**AUDITORÍA INFORMÁTICA EN LA EMPRESA MOTOREPUESTOS CUMARAL**

Edinson Fabian Guzmán Ladino (Auditor)

Corporación Universitaria Del Meta (UNIMETA)

Auditoría Informática

Omar Edgardo Vargas Rojas (Asesor)

27/04/2024

**Lista de tablas**

[Tabla 1 Cronograma Ciclo Deming 10](#_Toc164522446)

[Tabla 2 Programación de auditoría física 23](#_Toc164522447)

[Tabla 3 Cronograma de plan de acción para los hallazgos 26](#_Toc164522448)

**Lista de ilustraciones**

[Ilustración 1 Especificaciones de Windows 4](#_Toc164522439)

[Ilustración 2 Especificaciones del dispositivo 4](#_Toc164522440)

[Ilustración 3 Herramientas de visualización de datos 13](#_Toc164522441)

Introducción

Estimados miembros de la dirección y equipo de *MotoRepuestos Cumaral* – Venta de Repuestos para Moto.

Nos complace presentarles el informe de auditoría informática realizada en su organización, con el objetivo de evaluar la integridad, seguridad y eficiencia de los sistemas de información y tecnologías de la empresa relacionados con la gestión de inventarios, ventas y operaciones comerciales de repuestos para motos.

En el entorno empresarial actual, la tecnología juega un papel fundamental en la optimización de los procesos operativos, la toma de decisiones estratégicas y la satisfacción del cliente. La auditoría informática se ha llevado a cabo con el fin de proporcionar una evaluación objetiva y detallada de los controles, políticas y procedimientos implementados en la gestión de la información y la seguridad de los sistemas de información utilizados en su empresa.

Durante el proceso de auditoría, se han examinado diversos aspectos clave, incluyendo la gestión de inventarios, la integridad de los datos, los controles de acceso y seguridad, la continuidad operativa, y el cumplimiento de las normativas y estándares aplicables. Los hallazgos y recomendaciones presentados en este informe tienen como objetivo identificar áreas de mejora, fortalecer los controles internos y promover las mejores prácticas en la gestión de la tecnología de la información en su organización.

Esperamos que este informe sea una herramienta valiosa para la dirección y el equipo de *MotoRepuestos Cumaral* en la identificación de oportunidades de mejora, la implementación de acciones correctivas y la promoción de una cultura de excelencia y seguridad en el uso de la tecnología de la información.

Agradecemos su cooperación y compromiso durante el proceso de auditoría, y quedamos a su disposición para cualquier consulta o aclaración adicional que puedan requerir.

Atentamente,

Edinson Fabián Guzmán Ladino

Corporación Universitaria del Meta

27/04/2024

Descripción

Auditoria informática realizada a empresa dedicada a la venta de repuestos, reparación y mantenimiento de Motos ubicado en el Municipio de Cumaral-Meta, lleva aproximadamente 3 años en funcionamiento, no cuenta con registro ante Cámara y Comercio, cuentan con un software en el que llevan el registro de todos los clientes, ventas o servicios realizados y productos que tienen en stock.

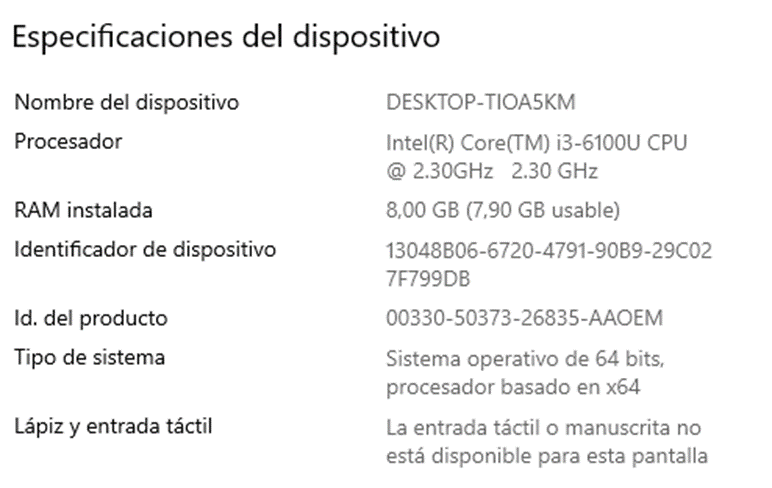
Configuración del computador base

El computador en el cual se usa el software anteriormente mencionado cuenta con las siguientes especificaciones.

