

También se implementó una entrevista a través de un cuestionario, la cual va dirigida al gerente del departamento de tecnologías de la información TI. La cual tiene como objetivo la recolección de la información sobre el conocimiento de las medidas de seguridad en la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.

Adicionalmente, para comprender mejor la seguridad de la base de datos y las medidas de ciberseguridad que se encuentran aplicadas en la base de datos personal se utilizó la ficha de observación.

Entrevista dirigida al jefe del departamento de Tecnologías de la Información TI de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA

El objetivo de la entrevista es recopilar información sobre el conocimiento las medidas de seguridad en la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, aplicando compliance de Ciberseguridad.

CUESTIONARIO:

1. **Según su perspectiva general sobre la seguridad en la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA. ¿Cree usted que es un tema importante en la actualidad?**

2. **¿Cómo describiría la política de seguridad de la información en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

3. **¿Cómo describiría la seguridad de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

4. **¿Cuáles considera que son los desafíos más significativos o las amenazas más significativas para la seguridad de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

5. **¿Cuál es su experiencia en el manejo y seguridad de bases de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

6. **¿Existe alguna política o procedimiento establecido para el acceso y manejo de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

7. **¿Se fomenta la conciencia de seguridad entre los empleados en relación con el manejo de la base datos personales en la empresa municipal de agua potable y alcantarillado EMAPA? ¿Cómo?**

---

8. **¿Ha recibido quejas o preocupaciones de empleados o clientes relacionadas con la seguridad de sus datos personales en la empresa municipal de agua potable y alcantarillado EMAPA? ¿Puede proporcionar ejemplos de estas quejas y cómo se abordaron?**

9. **¿Usan tecnologías o herramientas que ayuden con la seguridad de las bases de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

10. **¿Se realizan auditorías periódicas para evaluar la seguridad de la base de datos personal en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

11. **¿Cuáles son las medidas de seguridad considera más efectivas o esenciales para proteger la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

12. **¿Qué acciones cree que deben tomar los gobiernos, las empresas y los usuarios para la protección de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA y garantizar la privacidad?**

---

13. **¿Qué medidas toma para promover la colaboración y la concienciación sobre seguridad de la información en la empresa municipal de agua potable y alcantarillado EMAPA?**

---

14. **¿Hay algún otro comentario o perspectiva que le gustaría agregar sobre la seguridad en las bases de datos personales?**

Encuesta dirigida al personal del departamento de Tecnologías de la Información TI de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA

El objetivo de la encuesta es recopilar información sobre el conocimiento las medidas de seguridad en la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, aplicando compliance de Ciberseguridad.

CUESTIONARIO:

1. **¿Cuál es su función en el departamento de TI la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

   _____

2. **En una escala del 1 al 10, donde 1 es "muy inseguro" y 10 es "muy seguro", ¿cómo calificaría la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA desde su perspectiva?**

1	2	3	4	5	6	7	8	9	10

3. **¿Ha experimentado alguna vez una violación de la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

   ( ) Si
   ( ) No

4. **¿Cuáles de los siguientes problemas o preocupaciones relacionados con la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA le inquietan más? (Puede seleccionar varias opciones)**

( ) Robo de identidad

( ) Acceso no autorizado a cuentas

( ) Fuga de información personal

( ) Pérdida de datos por fallas técnicas

( ) Brechas de seguridad en servicios en línea

( ) Otra (especificar)_____

5. **En una escala del 1 al 10, donde 1 es "muy inseguro" y 10 es "muy seguro", ¿qué tan seguro siente que están sus datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

1	2	3	4	5	6	7	8	9	10

6. **¿Ha experimentado o conocido casos de problemas relacionados con la seguridad de los datos personales en de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

( ) Filtraciones de datos

( ) Acceso no autorizado

( ) Pérdida de datos

( ) Otra (especificar)_____

7. **Desde su perspectiva en el departamento de TI, ¿cuáles considera que son los problemas más importantes en cuanto a la seguridad de los datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

( ) Falta de Conciencia y Cultura de Seguridad

( ) Acceso no Autorizado

( ) Protección Insuficiente de Datos

( ) Falta de Políticas y Procedimientos de Seguridad

( ) Falta de Capacitación

( ) Cumplimiento Legal y Normativo

( ) Otra (especificar)_____

8. **¿Ha habido incidentes de seguridad de datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, en el pasado en EMAPA? Si es así.**

   ( ) Si
   ( ) No

9. **¿Qué medidas y soluciones de seguridad de datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, se han implementado o propuesto en el departamento de TI para abordar los problemas de inseguridad?**

   ( ) Acceso restringido
   ( ) Encriptación
   ( ) Auditorias y seguimientos
   ( ) Actualizaciones y parches
   ( ) Copias de seguridad
   ( ) Capacitación

10. **¿Cuáles considera que son las áreas o departamentos donde se pueden realizar mejoras significativas en la seguridad de datos personales en de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

    ( ) Departamento de Tecnología de la Información (TI)
    ( ) Departamento de Recursos Humanos
    ( ) Departamento de Servicio al Cliente
    ( ) Departamento de Marketing y Ventas
    ( ) Otra (especificar)_____

11. **¿Cómo colaboraría el departamento de TI con otros departamentos de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA en asuntos relacionados con la seguridad de los datos personales?**

    ( ) Implementación de medidas de seguridad adecuadas
    ( ) Educación y concientización
    ( ) Auditorías y monitoreo periódicas

( ) Cumplimiento normativo

( ) Gestión de incidentes de seguridad

( ) **Colaboración en Proyectos**

( ) **Otra (especificar) _____**

12. **¿Qué programas de educación o concienciación sobre seguridad de datos personales se han implementado para el personal de EMAPA, incluyendo el departamento de TI?**

    ( ) Talleres y capacitación

    ( ) Recursos educativos

    ( ) Colaboraciones con instituciones

    ( ) Programas de mentoría

    ( ) Otra (especificar)_____

    ( ) No se ha implementado nada

13. **¿Tiene algún comentario adicional o experiencia personal que desee compartir sobre la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?**

    _____

Fichas de Observación

Ficha de observación				
Ficha Nº	Uno			
Fecha de la Observación				
Tipo de Observación	Seguridad de Base de Datos			
Departamento	Departamento de Tecnologías de la Información (TI)			
Observador	Christian Jara			
Objetivo	Evaluar la seguridad de la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, y verificar si se está aplicando medidas de ciberseguridad.			
OBSERVADO	**NIVEL**			**COMENTARIO**
Autorización de accesos	**Alto**	**Medio**	**Bajo**	
Cifrado de datos	**Alto**	**Medio**	**Bajo**	
Auditoría y monitorización	**Alto**	**Medio**	**Bajo**	
Protección contra ataques externos	**Alto**	**Medio**	**Bajo**	
Autenticación y Contraseñas	**Alto**	**Medio**	**Bajo**	
Políticas de Respaldos	**Alto**	**Medio**	**Bajo**	

Ficha de observación				
Ficha Nº	Dos			
Fecha de la Observación				
Tipo de Observación	Medidas de Ciberseguridad			
Departamento	Departamento de Tecnologías de la Información (TI)			
Observador	Christian Jara			
Objetivo	Evaluar la seguridad de la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, y verificar si se está aplicando medidas de ciberseguridad.			
OBSERVADO	**NIVEL**			**COMENTARIO**
Concienciación y capacitación	**Alto**	**Medio**	**Bajo**	
Protocolo de respuesta a incidentes	**Alto**	**Medio**	**Bajo**	
Gestión de activos	**Alto**	**Medio**	**Bajo**	
Documentación y normativa	**Alto**	**Medio**	**Bajo**	
Auditorias de ciberseguridad	**Alto**	**Medio**	**Bajo**	
Infraestructura de red	**Alto**	**Medio**	**Bajo**	

2.2 Métodos

2.2.1 Modalidad de la investigación

EL presente estudio se enmarcó dentro del enfoque de investigación de la modalidad de Bibliográfica, Descriptiva, Aplicada.

a. Investigación Bibliográfica

Esta investigación se llevó a cabo como un estudio bibliográfico debido a que su objetivo principal fue recopilar, revisar y analizar la literatura existente sobre seguridad en la base de datos personales y el cumplimiento de ciberseguridad en el contexto de la empresa municipal de agua potable y alcantarillado EMAPA. En lugar de realizar una investigación de campo o recopilar datos primarios, se utilizó la información disponible en fuentes bibliográficas, como libros, artículos científicos, informes y documentos relevantes. El enfoque bibliográfico permitió obtener una visión exhaustiva y actualizada sobre el tema de estudio, así como analizar las mejores prácticas y recomendaciones existentes en el ámbito de la seguridad de datos y la ciberseguridad en organizaciones similares

b. Investigación Descriptiva

La presente investigación se clasifica como descriptiva debido a que su objetivo principal es describir y analizar la situación actual de la seguridad en la base de datos personales y la aplicación del cumplimiento de ciberseguridad en la empresa municipal de agua potable y alcantarillado EMAPA. A través de la recopilación y análisis de información bibliográfica, se busca proporcionar una visión detallada y precisa de cómo se aborda actualmente la seguridad de los datos en esta organización y cómo se implementan las medidas de ciberseguridad para proteger la información personal de los individuos. El estudio no pretende establecer relaciones causales ni realizar predicciones, sino más bien obtener un panorama claro de la situación actual y proporcionar recomendaciones para mejorar la seguridad de la base de datos y el cumplimiento de las normativas de ciberseguridad en EMAPA.

c. Investigación Aplicada

La investigación es aplicada, ya que involucraría la recopilación y el análisis de datos relevantes, como los requisitos de cumplimiento normativo, las políticas y los procedimientos actuales de seguridad, así como los posibles riesgos y amenazas específicos para la base de datos personal en EMAPA. A partir de esta información, se desarrollarían y probarían soluciones prácticas, como la implementación de controles de seguridad, la capacitación del personal y la mejora de los procesos internos.

2.2.2 Población y muestra

La población con la que se trabajó, es el personal encargado del departamento de Tecnologías de la Información, además del gerente encargado de dicho departamento.

Tabla 1. Población de estudio

Población	Número	Porcentaje
Gerente	1	16.67 %
Personal administrativo	5	83.33 %
Total	6	100 %

2.2.3 Recolección de información

El proyecto se basa en una base de datos que fue migrada de SQL Server a PostgreSQL, utilizando la versión 14.0, la cual se actualizó en noviembre de 2023. Esta base de datos, llamada "Base de Datos Comercial", tiene un tamaño aproximado de 12 GB y consta de alrededor de 100 tablas. Se encuentra alojada en un servidor dedicado con 2 terabytes de memoria y 64 GB de RAM, utilizando un sistema Linux-Ubuntu.

La tabla de usuarios contiene 90,000 registros y crece mensualmente con la adición de 300 usuarios, generando aproximadamente 100,000 nuevos registros por usuario al mes, aunque estas cantidades pueden variar. Los registros de los usuarios se

realizan en el departamento de atención al cliente y se actualizan diariamente. El crecimiento de la base de datos está alineado con el crecimiento de la EMAPA.

Además, existe una segunda base de datos conocida como "Base de Datos Administrativa", que tiene un tamaño aproximado de 9 GB y se utiliza para fines internos de gestión.

Anteriormente, ambas bases de datos formaban parte de una sola entidad sin nombre, dividida por oficinas, antes de ser separadas en dos bases de datos distintas.

Las técnicas empleadas para le recolección de la información será la entrevista dirigida al gerente de TI, la encuesta dirigida al personal administrativo de mismo departamento, adicionalmente se utilizó la ficha de observación para recolectar información de la seguridad y las medidas de ciberseguridad de la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.

Resultados de la entrevista

Una vez realizado la entrevista se obtuvo los siguientes resultados:

Primera pregunta

Según su perspectiva general sobre la seguridad en la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA. ¿Cree usted que es un tema importante en la actualidad?

Respuesta

Si, porque se maneja información delicada tanto de los clientes como del personal de la EMAPA. La protección de los datos es esencial para garantizar la privacidad.

Segunda Pregunta

¿Cómo describiría la política de seguridad de la información en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

La seguridad de la información se tiene controlado en la medida de lo posible, entre las personas autorizadas para el acceso a la base de datos dos 2 los cuales pertenecen al área de TI. Entre las medidas tomadas se tiene los puertos de la administración de los servidores se encuentran habilidades únicamente para uso interno.

Tercera Pregunta

¿Cómo describiría la seguridad de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

Es controlado con la seguridad que se puede mantener, ya que se necesita una actualización de equipos y softwares. Entre la seguridad que se tiene esta el acceso restringido, la base de datos está en un servidor dedicado, el acceso por medio se software está habilitado solo para 2 ingenieros del área.

Cuarta Pregunta

¿Cuáles considera que son los desafíos más significativos o las amenazas más significativas para la seguridad de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

La piratería informática, puesto que el servidor tiene conexión a internet. Aunque está protegido en todo lo posible.

Quinta Pregunta

¿Cuál es su experiencia en el manejo y seguridad de bases de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

La experiencia fue adquirida de forma empírica, ya que en la misma empresa EMAPA se necesitaba dichos conocimientos. Además, se han ido mejorando con los años.

Sexta Pregunta

¿Existe alguna política o procedimiento establecido para el acceso y manejo de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

La política si esta aplicada, pero no existe de forma escrita, todo está bajo la supervisión de los ingenieros autorizado del área de TI.

Séptima Pregunta

¿Se fomenta la conciencia de seguridad entre los empleados en relación con el manejo de la base datos personales en la empresa municipal de agua potable y alcantarillado EMAPA? ¿Cómo?

Respuesta

No, solo se tiene en cuanta el cambio de contraseñas. Siempre y cuando aya sucedido algo.

Octava Pregunta

¿Ha recibido quejas o preocupaciones de empleados o clientes relacionadas con la seguridad de sus datos personales en la empresa municipal de agua potable y alcantarillado EMAPA? ¿Puede proporcionar ejemplos de estas quejas y cómo se abordaron?

Respuesta

No.

Novena Pregunta

¿Usan tecnologías o herramientas que ayuden con la seguridad de las bases de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

Si, se usa antivirus y también se usa el firewall, para la ayuda con el control de los accesos.

Décima Pregunta

¿Se realizan auditorías periódicas para evaluar la seguridad de la base de datos personal en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

No.

Décima primera pregunta

¿Cuáles son las medidas de seguridad considera más efectivas o esenciales para proteger la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

Los accesos restringidos, acceso solo a los administradores de los servidores.

Décima segunda pregunta

¿Qué acciones cree que deben tomar los gobiernos, las empresas y los usuarios para la protección de la base de datos personales en la empresa municipal de agua potable y alcantarillado EMAPA y garantizar la privacidad?

Respuesta

Ayudar con la actualización de conocimientos con respecto a la seguridad de la información. Crear una legislación, para el desarrollo e implementación de una normativa jurídica para la seguridad de la información.

Décima tercera pregunta

¿Qué medidas toma para promover la colaboración y la concienciación sobre seguridad de la información en la empresa municipal de agua potable y alcantarillado EMAPA?

Respuesta

Se recomienda a los usuarios y personal de la empresa el cambio de las contraseñas y no abrir correos de origen desconocido.

Décima cuarta pregunta

¿Hay algún otro comentario o perspectiva que le gustaría agregar sobre la seguridad en las bases de datos personales?

Respuesta

A medida que surgen nuevas actualizaciones en cuanto a servidores y a control de las Base de Datos, de la misma manera surgen nuevas vulnerabilidades y para ello se debe controlar con el uso de la tecnología de punta para ayudar con la mitigación de estos riesgos.

Conclusión:

Las respuestas resaltan la importancia de garantizar la seguridad de la información en la empresa municipal de agua potable y alcantarillado EMAPA. Sin embargo, también indican áreas que requieren mejoras, como establecer políticas de seguridad formales, concienciar a los empleados sobre seguridad de datos y considerar auditorías regulares para evaluar y mejorar la seguridad de las bases de datos personales. Además, se subraya la necesidad de implementar una política de seguridad formal y proporcionar capacitación en seguridad de datos para el personal. También se reconoce la relevancia de la colaboración y la legislación para fortalecer la seguridad de la información en la empresa municipal de agua potable y alcantarillado EMAPA.

Validación del instrumento

Kuder-Richardson en la encuesta aplicada al personal del área de TI de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.

La confiabilidad y la validez son factores importantes en la recopilación de los datos.

Para evaluar la consistencia interna del conjunto de preguntas formuladas en el cuestionario se aplicó el coeficiente de Kuder-Richardson, que se aplicó a 2 de las 13 preguntas formuladas al personal de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, las cuales son dicotómicas, es decir, brindan dos respuestas si y no, para un acceso rápido y claro a la información que ayudará al progreso de su investigación.

Para realzar el cálculo se utilizó la siguiente formula:

$$r_{kr20} = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum pq}{\sigma^2}\right)$$

Los cálculos se realizaron en Excel para permitir un fácil cálculo de fórmulas mediante la creación de tablas con respuestas recopiladas en las encuestas realizadas anteriormente (Ver Anexo 1).

Tabla 2. Confiabilidad Kuder-Richardson en la encuesta para el Personal del área de TI.

Simbología	**Valor**
k (número de ítems)	2
p (porcentaje de personas que respondieron si en cada ítem)	0,40 & 0,40
q (porcentaje de personas que respondieron si en cada ítem)	0,60 & 0,60
σ^2 (varianza total del Instrumento)	0,80
KR-20	0,80

Tabla 3. Interpretación de la escala de Kuder-Richardson

KR-20	**Interpretación**
0,9 – 10	Excelente
0,8 – 0,89	Buena
0,7 – 0,79	Aceptable
0,6 – 0,69	Débil
0,5 – 0,59	Pobre
< 0,49	Inaceptable

Por tanto, Kuder-Richardson da como valor es de 0,80. Considerando que la fiabilidad de las respuestas del personal del área de TI de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA se encuentra dentro del rango Bueno.

Alfa de Cronbach en la encuesta aplicada al personal del área de TI de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA.

Para validar las demás preguntas desarrolladas en escala de Likert se aplicó otra medida de confiabilidad denominada Alfa de Cronbach.

Para el cálculo del Alfa de Cronbach se aplica la siguiente fórmula:

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum v_1}{vt}\right)$$

Los cálculos se realizaron en Excel para permitir un fácil cálculo de fórmulas mediante la creación de tablas con respuestas recopiladas en las encuestas realizadas anteriormente (Ver Anexo 2).

Tabla 4. Confiabilidad Alfa de Cronbach en la encuesta para el Personal del área de TI

Simbología	Valor
α (alfa)	0,89
k (número de ítems)	2
$\sum v_i$ (varianza de cada ítem)	1.2
vt (varianza total)	2,16

Tabla 5. Interpretación de la escala del Alfa de Cronbach

Alfa de Cronbach	**Interpretación**
0,9 – 10	Excelente
0,8 – 0,89	Buena
0,7 – 0,79	Aceptable
0,6 – 0,69	Débil
0,5 – 0,59	Pobre
< 0,49	Inaceptable

Por tanto, el Alfa de Cronbach da un valor de 0,95. Considerando que la fiabilidad de las respuestas del personal del área de TI de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA se encuentra dentro del rango bueno.

Resultados de las encuestas

La encuesta fue aplicada a un total de 5 personas, las cuales son el personal administrativo del departamento de TI.

Primera pregunta: ¿Cuál es su función en el departamento de TI la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 6. Resultados pregunta 1

Opciones de respuesta	Cantidad	Porcentaje
Analista Técnico	1	20%
Analista de Redes y Telecomunicaciones	1	20%
Analista de TI	3	60%
Total	5	100%

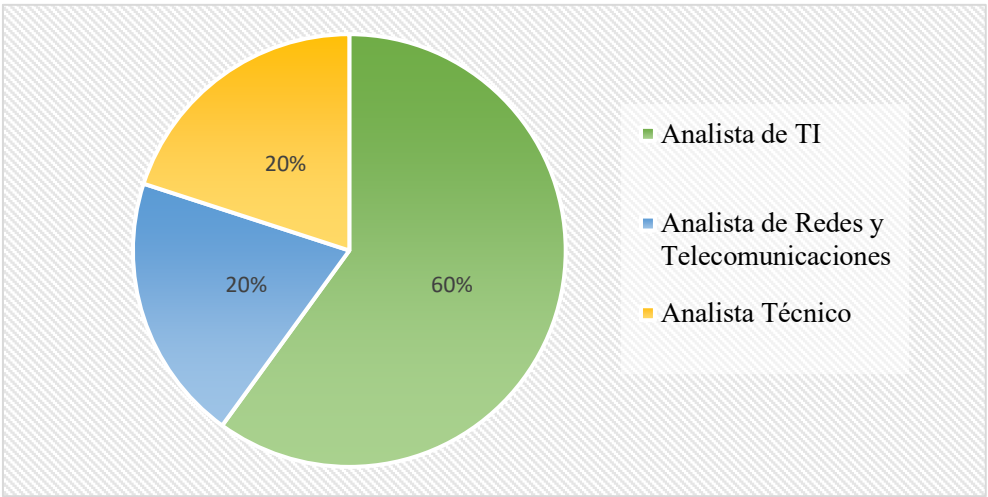


Figura A. Tabulación de resultados pregunta 1

Análisis e interpretación de resultados

De acuerdo con los resultados de la pregunta uno y su análisis en la Figura 1, se tiene que el 100% de los profesionales de la ingeniería trabajan como analistas. El 60% lo

cual representa a tres profesionales se dedican al análisis de TI, el 20% que representa a un profesional es analista de Redes y Telecomunicaciones, y 20% que también representa un profesional, es analista técnico. Estos resultados señalan la predominancia de analistas en el departamento de Tecnologías de la Información (TI), además sugiere que la EMAPA tiene una fuerte orientación a la tecnología.

Segunda pregunta: En una escala del 1 al 5, donde 1 es "muy inseguro" y 5 es "muy seguro", ¿cómo calificaría la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA desde su perspectiva?

Tabla 7. Resultados pregunta 2

Opciones de respuesta	Cantidad	Porcentaje
Muy seguro	0	0%
Seguro	0	0%
Neutral	3	60%
Algo seguro	2	40%
Muy inseguro	0	0%
Total	**5**	**100%**

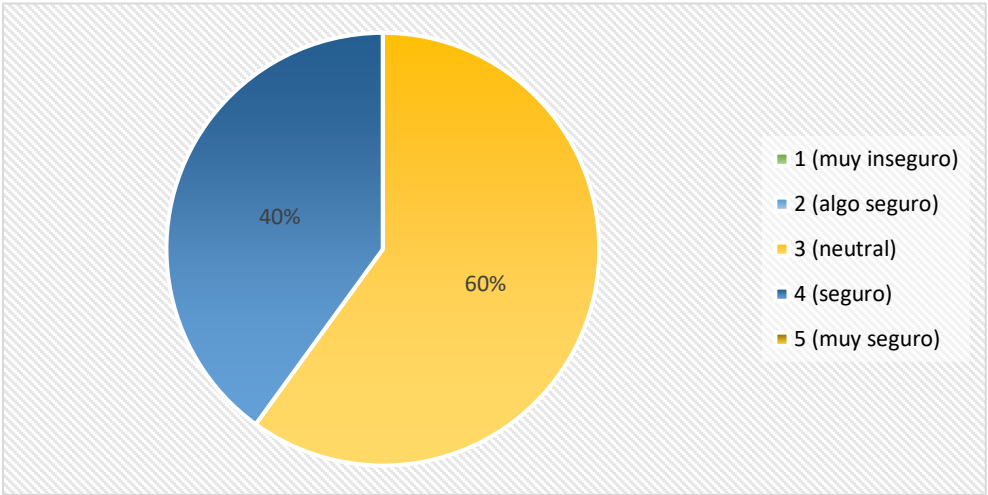


Figura B. Tabulación de resultados pregunta 2

Según los resultados de la Figura 2, la segunda interrogante permite conocer que el 60% de los encuestados, esto representa a tres profesionales señalan que los datos personales se encuentran en un estado neutral, y el 40% que representa a dos

profesionales indican que los datos personales están seguros. Como resultado se evidencia que existe una división de opiniones, lo que indica una necesidad de mejora en la protección de los datos personales.

Tercera pregunta: ¿Ha experimentado alguna vez una violación de la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 8. Resultados pregunta 3

Opciones de respuesta	Cantidad	Porcentaje
Si	2	40%
No	3	60%
Total	5	100%

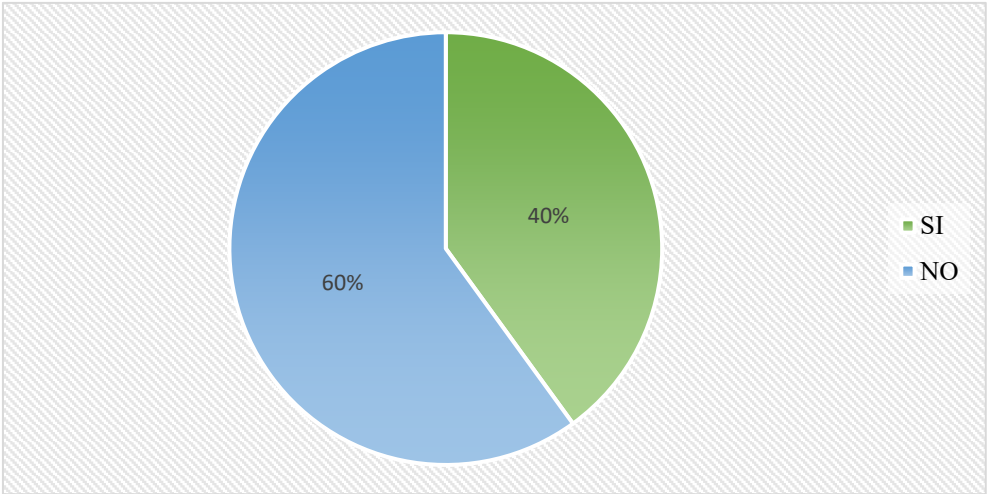


Figura C. Tabulación de resultados pregunta 3

Análisis e interpretación de resultados

Con los resultados obtenidos en la pregunta y correspondiente a la Figura 3, se obtiene como resultado que el 60% es decir tres de los profesionales, no han experimentado violaciones a la seguridad de los datos personales, mientras que el 40% que representa a dos profesionales, si han experimentado estas violaciones. De esta manera se identifica la necesidad de mejorar los conocimientos de los administrativos del departamento de TI para una mejor reacción ante una futura violación a la seguridad de la base de datos.

Cuarta pregunta: ¿Cuáles de los siguientes problemas o preocupaciones relacionados con la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA le inquietan más? (Puede seleccionar varias opciones).

Tabla 9. Resultados pregunta 4

Opciones de respuesta	Cantidad	Porcentaje
Robo de identidad	2	40%
Accesos no autorizados a cuentas	5	100%
Fuga de información	1	20%
Perdida de datos por fallas	2	40%
Brecha de seguridad en servicios en línea	5	100%

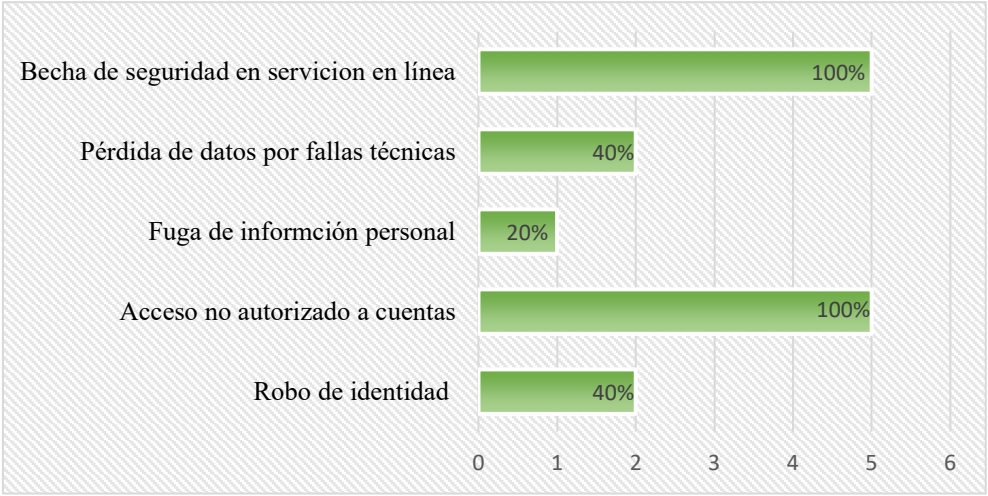


Figura D. Tabulación de resultados pregunta 4

Análisis e interpretación de resultados

Con los resultados obtenidos y representados en la Figura 4, el 100% de los encuestados, el cual representa a cinco profesionales les preocupa la brecha de seguridad en servicios en línea, los cuales tienen una relación directa con la seguridad de los datos personales ya que el servidor tiene conexión directa con el internet. El 100% de los encuestados, representando a cinco profesionales señalan que el acceso no autorizado a cuentas de la EMAPA también es un punto preocupante. Mientras que el 40% de los encuestados, representando a dos profesionales les preocupa que la inseguridad de los datos se da por el robo de identidad, ya que en la actualidad es

la forma más conocida de poner en riesgo los datos personales. El 40% de los encuestados, representando a dos profesionales tienen la preocupación de perder los datos personales por fallas técnicas, como el uso de equipos obsoletos que necesitan actualización constante. Por último, el 20% de los encuestados que representa a un profesional, señala que la preocupación también se encuentra en la fuga de información personal, ya que puede suceder que una persona no autorizada tome por la fuerza algún permiso o acceso a la base de datos. En conclusión, la EMAPA debe prestar especial atención a las amenazas que son más preocupante para los administradores del departamento de TI, y desde ese punto corregir las amenazas menos preocupantes.

Quinta pregunta: En una escala del 1 al 5, donde 1 es "muy inseguro" y 5 es "muy seguro", ¿qué tan seguro siente que están sus datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 10. Resultados pregunta 5

Opciones de respuesta	Cantidad	Porcentaje
Muy seguro	0	0%
Seguro	0	0%
Neutral	3	60%
Algo seguro	0	0%
Muy inseguro	2	40%
Total	**5**	**100%**

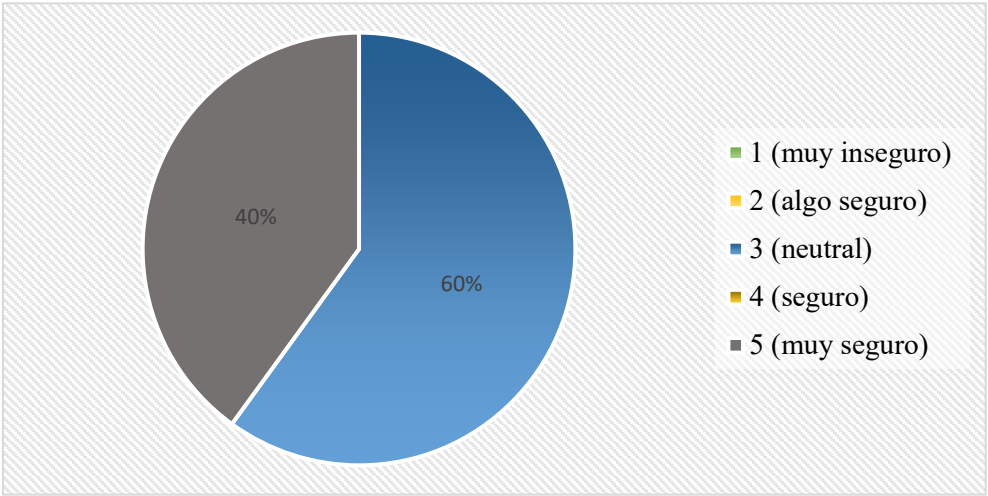


Figura E. Tabulación de resultados pregunta 5

Análisis e interpretación de resultados

Con los resultados obtenidos de la quinta pregunta y referenciados en la Figura 5, se demuestra que el 60% que representa a tres profesionales señalan que los datos personales están en un punto medio, ni seguro, ni inseguro, en cuanto al 40% que representa a dos profesionales, sienten que sus datos están muy seguros. Estos resultados resaltan la importancia de establecer medidas de seguridad apropiadas con el fin de asegurar la protección de la información personal dentro de la EMAPA.

Sexta pregunta: ¿Ha experimentado o conocido casos de problemas relacionados con la seguridad de los datos personales en de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 11. Resultados pregunta 6

Opciones de respuesta	Cantidad	Porcentaje
Filtración de datos	0	0%
Acceso no autorizado	5	100%
Perdida de datos	0	0%
Otro	0	0%
Total	5	100%

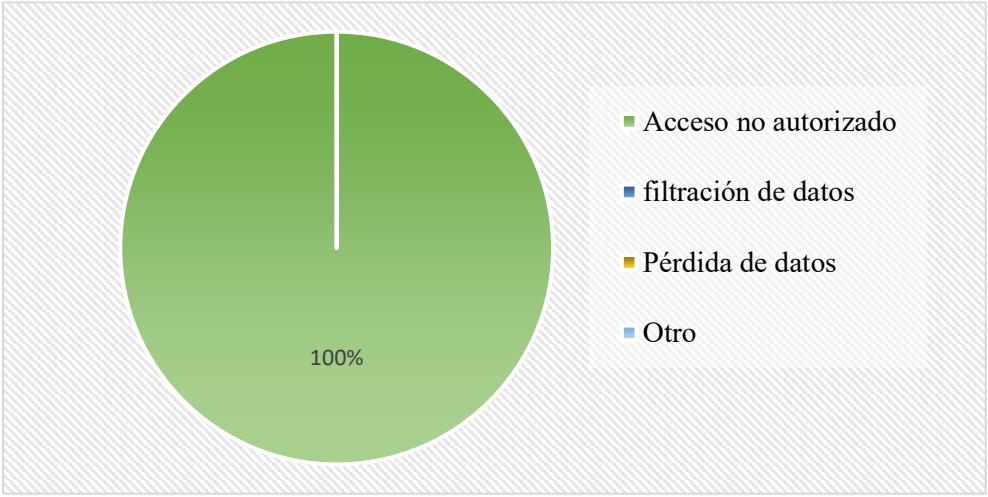


Figura F. Tabulación de resultados pregunta 6

Análisis e interpretación de resultados

De los resultados obtenidos de la pregunta 6, se comprende que el 100% de los encuestados los cuales representan a los cinco profesionales coinciden que el Acceso no autorizado es el principal problema con la seguridad de la base de datos personales. Se entiende que, todos los encuestados coinciden en que el acceso no autorizado es un desafío significativo que se debe controlar para generar una mayor seguridad de la base de datos personal.

Séptima pregunta: Desde su perspectiva en el departamento de TI, ¿cuáles considera que son los problemas más importantes en cuanto a la seguridad de los datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 12. Resultados pregunta 7

Opciones de respuesta	Cantidad	Porcentaje
Falta de conciencia y cultura de seguridad	1	20%
Acceso no autorizado	3	60%
Protección insuficiente de datos	0	0%
Falta de políticas y procedimientos de seguridad	1	20%
Falta de capacitación	4	80%
Cumplimiento legal y normativo	4	80%

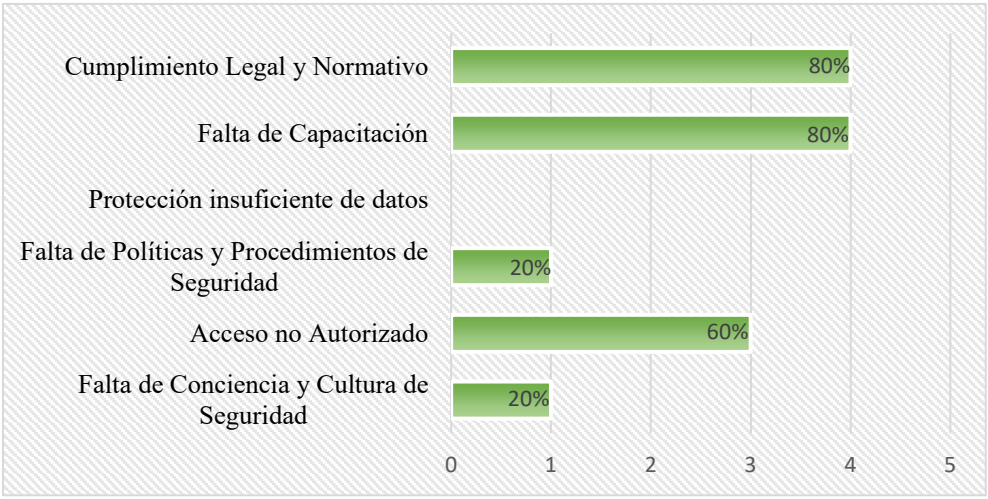


Figura G. Tabulación de resultados pregunta 7

Análisis e interpretación de resultados

En relación a la pregunta siente, el 80% de los encuestados lo cual representa a cuatro profesionales, consideran que uno de los problemas más importantes en cuanto a la seguridad de los datos personales es el cumplimiento Legal y Normativo, además también señalan que la Falta de Capacitación también forma parte de los problemas más importantes en cuando a la seguridad de los datos personales. El 60% que representa a tres profesionales, señalan que el acceso no autorizado también se debe tratar como un aspecto importante para ayudar con la seguridad de los datos personales. El 20% de encuestados que corresponde a un profesional, señala que la Falta de Políticas y Procedimientos de Seguridad, y Falta de Conciencia y Cultura de Seguridad son parte importante de los problemas de la seguridad de los datos personales. Estos resultados destacan la importancia de abordar estos problemas y establecer medidas adecuadas para garantizar la seguridad de los datos personales.

Octava pregunta: ¿Ha habido incidentes de seguridad con los datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, en el pasado?

Tabla 13. Resultados pregunta 8

Opciones de respuesta	Cantidad	Porcentaje
Si	2	40%
No	3	60%
Total	5	100%

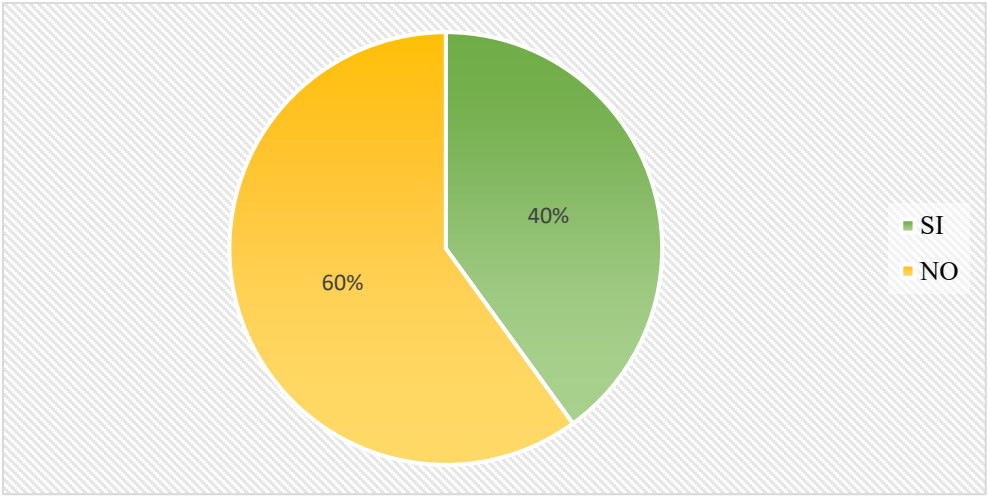


Figura H. Tabulación de resultados pregunta 8

Análisis e interpretación de resultados

En cuanto a los resultados alcanzados en la pregunta 8, el 60% de los encuestados lo que representa a tres profesionales señalan que no han existido incidentes con los datos personales dentro de la EMAPA. Mientras que el 40% de encuestados que corresponde a dos profesionales señalan que si ha habido incidentes con la seguridad de los datos personales en la EMAPA. Estos resultados resaltan la importancia de implementar medidas adecuadas para garantizar la seguridad de los datos personales en la EMAPA y prevenir futuros incidentes.

Novena pregunta: ¿Qué medidas y soluciones de seguridad de datos personales en la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, se han implementado o propuesto en el departamento de TI para abordar los problemas de inseguridad?

Tabla 14. Resultados pregunta 9

Opciones de respuesta	Cantidad	Porcentaje
Acceso restringido	3	60%
Encriptación	0	0%
Auditorias y seguimientos	3	60%
Actualización y parches	3	60%
Copias de seguridad	5	100%
Capacitación	0	0%

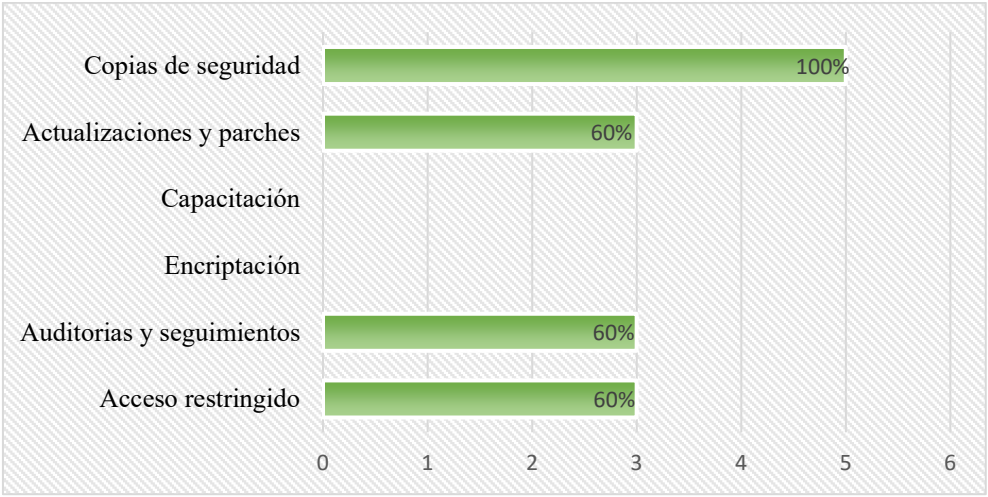


Figura I. Tabulación de resultados pregunta 9

Análisis e interpretación de resultados

Como resultado de la pregunta 9, se obtiene que el 100% de los encuestados que corresponde a cinco profesionales consideran que la medida más importante que se debe aplicar con respecto a la seguridad de los datos personales es las copias de seguridad. Mientras que el 60% de los encuestados, que representa a tres profesionales indican que mantener las actualizaciones, parches de seguridad, realizar auditorías, seguimientos de seguridad y mantener los accesos restringidos deben formar parte de las medidas o soluciones de la protección de seguridad de los datos personales. Pues, son medidas necesarias que mantendrán seguros los datos personales dentro de la EMAPA. Es así que, estos resultados solo resaltan la importancia y necesidad de adoptar un enfoque integral que incorpore medidas preventivas que aseguren un vigilancia activa y constante.

Décima Pregunta: ¿Cuáles considera que son las áreas o departamentos donde se pueden realizar mejoras significativas en la seguridad de datos personales en de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 15. Resultados pregunta 10

Opciones de respuesta	Cantidad	Porcentaje
Departamento de Tecnologías de la información TI	5	100%
Departamento de recursos humanos	0	0%
Departamento de servicio al cliente	0	0%
Departamento de marketing y ventas	0	0%

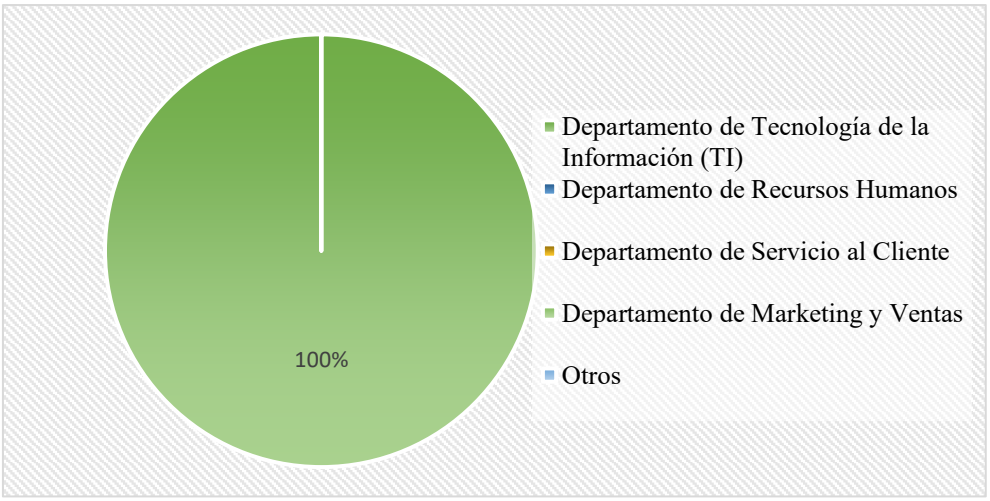


Figura J. Tabulación de resultados pregunta 10

Análisis e interpretación de resultados

En relaciona a la pregunta 10, el 100% de los encuestados que representa a cinco profesionales consideran que el área o departamento donde se pueden realizar mejoras significativas en la seguridad de los datos personales de la EMAPA es el departamento de Tecnologías de la Información (TI). De esta forma, se entiende que la seguridad de los datos debe ser controlada en mayor medida por el departamento de TI. Con los datos obtenidos, se puede considerar a esta unidad como el sector fundamental en el que se deben concentrar los esfuerzos para mejorar la seguridad de los datos personales de la EMAPA. Esto resalta la importancia de fortalecer las habilidades y medidas de seguridad en el departamento de TI, con el fin de asegurar la protección de los datos personales en la organización.

Décima primera pregunta: ¿Cómo colaboraría el departamento de TI con otros departamentos de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA en asuntos relacionados con la seguridad de los datos personales?

Tabla 16. Resultados pregunta 11

Opciones de respuesta	Cantidad	Porcentaje
Implementación de medidas de seguridad adecuadas	3	60%
Educación y concientización	5	100%
Auditorias y monitoreo periódicas	0	0%
Cumplimiento normativo	0	0%
Gestión de incidentes de seguridad	4	80%
Colaboración en proyectos	0	0%

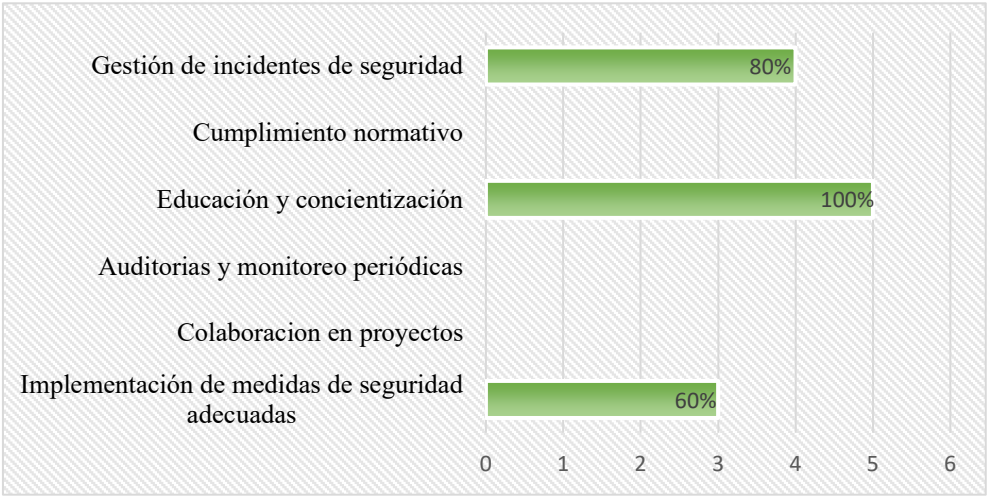


Figura K. Tabulación de resultados pregunta 11

Análisis e interpretación de resultados

En relación a los resultados ofrecidos por la pregunta 11, se entiende que el 100% de los encuestados que corresponde a cinco profesionales nos señala que la educación y concientización enfocada en los diferentes departamentos de la EMAPA es un aspecto clave e importante para la seguridad de los datos personales. El 80% correspondiente a cuatro profesionales, mencionan que la gestión de incidentes de seguridad también forma parte importante del trabajo conjunto con otros

departamentos. El 60% de encuestados que representa a tres profesionales, consideran que la implementación de medidas de seguridad adecuadas también forma parte importante para el fortalecimiento de la seguridad de los datos personales y, esto influye con la colaboración con otros departamentos de la EMAPA. Por lo tanto, los resultados subrayan la necesidad de fomentar una cultura de seguridad integral que comprometa a todos los departamentos de la EMAPA, ya que la importancia de ofrecer una educación continua garantiza una protección sólida de los datos.

Décima segunda: ¿Qué programas de educación o concienciación sobre seguridad de datos personales se han implementado para el personal de EMAPA, incluyendo el departamento de TI?

Tabla 17. Resultados pregunta 12

Opciones de respuesta	Cantidad	Porcentaje
Talleres y capacitación	1	20%
Recursos educativos	0	0%
Colaboración con instituciones	0	0%
Programas de mentoría	0	0%
No se ha implementado nada	4	80%

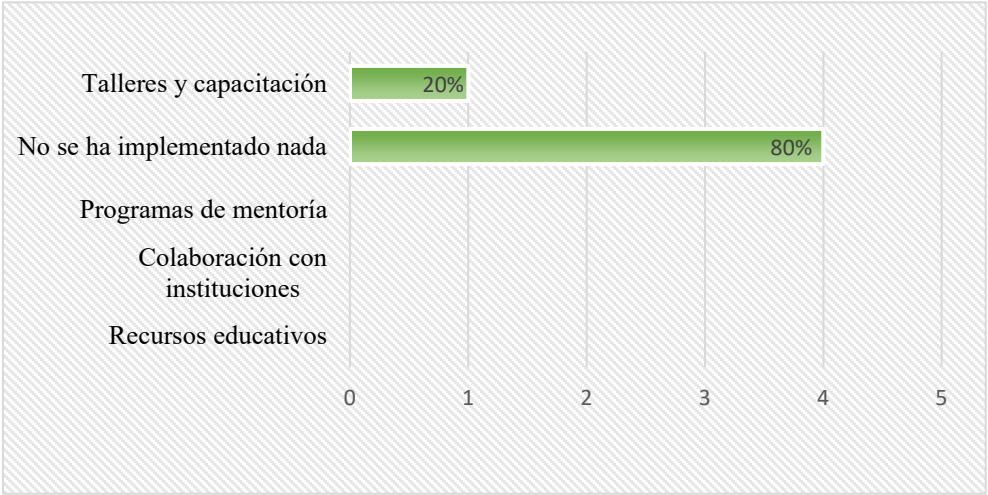


Figura L. Tabulación de resultados pregunta 12

Análisis e interpretación de resultados

En relación a la pregunta doceava y su representación en la Figura 12 , se obtiene que el 80% de los encuestados, los cuales corresponden a cuatro profesionales destacan que no se ha implementado programas de educación o concienciación sobre la seguridad de los datos personales en la EMAPA. Mientras que el 20% correspondiente a una profesional señala que si se ha implementado talleres y capacitaciones con respecto a los programas de educación en la EMAPA. En conclusión, es fundamental e imprescindible implementar programas de educación y concienciación sobre la seguridad de los datos en la EMAPA. Esto permitirá fomentar una comprensión sólida y promover una cultura organizacional de seguridad entre todos los miembros del personal.

Décime tercera: ¿Tiene algún comentario adicional o experiencia personal que desee compartir sobre la seguridad de los datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA?

Tabla 18. Resultados pregunta 13

Opciones de respuesta	Cantidad	Porcentaje
Ninguno	5	100%
Total	5	100%

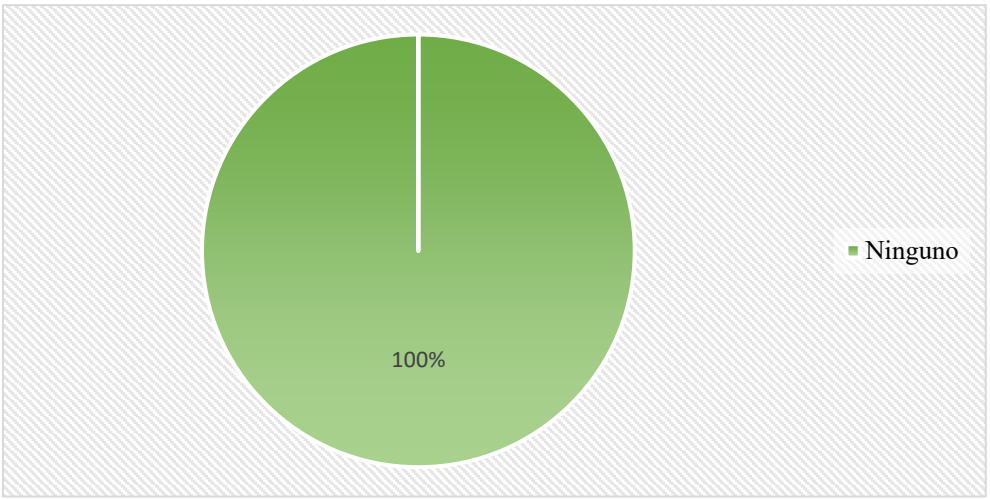


Figura M. Tabulación de resultados pregunta 13

Análisis e interpretación de resultados

En cuanto a la pregunta treceava y su representación en la Figura 13, permite conocer que el 100% de los encuestados correspondiente a los cinco profesionales señalan que no tiene ningún comentario adicional acerca de la seguridad de la base de datos personales de la EMAPA. En conclusión, el análisis de estos datos resalta la importancia de considerar la falta de comentarios como una indicación de que, al menos durante el momento de la encuesta, no se han identificado inquietudes adicionales o problemas significativos relacionados con la seguridad de la base de datos de la organización.

Resultados de la ficha de Observación

<table>
<tr><th colspan="5">Ficha de observación</th></tr>
<tr><td colspan="2">Ficha Nº</td><td colspan="3">Uno</td></tr>
<tr><td colspan="2">Fecha de la Observación</td><td colspan="3">12 de octubre del 2023</td></tr>
<tr><td colspan="2">Tipo de Observación</td><td colspan="3">Seguridad de Base de Datos</td></tr>
<tr><td colspan="2">Departamento</td><td colspan="3">Departamento de Tecnologías de la Información (TI)</td></tr>
<tr><td colspan="2">Tipo de Observación</td><td colspan="3">Seguridad de Base de Datos</td></tr>
<tr><td colspan="2">Objetivo</td><td colspan="3">Evaluar la seguridad de la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, y verificar si se está aplicando medidas de ciberseguridad.</td></tr>
<tr><td>OBSERVADO</td><td colspan="3">NIVEL</td><td>COMENTARIO</td></tr>
<tr><td rowspan="2">Autorización de accesos</td><td>Alto</td><td>Medio</td><td>Bajo</td><td rowspan="2">Se asignan diferentes roles y permisos a los usuarios según su nivel de responsabilidad. Sin embargo, algunos usuarios tienen más privilegios de los necesarios para su función.</td></tr>
<tr><td></td><td>X</td><td></td></tr>
<tr><td rowspan="2">Cifrado de datos</td><td>Alto</td><td>Medio</td><td>Bajo</td><td rowspan="2">Los datos almacenados en la base de datos no están cifrados, lo que los hace vulnerables a posibles ataques o fugas.</td></tr>
<tr><td></td><td></td><td>X</td></tr>
<tr><td rowspan="2">Auditoría y monitorización</td><td>Alto</td><td>Medio</td><td>Bajo</td><td rowspan="2">Las actividades o consultas realizadas a la base de datos no son registradas, además no se realiza revisiones con frecuencias. Si existe alguna anomalía no sería detectada.</td></tr>
<tr><td></td><td></td><td>X</td></tr>
</table>

Protección contra ataques externos	**Alto**	**Medio**	**Bajo**	Los servidores de la base de datos están conectados a internet, lo que los hace vulnerables a intrusiones y malware. Para este riesgo, se utilizan firewalls y antivirus, pero estos no son suficientes para garantizar la seguridad de la base de datos. A demás no se cuentan con actualizaciones de parches de seguridad.
		X		
Autenticación y Contraseñas	**Alto**	**Medio**	**Bajo**	El sistema de autenticación de la base de datos requiere que los usuarios utilicen contraseñas fuertes y que las cambien con regularidad. Además, se recomienda el uso de autenticación de dos factores para proporcionar una capa adicional de seguridad.
		X		
Políticas de Respaldos	**Alto**	**Medio**	**Bajo**	El proceso de respaldos de la base de datos es ineficiente e inseguro. No se realizan copias de seguridad periódicos de todos los datos, y las copias de seguridad que ya se han realizado no se almacenan de forma segura. Lo cual puede provocar la perdida de datos en caso de un incidente.
			X	

Conclusiones:

En base a la observación realizada en cuanto a la Seguridad de Base de Datos se ha identificado que; la evaluación de los diferentes aspectos de seguridad de la base de datos proporcionados luego de la observación demuestra una clara necesidad de mejorar las medidas de seguridad en varios frentes dentro de la Empresa Municipal de Agua Potable y Alcantarillado (EMAPA). Aunque, la organización ha logrado mantener un nivel de seguridad general moderado, existen algunas áreas específicas que requieren una atención inmediata para elevar el nivel de seguridad a uno más sólido y confiable.