Ilustración Especificaciones de Windows



Ilustración Especificaciones del dispositivo



El disco de estado sólido de 222GB no presenta particiones, ni dual boot. El computador no tiene antivirus instalado además del sistema de protección integrado en el SO Windows. El Firewall usado igualmente es el que viene con el SO (Firewall Windows Defender). El Windows está activado con una licencia digital. Tiene un total de 72 aplicaciones instaladas, incluyendo las que vienen por defecto con el SO.

Objetivos de los controles informáticos

Los controles internos informáticos tienen como objetivo principal salvaguardar los activos de información de una organización, garantizar la integridad, confidencialidad y disponibilidad de los datos, así como asegurar el cumplimiento de las políticas y normativas establecidas. Algunos de los objetivos específicos de los controles internos informáticos incluyen:

1. Seguridad de la información: Proteger la información contra accesos no autorizados, pérdida, robo o daño.
2. Integridad de los datos: Asegurar la exactitud y confiabilidad de la información, evitando su manipulación no autorizada o accidental.
3. Disponibilidad de sistemas y datos: Garantizar que los sistemas y la información estén disponibles cuando sea necesario y que se puedan recuperar en caso de fallos o desastres.
4. Cumplimiento normativo: Asegurar que la organización cumple con las leyes, regulaciones y políticas internas relacionadas con la gestión de la información y la seguridad informática.
5. Auditoría y monitoreo: Facilitar la supervisión continua de las actividades informáticas, detectando y respondiendo a eventos inusuales o no autorizados.
6. Gestión de accesos: Controlar y gestionar el acceso a sistemas y datos, asegurando que solo las personas autorizadas tengan permisos adecuados.
7. Protección contra malware y amenazas cibernéticas: Implementar medidas para prevenir, detectar y mitigar los riesgos asociados con virus, malware, ataques cibernéticos y otras amenazas.
8. Respuesta a incidentes: Establecer procedimientos para responder de manera efectiva a incidentes de seguridad informática, minimizando el impacto y restaurando la normalidad lo más rápido posible.
9. Segregación de funciones: Distribuir las responsabilidades y autoridades de manera que una sola persona no tenga un control completo sobre un proceso, reduciendo así el riesgo de fraudes o malas prácticas.
10. Respaldo y recuperación de datos: Implementar políticas y procedimientos para respaldar regularmente los datos críticos y asegurar su recuperación en caso de pérdida o daño.

Cuestionario de control interno para la seguridad en aspectos físicos de la aplicación.

1. ¿Existe control sobre el ingreso de funcionarios a la dependencia?

No existe un registro de ingresos y egresos físicamente, pero existe un control de quién es el vendedor qué está usando el software para las ventas.

1. ¿Existen programas de prevención contra desastres?

No existen programas de prevención contra desastres, porque es un negocio pequeño de un solo piso y no lo consideran necesario.

1. ¿Existe señalización de rutas de evacuación?

No, no existe ningún tipo de señalización

1. ¿Existen extinguidores dentro de la instalación?

Si, cuentan con un extinguidor pequeño.

1. ¿Existe un plan de contingencias?

No existen planes de contingencias con otras empresas privadas, solamente con la central de bomberos del municipio.

Cuestionario programas de la aplicación

1. ¿Son autorizadas y probadas las correcciones a programas antes de su puesta en marcha?

Si, cada corrección o nueva función es debidamente revisada y aprobada por los administradores.

1. ¿Se lleva un registro de los cambios efectuados a los programas?

Si se lleva un registro de los cambios efectuados a los programas pero no tan formalmente como se establece en el documento.

1. ¿Están adecuadamente documentados y probados los nuevos programas?

Si, tienen la respectiva documentación de su creación y modificaciones y es exhaustivamente probado antes de iniciar su uso.

1. ¿Existe planeación de las pruebas que deben ser realizadas a los programas?

Las pruebas al programa se realizan a criterio de los administradores y el programador cubriendo todas las necesidades para asegurar el completo funcionamiento.

1. ¿Existen librerías específicas para realizar las pruebas a los programas?