Ficha de observación				
Ficha Nº	Dos			
Fecha de la Observación	12 de octubre del 2023			
Tipo de Observación	Medidas de Ciberseguridad			
Departamento	Departamento de Tecnologías de la Información (TI)			
Observador	Christian Jara			
Objetivo	Evaluar la seguridad de la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA, y verificar si se está aplicando medidas de ciberseguridad			
OBSERVADO	**NIVEL**			**COMENTARIO**
Concienciación y capacitación	**Alto**	**Medio**	**Bajo**	La empresa no realiza campañas de sensibilización y formación periódicas para los empleados sobre las buenas prácticas de ciberseguridad y los riesgos potenciales. Esto puede provocar que los empleados cometan errores que puedan comprometer la ciberseguridad de la empresa.
			X	
Protocolo de respuesta a incidentes	**Alto**	**Medio**	**Bajo**	La empresa no tiene un plan para responder a los incidentes de ciberseguridad. Esto provoca que la empresa no pueda responder de manera efectiva a un incidente de ciberseguridad, lo que puede provocar la perdida de datos o la interrupción de los servicios.
			X	
Gestión de activos	**Alto**	**Medio**	**Bajo**	La empresa ha identificado y clasificado los activos de información según su criticidad y valor. Sin embargo, no ha implementado un proceso para actualizar el inventario ni para realizar un seguimiento del ciclo de vida de los mismos. Esto puede provocar que la empresa no tenga una visión actualizada de sus activos de información, lo que puede dificultar la protección de estos activos.
		X		
Documentación y normativa	**Alto**	**Medio**	**Bajo**	La empresa no cuenta con una documentación actualizada y detallada sobre la base de datos. Esto puede dificultar la comprensión de la base de datos y la implementación de medidas de seguridad efectivas. Sin embargo, la empresa
		X		

				cumple con las éticas sobre el tratamiento de los datos personales o sensibles.
Auditorias de ciberseguridad	**Alto**	**Medio**	**Bajo**	La empresa no realiza auditorías periódicas de seguridad. Esto puede provocar que la empresa no sea consciente de las vulnerabilidades y amenazas a las que está expuesta.
			X	
Infraestructura de red	**Alto**	**Medio**	**Bajo**	La empresa ha segmentado adecuadamente su red para reducir el riesgo de incidentes. Sin embargo, los servidores que contienen las bases de datos están conectados a la Internet, lo que aumenta el riesgo de que los datos de la empresa sean comprometidos.
		X		

Conclusiones:

Después, de haber realizado la observación sobre las medidas de ciberseguridad en la Empresa Municipal de Agua Potable y Alcantarillado (EMAPA), se pudo constatar que múltiples aspectos del sistema de seguridad requerían mejoras sustanciales. Si bien, la organización ha tomado algunas medidas para proteger su infraestructura tecnológica, todavía hay áreas críticas que requieren atención inmediata para fortalecer la postura general de ciberseguridad.

2.2.4 Procesamiento y análisis de datos

De los datos obtenidos en la recolección de la información mediate la entrevista, encuesta y la ficha de observación se determinó lo siguiente:

- La falta de políticas escritas para el acceso y la gestión de bases de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado (EMAPA) es una oportunidad para mejorar la seguridad mediante el establecimiento de protocolos formales y procedimientos claros.
- Se detecta una necesidad de capacitación continua en seguridad de la información, además de una legislación más firme para apoyar los esfuerzos de seguridad. Se aconseja una mayor colaboración y empatía para disminuir las amenazas y riesgos presentes en la seguridad de la información.

- Aunque EMAPA no ha recibido quejas o inquietudes específicas de empleados o clientes sobre la seguridad de sus datos personales, aún resalta la necesidad de aumentar la conciencia de seguridad de los empleados y tomar medidas proactivas para proteger las bases de datos personales.

- La identificación de incidentes pasados de violaciones de seguridad de datos, las preocupaciones sobre la falta de capacitación y políticas de seguridad indican la necesidad de implementar un plan de acción integral para prevenir violaciones de seguridad y fortalecer la infraestructura de protección de datos de EMAPA.

- La implementación de medidas preventivas, como copias de seguridad regulares, actualizaciones de seguridad y auditorías periódicas, son esenciales para mejorar la protección de datos personales en la EMAPA, incluso en ausencia de incidentes de seguridad reportados. Estas medidas pueden contribuir significativamente a fortalecer la postura de seguridad de la EMAPA y mitigar posibles amenazas.

- El departamento de TI fue identificado como el sector más importante donde EMAPA podría realizar mejoras significativas en la seguridad de los datos personales, destacando la importancia de fortalecer las capacidades de seguridad del sector.

- La seguridad de la información es una prioridad crítica, y esta evaluación indica las áreas que necesitan atención urgente y mejoras constantes. Se recomienda aplicar medidas de cifrado más robustas, reforzar las políticas de respaldo y optimizar la autenticación, monitorización y políticas de contraseñas. Estas acciones son fundamentales para reducir riesgos y asegurar la integridad, confidencialidad y disponibilidad de los datos almacenados en la base de datos. Estas evaluaciones resaltan la importancia de tener un enfoque más proactivo y riguroso en relación con la seguridad de la base de datos. Esta observación ofrece una orientación clara para las áreas que requieren mejoras.

- Resulta beneficioso asignar recursos adicionales y dedicar una atención más amplia a la concienciación y capacitación de los empleados en ciberseguridad, además, de establecer un protocolo de respuestas a incidentes más robusto y la

ejecución de auditorías regulares para detectar y reducir potenciales vulnerabilidades. Aunque la gestión de activos, la documentación y normativas están en un nivel aceptable, persistir en su mejora constante sigue siendo beneficioso

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

Luego de haber realizado la recolección de la información para saber el nivel de conocimiento del compliance de Ciberseguridad y las medidas de seguridad en la base de datos personales de la Empresa Municipal de Agua Potable y Alcantarillado EMAPA. Se realiza el desarrollo de la propuesta en base a los objetivos específicos planteados al inicio de este proyecto de investigación.

3.1.1 Importancia del compliance

Existen varios tipos de compliance que se aplican en diferentes áreas y sectores de una empresa. Algunos de los tipos de compliance más comunes incluyen:

a) Compliance legal

El cumplimiento legal es una práctica comercial diseñada para garantizar que una empresa cumpla con las leyes y regulaciones que se aplican a sus actividades. La finalidad es prevenir y detectar posibles infracciones, para así adoptar medidas correctivas y evitar que se repitan. En los últimos años, el cumplimiento legal se ha vuelto cada vez más importante debido a la creciente complejidad de las leyes, regulaciones y a la creciente atención de las agencias normalizadoras y del público.

El compliance legal implica diseñar, implementar, gestionar y supervisar un programa de cumplimiento en una empresa específica. Este programa debe incluir los siguientes elementos esenciales [21]:

- **Liderazgo:** La alta dirección de la empresa debe comprometerse con el cumplimiento legal y establecer una cultura de ética y cumplimiento en toda la organización.
- **Evaluación de riesgos**: La empresa debe identificar los riesgos legales a los que está expuesta y evaluar su probabilidad e impacto.

- **Normas y controles**: La empresa debe establecer políticas y procedimientos claros para prevenir y detectar infracciones legales, y establecer controles internos para asegurar su cumplimiento.

- **Capacitación y comunicación**: La empresa debe capacitar a sus empleados sobre las leyes y regulaciones aplicables a su actividad, y comunicarles las políticas y procedimientos de cumplimiento.

- **Monitoreo y revisión**: La empresa debe monitorear y revisar regularmente su programa de cumplimiento para asegurarse de que sigue siendo efectivo y adaptarlo a los cambios según las leyes y regulaciones.

Cumplir con la ley es una tendencia global impulsada por la presión de los estados y las demandas de los consumidores del mercado. Las empresas que implementan un programa de cumplimiento eficaz pueden reducir los riesgos legales, mejorar su reputación y sus relaciones con los clientes y otras partes interesadas.

b) Compliance financiero

El cumplimiento financiero es un conjunto de prácticas y procedimientos que las instituciones financieras deben seguir para garantizar que operan de conformidad con las leyes y regulaciones aplicables. Estas regulaciones están diseñadas para proteger a los inversores, mantener la estabilidad del sistema financiero y prevenir el fraude y el lavado de dinero. El cumplimiento financiero es un componente importante de la gestión de riesgos para las instituciones financieras y es responsabilidad de todos los empleados, desde la alta dirección hasta los empleados de nivel inferior.

El experto en regulación financiera, proporciona una visión detallada de los desafíos que enfrentan las instituciones financieras en términos de cumplimiento normativo. examina cómo las instituciones financieras pueden gestionar de manera efectiva la supervisión regulatoria y cumplir con las numerosas leyes y regulaciones que se les aplican.

El compliance financiero implica una serie de actividades, que incluyen [22]:

- Desarrollo de políticas y procedimientos internos para garantizar el cumplimiento de las leyes y regulaciones aplicables.
- Capacitación de empleados sobre las leyes y regulaciones relevantes y cómo cumplirlas.
- Monitoreo continuo de las operaciones de la institución financiera para identificar y abordar cualquier incumplimiento.
- Mantenimiento de registros precisos y completos de todas las transacciones y actividades.
- Cooperación con los reguladores y otras autoridades para garantizar el cumplimiento de las leyes y regulaciones.

También implica gestión de riesgos, ya que las instituciones financieras deben identificar y evaluar los riesgos asociados con sus operaciones y tomar medidas para mitigarlos. Esto incluye implementar controles internos y realizar auditorías periódicas para garantizar que los controles funcionen de manera efectiva.

El incumplimiento de las leyes y regulaciones financieras puede tener graves consecuencias para las instituciones financieras, incluidas multas, sanciones y daños a la reputación. Además, el incumplimiento puede poner en peligro la estabilidad de todo el sistema financiero, como se vio durante la crisis financiera de 2008.

c) Compliance en comercio internacional

El compliance del comercio internacional se refiere a regular el cumplimiento de las reglas del comercio internacional para evitar multas o violaciones de las leyes aduaneras y comerciales de los países involucrados en transacciones comerciales. Este enfoque se ha vuelto fundamental en el contexto actual de globalización, donde el comercio exterior es parte importante de la estrategia de las empresas que quieren ampliar sus horizontes y aprovechar las oportunidades que ofrecen los mercados internacionales.

El compliance en el comercio internacional abarca elementos comerciales, financieros, operativos y jurídicos tanto para la importación como para la exportación de diversas categorías y productos. Algunos de los aspectos más relevantes del compliance en el comercio internacional son:

- **Identificación de los riesgos a los que está expuesta la organización,** es importante conocer el marco legal del comercio exterior, el cual se encuentra en la Ley de Comercio Exterior, para establecer planes de prevención y contingencia que respondan a las necesidades de la organización, evitando así sanciones administrativas y/o penales, retrasos en la operación y paros en la producción.

- **Contratación de terceros,** en el comercio exterior es necesario contratar a terceros, como transportistas, almacenes, transitarios y agentes portuarios, para satisfacer la demanda relacionada con la logística, además de llevar a cabo negociaciones con las autoridades y otras partes interesadas en nombre de la empresa importadora o exportadora. Por lo tanto, la preocupación por la actuación de estos profesionales debe duplicarse para garantizar su buen desempeño cuando actúan en nombre de la institución.

- **Detección de posibles socios comerciales,** es fundamental analizar en profundidad a los posibles socios comerciales, garantizando el pleno cumplimiento de las normas de seguridad y conformidad, evitando futuros problemas.

- **Automatización de procesos,** la implementación de soluciones tecnológicas, como herramientas comerciales de detección, puede aumentar la visibilidad y la velocidad de los programas de compliance, evitando pérdidas de tiempo y mano de obra innecesaria, permitiendo a las empresas acelerar su crecimiento sin perder el control y la eficiencia.

- **Evaluación de riesgos,** es importante evaluar los riesgos del impacto que se puede generar por las inconsistencias detectadas en las operaciones de comercio exterior. Además, se deben desarrollar acciones correctivas para

prevenir contingencias futuras, teniendo en cuenta la importancia de cumplir con el código de ética corporativo y el marco legal de las organizaciones.

- **Dimensiones del compliance en el comercio internacional y aduanas,** el compliance en el comercio internacional y aduanas tiene una dimensión mayor que la simple supervisión de la clasificación arancelaria de la mercancía o la verificación de los certificados de origen. Involucra aspectos como la correcta declaración de los identificadores en la operación, la gestión de los riesgos aduaneros y la interpretación de los detalles que pueden afectar el cumplimiento de las normas [23].

El compliance en el comercio internacional es un proceso complejo y en constante evolución que requiere un enfoque integral y una gestión eficiente de los recursos. Las empresas que implementan con éxito políticas de cumplimiento efectivas pueden identificar errores, minimizar riesgos y maximizar los resultados de sus actividades internacionales.

d) Compliance en salud y seguridad

El compliance en salud y seguridad se refiere a un conjunto de prácticas y procedimientos que las empresas deben seguir para garantizar que cumplen con las leyes y regulaciones relacionadas con la salud y seguridad ocupacional. Estas regulaciones tienen como objetivo proteger a los trabajadores y prevenir accidentes laborales, enfermedades profesionales y otros riesgos laborales. El cumplimiento de las normas de salud y seguridad es una parte esencial de la gestión de riesgos de una empresa y es responsabilidad de todos los empleados, desde los altos directivos hasta el personal de nivel de entrada.

Una visión detallada de los desafíos que enfrentan las empresas en términos de cumplimiento normativo en materia de salud y seguridad ocupacional. El autor, un experto en salud y seguridad ocupacional, examina cómo las empresas pueden gestionar de manera efectiva la supervisión regulatoria y cumplir con las numerosas leyes y regulaciones que se les aplican. El compliance en salud y seguridad implica una serie de actividades, que incluyen [24]:

- Desarrollo de políticas y procedimientos internos para garantizar el cumplimiento de las leyes y regulaciones aplicables en materia de salud y seguridad ocupacional.

- Capacitación de empleados sobre las leyes y regulaciones relevantes y cómo cumplirlas.

- Monitoreo continuo de las operaciones de la empresa para identificar y abordar cualquier incumplimiento en materia de salud y seguridad ocupacional.

- Mantenimiento de registros precisos y completos de todas las transacciones y actividades relacionadas con la salud y seguridad ocupacional.

- Cooperación con los reguladores y otras autoridades para garantizar el cumplimiento de las leyes y regulaciones.

El compliance en salud y seguridad también involucra la gestión de riesgos, ya que las empresas deben identificar y evaluar los riesgos asociados a sus operaciones y tomar medidas para mitigarlos. Esto implica implementar controles internos y realizar auditorías periódicas para asegurar que los controles estén funcionando de manera efectiva. No cumplir con las leyes y regulaciones en salud y seguridad ocupacional puede tener consecuencias serias para una empresa, incluyendo multas, sanciones y daños a su reputación. Además, el incumplimiento puede poner en peligro la seguridad y salud de los trabajadores, lo que puede resultar en accidentes laborales, enfermedades profesionales y otros riesgos relacionados con el trabajo.

e) Compliance en ética empresarial

El compliance en ética empresarial abarca un conjunto de prácticas y procedimientos que las empresas deben seguir para asegurar que su funcionamiento esté alineado con las leyes y regulaciones pertinentes en el ámbito ético. Estas normativas se han establecido con el propósito de resguardar los derechos de los empleados, clientes, proveedores y demás partes interesadas, además de prevenir conductas empresariales deshonestas o ilícitas. Es un

componente integral de la gestión de riesgos de una compañía y representa una responsabilidad compartida por todos los miembros del personal, desde la alta dirección hasta el personal de nivel inicial.

Los desafíos que enfrentan las empresas en términos de cumplimiento normativo en materia de ética empresarial. El autor, un experto en ética empresarial, examina cómo las empresas pueden gestionar de manera efectiva la supervisión regulatoria y cumplir con las numerosas leyes y regulaciones que se les aplican. El compliance en ética empresarial implica una serie de actividades, que incluyen [25]:

- Desarrollo de políticas y procedimientos internos para garantizar el cumplimiento de las leyes y regulaciones aplicables en materia de ética empresarial.
- Capacitación de empleados sobre las leyes y regulaciones relevantes y cómo cumplirlas.
- Monitoreo continuo de las operaciones de la empresa para identificar y abordar cualquier incumplimiento en materia de ética empresarial.
- Mantenimiento de registros precisos y completos de todas las transacciones y actividades relacionadas con la ética empresarial.
- Cooperación con los reguladores y otras autoridades para garantizar el cumplimiento de las leyes y regulaciones.

El compliance en ética empresarial también implica la gestión de riesgos, ya que las empresas deben identificar y evaluar los riesgos asociados con sus operaciones y tomar medidas para mitigarlos. Esto incluye la implementación de controles internos y la realización de auditorías periódicas para garantizar que los controles estén funcionando de manera efectiva. El incumplimiento de las leyes y regulaciones en materia de ética empresarial puede tener graves consecuencias para una empresa, incluyendo multas, sanciones y daños a su reputación. Además, el incumplimiento puede poner en peligro la confianza de

los grupos de interés, lo que puede resultar en pérdida de clientes, proveedores y otros socios comerciales.

f) Compliance en seguridad de la información

El compliance en seguridad de la información se refiere al conjunto de prácticas y procedimientos que una organización debe seguir para garantizar la confidencialidad, integridad y disponibilidad de la información que maneja. La norma ISO 27001:2013 es un estándar internacional que establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) en una organización. El cumplimiento de esta norma es fundamental para proteger los activos de información de una organización y garantizar la confianza de sus partes interesadas.

Proporciona una visión general de los requisitos de la norma y ofrece consejos prácticos para su implementación. A continuación, se presentan algunos aspectos clave del compliance en seguridad de la información:

- Identificación de activos de información: Una organización debe identificar y clasificar sus activos de información para determinar su valor y el nivel de protección requerido.

- Evaluación de riesgos: Se deben realizar evaluaciones de riesgos para identificar las amenazas y vulnerabilidades que podrían afectar la seguridad de la información de una organización, y tomar las medidas necesarias para mitigar estos riesgos.

- Política de seguridad de la información: Una organización debe establecer una política de seguridad de la información que establezca sus objetivos y compromisos en materia de seguridad de la información.

- Gestión de accesos: Se deben implementar controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información.

- Gestión de incidentes de seguridad de la información: Una organización debe tener procedimientos en marcha para detectar, responder y recuperarse de los incidentes de seguridad de la información.

- Auditorías internas y revisiones de la dirección: Se deben realizar auditorías internas periódicas para evaluar la eficacia del SGSI de una organización, y la dirección debe revisar regularmente el SGSI para garantizar su adecuación y eficacia continua.

La ciberseguridad se refiere a la protección de los sistemas informáticos y la información que manejan contra amenazas cibernéticas, como ataques de hackers, malware y phishing. Para lograr la ciberseguridad, una organización debe implementar medidas de seguridad físicas, técnicas y organizativas adecuadas para proteger sus activos de información en todas las situaciones posibles [26].

g) Compliance orientado a las Bases de Datos personales

Compliance, o cumplimiento normativo, es un conjunto de procedimientos y buenas prácticas adoptadas por una organización para identificar y clasificar los riesgos operativos y legales que enfrenta. En caso de las bases de datos personales, el cumplimiento se refiere al procesamiento y protección de la información personal de un individuo de acuerdo con las regulaciones de protección de datos aplicables.

El objetivo principal del compliance de las bases de datos personales es garantizar el cumplimiento de las leyes y regulaciones que protegen la privacidad y los derechos de las personas en relación con el procesamiento de datos personales. Algunas de las normas vigentes en esta materia son:

- Ley de Protección de Datos Personales (LOPD) en España[27].

- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México[28].

- Ley orgánica de protección de datos personales[29].

El compliance en el manejo de bases de datos personales implica establecer medidas de seguridad apropiadas para resguardar la confidencialidad, integridad y disponibilidad de la información personal. Además, implica adoptar políticas y procedimientos que aseguren el respeto de los derechos de los titulares de los datos, como el derecho de acceder a su información, corregirla, cancelarla y oponerse a su uso (conocidos como derechos ARCO).

3.1.2 Importancia de la ciberseguridad

Existe varios tipos de ciberseguridad que se aplican en diferentes áreas y contextos. Algunos de los tipos más comunes incluyen:

a) Seguridad de la red

La seguridad de la red es un aspecto importante en el mundo actual, donde la información y los datos son activos valiosos y están constantemente amenazados.

La seguridad de la red se refiere a la protección de los activos de información y los recursos de una organización, a través de la implementación de medidas y controles para prevenir y detectar amenazas, y responder a ellas de manera efectiva. Los activos de información incluyen datos, sistemas, redes, dispositivos y aplicaciones.

Principios de la seguridad de la red [30]:

- **Confidencialidad,** garantizar que la información solo esté disponible para las personas autorizadas a acceder a ella.
- **Integridad,** asegurar que la información no se modifique de manera no autorizada o accidental.
- **Disponibilidad,** garantizar que la información y los recursos estén disponibles cuando se necesiten.
- **Autenticación,** verificar la identidad de los usuarios y los dispositivos.

- **Autorización,** otorgar a los usuarios los permisos adecuados para acceder a los recursos.

- **Responsabilidad,** rastrear las acciones de los usuarios y responsabilizarlos por sus acciones.

- **No repudio**, garantizar que una vez que se haya realizado una acción, no se pueda negar su realización.

La seguridad de la red es esencial para proteger la información y los datos en el mundo actual. La información y los datos son activos valiosos que están constantemente expuestos a amenazas. La implementación de medidas y controles adecuados, junto con una gestión efectiva de incidentes de seguridad, puede ayudar a proteger estos activos.

b) Seguridad de aplicaciones

La seguridad de las aplicaciones es de suma importancia en el proceso de desarrollo y lanzamiento de software. En un entorno cada vez más digitalizado, donde las aplicaciones web desempeñan un papel fundamental en la interacción con los usuarios y el manejo de información confidencial, es fundamental asegurar la protección de los datos y la integridad de los sistemas.

Las aplicaciones web frecuentemente fallan al autenticar, cifrar, y proteger la confidencialidad e integridad de tráfico de red sensible. Las aplicaciones web también frecuentemente redirigen y reenvían a los usuarios hacia otras páginas o sitios web, y utilizan datos no confiables para determinar la página de destino. Sin una validación apropiada, los atacantes pueden redirigir a las víctimas hacia sitios de phishing o malware, o utilizar reenvíos para acceder páginas no autorizadas.

La seguridad de las aplicaciones web puede producirse en varias etapas, pero el establecimiento de mejores prácticas se hace con mayor frecuencia en las fases de desarrollo de aplicaciones. Sin embargo, las empresas también pueden aprovechar diferentes herramientas y servicios posteriores al desarrollo. En

general, hay cientos de herramientas de seguridad a disposición de las empresas, cada una de las cuales sirve para propósitos únicos.

Las empresas saben que la seguridad de los centros de datos en general es importante, pero pocas tienen políticas de seguridad de aplicaciones bien definidas para seguirles el ritmo a los cibercriminales e incluso ir un paso adelante. Por lo tanto, es importante que las organizaciones realicen un esfuerzo significativo para asegurar que la información y recursos están protegidos [31].

c) Seguridad en la nube

La seguridad de las aplicaciones en la nube es un tema crítico en el entorno actual y muchas organizaciones están adoptando servicios en la nube para almacenar y procesar datos.

La seguridad de las aplicaciones en la nube implica la implementación de medidas y mejores prácticas para garantizar la protección de los datos y la integridad de los sistemas en un entorno de computación en la nube. Esto implica considerar aspectos específicos relacionados con la arquitectura, el desarrollo y el despliegue de aplicaciones en la nube.

En la seguridad de las aplicaciones en la nube, se deben tener en cuenta los siguientes aspectos [32]:

- **Autenticación y autorización,** es fundamental implementar mecanismos de autenticación sólidos para verificar la identidad de los usuarios y controlar su acceso a las aplicaciones en la nube. Además, se deben establecer políticas adecuadas de autorización que definan los permisos y privilegios de los usuarios.

- **Gestión de identidad,** la gestión adecuada de la identidad de los usuarios es esencial en la seguridad de las aplicaciones en la nube. Esto implica la implementación de sistemas de gestión de identidad y acceso (IAM) para administrar los usuarios, roles y permisos de manera eficiente y segura.

- **Segregación de datos,** es importante garantizar que los datos de diferentes clientes estén debidamente segregados en la nube para evitar el acceso no autorizado. Esto se logra mediante la implementación de mecanismos de aislamiento y cifrado de datos que protejan la confidencialidad y la integridad de la información.

- **Protección de datos en tránsito y en reposo, l**as aplicaciones en la nube deben garantizar la seguridad de los datos tanto en tránsito como en reposo. Esto implica el uso de protocolos de cifrado robustos, como SSL/TLS, para proteger la información durante la transmisión, así como el cifrado de los datos almacenados en la nube.

- **Auditoría y cumplimiento normativo,** es necesario implementar mecanismos de auditoría y registro de eventos para monitorear y rastrear las actividades en las aplicaciones en la nube. Además, se deben cumplir los requisitos normativos y legales aplicables a la protección de datos y la privacidad.

- **Pruebas de seguridad,** realizar pruebas de seguridad regulares para identificar y corregir posibles vulnerabilidades es fundamental en la seguridad de las aplicaciones en la nube. Esto puede incluir pruebas de penetración, análisis estático y dinámico de código, y revisiones de seguridad.

La seguridad de las aplicaciones en el contexto de la certificación CCSP es un aspecto crítico de la protección de datos, clientes y organizaciones en la nube. Los profesionales de CCSP deben demostrar competencia en el diseño, desarrollo, implementación y gestión de seguridad de aplicaciones en la nube, así como la capacidad de cumplir con los marcos de seguridad y las mejores prácticas relevantes.

d) Seguridad de dispositivos

La seguridad de los dispositivos es un aspecto importante en el mundo móvil actual, donde los dispositivos móviles se han convertido en una parte integral de la vida diaria. Las personas y las organizaciones utilizan dispositivos móviles

para realizar una variedad de tareas, desde realizar llamadas telefónicas hasta acceder a datos confidenciales.

La seguridad de los dispositivos móviles implica la implementación de medidas y buenas prácticas para proteger la información y los sistemas en estos dispositivos. Algunos aspectos clave a considerar son [33]:

- **Autenticación y control de acceso,** es fundamental implementar mecanismos de autenticación sólidos, como contraseñas seguras, reconocimiento biométrico o autenticación de dos factores, para garantizar que solo los usuarios autorizados puedan acceder al dispositivo.

- **Actualizaciones y parches,** mantener el sistema operativo y las aplicaciones actualizadas con las últimas correcciones de seguridad es esencial para proteger el dispositivo contra vulnerabilidades conocidas. Además, se deben aplicar los parches de seguridad tan pronto como estén disponibles.

- **Cifrado de datos, e**l cifrado de datos es una medida importante para proteger la confidencialidad de la información almacenada en el dispositivo. Se debe utilizar el cifrado de almacenamiento para proteger los datos en reposo y el cifrado de la comunicación para proteger los datos en tránsito.