No, todas las pruebas se realizan manualmente.

1. ¿Existe amplia difusión acerca de las pruebas a realizarse?

Si, cuando se realizarán las pruebas o modificaciones se pone a conocimiento de todos aquellos que usan el software de la empresa para que puedan brindar sus sugerencias en cuanto a posibles errores que hayan encontrado en su uso.

1. ¿Existe un mecanismo especial para reportar dificultades o inconsistencias?

Todos los errores encontrados en el uso del programa son anotados para luego ser presentados en los momentos de revisión.

1. ¿Existen circunstancias específicas que limitan la ejecución de la aplicación?

La aplicación puede ser usada solo por administradores o trabajadores de la empresa en horario laboral, de otro modo está restringido su uso por trabajadores y solo puede ser usada por administrador, para revisar o modificar inventario, etc.

1. ¿Existen controles permanentes que permitan detectar inconsistencias ocurridas durante el procesamiento de datos?

Si existen controles permanentes para detectar inconsistencias, cada usuario del programa tiene como una de sus funciones monitorear el correcto funcionamiento del software que están usando y reportar posibles fallos ocurridos.

1. ¿Realizan los programadores actividades relacionadas con la captura de datos?

Sí se han establecido parámetros que delimitan las funciones de cada integrante de la empresa y cuál es su rol específico.

1. ¿Qué posibilidad de reproceso tiene la aplicación?

Se lleva registro de los procesos más importantes realizados en caso de emergencia o fallo grave de parte de la aplicación.

Cuestionario de control interno para el software del sistema

1. ¿Es tenido en cuenta el criterio de los usuarios de la aplicación durante las diferentes etapas del ciclo de vida del sistema?

Sí existe una buena comunicación entre los usuarios del programa y el desarrollador y tomadas en cuenta todas las recomendaciones, igualmente de parte de los clientes.

1. ¿Los cambios y mejoras al software del sistema están debidamente justificadas?

Si, cada cambio que se realiza al programa se lleva a cabo porque es necesario hacerlo y documentado con su justificación.

1. ¿Son de total confianza las personas que hacen mantenimiento al sistema de información?

Si, el encargado de mantenimiento al programa es de total confianza, pues es alguien muy cercano a los administradores de la empresa.

1. ¿Está totalmente legalizado el software utilizado por la empresa?

No está totalmente legalizado el software.

1. ¿Existe un registro de aquellos problemas que se presentan con el software?

Sí, es una de las responsabilidades de todos los usuarios de la aplicación llevar registro de cualquier fallo encontrado.

1. ¿Existen controles adecuados cuando se están probando nuevas versiones del software o cuando se están aplicando programas de diagnóstico?

Si, todos los cambios y pruebas se realizan en horario no laboral para no intervenir en ninguno de los demás procesos de la empresa.

1. ¿Tiene el software adquirido contrato de mantenimiento?

Sí tiene contrato de mantenimiento el software, en cuanto a la auditoría esta es la primera que se realiza.

1. ¿Existe documentación del software del sistema?

Sí existe documentación del sistema desde su creación.

1. ¿Se llevan estadísticas o reseña de fraudes cometidos con respecto al software del sistema?

Hasta el momento no ha ocurrido ningún fraude respecto al uso del software.

Ciclo Deming (PDCA)

Aplicación de Ciclo Deming para realización de uno de los procesos a corregir encontrados en la empresa.

**Planificar:**

Identificar el área de mejora: Se detecta la falta de documentación formal de las políticas de seguridad y las vulnerabilidades en el software utilizado por la empresa.

Establecer objetivos específicos: El objetivo es mejorar la seguridad informática y la funcionalidad del software, asegurando el cumplimiento de la Norma ISO 27001.

Desarrollar un plan de acción: Se crea un plan que incluye la creación de documentación formal de políticas de seguridad y demás procesos internos, la corrección de vulnerabilidades en el software y la implementación de medidas preventivas.

Cronograma propuesto para realización del proceso encontrado.

Tabla Cronograma Ciclo Deming

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Actividades** | **Semanas** | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Establecimiento del proceso a corregir. |  |  |  |  |  |  |  |  |  |
| Implementación de las políticas de seguridad. |  |  |  |  |  |  |  |  |  |
| Corrección de vulnerabilidades en el software. |  |  |  |  |  |  |  |  |  |
| Implementación de medidas preventivas. |  |  |  |  |  |  |  |  |  |
| Evaluación y revisión. |  |  |  |  |  |  |  |  |  |

Descripción:

1. El proceso de establecimiento del proceso a corregir conlleva: Identificar el área de mejora, Establecer objetivos específicos, Desarrollar un plan de acción, Revisión y aprobación del plan.
2. El proceso de implementación de las políticas de seguridad implica: Crear documentos de políticas de seguridad, Revisión y aprobación de documentos, capacitación del personal sobre nuevas políticas.
3. El proceso de corrección de vulnerabilidades en el software comprende: Evaluación de vulnerabilidades existentes, Desarrollo y prueba de soluciones, Implementación de soluciones.
4. El proceso de implementación de medidas preventivas involucra: Identificar y priorizar medidas preventivas, Implementación de medidas, Capacitación del personal sobre nuevas medidas.
5. El proceso de Evaluación y revisión contiene: Evaluación del impacto de las mejoras, Revisión del cumplimiento de las Normas ISO 27001, Identificación de áreas adicionales de mejora.

**Hacer:**

Ejecutar el plan de acción: Se llevan a cabo las acciones planificadas, como la creación de documentación formal en cada proceso realizado en la empresa para tener registro legal y formal de todos los procedimientos internos, la corrección de vulnerabilidades encontradas en el software y la implementación de medidas preventivas.

La manera en la que se ejecutará el plan de acción es la siguiente:

Proceso de Establecimiento del proceso:

Para llevar a cabo esta actividad, se realizará un análisis exhaustivo de la situación actual de la empresa con el fin de identificar las áreas de mejora tanto en seguridad informática como en la funcionalidad del software. Una vez identificadas estas áreas, se procederá a establecer objetivos específicos en colaboración con los equipos relevantes.

Con base en los objetivos establecidos, se desarrollará un plan de acción detallado que incluirá las acciones específicas que se llevarán a cabo, asignando responsables y estableciendo fechas límite para cada tarea. Este plan será presentado a los responsables y partes interesadas relevantes para su revisión y aprobación, asegurándose de que esté alineado con los objetivos y recursos disponibles antes de proceder con su implementación.

Proceso de Implementación de Políticas de Seguridad:

Una vez que el plan de acción ha sido aprobado, se procederá con la implementación de las políticas de seguridad. Esto incluirá la creación de documentos que describan las políticas de seguridad de la empresa en colaboración con expertos en seguridad informática. Estos documentos serán sometidos a una revisión por parte de expertos y partes interesadas relevantes para garantizar su integridad y eficacia antes de su implementación.

Además, se organizarán sesiones de capacitación para todo el personal de la empresa sobre las nuevas políticas de seguridad, asegurándose de que comprendan sus responsabilidades y cómo cumplir con las políticas establecidas en sus roles y responsabilidades (Acá participarán tanto gerentes como empleados, las capacitaciones pueden realizarse en horario extralaboral para no afectar las operaciones), estas capacitaciones serán realizadas por parte de los creadores de las políticas de seguridad porque son quienes mejor las conocen, igualmente pueden participar los gerentes y demás involucrados en su creación.

Proceso de Corrección de Vulnerabilidades en el Software:

Una vez implementadas las políticas de seguridad, se procederá con el proceso de corrección de vulnerabilidades en el software. Esto implicará realizar un análisis del software utilizado por la empresa para identificar posibles vulnerabilidades de seguridad. Posteriormente, se trabajará en colaboración con desarrolladores y expertos en seguridad para diseñar y probar soluciones que aborden las vulnerabilidades identificadas, garantizando su eficacia antes de su implementación.

Finalmente, se coordinará con el equipo de TI para implementar las soluciones desarrolladas, siguiendo un proceso controlado y documentado para garantizar en todo momento el cumplimiento del proceso.