- **Gestión de aplicaciones, e**s importante descargar aplicaciones solo de fuentes confiables, como las tiendas oficiales de aplicaciones. Además, se deben revisar los permisos solicitados por las aplicaciones y limitar el acceso a la información y funciones del dispositivo solo a lo necesario.

- **Protección contra malware,** los dispositivos móviles son susceptibles a ataques de malware, como virus, troyanos y ransomware. Es fundamental contar con una solución de seguridad confiable que incluya un antivirus y una protección en tiempo real contra amenazas.

- **Conexiones seguras, a**l conectarse a redes Wi-Fi públicas, se debe tener precaución y utilizar una conexión segura mediante el uso de una VPN (Red Privada Virtual) para proteger la información transmitida.

- **Respaldo y recuperación de datos,** realizar copias de seguridad periódicas de los datos almacenados en el dispositivo es esencial para garantizar que la información no se pierda en caso de robo, pérdida o daño del dispositivo. Además, se debe tener un plan de recuperación de datos en caso de incidentes.

- **Educación y concientización,** la concientización sobre las mejores prácticas de seguridad es fundamental para proteger los dispositivos móviles. Los usuarios deben ser educados sobre la importancia de no hacer clic en enlaces sospechosos, no descargar aplicaciones de fuentes no confiables y proteger su información personal.

e) Seguridad de la información

La seguridad de la información es un aspecto fundamental en la protección de los activos de una organización, incluyendo los datos, la privacidad y la integridad de los sistemas y las comunicaciones.

Entre los aspectos más importantes relacionados con loa seguridad de la información, incluyen [34]:

- Los fundamentos de la seguridad de la información, como la confidencialidad, la integridad y la disponibilidad de los datos.

- Los principios de la gestión de la seguridad de la información, incluyendo la identificación de activos, la evaluación de riesgos, la implementación de controles y la monitorización de la efectividad de los controles.

- Las amenazas y los ataques comunes a la seguridad de la información, como el malware, el phishing, la ingeniería social y los ataques de denegación de servicio.

- Las tecnologías y las técnicas de seguridad de la información, incluyendo el cifrado, la autenticación, la autorización y la gestión de identidades.

- Los marcos y las mejores prácticas de seguridad de la información, como ISO 27001, NIST SP 800-53 y COBIT.

- Los aspectos legales, éticos y de cumplimiento de la seguridad de la información, incluyendo la privacidad de los datos, la protección de la propiedad intelectual y el cumplimiento de las regulaciones.

La seguridad de la información, abordando los fundamentos, las prácticas y las tecnologías relacionadas con la protección de los activos de una organización. Al adoptar un enfoque integral y proactivo hacia la seguridad de la información, las organizaciones pueden fortalecer su postura de seguridad y mitigar posibles riesgos y amenazas en un entorno digital cada vez más complejo y dinámico.

f) Seguridad de Base de Datos personales

La seguridad de las bases de datos personales es un aspecto crítico de la protección de la información personal confidencial. En un entorno cada vez más digital, donde se recopilan y almacenan grandes cantidades de datos personales, es fundamental garantizar una protección adecuada de esta información sensible.

Las amenazas a la seguridad de la base de datos personales pueden provenir de una variedad de fuentes, incluyendo [35][36][37][38]:

- **Ataques maliciosos,** los ataques maliciosos son realizados por personas u organizaciones con la intención de dañar o robar datos personales. Los ataques maliciosos pueden incluir ataques de malware, ataques de denegación de servicio y ataques de phishing.

- **Errores humanos,** los errores humanos pueden causar accidentes que pueden conducir a la pérdida o divulgación de datos personales. Los errores humanos pueden incluir errores de entrada de datos, errores de configuración y errores de uso.

- **Fallos de hardware o software,** los fallos de hardware o software pueden causar la pérdida o divulgación de datos personales. Los fallos de hardware

o software pueden incluir fallos de disco duro, fallos de software y fallos de red.

Los principios de seguridad de la base de datos personales son las pautas que se deben seguir para proteger los datos personales. Estos principios incluyen:

- **Confidencialidad,** la confidencialidad se refiere a la protección de los datos personales de acceso no autorizado.
- **Integridad,** la integridad se refiere a la protección de los datos personales de la modificación no autorizada.
- **Disponibilidad,** la disponibilidad se refiere a la protección de los datos personales de la pérdida o destrucción no autorizada.

3.1.3 Comparación de características entre compliance de base de datos personales y seguridad de base de datos personales.

El siguiente cuadro representa las características de compliance de base de datos personales y las características seguridad de base de datos personales con el fin de enfatizar su compatibilidad.

Tabla 19. Tabla de características de compliance de base de datos y seguridad de base de datos.

Características	Compliance de Base de datos personales	Seguridad de Base de datos personales
Objetivo	Garantizar el cumplimiento de la normativa de protección de datos personales.	Proteger la información personal del acceso, uso, divulgación, alteración o destrucción no autorizada.
Enfoque	Cumplimiento de normas y reglamentos en materia de protección de datos personales.	Protección activa de los datos personales contra accesos no autorizados o perdida de integridad.

Características	Compliance de Base de datos personales	Seguridad de Base de datos personales
Medidas y Controles	Políticas, procedimientos y prácticas para cumplir con la normativa.	Controles técnicos y de gestión para proteger los datos personales.
Elementos Clave	Políticas de privacidad, gestión de derechos de los titulares de datos.	Cifrado de datos, controles de acceso, prevención de amenazas.
Responsabilidades Clave	Asegurar que la recopilación y el tratamiento de datos se realicen de manera ética y legal.	Implementar medidas técnicas para proteger proactivamente la información personal contra posibles riesgos y amenazas.
Consideraciones legales	Cumplimiento de leyes de protección de datos como GDPR, CCPA, HIPAA, entre otras.	Cumplimiento de regulaciones específicas de seguridad de datos y leyes de privacidad en función del contexto de uso de los datos.
Beneficios	Evitar sanciones administrativas	Proteger la confidencialidad, integridad y disponibilidad de los datos personales

El compliance de la base de datos personal y la seguridad de la base de datos personal son dos ideas que se complementan. Los dos aspectos son cruciales para garantizar la protección de los datos personales, pero tienen enfoques ligeramente diferentes Mientras que el compliance se enfoca en seguir las regulaciones, la seguridad se concentra en resguardar la información personal

3.1.4 Metodologías para optimizar la seguridad de la base de datos personal.

La tabla comparativa que se muestra a continuación destaca las metodologías más eficientes para la optimizar la seguridad de la base de datos personal.

Tabla 20. Metodologías para la optimización de la seguridad de la base de datos personal

Características	Kanban	Scrum	Lean
Descripción	Método visual para administrar tareas y flujo de trabajo, originalmente desarrollado por Toyota en su sistema de producción.	Es un marco de trabajo ágil que se enfoca en la entrega rápida y continua de un producto de alto valor. Define roles claros y eventos.	Se centra en la eliminación de desperdicios y la mejora continua en los procesos de producción. Derivado del Sistema de Producción Toyota.
Enfoque	No se establece un periodo determinado. Reduce los tiempos de desarrollo.	Ciclos de trabajo fijos llamados sprints,	Determinar, analizar y entender realmente lo que sucede en la empresa.
Componentes	Tablero Kanban, tareas, columnas, tarjetas.	Sprints, backlog, sprint backlog, sprint review, sprint retrospective.	Valor agregado, flujo de valor, mapeo del flujo de valor, desperdicio.
Flexibilidad	Se adapta fácilmente a diferentes tipos de proyectos y equipos.	Adecuado para equipos que requieren una estructura más rígida.	Adaptable a diferentes contextos de producción.
Escalabilidad	A menudo se utiliza en equipos pequeños y proyectos simples.	Puede adaptarse a proyectos más grandes a con el uso de eventos de coordinación.	Puede aplicarse a empresas de diferentes tamaños.
Ventajas	Mejora la visibilidad, la eficiencia y la colaboración.	Es flexible y adaptable, permite iteraciones y entregas rápidas.	Es una filosofía general que puede aplicarse a cualquier proceso.

A través de la evaluación llevada a cabo en la **Tabla 20** sobre las metodologías para la optimización de la seguridad de la base de datos personal, se optó por la utilización de la metodología Kanban considerando sus características y beneficios como: flexibilidad por su alta adaptabilidad y se puede aplicar a varios proyectos, enfoque visual de flujo de trabajo a través de la gestión visual de tareas a través de tableros Kanban, no impone reuniones prescritas. Con lo cual ayuda a cumplir los requerimientos de la seguridad de la base de datos personales.

3.2 Desarrollo la propuesta

Para el desarrollo del proyecto se utilizaron ocho etapas, las cuales fueron evaluadas utilizando le metodología Kanban. Estas etapas permiten un desarrollo más ágil y flexible de la seguridad de la base de datos personales de la EMAPA aplicando compliance de ciberseguridad. Para la aplicación de la metodología Kanban se utilizó el software Kanban Flow:

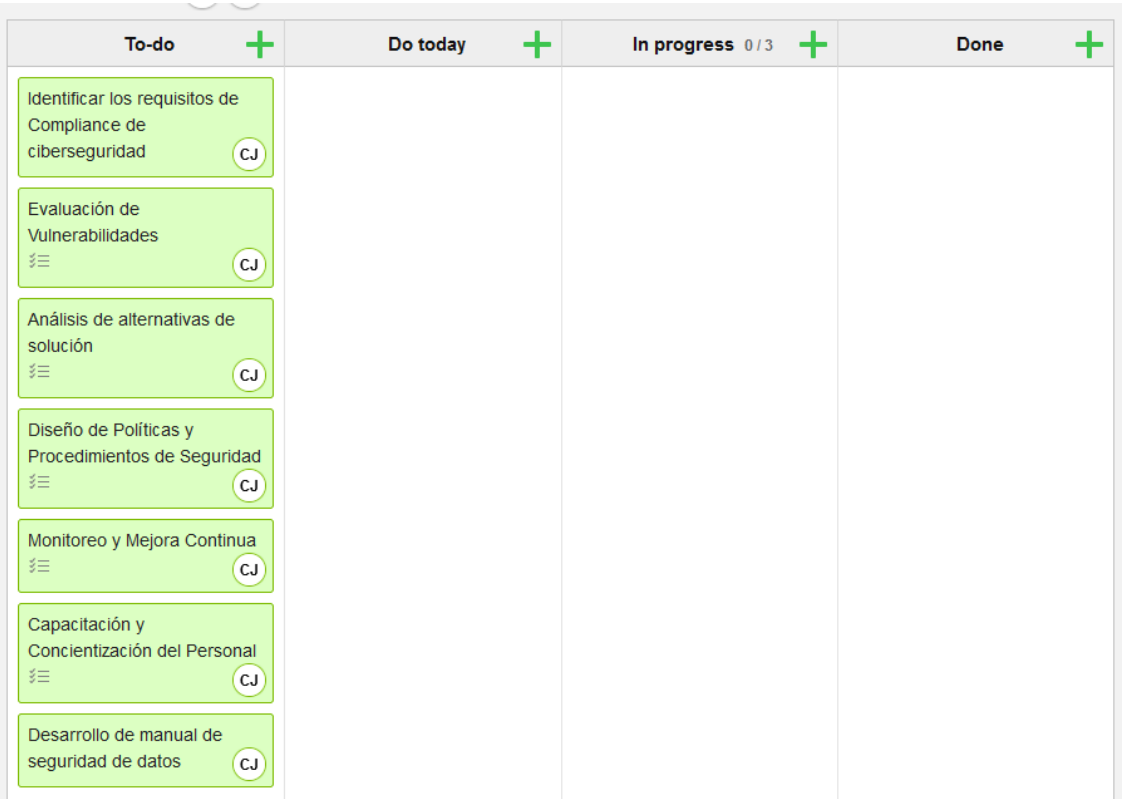


Figura N. Etapas de la metodología Kanban

3.2.1 Etapa uno: Identificar los requisitos de Compliance de ciberseguridad.

Para satisfacer las exigencias de cumplimiento de ciberseguridad para la base de datos personal, es esencial ajustarse a regulaciones específicas que gobiernan la salvaguarda de datos. Algunas de estas regulaciones abarcan el Reglamento NYDFS 23 NYCRR 500, el cual establece criterios en aspectos cruciales como la codificación de información confidencial, la designación de un director de Seguridad de la Información, la realización de evaluaciones de riesgos, entre otros. Además, la

implementación del principio de Confianza Cero puede contribuir al cumplimiento de los requisitos normativos y de cumplimiento al supervisar el acceso a datos personales y reducir los riesgos de seguridad. El cumplimiento en ciberseguridad implica adherirse a regulaciones para satisfacer las exigencias legales, contractuales o éticas, y tiene como objetivo garantizar que la información de la entidad cumpla con estándares y normativas específicas de seguridad. El cumplimiento en tecnologías de la información (IT), en el ámbito de la ciberseguridad, busca asistir a la organización en el cumplimiento de todas las obligaciones legales derivadas de normativas, reglamentaciones y leyes, enfocadas en entornos y sistemas digitales y la protección de la información.

Es importante tener en cuenta los requerimientos siguientes:

a) **Confidencialidad y seguridad de los datos,** es esencial garantizar la confidencialidad y seguridad de la información personal resguardada en la base de datos. Esto requiere la aplicación de medidas de protección apropiadas, tales como la codificación de datos y la limitación de acceso a la información confidencial.

b) **Cumplimiento de regulaciones,** se requiere examinar y adherirse a las normativas legales correspondientes, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. Estas normativas imponen condiciones particulares para la salvaguarda de datos personales y pueden diferir según el país o área geográfica.

c) **Gestión de activos,** reconocer y administrar de manera efectiva los recursos asociados con la base de datos, como la información, el personal, los dispositivos y los sistemas. Esto implica la aplicación de medidas de seguridad destinadas a resguardar dichos recursos contra amenazas y peligros potenciales.

d) **Análisis de riesgos,** conducir evaluaciones de riesgos con el objetivo de reconocer los recursos, amenazas y debilidades vinculadas a la base de datos. A partir de este análisis, es crucial instaurar medidas de seguridad apropiadas para contrarrestar los riesgos identificados.

El acatamiento de estos criterios de compliance en ciberseguridad puede asistir a la EMAPA en resguardar sus bases de datos personales frente a ciberataques, fallos humanos y otras posibles amenazas.

3.2.2 Etapa dos: Evaluación de vulnerabilidades.

Se realizó un análisis de riesgos que permita identificar las posibles amenazas y vulnerabilidades que pueden afectar la seguridad y privacidad de los datos personales, así como las medidas y controles que se pueden implementar para prevenir o mitigar estos riesgos. Tanto las amenazas como las vulnerabilidades fueron identificadas a través de los instrumentos de recopilación de información. Estos datos se analizaron meticulosamente para elaborar la siguiente tabla. Estas vulnerabilidades fueron analizadas utilizando una escala que categoriza los niveles de riesgo como alto, medio y bajo. Estas categorías están directamente vinculadas con la gravedad o riesgo relacionado con la vulnerabilidad detectada; un nivel bajo implica un impacto limitado o mínimo, el nivel medio indica un riesgo significativo, pero no crítico, mientras que el nivel alto indica que la vulnerabilidad representa un riesgo crítico y requiere atención inmediata

Tabla 21. Tabla de vulnerabilidades de la base de datos personal

Vulnerabilidad	**Escala**					
Falta de control de acceso	**Bajo**		**Medio**	X	**Alto**	
Contraseñas débiles	**Bajo**		**Medio**	X	**Alto**	
Falta de cifrado	**Bajo**	X	**Medio**		**Alto**	
Copias de seguridad insuficientes o no actualizadas	**Bajo**		**Medio**		**Alto**	X
Falta de monitoreo continuo	**Bajo**	X	**Medio**		**Alto**	
Actualización de equipos	**Bajo**		**Medio**	X	**Alto**	
Actualización de software	**Bajo**		**Medio**	X	**Alto**	
Políticas de protección no escritas	**Bajo**		**Medio**	X	**Alto**	
Manual de respuesta a vulnerabilidades no escritas	**Bajo**	X	**Medio**		**Alto**	
Falta de control a posibles ataques	**Bajo**		**Medio**	X	**Alto**	
Parches de seguridad	**Bajo**		**Medio**	X	**Alto**	
Errores humanos	**Bajo**	X	**Medio**		**Alto**	
Sugerencia de curso, para mayor preparación	**Bajo**		**Medio**	X	**Alto**	

Vulnerabilidad	Escala					
Falta de programas o charlas de concientización	**Bajo**	X	**Medio**		**Alto**	

a) Análisis de riesgos

El análisis de riesgos de seguridad en una base de datos personales de la EMAPA es esencial para identificar y reducir posibles amenazas a la privacidad y la integridad de los datos. Este procedimiento implica evaluar los riesgos potenciales y aplicar controles de seguridad adecuados para proteger la información.

El Reglamento General de Protección de Datos (RGPD) establece la obligación de realizar un análisis de riesgos en el tratamiento de datos personales. Este análisis implica identificar y determinar los riesgos asociados a la protección de los datos personales, así como establecer medidas de control y seguridad para garantizar el cumplimiento de los principios de protección desde el diseño y por defecto.

Entre los riesgos asociados a la seguridad de la base de datos personales tenemos:

- **Falta de parches de seguridad,** la falta de actualizaciones y parches de seguridad en la base de datos puede dejarla vulnerable a ataques. Los desarrolladores y administradores de la base de datos deben asegurarse de mantenerla actualizada con los últimos parches de seguridad y actualizaciones para protegerla contra vulnerabilidades conocidas.

- **Falta de actualización de equipos,** la falta de actualización de equipos es un riesgo para la seguridad de la base de datos personales de la EMAPA, ya que puede facilitar el acceso no autorizado o el daño a los datos personales por parte de agentes externos, como hackers, ciberdelincuentes, estafadores, ladrones, espías o competidores. Estos agentes pueden aprovechar las vulnerabilidades o fallos de seguridad presentes en los equipos desactualizados para infiltrarse en la base de datos y robar, modificar, eliminar, cifrar o compartir los datos personales sin el consentimiento de sus titulares. Esto puede tener consecuencias negativas para la privacidad, la

seguridad y la reputación de las personas cuyos datos personales se ven comprometidos, así como para las organizaciones que almacenan o procesan dichos datos.

- **Actualización de software,** es esencial actualizar el software de seguridad de una base de datos personales de la EMAPA para resguardar la información y garantizar la confidencialidad y la integridad de los datos. Algunas medidas importantes para preservar la seguridad de una base de datos son:

    - **Herramientas y software,** emplear sistemas de gestión de bases de datos (DBMS) como MySQL, Oracle, SQL Server y PostgreSQL, que brindan funcionalidades incorporadas para el cuidado y la gestión de bases de datos, incluyendo herramientas de respaldo, seguimiento de rendimiento y actualización de software.

    - **Proveedores de software,** las empresas dedicadas al software de gestión de bases de datos proveen soluciones y herramientas para conservar y actualizar bases de datos de manera eficaz. Pueden ofrecer asistencia técnica, actualizaciones y mejoras constantes.

    - **Configurar actualizaciones automáticamente,** para facilitar la actualización de software en dispositivos personales, establecer las actualizaciones para que se ejecuten automáticamente y no desatender los avisos de actualización.

b) Identificar posibles amenazas

Las bases de datos personales de la EMAPA pueden enfrentar diversas amenazas y vulnerabilidades que pueden comprometer su seguridad. Algunas de las amenazas incluyen el acceso no autorizado a través de vulnerabilidades en el software de la base de datos, el robo de datos y la interceptación de información confidencial. Además, las bases de datos personales también pueden ser vulnerables a amenazas como la destrucción de registros y dispositivos, actos de vandalismo, robos o hurtos.

Las amenazas de la base de datos personales se pueden dividir en dos grandes categorías:

- **Amenazas internas:** Las amenazas internas en las bases de datos personales de la EMAPA se refieren a aquellas que surgen de personas que tienen acceso autorizado a los datos personales de otros individuos, ya sea debido a su empleo, relación o cualquier otro motivo, y que los utilizan de manera inapropiada, malintencionada o negligente. Estas amenazas pueden ocasionar daños a la privacidad, seguridad y reputación de las personas cuyos datos personales se ven comprometidos, así como a las organizaciones que almacenan o procesan dichos datos.

  Entre las amenazas internas que la base de datos personales de la EMAPA puede presentar tenemos:

  - Accede a los datos personales de los clientes sin una razón legítima para su venta a terceros o los utiliza para fines personales.

  - Un empleado que se lleva consigo una copia de los datos personales de la empresa y los utiliza para extorsionar, chantajear o perjudicar a la empresa o a sus clientes.

  - Un usuario interno que comete errores involuntarios que dejan la base de datos personal vulnerable a ataques externos o que borran u alteran los datos personales.

  - Un empleado o varios empleados que están en constante contacto con la base de datos personales de la EMAPA y no tienen los conocimientos actualizados.

- **Amenazas externas:** Las amenazas externas de la base de datos personales de la EMAPA son aquellas que provienen de personas o entidades que no tienen acceso autorizado a los datos personales de otras personas, pero que intentan obtenerlos o dañarlos mediante técnicas maliciosas, como ataques informáticos, malware, phishing, robo de dispositivos o medios de almacenamiento, entre otros. Estas amenazas pueden ocasionar daños a la

privacidad, seguridad y reputación de las personas cuyos datos personales se ven comprometidos, así como a las organizaciones que almacenan o procesan dichos datos.

Entre las amenazas que la base de datos personales de la EMAPA a experimentado tenemos:

- **Ataques de fuerza bruta**, los ataques de fuerza bruta se utilizan para intentar adivinar las contraseñas de los usuarios. Estos ataques pueden ser automatizados y pueden ser muy efectivos si las contraseñas son débiles.

  Un ataque de fuerza bruta consiste en realizar intentos sistemáticos utilizando todas las combinaciones posibles de caracteres hasta lograr encontrar la contraseña correcta. Visualmente, este proceso puede representarse como un flujo de trabajo en el cual se generan diversas combinaciones de caracteres para ser comparadas con la contraseña almacenada en la base de datos.

  Uno de los códigos más usado para adivinar la contraseña de un usuario de la base de datos personales es:

```python
import hashlib

def fuerza_bruta_contrasena_base_datos(contrasena_hash,
                                       diccionario_contrasenas,
                                       lista_nombres):
    for nombre in lista_nombres:
        for contrasena in diccionario_contrasenas:
            contrasena_hash_adivinada = hashlib.sha256(nombre +
                                                       contrasena.encode()).hexdigest()
            if contrasena_hash_adivinada == contrasena_hash:
                return nombre + contrasena
    return None


if __name__ == "__main__":
    contrasena_hash = "21232f297a57a5a743894a0e4a801fc3"
    diccionario_contrasenas = ["contrasena1",
                               "contrasena2",
                               "contrasena3"]
    lista_nombres = ["juan",
                     "maria",
                     "jose"]
    contrasena_adivinada = fuerza_bruta_contrasena_base_datos(contrasena_hash,
                                                              diccionario_contrasenas,
                                                              lista_nombres)
    print(contrasena_adivinada)

```

Figura O. Código usado para un ataque de fuerza brutra.

Este código utiliza un disccionario o listado de contraseñas que se usan comunmente, ademas de un listado de nombre de usuario, los cuales sirben para probrar las posibles combinaciones de caracteres.

La función fuerza_bruta_base_datos() usa tres parámetros: un listado de nombres, un listado de contraseñas y la hash de la víctima. La función compara la lista de nombre y contraseñas con las que usa la víctima, al encontrar el incidente, la función devuelve la contraseña adivinada.

Resultados del ataque de fuerza bruta:

El tamaño de la base de datos utilizada en esta práctica rondaba aproximadamente los 100 Mb, aunque en realidad la base de datos completa es de más de 11 GB. La duración del ataque de fuerza bruta fue de 5 horas y 55 minutos debido a la falta de seguridad en las contraseñas y al equipo no actualizado. Este tipo de ataque resulta factible debido a la sensibilidad y la importancia de la información contenida en la base de datos para la empresa, sumado a la debilidad de las contraseñas. Aunque se requiere tiempo y esfuerzo, el ataque fue exitoso después de un prolongado período.

- **Ataques de inyección de SQL,** los ataques de inyección de SQL se utilizan para insertar código malicioso en una base de datos. Este código malicioso puede ser utilizado para robar datos o dañar la base de datos. Este ataque a la base de datos implica engañar a la base de datos para que se permita realizar consultas maliciosas, de este modo los hackers acceden, modifican o dañan las bases de datos personales. El presente código es uno de los más usados para este ataque:

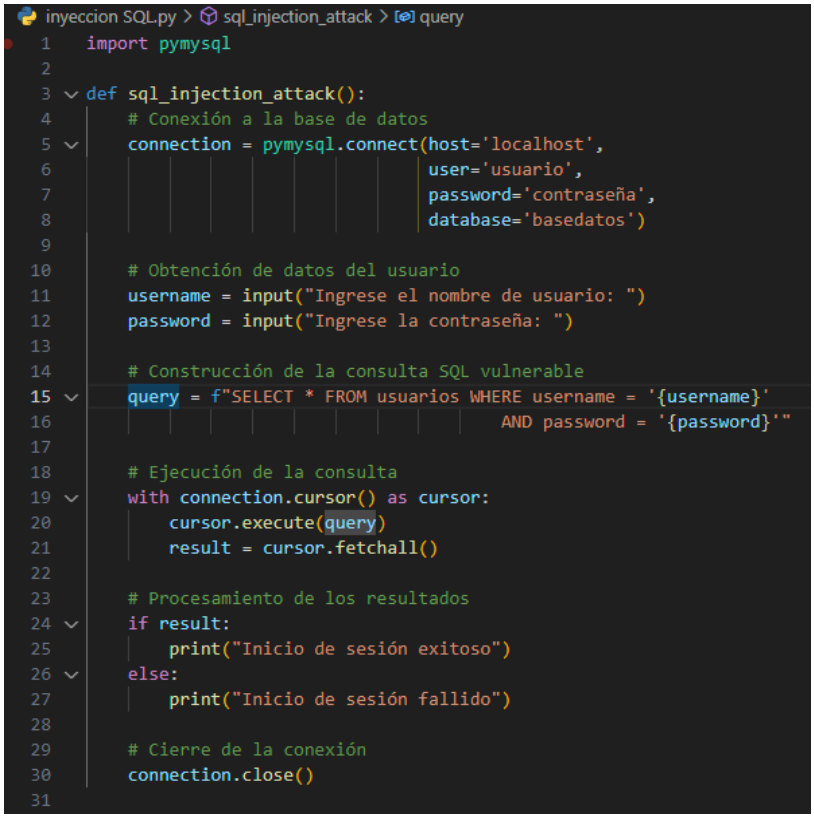


Figura P. Código usado para una inyección SQL.

El código realiza una conexión con la base de datos utilizando los parámetros de usuario y contraseña, y el nombre de la base de datos. Después construye una consulta SQL utilizando los valores que ingreso el usuario, ejecuta dicha consulta y obtiene los resultados de la base de datos. Prosesa los datos para determinar si el inicio de sesión tubo resultados o no.

Resultados del ataque de inyección SQL:

El tamaño de la base de datos utilizada para esta práctica era de aproximadamente 250 Mb, pero la base de datos completa supera los 11 GB. El ataque de fuerza bruta duró 5 horas y 59 minutos debido a contraseñas débiles y un equipo desactualizado. Estos ataques son comunes y pueden ser muy efectivos si no se implementan medidas de seguridad adecuadas. Dada la sensibilidad de la información en la base de datos y la debilidad de las contraseñas, este tipo de ataque tiene una

probabilidad de éxito del 70%. A pesar de requerir esfuerzo y habilidad del atacante, el ataque fue exitoso después de un período prolongado de tiempo, lo que representa un riesgo y facilita la extracción de información de la base de datos a través de la inyección SQL.

- **Malware,** el malware, como los virus y los troyanos, puede ser utilizado para robar datos o dañar una base de datos. El malware puede propagarse a través de enlaces de correo electrónico, archivos adjuntos y otras vías. Un ataque por malware es un intento de acceder, modificar o destruir información almacenada en una base de datos personal mediante el uso de un software malicioso o malintencionado.

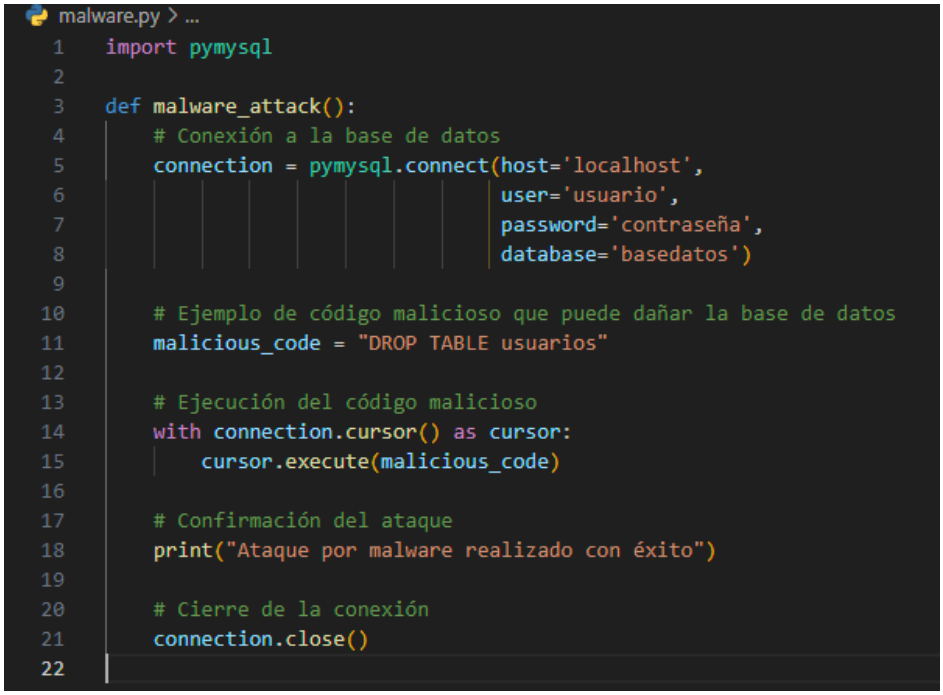


Figura Q. Código usado para un ataque por malware.

Para la práctica se utilizó el código malicio “DROP TABLE”, utilizado para la eliminación de una tabla.

Resultados del ataque de inyección SQL:

El tamaño de la base de datos utilizada para esta práctica fue de 1GB, El tamaño de la base de datos utilizada para esta práctica fue de 100

Mb, en realidad la base de datos completa es de más de 11 GB. El ataque a través de malware no resultó completamente efectivo, ya que la eficacia del malware utilizado no fue óptima y no se identificó el mejor para el propósito. La duración del ataque fue de aproximadamente 1 hora y 25 minutos.

Dado que el ataque no tuvo éxito, esta intrusión no puede considerarse factible debido a la detección temprana del malware. Aunque este tipo de ataque es común y puede causar interrupciones en los servicios.

- **Falta de manual de respuestas a vulnerabilidades,** La falta de un manual de respuestas a vulnerabilidades para la seguridad de una base de datos personal puede representar un desafío, además de tener una serie de consecuencias negativas, entre las que se incluyen:

  - Dificultades para cumplir con las regulaciones**,** Las entidades que gestionan bases de datos personales, como la EMAPA están sometidas a una serie de normativas que exigen la salvaguarda de la información confidencial. La ausencia de un plan de respuesta a vulnerabilidades puede obstaculizar la demostración de que la entidad está adoptando las medidas pertinentes para proteger los datos.

  - Reducción de la confianza de los clientes*,* Los clientes depositan su confianza en las organizaciones que gestionan sus datos personales. La ausencia de un plan de respuesta a vulnerabilidades puede erosionar la confianza de los clientes y ocasionar una reducción de los ingresos.

c) Vulnerabilidades

Existen diferentes tipos de vulnerabilidades que pueden afectar la seguridad de una base de datos personal de la EMAPA. Estas vulnerabilidades pueden ser de tipo hardware, software, de redes o humanas, y pueden surgir debido a errores y

fallas de diseño o configuración, así como a la ausencia de procedimientos adecuados.

Se pueden clasificar en las siguientes categorías:

- **Vulnerabilidades de diseño,** Estas vulnerabilidades se encuentran en el diseño de la base de datos. Pueden incluir errores en la arquitectura de la base de datos, en el diseño de los datos o en los procedimientos de seguridad.

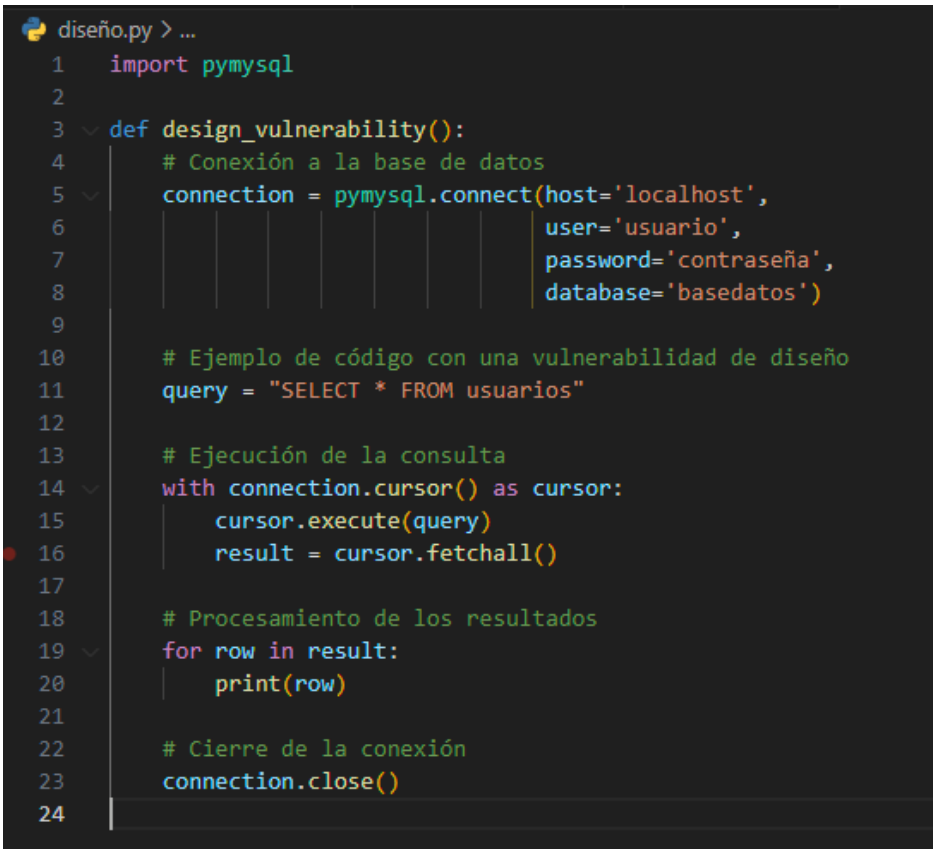


Figura R. Código de consulta SELECT.

Código con una consulta SELECT a la tabla usuarios en una base de datos sin tener filtros. Esta acción puede permitir a un atacante obtener los datos de una tabla, la cual puede tener información delicada.

Resultados del ataque de inyección SQL:

El tamaño de la base de datos utilizada para esta práctica era de aproximadamente 200 Mb, pero en realidad la base de datos completa es de

más de 11 GB. La consulta duró 35 minutos, ya que extrajo toda la información de la tabla (en este caso, la tabla de usuarios). El ataque resultó factible debido a la falta de control de privilegios.

El resultado de la consulta es grave, ya que expone información delicada almacenada en la base de datos. Desde el punto de vista de la seguridad, este ataque no se considera "bueno", ya que revela deficiencias en el diseño de la base de datos.

- **Vulnerabilidades de implementación,** estas vulnerabilidades se encuentran en la implementación de la base de datos. Pueden incluir errores en el código, en la configuración o en los procedimientos de administración.

- **Vulnerabilidades de uso,** estas vulnerabilidades se encuentran en el uso de la base de datos. Pueden incluir errores cometidos por los usuarios, como el uso de contraseñas débiles o la introducción de datos incorrectos.

Las vulnerabilidades más comunes tenemos:

- **Falta de control de acceso,** puede ocurrir cuando los mecanismos de autenticación y autorización no se implementan de manera adecuada. Esto implica que cualquier usuario, incluso aquellos no autorizados, puede acceder, modificar o eliminar datos en la base de datos sin restricciones.

- **Falta de encriptación,** los datos personales que no están encriptados pueden ser fácilmente leídos por cualquier persona que tenga acceso a la base de datos. Esto puede incluir empleados, contratistas, competidores o ciberdelincuentes.

- **Falta de auditorías,** la seguridad de los datos se puede evaluar mediante auditorías que detectan debilidades y peligros. Pero si no se hacen auditorías de seguridad, las organizaciones pueden quedar expuestas a riesgos ignorados.

- **Falta de conciencia de seguridad,** la falta de conocimiento y formación en materia de seguridad por parte de los usuarios puede resultar en conductas inseguras, como el intercambio de contraseñas.

- **Falta de gestión de respaldos,** la falta de realización periódica de copias de seguridad o una mala gestión de las mismas aumenta el peligro de sufrir pérdida de datos en situaciones imprevistas.

- **Falta de Monitoreo,** la falta de implementación de sistemas de detección de intrusiones o la ausencia de monitoreo de actividades anómalas dificulta la capacidad de identificar de manera precoz posibles amenazas.

- **Falta de Políticas,** para proteger la privacidad de los datos, se requieren políticas claras y procedimientos que establezcan cómo manejarlos. De lo contrario, se pueden producir violaciones de la privacidad.

- **Contraseñas débiles,** las contraseñas débiles pueden representar un peligro para la seguridad de una base de datos personal. Según una encuesta realizada por Harris Poll, las contraseñas débiles son la principal causa de filtraciones de datos. Muchas personas utilizan contraseñas comunes o fáciles de adivinar, como números en secuencia o combinaciones simples de letras y números. Además, muchos usuarios solo realizan cambios mínimos en sus contraseñas cuando se les solicita actualizarlas. Para reducir este riesgo, es importante tomar medidas como actualizar y fortalecer las contraseñas, evitar reutilizar las mismas contraseñas y evaluar regularmente la seguridad de las contraseñas utilizadas.

3.2.3 Etapa tres: Análisis de alternativas de solución.

Las medidas de seguridad, ya sean técnicas, organizativas o legales, tienen el propósito de evitar, detectar, responder y recuperarse de los incidentes que puedan afectar los datos personales. La implementación de estas medidas implica un proceso constante y dinámico que requiere la participación y compromiso de todos los involucrados en el manejo de los datos personales, desde los responsables y encargados hasta los usuarios y empleados.

a) Aplicar cifrado a datos sensible

La implementación del cifrado de datos sensibles en la base de datos personales de la EMAPA es crucial para garantizar la confidencialidad y protección de la información. Este proceso implica transformar los datos en un formato ilegible mediante el uso de técnicas criptográficas, lo que evita que sean accesibles para personas no autorizadas. Existen diferentes tipos de cifrado, como el cifrado simétrico y el asimétrico, los cuales emplean claves para encriptar y desencriptar la información. Esencialmente, cifrar los datos sensibles, como aquellos relacionados con el origen étnico, opiniones políticas, datos genéticos, entre otros, es fundamental para cumplir con las regulaciones como el Reglamento General de Protección de Datos (RGPD).

Además de cumplir con las normativas, el cifrado de datos sensibles mitiga el riesgo asociado con el tratamiento de dicha información y protege contra amenazas externas, como el acceso no autorizado y el robo de datos. Implementar medidas de seguridad, es crucial para proteger la base de datos personal de posibles vulnerabilidades y garantizar el cumplimiento de las regulaciones de privacidad de datos.

b) Configurar auditorías de seguridad

Las auditorías de seguridad de una base de datos personales son un proceso importante que ayuda a identificar vulnerabilidades y amenazas. Estas auditorías pueden ayudar a las organizaciones a proteger sus bases de datos personales contra el acceso no autorizado, el robo de datos y otros daños.

Para realizar una auditoria existen diferentes enfoques y herramienta:

- **Configuración de auditorías nativas de la base de datos,** muchas bases de datos ofrecen características integradas para llevar a cabo auditorías de seguridad. Por ejemplo, en Oracle Database, es posible especificar políticas de auditoría unificadas para registrar la actividad de la base de datos y cifrarla antes de enviarla a una secuencia de datos en Amazon Kinesis.

- **Utilización de herramientas de auditoría de terceros,** existen herramientas de auditoría de terceros que ofrecen más opciones y capacidades para personalizar las auditorías. Estas herramientas permiten definir auditorías específicas para vigilar y registrar los eventos de seguridad en la base de datos personal. Entre las herramientas más usadas se encuentran:

    - Imperva SecureSphere Database Security, la cual ofrece la capacidad de realizar auditorías y monitoreo en tiempo real, además de detectar y prevenir amenazas en las bases de datos.

    - IBM Guardium, brinda el servicio de auditoria en tiempo real, detección de datos confidenciales y supervisión de actividades en base de datos para contribuir en la protección contra posibles amenazas.

    - Trustwave DbProtect, ofrece servicios de auditoría y seguridad para base de datos, que incluyen la identificación de datos, la evaluación de riesgos y la supervisión de actividades.

- **Implementación de políticas y procedimientos de auditoría,** además de configurar las auditorías técnicas, es fundamental establecer políticas y procedimientos claros para el manejo de la seguridad de la base de datos personal. Esto implica definir quién tiene acceso a la base de datos, cómo se gestionan los registros de auditoría y cómo se responden a los incidentes de seguridad.

    Los pasos generales para llevar a cabo una configuración de auditoria:

    1. Definir objetivos y alcance,
    2. Recopilar información
    3. Configurar la auditoría
    4. Implementar medidas de seguridad
    5. Realizar auditorías periódicas

c) Establecer permisos y roles

Los permisos y roles de la base de datos personales de la EMAPA son un conjunto de reglas que determinan qué usuarios pueden hacer con los datos de la base de datos. Los permisos permiten a los usuarios realizar acciones específicas, como leer, escribir, modificar o eliminar datos en la base de datos. Los roles, por otro lado, agrupan permisos y se asignan a los usuarios para simplificar la administración de permisos. Al asignar roles a los usuarios, se les otorgan automáticamente los permisos asociados con ese rol.

Para asignar roles y permisos, se pude seguir los pasos siguientes:

- **Identificar los datos que desea proteger,** los primeros pasos para establecer permisos y roles es identificar los datos que desea proteger. Esto incluye determinar qué datos son confidenciales o sensibles y quién necesita acceso a esos datos.

- **Definir los permisos que necesita,** Una vez que haya identificado los datos que desea proteger, debe definir los permisos necesarios para protegerlos. Algunos permisos comunes incluyen: lectura, escritura, modificación, eliminación.

- **Asignar permisos a los usuarios,** Una vez que haya definido los permisos que necesita, debe asignarlos a los usuarios. Esto se puede hacer mediante la creación de roles y la asignación de permisos a los roles.

d) Parches de seguridad

Los parches de seguridad en la base de datos personales de la EMAPA son actualizaciones que se aplican para corregir vulnerabilidades y mejorar la protección de los datos almacenados. Estos parches son desarrollados y distribuidos por los proveedores de software y se utilizan para solucionar problemas de seguridad conocidos. Al instalar los parches de seguridad, se fortalece la base de datos y se reduce el riesgo de posibles ataques o violaciones de datos.

Es importante mantenerse al día con los parches de seguridad y aplicarlos de manera regular para garantizar la integridad y confidencialidad de los datos en la base de datos personal. Los proveedores de software suelen enviar notificaciones sobre la disponibilidad de nuevos parches de seguridad, y es recomendable instalarlos tan pronto como estén disponibles para mantener la base de datos protegida.

3.2.4 Etapa cuatro: Diseño de políticas y procedimientos de seguridad.

El diseño de políticas y procedimientos de seguridad es esencial para asegurar la protección de la base de datos personales de la EMAPA. Estas políticas y procedimientos definen las normas y acciones necesarias para salvaguardar la información confidencial y evitar accesos no autorizados.

Al diseñar estas políticas y procedimientos, es crucial considerar los siguientes aspectos:

a) Crear políticas de contraseñas

Establecer directrices de seguridad de contraseñas para la base de datos personal de la EMAPA es una acción fundamental para salvaguardar datos confidenciales y proteger su privacidad. Entre las políticas más conocidas se encuentran:

- **Complejidad de las contraseñas:** Para maximizar la seguridad de las contraseñas, es importante incrementar su complejidad para evitar que sean adivinadas por personas no autorizadas. Se sugiere utilizar una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

- **Longitud mínima:** Para mejorar la seguridad de las contraseñas, se debe mejorar la longitud mínima establecida. Por ejemplo, se puede establecer una longitud de ocho caracteres, lo cual asegura que las contraseñas sean lo suficientemente extensas como para dificultar su descifrado.

- **Cambio regular de contraseñas:** Para incrementar la seguridad de las contraseñas, es indispensable mejorar la implementación de un requisito de cambio periódico de contraseñas. Por ejemplo, establecer un período de

cambio de cada 90 días ayuda a prevenir el uso de contraseñas comprometidas o conocidas.

- **Bloqueo tas intentos fallidos:** Para aumentar la seguridad de las contraseñas, es recomendable configurar un bloqueo automático después de varios intentos fallidos de inicio de sesión. Esto ayuda a proteger contra ataques de fuerza bruta, donde los atacantes intentan adivinar la contraseña probando diferentes combinaciones. Al bloquear automáticamente la cuenta después de un número determinado de intentos fallidos, se dificulta que los atacantes continúen intentando adivinar la contraseña.

- **Verificación en dos pasos:** Para elevar la seguridad de las contraseñas, es recomendable mejorar considerando la implementación de la verificación en dos pasos. Esta medida agrega una capa adicional de seguridad al requerir que el usuario proporcione un segundo factor de autenticación, como un código enviado a su teléfono móvil. Al agregar esta segunda capa de autenticación, se dificulta aún más el acceso no autorizado a la cuenta, ya que los atacantes necesitarían no solo la contraseña, sino también el factor de autenticación adicional para iniciar sesión.

b) Establecer políticas de control de acceso

Las políticas de control de acceso son fundamentales para garantizar la seguridad de la base de datos personales de la EMAPA. Estas políticas definen los criterios para acceder a la base de datos, como limitar el acceso solo a empleados autorizados y permitir a los usuarios acceder únicamente a la información necesaria para llevar a cabo sus tareas.

Las políticas de control de acceso deben ser creadas de manera que se alineen con los objetivos de seguridad de la organización. Estos objetivos pueden abarcar la protección de la confidencialidad, integridad y disponibilidad de los datos. Es importante que las políticas también consideren las amenazas y vulnerabilidades particulares a las que se enfrentan las bases de datos personales.

Controles de acceso más usados:

- **Requerir autenticación:** La autenticación implica verificar la identidad de un usuario, y las organizaciones deben solicitar a los usuarios que se autentiquen antes de poder acceder a la base de datos.

- **Requerir autorización:** La autorización implica determinar si un usuario tiene los permisos necesarios para llevar a cabo una acción. Las organizaciones deben asegurarse de que los usuarios estén autorizados para acceder a los datos específicos que requieren.

- **Revisar periódicamente los permisos:** Las organizaciones deben realizar revisiones periódicas de los permisos de acceso para garantizar su precisión y actualización.

c) Desarrollar políticas de cifrado

Existen varios métodos de cifrado que se pueden emplear para salvaguardar los datos en la base de datos personales de la EMAPA. Uno de los más utilizados es el cifrado de datos en reposo, que consiste en encriptar la información cuando se almacena en un disco duro u otro dispositivo de almacenamiento. El cifrado de datos en tránsito, que se emplea para proteger los datos mientras se transmiten de un lugar a otro, como cuando se envían a través de una red.

Desarrollar políticas de cifrado esencial para asegurar la seguridad de la base de datos personales de la EMAPA y proteger la información confidencial. El cifrado de datos en reposo y en tránsito, junto con otras medidas de seguridad, garantizará la protección de los datos contra accesos no autorizados y posibles violaciones de seguridad.

d) Mejorar las copias de seguridad

Para mejorar o realizar copias de seguridad de una base de datos personal, es importante tener en cuenta la automatización de las copias de seguridad y la diversificación de dónde y cómo se almacenan los datos. También es esencial

realizar pruebas periódicas del proceso de copia de seguridad para asegurarse de que sea efectivo.

El cifrado es una técnica esencial para proteger la base de datos y evitar que los datos personales sean legibles por personas no autorizadas. Esto puede liberar a las entidades responsables de informar sobre una violación de seguridad en caso de que se produzca un acceso indebido.

Es importante tomar en cuenta la adopción de herramientas de inteligencia artificial con el propósito de optimizar el proceso de copia de seguridad y la recuperación de datos, haciéndolos más eficientes.

e) Controles ante posibles denegaciones de servicios

Para prevenir los efectos de los ataques de denegación de servicio en la seguridad de la base de datos personales de la EMAPA, es importante aplicar medidas que reduzcan el daño de estos eventos. Algunas acciones sugeridas son la distribución de la localización y el modo de almacenamiento de las copias de seguridad, la ejecución automática de las copias de seguridad y la verificación regular para asegurar su funcionamiento.

Algunas de las medidas más utilizadas:

- **Monitoreo y detección de anomalías:** Usar sistemas de monitoreo y detección de anomalías puede contribuir a detectar actividades anormales o patrones de tráfico extraños que podrían señalar un ataque de denegación de servicio. Esto facilita una reacción inmediata y la aplicación de acciones de solución.

- **Balanceo de carga y redundancia:** Para evitar los impactos de un ataque de denegación de servicio, es recomendable distribuir la carga de trabajo en varios servidores y contar con redundancia en la infraestructura. De esta forma, se asegura que la base de datos pueda seguir operando, aunque uno de los servidores se vea afectado.

3.2.5 Etapa cinco: Monitoreo y mejora continua.

El monitoreo constantemente y la realización de mejoras continuas para garantizar la seguridad de la base de datos personales de la EMAPA. Esto implica supervisar de manera constante el estado de la base de datos, identificar posibles vulnerabilidades o actividades sospechosas, y tomar medidas correctivas de manera oportuna. Por otro lado, la mejora continua implica implementar cambios y actualizaciones en los sistemas y procesos de seguridad para fortalecer la protección de los datos personales. Estos esfuerzos de monitoreo y mejora continua contribuyen a mantener la integridad, confidencialidad y disponibilidad de la base de datos personal.

a) Implementar herramientas de monitoreo

La implementación de herramientas de monitoreo para la seguridad de una base de datos personal de la EMAPA es un proceso crucial que puede ayudar a las organizaciones a detectar y responder de manera ágil a las posibles amenazas.

El primer paso en la implementación de herramientas de monitoreo es establecer los objetivos de seguridad. Esto implica determinar qué aspectos de la seguridad de la base de datos de la EMAPA se desean monitorear, como el acceso a la base de datos, la actividad de la base de datos o la seguridad en general.

Una vez que se hayan establecido los objetivos de seguridad, se puede seleccionar las herramientas de monitoreo adecuadas. Existe una variedad de herramientas disponibles, cada una con sus propias fortalezas y debilidades.

Entre las herramientas más utilizadas están:

- **Sistemas de gestión de eventos de seguridad (SIEM):** Los Sistemas de Gestión de la Información y Eventos de Seguridad (SIEM) recopilan y analizan información de seguridad proveniente de diversas fuentes, tales como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS).

- **Sistemas de detección de intrusiones (IDS):** Los Intrusion Detection Systems (IDS) tienen la capacidad de identificar acciones maliciosas en la red, como intentos de acceso no autorizados o ataques de malware.

- **Sistemas de prevención de intrusiones (IPS):** Los Sistemas de Prevención de Intrusiones (IPS) tienen la capacidad de bloquear la actividad maliciosa en la red.

b) Establecer alertas de seguridad

Para asegurar la protección de la base de datos personales de la EMAPA, es esencial utilizar un sistema de monitoreo y alertas que pueda identificar actividades no autorizadas y prevenir posibles incidentes de seguridad.

Entre las herramientas más usadas:

- **Tableros de control para monitoreo y generación de alertas:** Crear paneles de control que permitan supervisar y recibir notificaciones sobre las consultas realizadas a la base de datos, utilizando como referencia los registros (logs) de las transacciones.

- **Herramientas de monitoreo de red:** Utilizar herramientas de monitoreo de red, como SolarWinds o Zabbix, implica aprovechar su capacidad para programar alertas personalizadas y supervisar el tráfico de la red en tiempo real. Estas herramientas permiten visualizar el tráfico de la red en tiempo real y recibir notificaciones personalizadas cuando se detectan eventos o condiciones específicas.

- **Herramientas de generación de informes en tiempo real:** Utilizar herramientas de monitoreo de red en tiempo real permite obtener información sobre el rendimiento de la red de forma inmediata. Esto facilita la detección temprana de problemas de seguridad y ayuda a evitar interrupciones en el funcionamiento de la red. Estas herramientas proporcionan datos actualizados sobre el tráfico de la red, permitiendo identificar patrones anormales o actividades sospechosas que podrían indicar posibles amenazas.

c) Revisar y analizar registros

Para revisar y analizar los registros de seguridad de la base de datos personales de la EMAPA, es fundamental emplear herramientas apropiadas que faciliten el acceso a dichos registros y permitan llevar a cabo un análisis exhaustivo. Estas herramientas son de gran utilidad para obtener información relevante sobre posibles vulnerabilidades de seguridad, actividades sospechosas o intentos de acceso no autorizados.

Es relevante señalar que, al analizar los registros de seguridad de la base de datos personales de la EMAPA, es fundamental seguir las políticas y regulaciones actuales de protección de datos. Esto implica asegurar la confidencialidad y privacidad de la información personal almacenada en la base de datos, así como cumplir con las normativas aplicables en materia de protección de datos.

Utilizar herramientas de monitoreo de red como SolarWinds o Zabbix, que posibilitan la programación de alertas personalizadas y el seguimiento en tiempo real del tráfico de la red, es esencial para examinar y analizar los registros de seguridad de una base de datos personal. Esto contribuye a identificar de manera temprana problemas de seguridad y prevenir interrupciones en el funcionamiento de la base de datos.

3.2.6 Etapa seis: Capacitación y concientización del personal.

La capacitación y sensibilización del personal acerca de la seguridad de una base de datos personal de la EMAPA es esencial para asegurar una protección adecuada de los datos personales. Es fundamental que la EMAPA se centren en proporcionar formación y concienciación a su personal sobre las prácticas recomendadas de seguridad de datos y las normativas vigentes.

La capacitación puede abarcar temas como la importancia de salvaguardar la información personal, la identificación y prevención de posibles brechas de seguridad, el manejo adecuado de contraseñas y el uso seguro de la red. También es fundamental que el personal esté familiarizado con las políticas y procedimientos internos relacionados con la seguridad de la base de datos.

La concientización del personal implica fomentar una cultura de seguridad en la empresa, donde todos los empleados comprendan la importancia de proteger los datos personales y estén comprometidos en seguir las mejores prácticas de seguridad. Esto se puede lograr mediante campañas de sensibilización, recordatorios periódicos y promoviendo una actitud proactiva hacia la seguridad de los datos.

a) Capacitar al personal sobre ciberseguridad

La capacitación del personal en ciberseguridad y en la protección de la base de datos personales de la EMAPA es esencial para asegurar la adecuada salvaguarda de los datos. Es importante brindar a los empleados formación sobre la importancia de proteger la información personal, cómo identificar y prevenir posibles vulnerabilidades de seguridad, el manejo adecuado de contraseñas y el uso seguro de la red. Además, es fundamental que el personal esté al tanto de las políticas y procedimientos internos relacionados con la seguridad de la base de datos. La concientización del personal implica crear una cultura de seguridad en la organización, donde todos los empleados comprendan la importancia de proteger los datos personales y estén comprometidos en seguir las mejores prácticas de seguridad. Esto se puede lograr a través de campañas de sensibilización, recordatorios periódicos y promoviendo una actitud proactiva hacia la seguridad de los datos.