Proceso de Implementación de Medidas Preventivas:

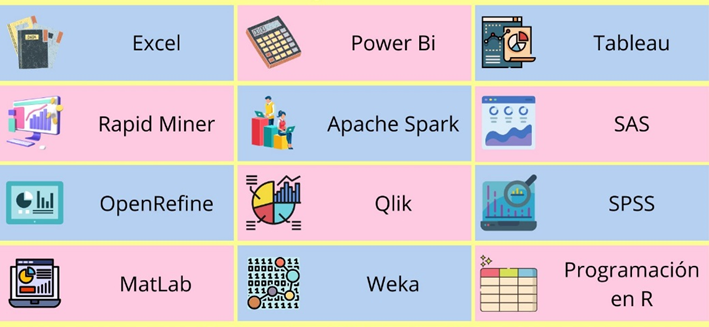
En paralelo con la corrección de vulnerabilidades, se llevará a cabo el proceso de implementación de medidas preventivas. Esto será realizado por el mismo equipo encargado de la corrección de vulnerabilidades. Una vez identificadas, se coordinará con los equipos pertinentes para implementar estas medidas, asegurándose de su correcta configuración y funcionamiento. Además, se agregarán a las sesiones de capacitación para garantizar que el personal esté adecuadamente informado sobre las nuevas medidas y su importancia para la seguridad de la empresa.

Proceso de Evaluación y Revisión:

Una vez implementadas todas las medidas, se procederá con el proceso de evaluación y revisión para asegurar su efectividad continua. Esto implicará realizar análisis de datos y evaluaciones para medir el impacto de las mejoras implementadas en términos de seguridad informática y funcionalidad del software. También se realizarán auditorías internas y revisiones periódicas para garantizar el cumplimiento continuo de las normas ISO 27001. Además, se facilitarán sesiones de retroalimentación y revisión con los equipos pertinentes para identificar y abordar áreas adicionales de mejora conforme surjan.

Recopilar datos: Se recopilan datos sobre las acciones realizadas y los cambios implementados en el sistema de seguridad informática. Se hace uso de herramientas como Microsoft Power Bi y Google Data Studio para visualizar y analizar los distintos datos encontrados en los procesos mencionados anteriormente; En el proceso de creación de documentación se deben conocer completamente todos los procesos realizados, estos procesos conllevan grandes cantidades de datos útiles para la empresa, pero el desconocimiento de esto hace que el personal encargado no cree la documentación respectiva y deje perder parte de esta valiosa información. Igualmente en el proceso de corrección de vulnerabilidades se debe tener registro de todos los errores encontrados e igualmente de las soluciones propuestas y/o implementadas, esto posteriormente se debe almacenar en una base de datos (cualquiera de preferencia de los encargados) y ser visualizado para la toma de decisiones. Además de las herramientas de visualización de datos también se deben usar las herramientas para su procesamiento como pueden ser: Microsoft Excel, R, Python, Qlik Sense, SAS, entre otras.

Ilustración Herramientas de visualización de datos



**Verificar:**

Comparar resultados: Se comparan los datos recopilados antes y después de la implementación del plan para determinar si se ha mejorado la seguridad informática y la funcionalidad del software. Para esto se pueden usar las herramientas mencionadas anteriormente para visualización de datos, pues en estas se pueden crear gráficas, estadísticas, tablas y otros elementos bastante útiles. Los gerentes tendrán una buena visualización de los diferentes procesos que se llevan a cabo en la empresa ya que es más fácil entender la información por medio de gráficos y estadísticas, esto se logra mediante el análisis de datos, este proceso permite tomar toda la información y simplificarla de manera que sea más entendible por el usuario final. De esta manera, al tener el registro del estado anterior y el estado actual de la empresa luego de haber realizado el proceso seleccionado se podrá evidenciar claramente las diferencias, esto facilitará enormemente a los gerentes poder tomar decisiones sobre qué mejorando a corto o largo plazo de acuerdo a su grado de importancia y qué deben seguir haciendo de determinada manera en caso de que esté saliendo muy bien y brindando beneficios.

Evaluar el cumplimiento de los objetivos: Se evalúa si se ha logrado el objetivo de mejorar la seguridad informática y la funcionalidad del software, asegurando el cumplimiento de la Norma ISO 27001. Esto proporcionará una medida clara del éxito del proyecto y ayudará a identificar áreas adicionales de mejora si es necesario.

Además, se puede implementar un feedback por parte de los usuarios del sistema, tanto antes como después de la implementación del plan. Esto proporcionará información valiosa sobre la percepción del usuario sobre la seguridad y funcionalidad del software, así como posibles áreas de mejora desde su perspectiva.