Las capacitaciones usualmente tratan de los siguientes temas:

- **Los riesgos a los que está expuesta la base de datos:** El personal debe tener conocimiento de los peligros a los que se enfrenta la base de datos, como ataques de malware, intentos de acceso no autorizados y errores humanos.

- **Las políticas y procedimientos de seguridad:** El personal debe tener conocimiento de las políticas y procedimientos de seguridad de la base de datos, como las prácticas de autenticación y autorización, las políticas de uso de dispositivos móviles y las políticas de cifrado.

- **Cómo identificar y reportar amenazas:** El personal debe tener la capacidad de reconocer y comunicar posibles peligros que pongan en riesgo la seguridad de la base de datos.

b) Conducir simulacros de seguridad

Realizar ejercicios de simulación de seguridad en la protección de a base de datos personal de la EMAPA es una práctica recomendada para asegurar que el personal esté preparado ante posibles amenazas. Estos simulacros permiten a los empleados practicar cómo identificar y responder a situaciones de riesgo, como intentos de acceso no autorizado o brechas de seguridad. Además, los simulacros brindan la oportunidad de evaluar la efectividad de los procedimientos de seguridad existentes y realizar mejoras si es necesario. Al llevar a cabo estos ejercicios de forma regular, se promueve una mayor conciencia y preparación en el personal, lo que contribuye a fortalecer la seguridad de la base de datos personal.

c) Charla sobre seguridad en la base de datos aplicando compliance de ciberseguridad.

Durante esta presentación, se examinó la relevancia del cumplimiento de ciberseguridad y su repercusión en la salvaguardia de la información personal resguardada en una base de datos. Los objetivos fundamentales consistieron en evidenciar la trascendencia del cumplimiento de ciberseguridad y sensibilizar a los empleados del departamento de Tecnologías de la Información sobre la importancia de proteger las bases de datos personales, destacando el papel influyente que el cumplimiento de ciberseguridad desempeña en esta protección. La protección de la base de datos personales implica resguardar la información personal almacenada en ella, como nombres, direcciones, números de teléfono, detalles financieros y otros datos personales. Es esencial garantizar la seguridad de estas bases de datos para mantener la privacidad y seguridad de las personas. El cumplimiento de ciberseguridad se refiere a seguir las normas y regulaciones establecidas para resguardar la seguridad de la información en el ámbito de la ciberseguridad. La importancia del cumplimiento de ciberseguridad radica en su capacidad para proteger la información personal almacenada en una base de

datos. Estas normas y regulaciones establecen estándares que las empresas que las siguen están mejor preparadas para proteger la información personal de clientes y empleados. El cumplimiento de ciberseguridad contribuye a proteger la base de datos personal mediante la implementación de políticas y procedimientos de seguridad, evaluaciones de riesgos y capacitación de empleados. Estas acciones ayudan a establecer una estructura efectiva para controles de seguridad y a aumentar la conciencia sobre la importancia de la seguridad de la información.

3.2.7 Etapa siete: Desarrollo del manual de seguridad de datos

MANUAL DE SEGURIDAD DE DATOS

Tabla 22. Registro de la versión

Versión	Descripción de la creación	Realizado / Aprobado	Cargo	Fecha de elaboración
1.0	Creación	Christian Jara / Ing.	Estudiante / Ing.	

Índice y Contenido

1. Información básica

    1.1. Propósito

    1.2. Consideraciones para el desarrollo

    1.3. Marco Legal

    1.4. Objetivos

    1.5. Alcance de la seguridad de la base de datos personales

    1.6. Normas generales

2. Descripción de actividades para la planificación de seguridad de la base de datos personales.

2.1. Evaluación de riesgos

2.2. Desarrollo de la estrategia de seguridad

2.3. Implementación de los controles de seguridad

2.4. Supervisión y evaluación

2.5. Manejo de incidentes

3. Descripción de actividades para la implementación de seguridad de la base de datos personales.

3.1. Control de acceso

3.2. Cifrado de datos

3.3. Gestión de contraseñas

3.4. Backup y recuperación

3.5. Medidas de seguridad físicas

3.6. Actualización y parches

3.7. Monitoreo continuo

3.8. Capacitación al personal

3.9. Programar auditorias de seguridad

3.10. Herramientas de seguridad

4. Monitoreo de la implementación de las actividades de seguridad de la base de datos personales

4.1. Registros de Auditorías

4.2. Accesos no Autorizados

4.3. Actividades de Cifrado

4.4. Actualizaciones y Parches

4.5. Configuraciones de Seguridad

4.6. Actividades de Copias de Seguridad

4.7. Actividades de Formación

4.8. Actividades Físicas de Seguridad

4.9. Configuraciones de Seguridad

4.10. Herramientas de Seguridad

1. Información básica

1.1. Propósito

Establecer directrices claras y prácticas para proteger la privacidad y confidencialidad de la información de la base de datos personales de la empresa municipal de agua potable y alcantarillado EMAPA, garantizar el cumplimiento de las leyes y regulaciones aplicables, y minimizar los riesgos asociados al tratamiento de datos personales. Esto se logra mediante la implementación de procesos de supervisión y administrativos internos, la administración de riesgos tecnológicos, la creación de controles, procesos, procedimientos, políticas y reglamentos que permitan asegurar la confidencialidad, disponibilidad e integridad de la información.

1.2. Consideraciones para el desarrollo

- Inexistencia de normar o regulaciones escritas para el control de acceso a la base de datos personales, además de la falta de monitoreo continuo.

- Falta de control para la reducción de riesgos y repuesta a posibles amenazas de ataque cibernéticos.

- Necesidad del cumplimento legal y las regulaciones establecidas por las organizaciones de control.

- La ausencia de equipos actualizados, la actualización de software y de parches de seguridad.

1.3. Marco legal

- Ley Orgánica de Protección de Datos Personales (LOPD) [39].

- Reglamento General a la Ley Orgánica de Protección de Datos Personales (RLOPD) [40].

- Superintendencia de Datos Personales (SDP) [41].

- Reglamento General de Protección de Datos (GDPR) [42].

- Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) en México [28].

- Ley de Privacidad del Consumidor de California (CCPA) [43].

1.4. Objetivos

- Garantizar que los datos de la organización estén protegidos de forma confidencial, evitando su acceso no autorizado, y mantener su integridad y disponibles cuando sean necesarios.

- Asegurar el cumplir de las leyes y regulaciones aplicables en el ámbito legal y normativo.

- Reducir la posibilidad de sufrir ataques cibernéticos, al mismo tiempo prevenir el robo y la pérdida de datos.

1.5. Alcance de la seguridad de la base de datos personales

La seguridad de la base de datos personales abarca la protección de la privacidad y confidencialidad de la información personal que la empresa

municipal de agua potable y alcantarillado EMAPA maneja. Esto implica implementar medidas de seguridad administrativas, físicas y técnicas en los sistemas de datos, así como establecer un sistema de supervisión y vigilancia tanto interna como externa. Asimismo, es fundamental identificar y clasificar los datos personales según su importancia y sensibilidad, y asignar responsables y encargados para gestionar y proteger los sistemas de datos personales

1.6. Normas generales

- Asegurar de que todas las prácticas de seguridad estén en conformidad con las leyes y regulaciones locales implica garantizar que se cumplan todas las normas y disposiciones legales aplicables en el ámbito de la seguridad de la base de datos personales.

- Establecer medidas para garantizar la confidencialidad de los datos personales implica asegurarse de que solo las personas autorizadas tengan acceso a esta información.

- Garantizar la disponibilidad de los datos personales cuando sea necesario implica asegurarse de que la información esté accesible y disponible para su uso cuando sea requerida.

- Establecer registros detallados de actividades en la base de datos es una práctica importante para facilitar la auditoría y el monitoreo continuo de la seguridad.

- Implementar medidas de seguridad física implica tomar acciones para proteger los servidores y dispositivos que almacenan la base de datos.

- Mantener actualizados todos los sistemas y software relacionados con la base de datos,

- Proteger los datos personales contra la pérdida, la destrucción o la alteración no autorizadas.

1.7. Diagrama de entidad relación de la base de datos

Para una apreciación más detallada revisar los Anexos desde el Anexo C, al Anexo L.

Tabla 23. Información de la Base de Datos

Información de la Base de Datos	
Nombre	Base de Datos Comercial
Versión de PostgreSQL	14.10 Actualizado en noviembre del 2023
Tamaño	Aproximadamente 12 GB
Cantidad de tablas	Aproximadamente 100 tablas
Contenido por tabla	Mas de 90,000 registros
Crecimiento de la base de datos	Aproximadamente 300 registros nuevos por mes
Actualización de registros	Diariamente

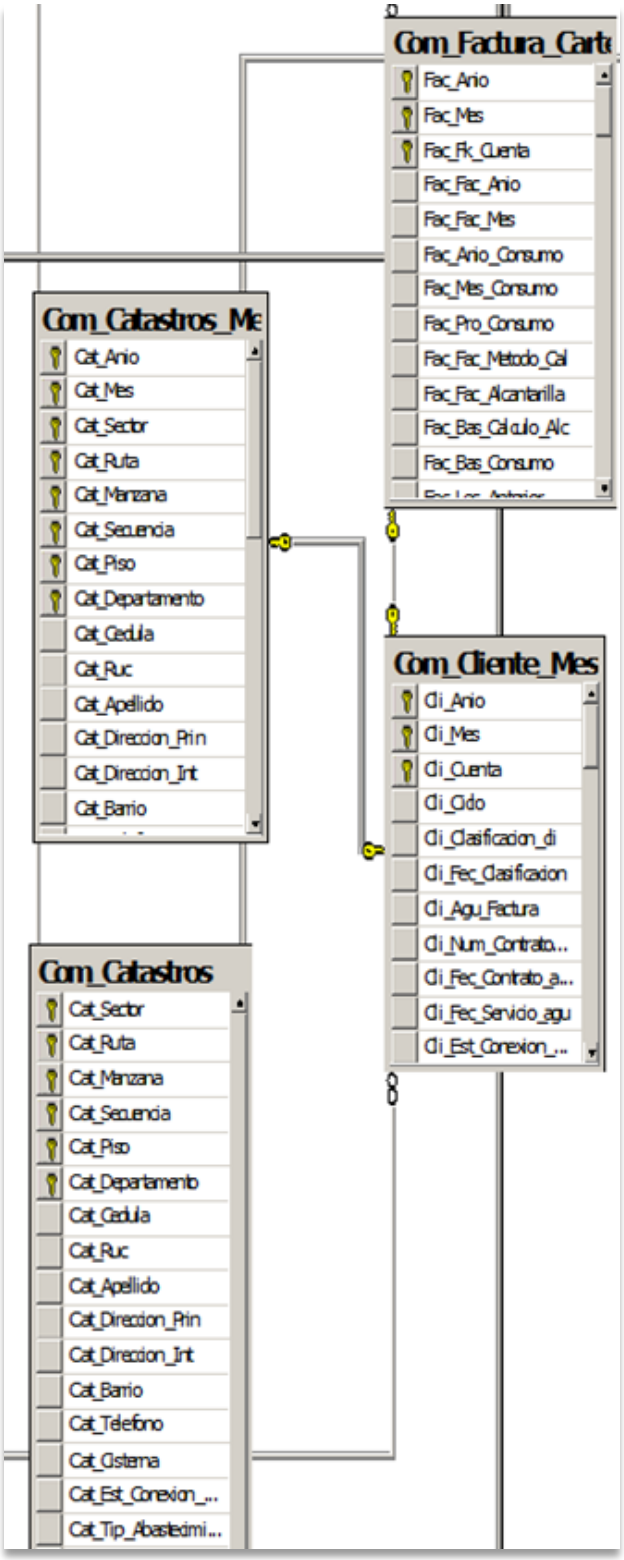


Figura S. Diagrama de entidad relación de la base de datos[44].

2. Descripción de actividades para la planificación de seguridad de la base de datos personales

Para la planificación de seguridad de una base de datos personales, se pueden considerar diversas actividades y controles que permitan proteger la información almacenada. Algunas de estas actividades y controles incluyen:

2.1. Evaluación de riesgos

- Identificar los activos y los datos personales que se almacenan en la base de datos, esta actividad ayuda a determinar los activos de mayor valor que necesitan una protección más sólida.

- Identificar los riesgos a los que están expuestos los datos personales almacenados en la base de datos, esta acción contribuye a mejorar la detección de posibles amenazas y vulnerabilidades que podrían comprometer la seguridad de la base de datos personales de la EMAPA.

- Evaluar la probabilidad e impacto de los riesgos identificados, esta labor permite determinar la prioridad de los controles de seguridad que deben implementarse.

2.2. Desarrollo de la estrategia de seguridad

- Establecer los objetivos de seguridad para la base de datos personal, los objetivos de seguridad deben ser claros, medibles, alcanzables, relevantes y oportunos. Estos objetivos deben ser específicos y comprensibles, de modo que todos los involucrados puedan entenderlos claramente.

- Seleccionar los controles de seguridad que se implementarán para cumplir con los objetivos de seguridad, los controles de seguridad deben ser efectivos, eficientes y adaptables. Estos controles deben cumplir con su propósito de proteger los activos y garantizar la seguridad de una manera que sea eficaz, es decir, que logren su objetivo de manera exitosa.

- Documentar la estrategia de seguridad, la documentación de la estrategia de seguridad es fundamental para asegurar su implementación y mantenimiento de manera efectiva.

2.3. Implementación de los controles de seguridad

- Implementar los controles de seguridad seleccionados, se debe llevarse a cabo siguiendo las instrucciones proporcionadas por el fabricante o proveedor del control de seguridad. Es importante seguir las indicaciones específicas para garantizar que la actividad se realice de manera adecuada y segura.

- Documentar la implementación de los controles de seguridad, la documentación detallada de la implementación de los controles de seguridad es esencial para asegurar su configuración y uso adecuado. Contar con una documentación clara y detallada, proporciona una guía precisa que ayuda a garantizar que los controles se implementen según las instrucciones del fabricante o proveedor.

2.4. Supervisión y evaluación

- Supervisar periódicamente los controles de seguridad para garantizar que sean efectivos, permite identificar las áreas que requieren mejoras o actualizaciones. Al llevar a cabo esta actividad, se pueden evaluar diferentes aspectos y determinar qué áreas necesitan ser modificadas o actualizadas para mejorar su rendimiento o cumplir con los estándares establecidos.

- Evaluar periódicamente los controles de seguridad para garantizar que siguen siendo efectivos, la ejecución de esta actividad permite identificar los cambios en los riesgos a los que están expuestos los datos personales y que requieren modificaciones en los controles de seguridad. Se pueden evaluar los riesgos actuales y futuros que afectan la seguridad de los datos personales, y determinar qué controles de seguridad deben ser ajustados o actualizados para mitigar esos riesgos.

2.5. Manejo de incidente

- Desarrollo de procedimientos de manejo de incidentes que especifiquen cómo responder a los incidentes de seguridad, los procedimientos de manejo de incidentes permiten a las organizaciones responder de manera efectiva a los incidentes de seguridad. Estos procedimientos proporcionan pautas y protocolos claros sobre cómo identificar, evaluar y abordar los incidentes de seguridad de manera oportuna y eficiente.

- Capacitar al personal sobre el manejo de incidentes, la capacitación del personal es crucial para asegurar que aquellos que responden a los incidentes de seguridad estén preparados para hacerlo. Al proporcionar capacitación adecuada, se garantiza que el personal adquiera los conocimientos y habilidades necesarios para identificar, evaluar y responder de manera efectiva a los incidentes de seguridad.

3. Descripción de actividades para la implementación de seguridad de la base de datos personales

La implementación de seguridad de una base de datos personales implica llevar a cabo diversas actividades que van desde la configuración técnica hasta la capacitación del personal. Estas actividades incluyen:

3.1. Control de acceso

Establecer un mecanismo de control de acceso que permita a los administradores determinar quién puede acceder a la base de datos personal y qué grado de permiso tiene cada usuario. Revocar el acceso a los usuarios que ya no requieren acceder a la base de datos personal. Entre las actividades que se deben realizar:

1. Configuración del sistema de gestión de acceso, configurar el sistema para que pueda gestionar el acceso de los usuarios según los criterios de la EMAPA. Para ello, se deben asignar roles, autorizaciones y grados de acceso a cada usuario de acuerdo con sus funciones y responsabilidades.

2. Creación de perfiles de usuario, es necesario establecer perfiles de usuario que representen los distintos niveles de acceso necesarios. Cada perfil debe contar con los permisos apropiados para garantizar un acceso y manipulación seguros de la información personal.

3. Asignación de permisos y roles, es responsabilidad de los administradores asignar los roles y permisos adecuados a cada usuario según sus responsabilidades y requisitos de acceso. Esto asegura que cada usuario tenga únicamente el nivel de acceso necesario para llevar a cabo sus tareas, sin comprometer la seguridad de los datos personales.

4. Monitoreo y auditoría del acceso, resulta fundamental instaurar un sistema de supervisión y revisión que registre y supervise las acciones de acceso a la base de datos personal. Esto posibilita la detección temprana de cualquier actividad sospechosa o inadecuada, permitiendo la aplicación de medidas correctivas de manera oportuna.

5. Retiro de acceso a usuarios no autorizados, resulta esencial retirar los privilegios de acceso a la base de datos personal a aquellos usuarios que ya no requieren dicho acceso. Esta acción debe llevarse a cabo de manera inmediata para asegurar que únicamente personas autorizadas tengan la capacidad de acceder a los datos, disminuyendo así el riesgo de posibles violaciones de seguridad.

3.2. Cifrado de datos

Establecer un sistema de control de acceso que permita a los administradores gestionar el acceso a la base de datos personal, determinando quiénes pueden acceder y qué nivel de acceso tienen. Además, se debe retirar el acceso a los usuarios que ya no necesitan acceder a la base de datos personal para garantizar la seguridad de la información almacenada. Los pasos sugeridos para el cifrado de datos son:

1. Identifica los datos sensibles, reconoce y categoriza los datos sensibles que necesitan ser resguardados, como datos personales, detalles financieros u otra información confidencial.

2. Selecciona un algoritmo de cifrado, existen distintos tipos de cifrado, como el simétrico y el asimétrico. Selecciona el algoritmo de cifrado que mejor se ajuste a las necesidades y características de la información que deseas cifrar.

3. Genera claves de cifrado, la clave de cifrado es esencial para desencriptar los datos cifrados. Tienes la opción de generar tu propia clave o utilizar una clave pública o privada, como en el caso del cifrado asimétrico.

4. Implementa el cifrado en tu sistema, implementar el cifrado de datos en reposo para proteger la información almacenada en la base de datos cuando no está en uso. Esto implica encriptar los archivos y registros de la base de datos. Asegúrate de que los datos estén cifrados durante la transmisión entre la aplicación y la base de datos. Utiliza conexiones seguras como HTTPS para proteger la transferencia de datos.

5. Gestiona las claves de cifrado, establece un sólido sistema de gestión de claves. Las claves de cifrado deben ser almacenadas de manera segura, y el acceso a ellas debe ser restringido únicamente al personal autorizado.

6. Realiza pruebas y auditorías, realizar pruebas de seguridad y evaluaciones periódicas para detectar posibles vulnerabilidades en el sistema de cifrado y corregirlas de manera inmediata.

3.3. Gestión de contraseñas

Instruir a los usuarios de la base de datos elaboren contraseñas robustas que contengan al menos ocho caracteres, una combinación de letras mayúsculas y minúsculas, números y símbolos, y que cambien regularmente sus contraseñas. A continuación, se prestan las practicas más usadas para la gestión de contraseñas:

1. Evitar contraseñas básicas, se debe evitar contraseñas como "123456", "abcdef" o "qwerty", así como aquellas que incluyan información personal predecible.

2. Crear contraseñas robustas, las contraseñas deben tener al menos 12 caracteres y combinar letras mayúsculas, minúsculas, números y símbolos para aumentar su complejidad.

3. Utilizar una contraseña distinta para cada servicio, no se debe utilizar la misma contraseña para varios servicios, ya que esto incrementa el riesgo en caso de que una contraseña sea comprometida.

4. Gestionar las contraseñas de forma segura, utilizar un administrador de contraseñas con un alto nivel de cifrado para guardar y administrar las contraseñas de forma segura.

5. No compartir contraseñas, las contraseñas deben ser confidenciales y no deben compartirse a través de canales inseguros como el correo electrónico, mensajes de texto o redes sociales.

6. Implementar la rotación de contraseñas, modificar regularmente las contraseñas con el fin de incrementar la seguridad de las cuentas.

7. Utilizar la autenticación de dos factores, cuando sea posible, se tiene que activar la autenticación de dos factores para agregar una capa extra de seguridad a las cuentas

8. Mantener el software actualizado, es fundamental mantener al día tanto el software de administración de contraseñas como el software de los servicios utilizados, con el fin de asegurar la protección de las cuentas.

3.4. Backup y recuperación

Implementar un plan de respaldo y recuperación que posibilite la restauración de los datos en caso de que se pierdan o corrompan. Uno de los mecanismos más usados es la automatización de respaldos con el fin de garantizar la disponibilidad y recuperación de datos en caso de pérdida o corrupción.

Configurar y automatizar el proceso de copias de seguridad, asegurándose de que los respaldos sean íntegros y almacenándolos en ubicaciones seguras. Para realizar los backup automáticos se pueden seguir los siguientes pasos:

1. Seleccionar un software de respaldo automático, seleccionar un software de respaldo automático que se ajuste a las necesidades de la EMAPA y que brinde características como cifrado, encriptación y almacenamiento en múltiples ubicaciones seguras.

2. Configurar y automatizar el proceso de copias de seguridad, instalar el software de respaldo, configura los parámetros correspondientes y programa las copias de seguridad. Una vez completada la configuración inicial, el software de respaldo automático generará copias de los datos seleccionados según tus preferencias, sin necesidad de intervención humana.

3. Verificar la integridad de los respaldos, asegurarse de que los respaldos sean completos y que la información almacenada en ellos sea accesible y recuperable en caso de necesidad.

4. Almacenar los respaldos en ubicaciones seguras, mantenga una copia de los datos tanto en almacenamiento físico como en la nube para asegurar la exitosa recuperación de archivos individuales o una imagen completa del sistema.

5. Cambiar regularmente las contraseñas, los usuarios deben cambiar sus contraseñas regularmente para garantizar la seguridad de la información almacenada en su base de datos personal.

3.5. Medidas de seguridad físicas

Implementar medidas físicas para salvaguardar los servidores y dispositivos que almacenan la base de datos, garantizando su protección contra amenazas físicas y accesos no autorizados. Establecer controles de acceso físico, como sistemas de seguridad y cámaras de vigilancia, en las instalaciones donde se encuentran los servidores.

A continuación, se presentan los pasos más usados para la seguridad física:

1. Evaluar los riesgos físicos, la primera medida para establecer una sólida seguridad física consiste en analizar los riesgos a los que la base de datos podría estar expuesta. Este proceso engloba la evaluación de amenazas internas, tales como el robo o actos de vandalismo, así como amenazas externas, como posibles ataques cibernéticos,

2. Implementar controles físicos, después de haber evaluado los riesgos físicos, proceda a poner en marcha medidas de control físico. Estas medidas pueden abarcar:

   - Control de acceso, medidas para limitar el acceso a la base de datos, tales como puertas con cerraduras, sistemas de control de acceso y sistemas de videovigilancia.

   - Protección contra desastres, controles para resguardar la base de datos ante eventos naturales o provocados, como incendios, inundaciones y cortes de suministro eléctrico.

   - Protección contra el robo, medidas de seguridad para salvaguardar la base de datos contra posibles robos, incluyendo el uso de cajas fuertes y gabinetes de seguridad.

3. Mantener los controles físicos actualizados, Mantenga al día los controles físicos. Es esencial mantener una actualización constante de los controles físicos para asegurar su efectividad continua. Esto implica llevar a cabo inspecciones regulares, reparar o sustituir controles dañados, y realizar actualizaciones según sea necesario.

3.6. Actualización y parches

Es fundamental mantener actualizados todos los sistemas y software relacionados con la base de datos mediante la aplicación oportuna de parches de seguridad. Además, se debe establecer un proceso para supervisar las

actualizaciones de seguridad y aplicar regularmente los parches correspondientes con el fin de mitigar posibles vulnerabilidades conocidas.

1. Evaluar las actualizaciones disponibles, realizar una evaluación de las actualizaciones y parches disponibles para la base de datos en uso. Este proceso implica revisar la documentación proporcionada por el proveedor de la base de datos, consultar fuentes confiables y mantenerse informado sobre las versiones más recientes y las correcciones de seguridad pertinentes.

2. Planificar y programar las actualizaciones, elaborar un plan estructurado y planificado para llevar a cabo la implementación de actualizaciones y parches. Este plan puede comprender la creación de un calendario específico para las actualizaciones, la evaluación de la disponibilidad de sistemas y la coordinación efectiva con el equipo de Tecnologías de la Información (TI) con el fin de minimizar cualquier impacto en las operaciones regulares.

3. Realizar copias de seguridad, previo a la aplicación de cualquier actualización o parche, es fundamental realizar copias de seguridad integrales y verificadas de la base de datos. Esta medida asegura que, en caso de enfrentar cualquier inconveniente durante el procedimiento de actualización, se pueda restablecer la base de datos a un estado anterior sin experimentar pérdida de datos.

4. Aplicar las actualizaciones y parches, siguiendo las directrices proporcionadas por el proveedor de la base de datos, proceder a implementar las actualizaciones y parches correspondientes. Este proceso podría involucrar la descarga de archivos de actualización, la ejecución de scripts de instalación y el seguimiento de los pasos recomendados para llevar a cabo de manera integral el procedimiento de actualización.

5. Realizar pruebas y verificaciones, tras la implementación de las actualizaciones y parches, es imperativo llevar a cabo pruebas exhaustivas para garantizar el correcto funcionamiento de la base de datos. Este

proceso abarca la evaluación de la funcionalidad, la verificación de la integridad de los datos y la realización de pruebas de seguridad con el fin de detectar posibles vulnerabilidades.

6. Monitorear y mantener, implementar un sistema de monitoreo constante con el objetivo de identificar posibles problemas o vulnerabilidades en la base de datos. Asimismo, mantenerse informado sobre las más recientes actualizaciones y parches ofrecidos por el proveedor de la base de datos, aplicándolos de manera puntual.

3.7. Monitoreo continuo

Establecer un sistema de vigilancia continua para detectar de manera inmediata actividades sospechosas o anómalas en tiempo real. Configurar alertas para eventos específicos, realizar revisiones periódicas de los registros de actividad y utilizar herramientas de detección de intrusiones. Para implementar un monitoreo efectivo, se debe seguir los siguientes pasos:

1. Evalúe las necesidades de monitoreo, Analizar los requisitos de supervisión. En una primera instancia, es fundamental evaluar las necesidades de supervisión de la base de datos. Este proceso implica tener en cuenta los datos almacenados en la base de datos.

2. Seleccione las herramientas de monitoreo, elegir las herramientas de supervisión. Después de analizar las necesidades de supervisión, proceda a seleccionar las herramientas correspondientes. Estas herramientas desempeñan un papel crucial al recopilar información sobre la actividad de la base de datos, detectar patrones inusuales y notificar a los usuarios acerca de posibles problemas.

3. Implemente las herramientas de monitoreo, una vez que se han elegido las herramientas de supervisión, es posible iniciar su implementación. Es crucial seguir las directrices proporcionadas por el fabricante o proveedor de estas herramientas para llevar a cabo su implementación de manera segura.

4. Configure las alertas, resulta esencial establecer alertas para eventos que podrían señalar la presencia de problemas potenciales, tales como intentos de acceso no autorizado, modificaciones de datos sin autorización o disminución del rendimiento.

5. Supervise los resultados del monitoreo, es crucial realizar un monitoreo periódico de los resultados para detectar posibles problemas.