**Actuar:**

Tomar medidas correctivas: Si los resultados obtenidos durante la fase de Verificar no cumplen con los objetivos establecidos, se realizará un análisis detallado para identificar las causas de las deficiencias. Esto implicará examinar los datos recopilados, revisar los procesos implementados y recabar feedback de los usuarios y partes interesadas. Una vez identificadas las causas raíz de los problemas, se tomarán medidas correctivas adecuadas. Estas medidas pueden incluir ajustes en el plan de acción, realineamiento de recursos, revisión de políticas y procedimientos, o proporcionar más formación y capacitación al personal para mejorar su comprensión y cumplimiento de las políticas de seguridad. Es importante asegurarse de abordar no solo lo superficial, sino también las causas implícitas para garantizar una mejora efectiva y sostenible en la seguridad informática y la funcionalidad del software.

Implementar mejoras: Se dará prioridad a aquellas mejoras que se consideren más críticas o que tengan el potencial de generar el mayor impacto positivo en la seguridad informática y la funcionalidad del software. Es importante documentar y comunicar claramente todas las mejoras implementadas a todo el personal relevante, asegurando su comprensión y compromiso con el proceso de mejora continua. Una vez implementadas las mejoras, se reiniciará el ciclo PDCA para continuar el proceso de mejora continua, asegurando así que la empresa se mantenga alineada con las mejores prácticas y estándares de seguridad informática.

Análisis PESTEL

## **Políticos**

- Registro y cumplimiento legal: La empresa debe asegurarse de cumplir con todas las regulaciones y normativas gubernamentales relacionadas con la venta de repuestos de moto y servicios de reparación y mantenimiento. Esto incluye aspectos como los impuestos, licencias comerciales, y cualquier otra normativa relacionada con la operación del negocio.

Las empresas que se dedican a la venta de repuestos para motos en Colombia deben cumplir con una serie de regulaciones legales y fiscales, establecidas a nivel nacional, departamental y municipal.

Impuesto sobre la Renta (IR): Las empresas deben declarar y pagar el IR sobre sus utilidades gravables. La tasa general del IR es del 35%, pero existen algunas tarifas reducidas para pequeñas y medianas empresas.

Impuesto al Valor Agregado (IVA): La venta de repuestos para motos está gravada con el IVA a la tasa general del 19%. Sin embargo, algunos repuestos, como los cascos y las llantas, están exentos del IVA.

Impuesto de Industria y Comercio (ICA): Este impuesto es de carácter municipal y su tasa varía de un municipio a otro. Las empresas deben declarar y pagar el ICA sobre sus ingresos brutos.

Regulaciones de calidad:

Normas Técnicas Colombianas (NTC): Los repuestos para motos deben cumplir con las NTC establecidas para cada tipo de repuesto. Estas normas establecen las especificaciones técnicas que deben cumplir los productos para garantizar su seguridad y calidad.

INM: El Instituto Nacional de Metrología es el organismo encargado de la verificación y control de la calidad de los productos en Colombia. Las empresas pueden solicitar al INM la certificación de sus productos para demostrar que cumplen con las NTC.

## **Económicos**

- Impacto económico de las medidas de seguridad: La implementación de medidas de seguridad adicionales podría representar un costo adicional para la empresa. Deberán evaluar el impacto económico de estas medidas y asegurarse de que son financieramente viables a largo plazo.

- Registro financiero: Mejorar la regulación financiera de la empresa podría tener un impacto positivo en su gestión financiera y en la toma de decisiones estratégicas.

Factores macroeconómicos:

Crecimiento del PIB: El crecimiento del Producto Interno Bruto (PIB) del país tiene un impacto directo en la demanda de repuestos para motos. Un mayor crecimiento del PIB generalmente conduce a un aumento en el ingreso disponible de los hogares, lo que puede llevar a un mayor gasto en bienes y servicios, incluyendo la compra de motocicletas y repuestos.

Inflación: La inflación, medida como el aumento generalizado de los precios en la economía, afecta negativamente a las empresas de venta de repuestos para motos al aumentar sus costos de producción y operación. Esto puede conducir a una disminución de los márgenes de ganancia y a una menor rentabilidad.