3.8. Capacitación al personal

Brindar capacitación periódica al personal sobre prácticas seguras y la importancia de proteger los datos personales. Realizar sesiones de formación, llevar a cabo pruebas de conocimiento y mantener al personal actualizado sobre las últimas amenazas y las mejores prácticas en materia de seguridad. Para implementar una capacitación efectiva, seguir los siguientes pasos:

1. Evalúe las necesidades de capacitación, Analice los requisitos de formación. La primera etapa consiste en evaluar las necesidades de capacitación del personal. Esto incluye los roles y responsabilidades del personal.

2. Desarrolle un plan de capacitación, Una vez que se hayan analizado las necesidades de formación, es posible elaborar un plan de capacitación.

3. Implemente la capacitación, tras haber creado un plan de capacitación, se puede iniciar su implementación. Resulta crucial que la formación sea conducida por un instructor cualificado con experiencia en seguridad de bases de datos.

4. Evalúe la capacitación, resulta fundamental realizar una evaluación de la formación con el fin de asegurar su eficacia. Este proceso puede llevarse a cabo mediante pruebas de conocimientos, evaluaciones de rendimiento o encuestas de satisfacción.

3.9. Programar auditorias de seguridad

Establecer auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y detectar posibles vulnerabilidades o debilidades. Configurar registros de auditoría, revisar regularmente dichos registros y realizar análisis para evaluar la efectividad de los controles implementados.

Las auditorías regulares son fundamentales para garantizar el cumplimiento de las políticas de seguridad y detectar posibles brechas o debilidades en el sistema. Para programar una buena auditoria se puede seguir los siguientes pasos:

1. Establezca los objetivos de la auditoría, en la etapa inicial, se deben definir los objetivos de la auditoría con el propósito de especificar el alcance y los métodos a emplear.

2. Identifique los riesgos, después de fijar los objetivos de la auditoría, es necesario identificar los riesgos que afectan la base de datos. Este procedimiento facilitará la determinación de los controles que deben ser sometidos a auditoría.

3. Seleccione los controles a auditar, a partir de los riesgos identificados, se requiere elegir los controles que se someterán a auditoría. Es crucial dirigir la atención hacia los controles que tienen mayor relevancia para la salvaguarda de los datos personales.

4. Desarrolle un plan de auditoría, el plan de auditoría debe detallar los objetivos, riesgos identificados, controles seleccionados para la auditoría, métodos a emplear y los recursos necesarios.

5. Implemente la auditoría, una vez formulado el plan de auditoría, se puede proceder a su implementación. Es crucial que la auditoría sea llevada a cabo por un auditor capacitado con experiencia en la seguridad de bases de datos.

6. Evalúe los resultados de la auditoría, tras finalizar la auditoría, es esencial evaluar los resultados para detectar posibles áreas de mejora en la seguridad de la base de datos.

3.10. Herramientas de seguridad

Implementar herramientas de seguridad, como cortafuegos y sistemas de detección de intrusiones, con el objetivo de reforzar la protección de la base de datos. Configurar y mantener estas herramientas de seguridad, ajustando los parámetros según sea necesario para adaptarse al entorno y a las amenazas actuales.

Desplegar y configurar adecuadamente herramientas de seguridad es crucial para proteger eficazmente la base de datos contra posibles amenazas y ataques. Para implementar una buena herramienta de seguridad, se debe seguir los siguientes pasos:

1. Evalúe las necesidades de seguridad, en la fase inicial, se debe realizar una evaluación de los requisitos de seguridad de la base de datos, esto incluye considerar los datos almacenados en la base de datos.

2. Seleccione las herramientas de seguridad, después de analizar los requisitos de seguridad, es posible elegir las herramientas de seguridad adecuadas. Estas herramientas desempeñan un papel crucial en la protección de la base de datos contra diversas amenazas, incluyendo ataques cibernéticos, errores humanos y desastres naturales.

3. Implemente las herramientas de seguridad, tras la elección de las herramientas de seguridad, se puede proceder con su implementación. Resulta esencial seguir las indicaciones proporcionadas por el fabricante o proveedor de estas herramientas para garantizar su implementación de manera segura

4. Configure las herramientas de seguridad, es crucial realizar la configuración de las herramientas de seguridad de acuerdo con las necesidades particulares de la organización. Esto implica ajustar las

políticas de seguridad, establecer límites para las alertas y definir los procedimientos de respuesta ante incidentes

5. Supervise el rendimiento de las herramientas de seguridad, e s fundamental configurar las herramientas de seguridad de manera que se adapten a las necesidades específicas de la organización. Esto puede implicar establecer las políticas de seguridad, los umbrales de alerta y los procedimientos de respuesta ante incidentes de forma personalizada.

4. Monitoreo de la implementación de las actividades de seguridad de la base de datos personales

El monitoreo continuo de las actividades relacionadas con la seguridad de los datos personales es fundamental para detectar posibles amenazas, evaluar la efectividad de los controles implementados y responder de manera rápida a incidentes. Entre las actividades se encuentran:

4.1. Registros de Auditorías

El registro de auditorías implica documentar y analizar de manera sistemática los eventos relacionados con la seguridad de una base de datos. Esto implica supervisar de manera continua y sistemática los eventos registrados para garantizar la seguridad de una base de datos. Esto implica revisar regularmente los registros, identificar patrones y anomalías, y generar informes detallados. El monitoreo permite una respuesta rápida ante posibles amenazas o actividades no autorizadas, lo que contribuye a la gestión proactiva de la seguridad y privacidad de la información almacenada. Este proceso se adapta y mejora de manera continua para mantener su efectividad frente a cambios en el entorno operativo o normativo.

4.2. Accesos no Autorizados

Mantener una supervisión constante de los intentos de acceso no permitidos a sistemas o recursos. Este proceso incluye la revisión en tiempo real o periódica de los registros de acceso, la detección de patrones sospechosos y la generación de alertas ante actividades inusuales. El monitoreo busca identificar posibles

amenazas, como intentos de intrusión o comportamientos anómalos, permitiendo una respuesta rápida para mitigar riesgos y preservar la seguridad de los sistemas y la información. Este proceso se ajusta continuamente para adaptarse a nuevas amenazas y cambios en el entorno operativo.

4.3. Actividades de Cifrado

La verificación periódica es supervisar de manera continua el estado y la eficacia de las medidas de cifrado implementadas en un sistema o red. Esto implica revisar eventos relacionados con el cifrado, verificar la correcta aplicación de algoritmos y claves, y detectar posibles intentos de manipulación o vulnerabilidades en la seguridad del cifrado. El monitoreo busca garantizar la integridad y confidencialidad de la información, identificando cualquier anomalía que pueda comprometer la eficacia del cifrado. Este proceso se adapta y actualiza de forma continua para hacer frente a las amenazas emergentes y los avances en técnicas de cifrado.

4.4. Actualizaciones y Parches

Mantenerse informado sobre las actualizaciones y parches de seguridad disponibles y asegurar su aplicación de manera oportuna. Las actualizaciones de software y la implementación de parches en un sistema implican revisar regularmente las notificaciones de actualizaciones, verificar la aplicabilidad y relevancia de los parches, y planificar su implementación. El objetivo del monitoreo es garantizar que los sistemas estén protegidos contra vulnerabilidades conocidas y que las actualizaciones críticas se realicen de manera oportuna para mantener la seguridad y estabilidad del entorno tecnológico. Este proceso se ajusta continuamente para adaptarse a los requisitos de seguridad y las mejores prácticas de la industria.

4.5. Configuraciones de Seguridad

Llevar a cabo una supervisión y evaluación periódica de la configuración de los controles de seguridad para garantizar su alineación con las políticas establecidas. La supervisión continua de los ajustes de seguridad en un sistema

o red implica revisar regularmente las configuraciones para garantizar el cumplimiento de las políticas de seguridad, detectar posibles desviaciones o cambios no autorizados, y generar alertas en caso de configuraciones inseguras. El monitoreo tiene como objetivo mantener la integridad y la eficacia de las configuraciones de seguridad, asegurando que estén en línea con las mejores prácticas y los estándares establecidos. Se realiza de manera constante para adaptarse a los cambios en el entorno y prevenir posibles riesgos de seguridad.

4.6. Actividades de Copias de Seguridad

Asegurarse de que se realicen regularmente copias de seguridad y de que se puedan restaurar correctamente. Implica revisar regularmente los registros de copias de seguridad, verificar la ejecución exitosa de los respaldos y generar alertas en caso de fallas o irregularidades. El objetivo del monitoreo es garantizar la integridad y disponibilidad de los datos, identificando posibles problemas en el proceso de copia de seguridad y asegurando que se realice de acuerdo con las políticas y programaciones establecidas. Este proceso se ajusta continuamente para adaptarse a cambios en los requisitos de respaldo y mitigar riesgos potenciales.

4.7. Actividades de Formación

Es fundamental evaluar la eficacia de los programas de formación en seguridad y adaptarlos en función de la retroalimentación y las necesidades cambiantes. La revisión de los cursos, evaluaciones y participación de los empleados, así como la medición de los resultados y el impacto de la formación en el desarrollo de habilidades, busca garantizar la efectividad de los programas de formación, identificar áreas de mejora y asegurar que los empleados adquieran los conocimientos necesarios. Este proceso se realiza de manera constante para adaptarse a las necesidades cambiantes y mejorar continuamente las iniciativas de formación.

4.8. Actividades Físicas de Seguridad

La supervisión constante de medidas y procedimientos físicos destinados a proteger los activos y la infraestructura de una organización. El monitoreo incluye la revisión de sistemas de videovigilancia, control de accesos, alarmas y patrullas de seguridad. El objetivo del monitoreo es asegurar la integridad de las instalaciones, detectar comportamientos o eventos inusuales, y responder rápidamente a posibles amenazas físicas. Este proceso se lleva a cabo de forma continua para garantizar la eficacia de las medidas de seguridad física y adaptarse a cambios en el entorno o en los riesgos identificados.

4.9. Configuraciones de Seguridad

La supervisión continua de las configuraciones tiene como objetivo garantizar el cumplimiento de políticas y normativas, detectar posibles cambios no autorizados y generar alertas en caso de configuraciones inseguras. El monitoreo busca mantener la integridad y eficacia de las configuraciones de seguridad, asegurando que estén alineadas con las mejores prácticas y estándares establecidos. Este proceso se realiza de manera constante para adaptarse a cambios en el entorno y prevenir posibles riesgos de seguridad.

4.10. Herramientas de Seguridad

El rendimiento y las alertas generadas por las herramientas de seguridad, realizando los ajustes necesarios. La evaluación de los eventos producidos por dichas herramientas, la identificación de posibles amenazas o vulnerabilidades, así como la emisión de alertas ante actividades anómalas, son parte integral del monitoreo. Este proceso tiene como objetivo asegurar la eficacia de las herramientas de seguridad, detectar incidentes de forma temprana y responder de manera ágil ante posibles riesgos. Se lleva a cabo de manera constante para ajustarse a las variaciones en las amenazas cibernéticas y garantizar la robustez de las defensas de seguridad.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Durante la evaluación, se detectaron posibles debilidades en la infraestructura de la base de datos, lo que permitió tener una comprensión precisa de los aspectos que necesitan ser atendidos y reforzados.

- El compliance en ciberseguridad no se limita únicamente a una obligación normativa, además se configura como una táctica proactiva destinada a preservar la integridad de los datos, proteger la reputación de la entidad y promover la capacidad de recuperación frente a posibles amenazas.

- El entorno de ciberseguridad cambia constantemente, por lo que es crucial que las empresas revisen y actualicen regularmente su programa de cumplimiento. Esto garantizará que la organización cumpla con las normativas y regulaciones vigentes. El cumplimiento en ciberseguridad es un componente estratégico esencial para garantizar la continuidad operativa de la empresa. No solo evita pérdidas financieras, sino que también protege la reputación corporativa en un entorno digital cada vez más complejo y desafiante.

- La validación de la efectividad de los protocolos de seguridad en la base de datos personales de la EMAPA resalta la importancia de preservar y desfortalecer estos elementos para garantizar la integridad y confidencialidad de la información almacenada.

- La implementación del compliance de ciberseguridad en la EMAPA instaura una cultura de seguridad en la entidad, la cual cada miembro asume la responsabilidad de proteger la base de datos personales, implicando la formación del personal y la aplicación de las normas de protección.

- La aplicación del compliance de ciberseguridad no solo ha fortalecido la seguridad de la base de datos personal de EMAPA, sino que también ha resultado esencial para cumplir con regulaciones y normativas que protegen la privacidad

y la integridad de los datos, garantizando de esta manera la legalidad e integridad en el manejo de la información.

4.2 Recomendaciones

- Desarrollar e implementar un conjunto de medidas preventivas con el propósito de fortalecer la seguridad de la base de datos personales, incluya medidas que permitan su actualización periódica.

- Implementar un programa de cumplimiento normativo en el ámbito de la ciberseguridad que englobe todas las regulaciones y normativas que son pertinentes para la entidad. Esto implica la necesidad de mantenerse informado acerca de las modificaciones en las leyes y regulaciones vinculadas con la protección de datos y la seguridad cibernética.

- Establecer periódicamente ciclos de revisión para evaluar la eficacia y pertinencia del programa de cumplimiento. Esto permitirá realizar ajustes oportunamente en respuesta a los cambios en el entorno cibernético y en las regulaciones.

- Es indispensable que la EMAPA fomente una cultura organizacional sólida fundamentada en la ciberseguridad. Esto implica establecer prácticas seguras en todos los estratos de la organización, abarcando desde la alta dirección hasta el personal operativo. Cultivar la conciencia y la responsabilidad de todos los empleados en relación con la ciberseguridad será una contribución significativa para prevenir amenazas y salvaguardar la continuidad operativa.

- La EMAPA requiere implementar un plan de actualizaciones periódicas para los protocolos de seguridad. La confirmación de la eficacia de los protocolos enfatiza la necesidad de mantener estas medidas alineadas con las tendencias y amenazas más recientes en ciberseguridad, mediante la introducción de actualizaciones de forma regular asegurará que los protocolos de seguridad se adapten a los cambios en el entorno de amenazas.

- Asegurarse de implementar las salvaguardias de seguridad indispensables para resguardar la base de datos personal de EMAPA. Estas medidas pueden comprender la encriptación de datos, la autenticación de dos factores y la instauración de políticas de acceso y control de datos.

REFERENCIAS BIBLIOGRÁFICAS

[1] G. C. Garzón, “Análisis de seguridad en base de datos: Aplicación Oracle versión 11g”.

[2] M. Joe, “UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL”.

[3] M. Alassaf y A. Alkhalifah, “Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review”, *IEEE Access*, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 162687–162705, 2021. doi: 10.1109/ACCESS.2021.3132574.

[4] F. E. Vela Vela, “UNIVERSIDAD TECNOLÓGICA ISRAEL Título del artículo ESTUDIO DE UN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PARA BASE DE DATOS SQL SERVER CASO DE ESTUDIO: MINISTERIO DE RELACIONES EXTERIORES Y MOVILIDAD HUMANA Línea de Investigación: SEGURIDAD INFORMÁTICA Campo amplio de conocimiento: TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Autor”, 2022.

[5] Aspiazu Soto Erick Josué y Tacuri Valdivieso Erik Joel, “ANÁLISIS DE TÉCNICAS DE SEUDONIMIZACIÓN PARA LAPROTECCIÓN DE DATOSCOMO MEDIDAS DESEGURIDADEN LA APLICACIÓN DE LALEYORGÁNICA DEPROTECCIÓNDEDATOSPERSONALESDELECUADOR (LOPD)”.

[6] Alexander Quimis, “Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica”.

[7] Patricio Neptali Vaca Escobar., “MODELO DE GESTIÓN DE EGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓNDE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR”.

[8] Mayra Gabriela Cordero Núñez, “POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADAS EN NORMAS INTERNACIONALES PARA GARANTIZAR CONTROLES ANTE AMENAZAS Y VULNERABILIDADES EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA”.

[9] Joaquim Cuevas, “Innovación técnica y estructura empresarial”, *Universidad dÁlacant*.

[10] “¿Qué es gestión empresarial? Management en 2022 | Blog Becas Santander”. Consultado: el 14 de mayo de 2023. [En línea]. Disponible en: https://www.becas-santander.com/es/blog/gestion-empresarial.html

[11] “Compliance y Protección de Datos ¿Cómo se relacionan? | Grupo Atico34”. Consultado: el 5 de mayo de 2023. [En línea]. Disponible en: https://protecciondatos-lopd.com/empresas/relacion-compliance-y-proteccion-de-datos/

[12] C. Belloch, “Las Tecnologías de la Información y Comunicación en el aprendizaje”, 2002. [En línea]. Disponible en: http://www.clubcultura.com/clubliteratura/clubescritores/sampedro/miradas_global.htm

[13] “Seguridad informática - Purificación Aguilera López - Google Libros”.

[14] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, y J. A. Saltos-Gómez, “La seguridad informática y la seguridad de la información”, *Polo del Conocimiento*, vol. 2, núm. 12, p. 145, mar. 2018, doi: 10.23857/pc.v2i12.420.

[15] “Seguridad de las bases de datos: guía básica | IBM”. Consultado: el 14 de mayo de 2023. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/database-security

[16] A. Fernando y S. Oñate, “Metodologías ágiles Scrum, XP, SLeSS, Scrumban, HME, Mobile-D y MASAN empleadas en la industria de dispositivos móviles: Un contraste en favor de la industria del desarrollo móvil”. Universidad Peruana Unión, el 20 de diciembre de 2020. Consultado: el 19 de noviembre de 2023. [En línea]. Disponible en: https://repositorio.upeu.edu.pe/handle/20.500.12840/3906

[17] D. L. Gómez-Molina y J. Moyano-Fuentes, “Lean management in universities: a systematic literature review”, *International Journal of Lean Six Sigma*, vol. 13, núm. 1, pp. 156–177, ene. 2022, doi: 10.1108/IJLSS-12-2020-0224/FULL/XML.

[18] Julia Martins, “Scrum: conceptos clave y cómo se aplica en la gestión de proyectos”, Asana. Consultado: el 19 de noviembre de 2023. [En línea]. Disponible en: https://asana.com/es/resources/what-is-scrum

[19] N. Ozkan, S. Bal, T. G. Erdogan, y M. S. Gok, “Scrum, Kanban or a Mix of Both? A Systematic Literature Review”, *Proceedings of the 17th Conference on Computer Science and Intelligence Systems, FedCSIS 2022*, pp. 883–893, 2022, doi: 10.15439/2022F143.

[20] M. O. Ahmad, J. Markkula, y M. Oivo, “Kanban in software development: A systematic literature review”, pp. 9–16, 2019, doi: 10.1109/SEAA.2013.28.

[21] Theodore L. Banks y Frederick Z. Banks, *Corporate Legal Compliance Handbook*, Segunda. United States: Aspen Publishers, 2019.

[22] David Kotz, *Financial Regulation and Compliance: How to Manage Competing and Overlapping Regulatory Oversight*, Primera. Wiley, 2018.

[23] I. Carr y P. Stone, *International Trade Law*, 6th Edition. London: Routledge, 2019. doi: 10.4324/9781315543970.

[24] Charles D. Reese, *Occupational Health and Safety Management: A Practical Approach, Third Edition*, 3rd Edition. CRC Press, 2020.

[25] Joseph W. Weiss, *Business Ethics: A Stakeholder and Issues Management Approach*, vol. 5a edición. Oakland: Cengage Learning, 2021.

[26] Alan Calder, *ISO27001 / ISO27002: A Pocket Guide*, Segunda. It Governance Publishing, 2021.

[27] *Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.* 2021. Consultado: el 2 de noviembre de 2023. [En línea]. Disponible en: https://www.boe.es/eli/es/lo/2021/05/26/7/con

[28] C. De Diputados, D. H. Congreso De, y L. A. Unión, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. 2010.

[29] Q. Suplemento, "Año II-Nº 459-70 páginas Quito, miércoles 26 de mayo de 2021 ASAMBLEA NACIONAL LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES".

[30] Michael T. Simpson y Kent Backman, *CISSP All-in-One Exam Guide, Eighth Edition*, Eighth Edition. McGraw Hill, 2021. Consultado: el 28 de octubre de 2023. [En línea]. Disponible en: https://dl.acm.org/doi/abs/10.5555/1594805

[31] Dafydd Stuttard y Marcus Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd edición. Indeanapolis: Wiley, 2021.

[32] Brian T. O'Hara y Ben Malisow, *CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide*, 2nd Edition. Sybex, 2020.

[33] Neil. Bergman, Mike. Stanfield, Jason. Rouse, y Joel. Scambray, *Hacking exposed mobile: security secrets & solutions*. McGraw-Hill Education, 2022. Consultado: el 28 de octubre de 2023. [En línea]. Disponible en: https://mhebooklibrary.com/doi/book/10.1036/9780071817028

[34] Autor: Michael E. Whitman y Herbert J. Mattord, *Principles of Information Security*, Fourth Edition. Kennesaw State University: Cengage Learning, 2022.

[35] R. M. Alguliyev, R. M. Aliguliyev, y F. J. Abdullayeva, "Privacy-preserving deep learning algorithm for big personal data analysis", *J Ind Inf Integr*, vol. 15, pp. 1–14, sep. 2020, doi: 10.1016/J.JII.2019.07.002.

[36] R. Sharma, S. Dangi, y P. Mishra, "A Comprehensive Review on Encryption based Open Source Cyber Security Tools", *Proceedings of IEEE International Conference on Signal Processing,Computing and Control*, vol. 2021-October, pp. 614–619, 2021, doi: 10.1109/ISPCC53510.2021.9609369.

[37] A. Keliris y M. Maniatakos, “Demystifying Advanced Persistent Threats for Industrial Control Systems”, *Mechanical Engineering*, vol. 139, núm. 03, pp. S13–S17, mar. 2019, doi: 10.1115/1.2017-MAR-6.

[38] C. Hu, W. Li, X. Cheng, J. Yu, S. Wang, y R. Bie, “A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds”, *IEEE Trans Big Data*, vol. 4, núm. 3, pp. 341–355, feb. 2020, doi: 10.1109/TBDATA.2016.2621106.

[39] Ley, “LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES”. [En línea]. Disponible en: www.lexis.com.ec

[40] *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. Quito: ASAMBLEA NACIONA, 2021.

[41] “Superintendencia de Protección de Datos”. Consultado: el 3 de enero de 2024. [En línea]. Disponible en: https://www.cpccs.gob.ec/designacion-de-autoridades/super-proteccion-datos/

[42] *REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ CE (Reglamento general de protección de datos)*. 2016.

[43] *Ley de Privacidad del Consumidor de California.* California, 2023. Consultado: el 3 de enero de 2024. [En línea]. Disponible en: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[44] EMAPA, “Diagrama de la Base de Datos”. Consultado: el 3 de diciembre de 2023. [En línea]. Disponible en: https://docs.google.com/spreadsheets/d/1useVEmiyxEmCXaRGUcMcWHDxW3P7m9dM/edit?usp=sharing&ouid=103209361986259157270&rtpof=true&sd=true

ANEXOS

Anexo A. Formula de Kuder-Richardson aplicada en la encuesta del personal del departamento de TI de la EMAPA.

En la figura A1 se muestra la aplicación de la fórmula de Kuder-Richardson para la validación del instrumento.

	Preguntas		
Individuos	**P3**	**P8**	
1	0	0	0
2	1	1	2
3	1	0	1
4	0	1	2
5	0	0	0
Totales	2	2	
p	0,4	0,4	
q	0,6	0,6	
p * q	0,24	0,24	
∑(p * q)	0,48		
σ^2	0,8		
k	2		

$\left(\frac{k}{k-1}\right)$ ➤ **2,00**

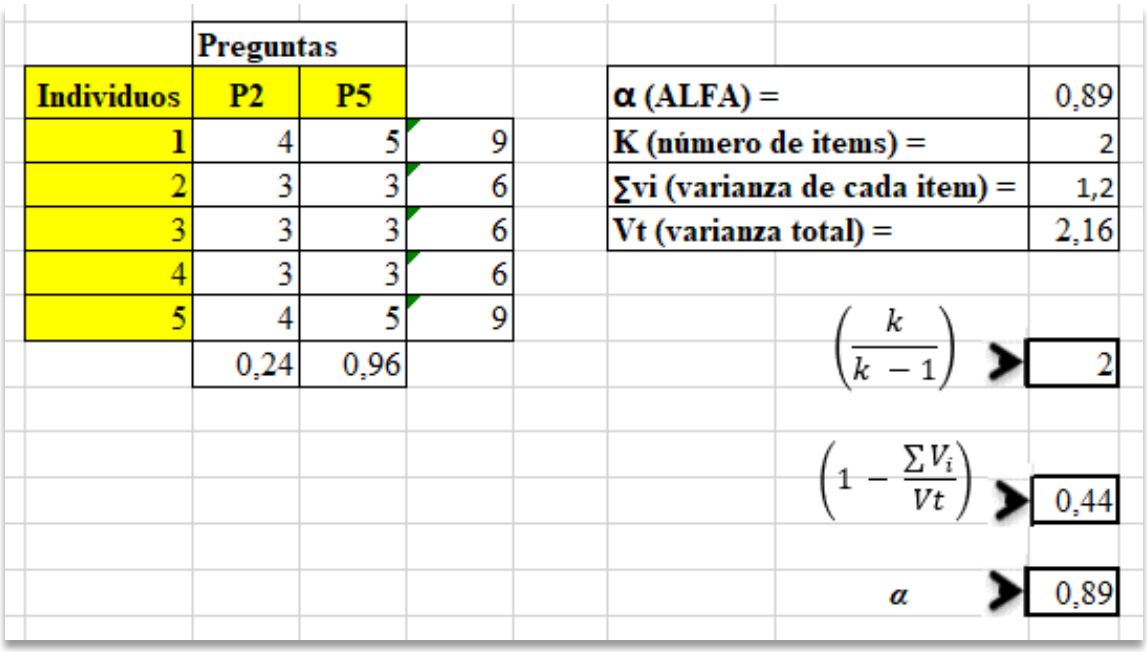
$\left(1-\frac{\sum pq}{\sigma^2}\right)$ ➤ **0,40**

➤ **KR-20** **0,80**

Figura A1. Formula de Kuder-Richardson

Anexo B. Formula de Alfa de Cronbach aplicada en la encuesta del personal del departamento de TI de la EMAPA

En la figura B1 se muestra la aplicación de la fórmula de Alfa de Cronbach para la validación del instrumento



	Preguntas		
Individuos	**P2**	**P5**	
1	4	5	9
2	3	3	6
3	3	3	6
4	3	3	6
5	4	5	9
	0,24	0,96	

α (ALFA) =	0,89
K (número de items) =	2
∑vi (varianza de cada item) =	1,2
Vt (varianza total) =	2,16

$\left(\frac{k}{k-1}\right)$ ➤ 2

$\left(1-\frac{\sum V_i}{Vt}\right)$ ➤ 0,44

α ➤ 0,89

Figura B1. Formula de Alfa de Cronbach

Anexo C. Diagrama de entidad relación de la base de datos.