Tipo de cambio: El tipo de cambio entre el peso colombiano y las monedas extranjeras afecta el costo de las importaciones de repuestos, especialmente para aquellos que se importan desde otros países. Una depreciación del peso colombiano puede hacer que las importaciones sean más costosas, lo que puede afectar negativamente la rentabilidad de las empresas.

Tasas de interés: Las tasas de interés establecidas por el Banco de la República afectan el costo del financiamiento para las empresas. Un aumento en las tasas de interés puede hacer que sea más costoso para las empresas obtener préstamos, lo que puede afectar negativamente su flujo de caja y su capacidad de inversión.

Factores microeconómicos:

Competencia: El nivel de competencia en el mercado de venta de repuestos para motos es un factor importante que afecta la rentabilidad de las empresas. Un mercado altamente competitivo puede presionar a la baja los precios y los márgenes de ganancia, lo que obliga a las empresas a buscar estrategias para diferenciarse y fidelizar a sus clientes.

Precios de los insumos: Los precios de los insumos utilizados en la producción o comercialización de repuestos para motos, como el metal, el plástico y los componentes electrónicos, pueden afectar significativamente la rentabilidad de las empresas. Un aumento en los precios de los insumos puede conducir a un aumento en los costos de producción y a una menor rentabilidad.

## **Sociales**

- Confianza del cliente: La seguridad de la información es un aspecto importante para los clientes, especialmente cuando se trata de datos personales. Mejorar la seguridad informática podría aumentar la confianza del cliente en los servicios de la empresa.

- Capacitación del personal: Es importante capacitar al personal en aspectos básicos de seguridad informática para garantizar que estén conscientes de los riesgos y puedan contribuir a mantener un entorno seguro.

Cultura del motociclismo:

Popularidad de las motocicletas: En Colombia, las motocicletas son un medio de transporte muy popular, especialmente en las zonas urbanas y rurales. Esto representa una gran oportunidad para las empresas de venta de repuestos, ya que existe una amplia demanda de estos productos.

Percepción social de las motocicletas: La percepción social de las motocicletas puede afectar la demanda de repuestos. En algunos casos, las motocicletas pueden ser vistas como un medio de transporte inseguro o de bajo estatus, lo que puede limitar la demanda de repuestos. Sin embargo, en los últimos años ha habido un cambio en la percepción social de las motocicletas, y estas son cada vez más vistas como un medio de transporte práctico, económico y divertido.

Cultura del motociclismo: En Colombia existe una fuerte cultura del motociclismo, con numerosos clubes, eventos y competiciones. Las empresas de venta de repuestos pueden aprovechar esta cultura para promocionar sus productos y fidelizar a los clientes.

Hábitos de consumo:

Disposición a pagar por repuestos de calidad: Los consumidores colombianos están cada vez más dispuestos a pagar por repuestos de calidad para sus motocicletas. Esto representa una oportunidad para las empresas que ofrecen productos de alta calidad y valor agregado.

Preocupación por la seguridad: Los consumidores colombianos están cada vez más preocupados por la seguridad vial. Esto puede generar una demanda de repuestos de seguridad, como cascos, frenos y llantas de alta calidad.

## **Tecnológicos**

- Vulnerabilidades del software: La empresa debe abordar las vulnerabilidades de su software para protegerse contra posibles ataques informáticos. Esto puede requerir inversiones en actualizaciones de software o en la adquisición de soluciones de seguridad adicionales.

- Control de acceso y autenticación: Implementar un sistema robusto de autenticación y control de acceso podría mejorar significativamente la seguridad de la información de la empresa.

Comercio electrónico:

Tiendas online: El auge del comercio electrónico ha abierto nuevas oportunidades para las empresas de venta de repuestos para motos. Las tiendas online permiten a las empresas llegar a una audiencia más amplia, ofrecer una mayor variedad de productos y brindar una experiencia de compra más cómoda para los clientes.

Marketplaces: Los marketplaces como Mercado Libre y Linio ofrecen a las empresas de venta de repuestos para motos una plataforma para vender sus productos a miles de potenciales clientes.

Redes sociales: Las redes sociales como Facebook, Instagram y YouTube son herramientas valiosas para las empresas de venta de repuestos para motos para promocionar sus productos, interactuar con sus clientes y construir una comunidad en torno a la marca.