En la figura C1 se muestra la primera parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

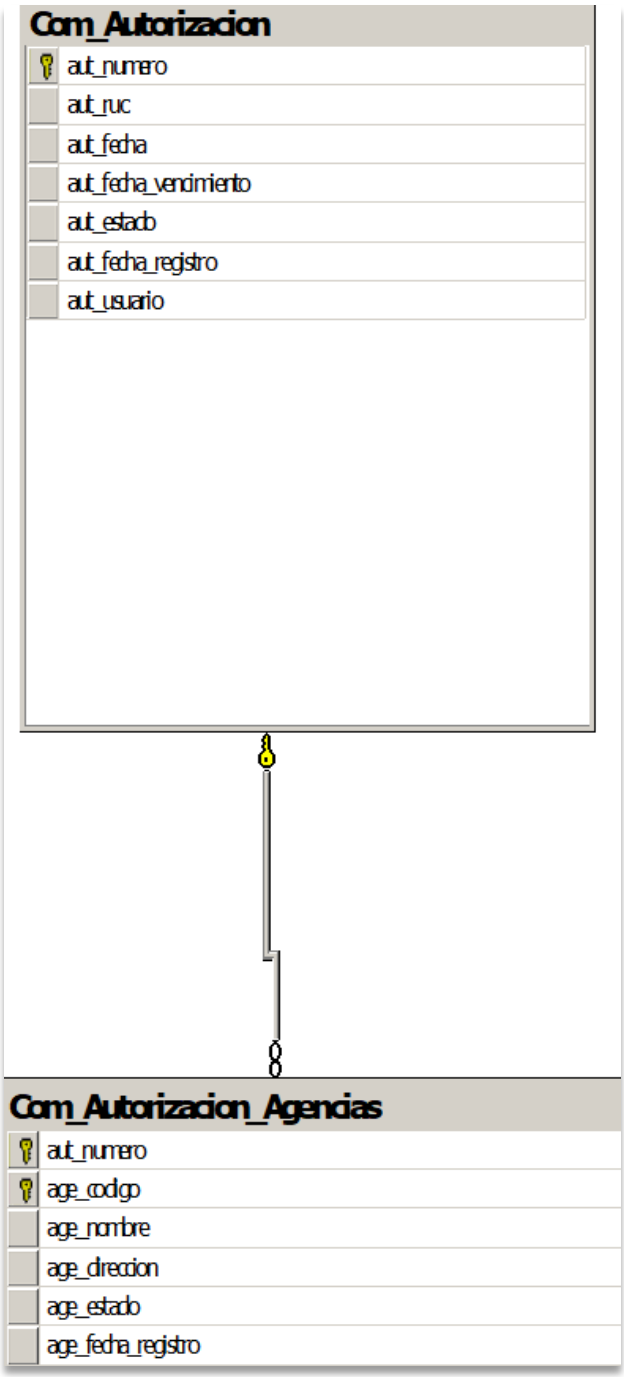


Figura C1. Diagrama de entidad relación.

Anexo D. Diagrama de entidad relación de la base de datos

En la figura D1 se muestra la segunda parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

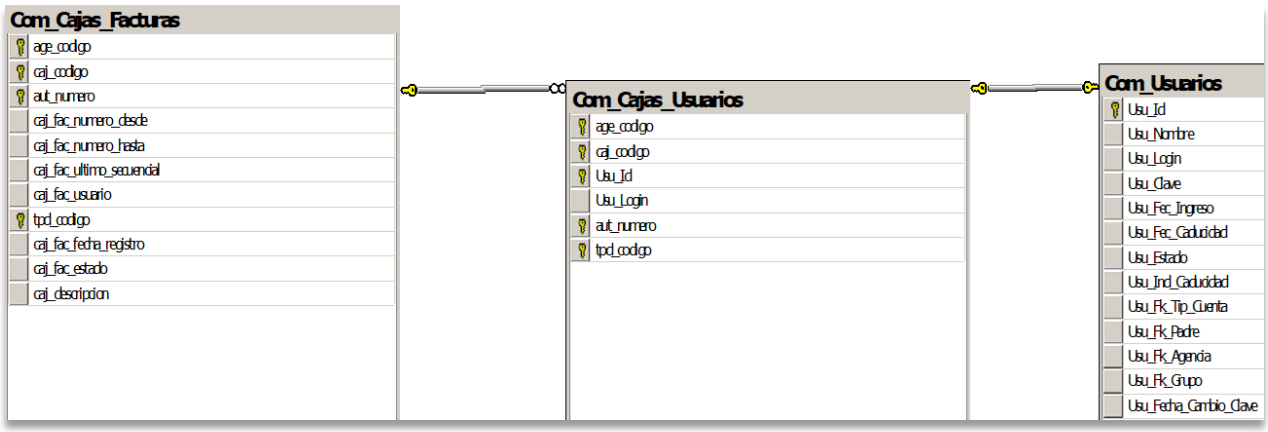


Figura D1. Diagrama de entidad relación.

Anexo E. Diagrama de entidad relación de la base de datos.

En la figura E1 se muestra la tercera parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

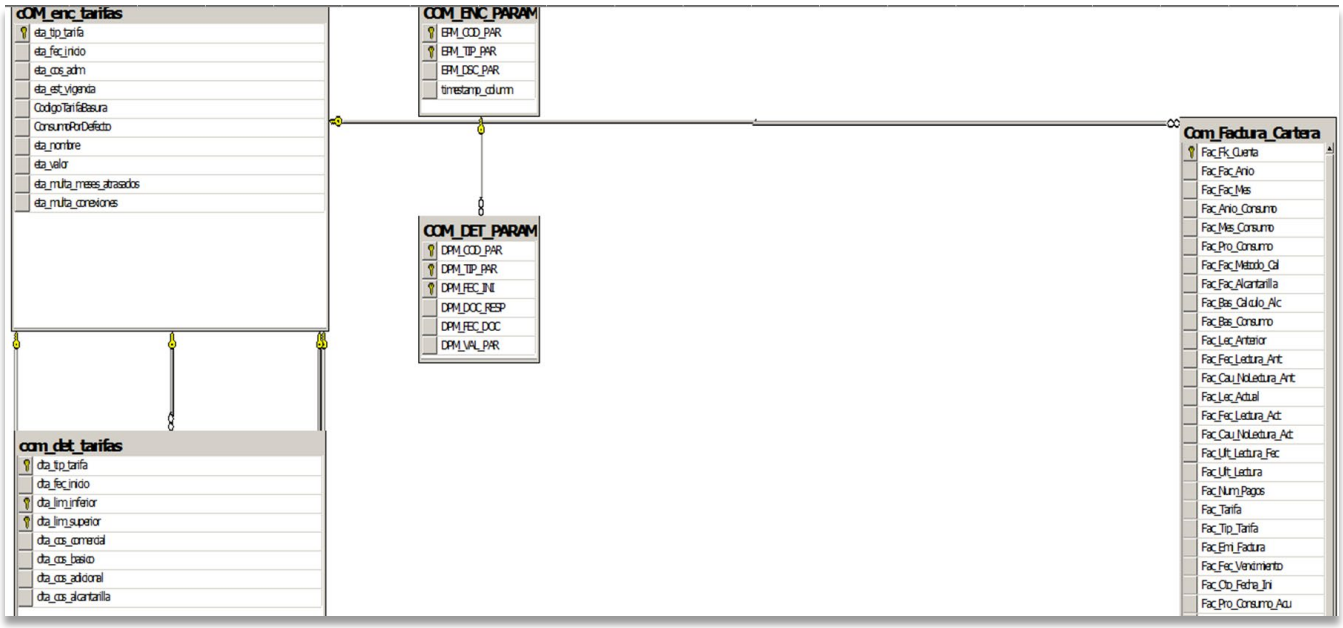


Figura E1. Diagrama de entidad relación.

Anexo F. Diagrama de entidad relación de la base de datos.

En la figura F1 se muestra la cuarta parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

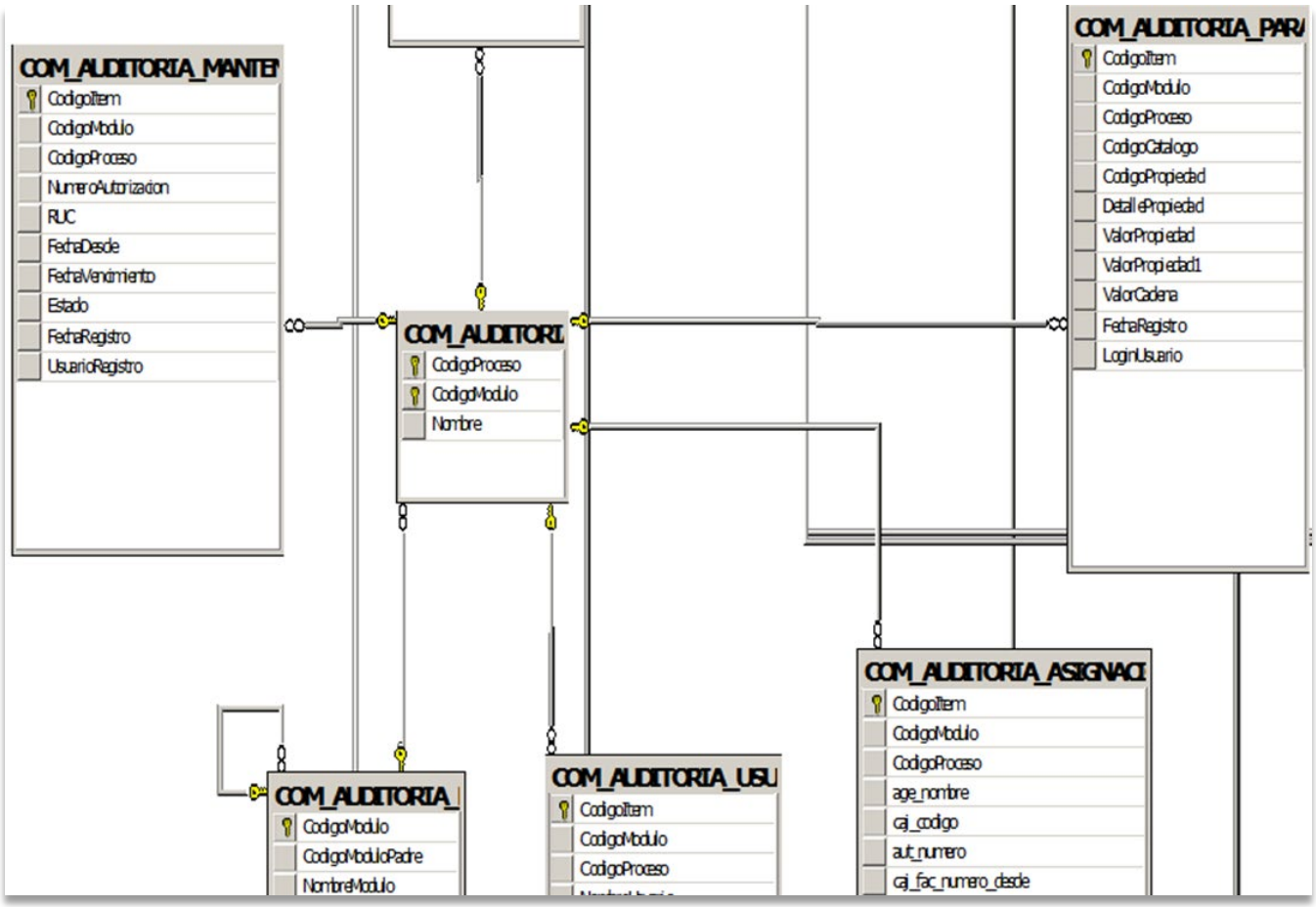


Figura F1. Diagrama de entidad relación.

Anexo G. Diagrama de entidad relación de la base de datos.

En la figura G1 se muestra la quina parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

Figura G1. Diagrama de entidad relación.

Anexo H. Diagrama de entidad relación de la base de datos.

En la figura H1 se muestra la sexta parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

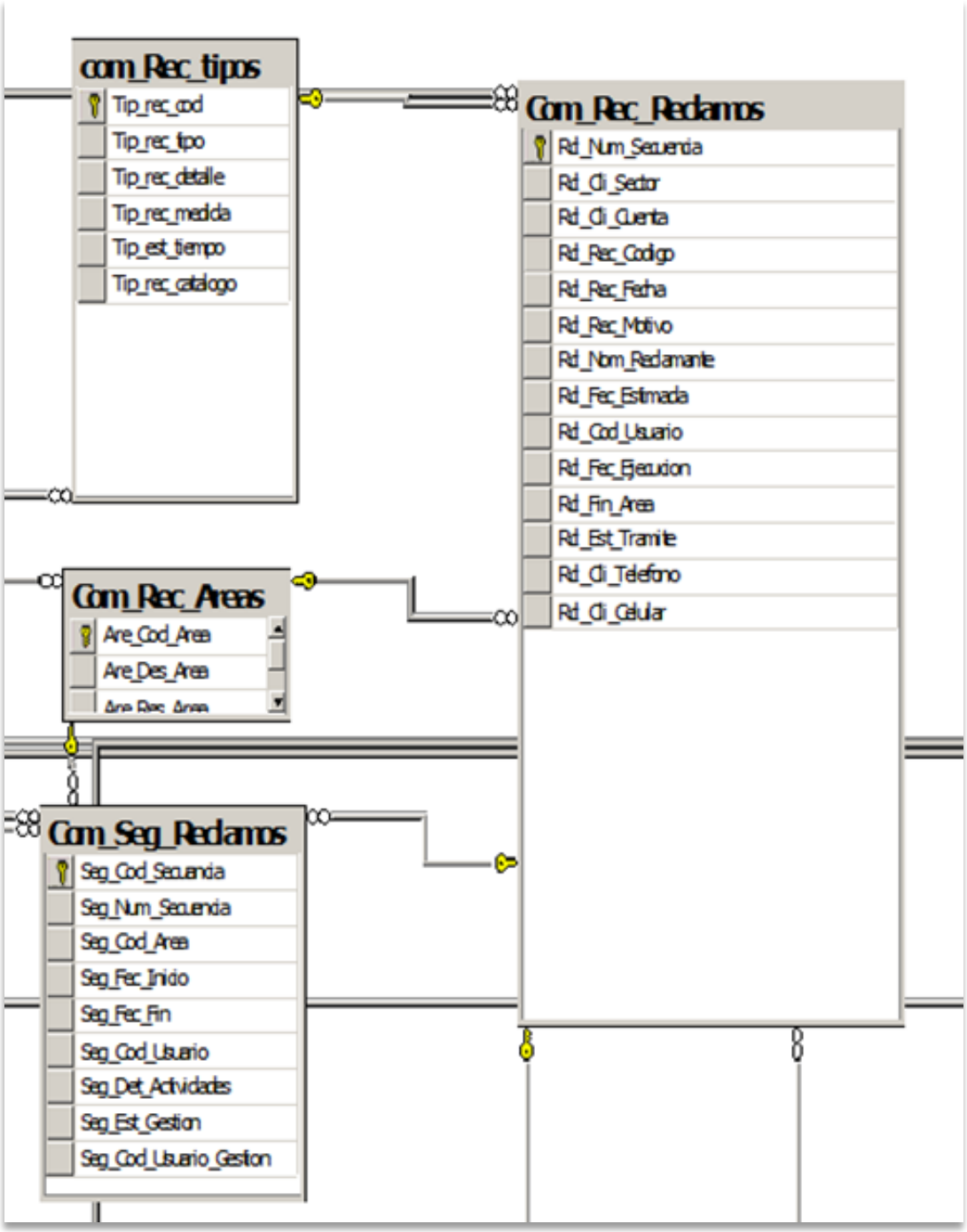


Figura H1. Diagrama de entidad relación.

Anexo I. Diagrama de entidad relación de la base de datos.

En la figura I1 se muestra la séptima parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

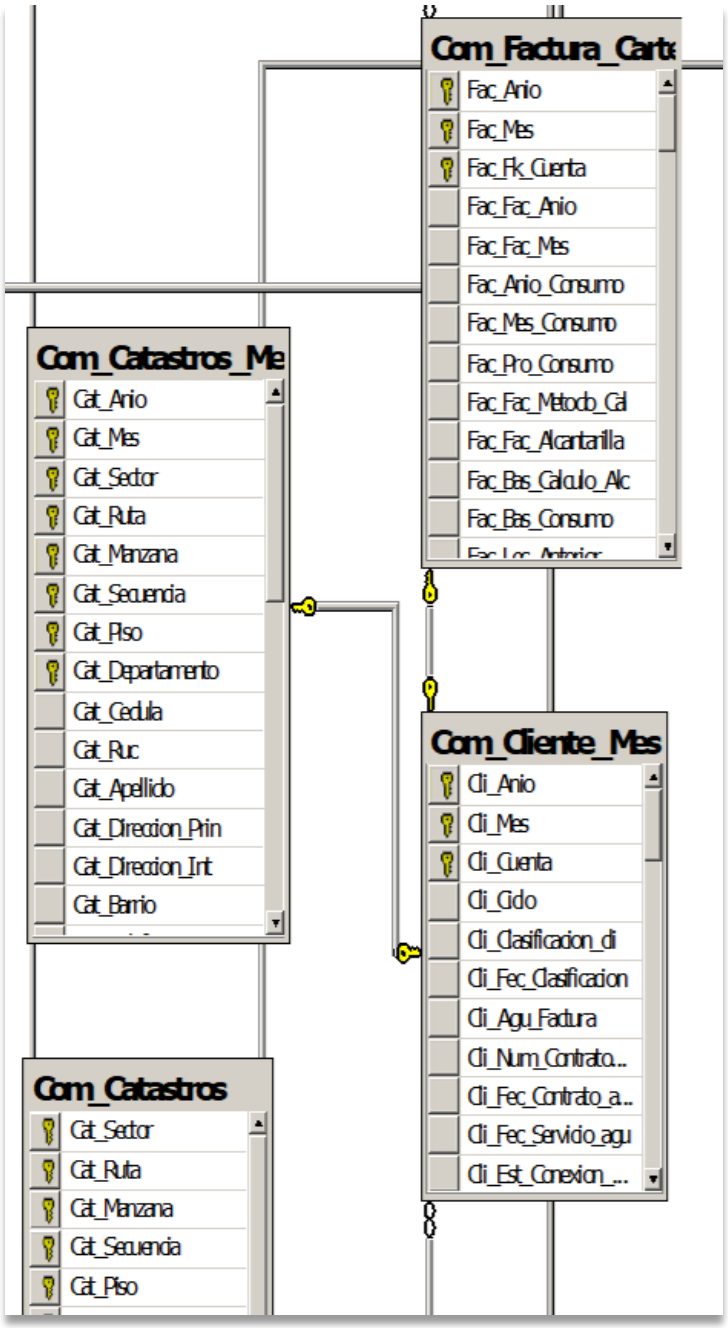


Figura I1. Diagrama de entidad relación.

Anexo J. Diagrama de entidad relación de la base de datos.

En la figura J1 se muestra la octava parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

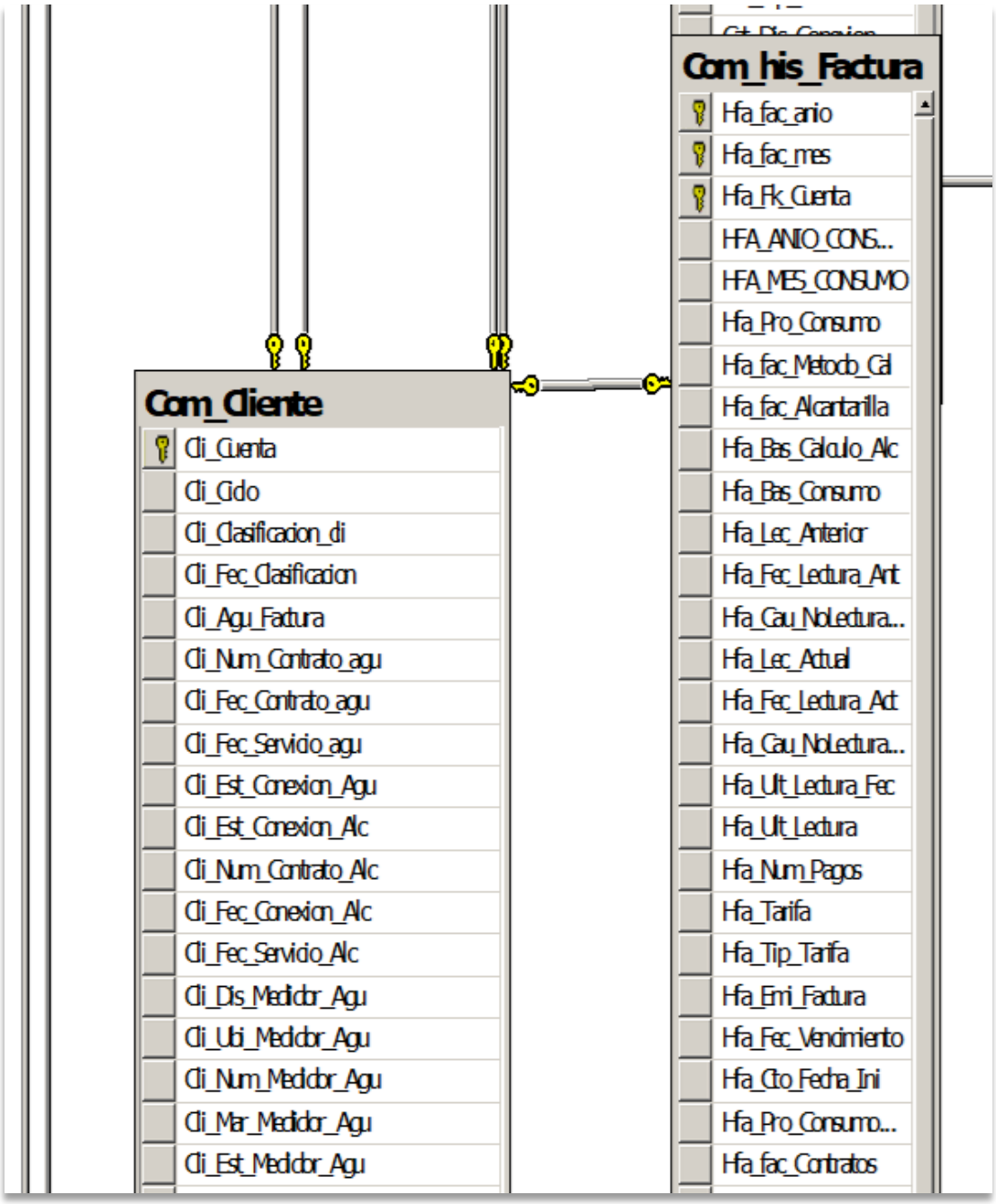


Figura J1. Diagrama de entidad relación.

Anexo K. Diagrama de entidad relación de la base de datos.

En la figura K1 se muestra la novena parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

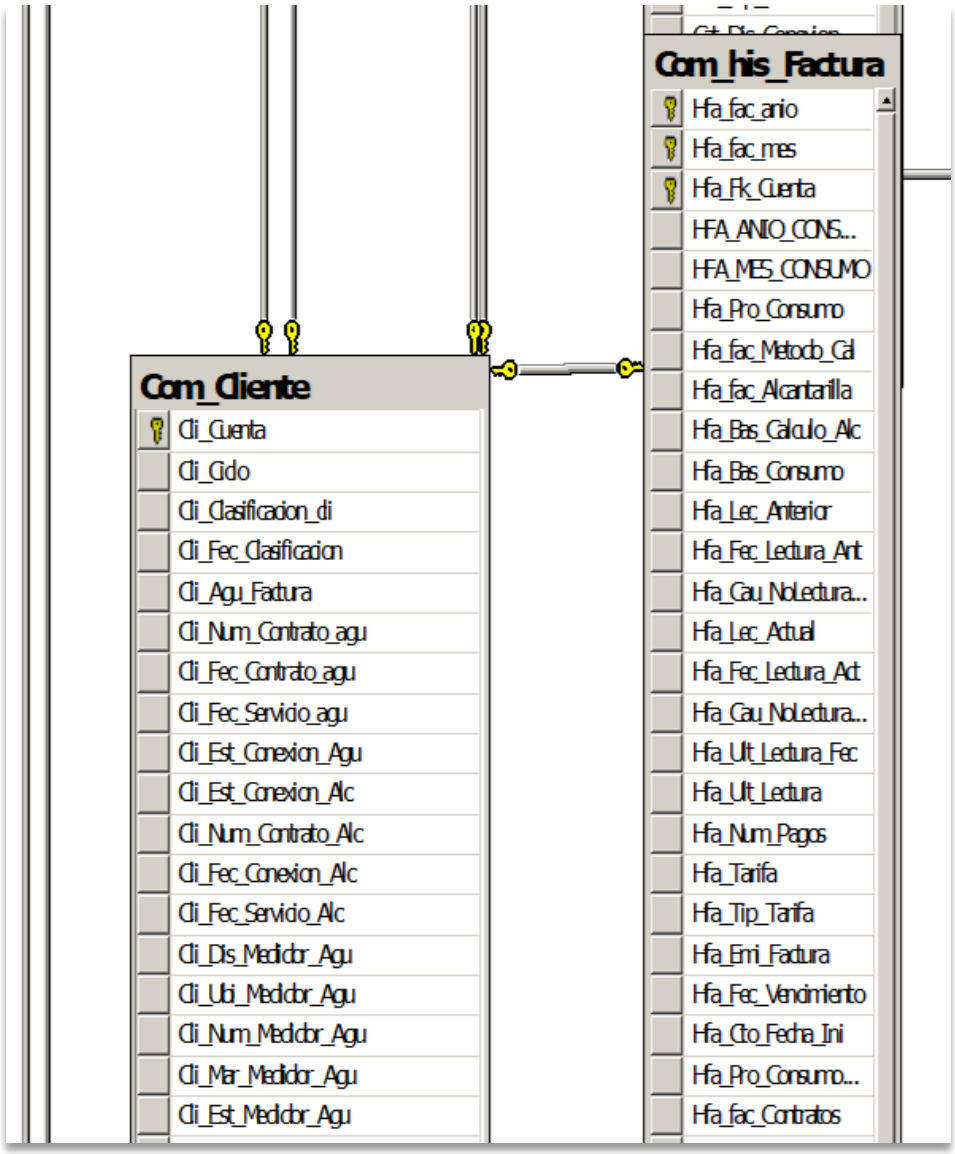


Figura K1. Diagrama de entidad relación

Anexo L. Diagrama de entidad relación de la base de datos.

En la figura L1 se muestra la décima parte del diagrama de entidad relación de la base de datos comercial de la EMAPA.

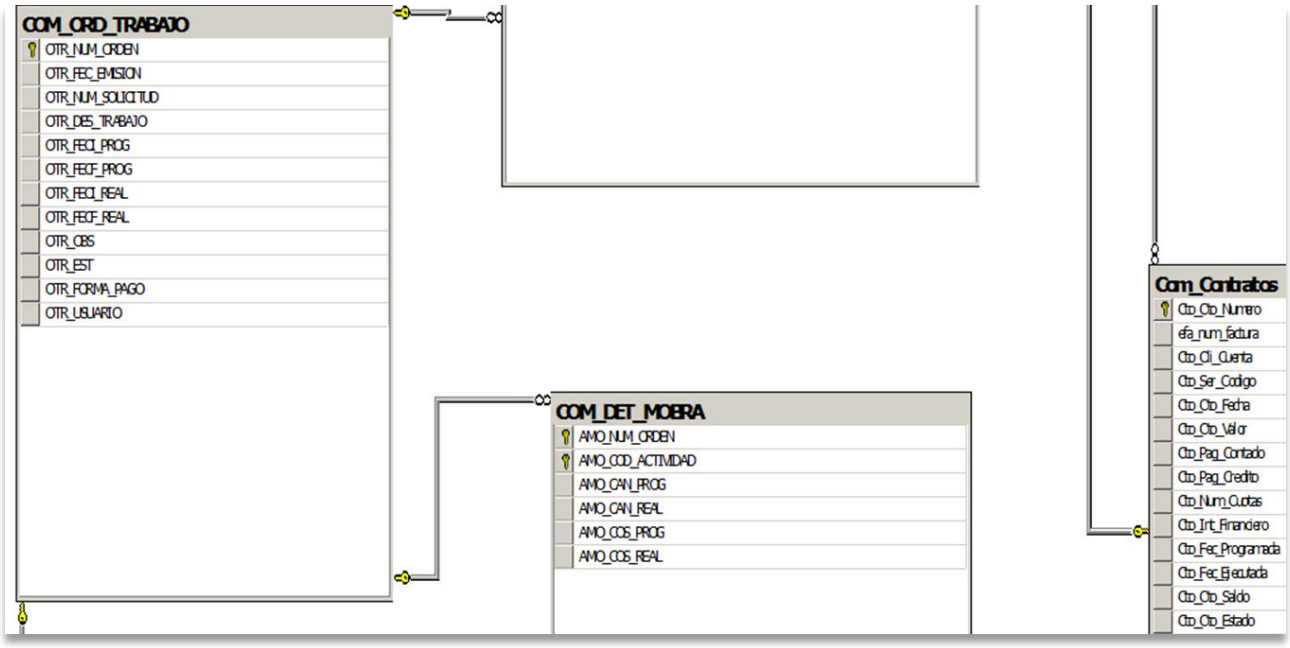


Figura L1. Diagrama de entidad relación