Logística y cadena de suministro:

Sistemas de gestión de inventario: Los sistemas de gestión de inventario (SGI) ayudan a las empresas a optimizar sus niveles de stock, reducir costos y mejorar la eficiencia de la cadena de suministro.

Rastreo de envíos: Las tecnologías de rastreo de envíos permiten a las empresas y a sus clientes seguir el estado de sus pedidos en tiempo real.

Big data y análisis de datos:

Análisis de ventas: El análisis de datos de ventas puede ayudar a las empresas a identificar tendencias, comprender mejor el comportamiento de sus clientes y tomar decisiones más informadas sobre sus estrategias de marketing y ventas.

Personalización: El análisis de datos también permite a las empresas personalizar sus ofertas y comunicaciones a los clientes individuales, lo que puede mejorar la experiencia del cliente y aumentar las ventas.

## **Ecológicos**

- Este factor puede tener un impacto limitado en este tipo de negocio, sin embargo, la empresa debe considerar cualquier regulación ambiental aplicable a sus operaciones, especialmente si está involucrada en el manejo de residuos o productos químicos.

Certificaciones ambientales: Las empresas de venta de repuestos para motos pueden obtener certificaciones ambientales, como la ISO 14001, para demostrar su compromiso con la protección del medio ambiente.

A nivel nacional, las principales normas ambientales que aplican a las empresas de venta de repuestos para motos son:

Ley 99 de 1993: Esta ley establece el marco general para la gestión ambiental en Colombia, incluyendo principios, instrumentos y procedimientos para la protección del medio ambiente.

Decreto 1076 de 1997: Este decreto reglamenta la gestión de residuos sólidos en Colombia, estableciendo obligaciones para la generación, almacenamiento, transporte y disposición final de los residuos.

## **Legales**

- Cumplimiento normativo: La empresa debe asegurarse de cumplir con todas las leyes y regulaciones relacionadas con la protección de datos, la privacidad del cliente y cualquier otra normativa aplicable a su sector.

- Documentación y registros: Es importante que la empresa mantenga documentación adecuada y registros de sus políticas de seguridad, así como de cualquier auditoría o evaluación realizada en el pasado, para demostrar su cumplimiento con las normativas legales y estándares de seguridad.

Código de Comercio: Este código establece las normas generales que rigen la actividad comercial en Colombia, incluyendo la constitución de sociedades, la contratación mercantil, la competencia y la propiedad intelectual.

Las principales autoridades legales que regulan a las empresas de venta de repuestos para motos en Colombia son:

Superintendencia de Industria y Comercio (SIC): Es la autoridad encargada de vigilar y controlar el cumplimiento de las normas de competencia en Colombia.

Superintendencia de Sociedades: Es la autoridad encargada de vigilar y controlar el cumplimiento de las normas societarias en Colombia.

Dirección de Impuestos y Aduanas Nacionales (DIAN): Es la autoridad encargada de administrar los impuestos nacionales en Colombia.

Ministerio del Trabajo: Es la autoridad encargada de vigilar y controlar el cumplimiento de las normas laborales en Colombia.

Matriz DOFA

## **Debilidades:**

Competencia de grandes cadenas de tiendas que también venden repuestos para motos.

Dependencia de un único proveedor para ciertos repuestos.

Falta de presencia en redes sociales y estrategias de marketing digital.

Limitaciones de espacio en el local físico para exhibir todo el inventario.

Inventario desactualizado o exceso de stock de ciertos productos.

Falta de presencia en el mercado internacional.

## **Oportunidades:**

Aumento en la demanda de repuestos debido al crecimiento del mercado de motocicletas.

Expansión del negocio en línea para llegar a un mercado más amplio.

Colaboración con talleres de reparación de motos para ofrecer servicios complementarios.

Diversificación del inventario para incluir accesorios y equipos para motocicletas.

Participación en eventos locales de motociclismo para promover la marca y aumentar la visibilidad.

Avances tecnológicos que pueden mejorar la eficiencia en los procesos de la empresa.

## **Fortalezas:**

Amplia variedad de repuestos disponibles para las distintas marcas de motos.

Excelente servicio al cliente por parte de todo el personal y atención de PQR’s.

Ubicación estratégica del local en el municipio.

Relaciones sólidas con proveedores de distintas empresas.

Oferta de productos de alta calidad.

Personal capacitado y con experiencia en el sector de repuestos para motos y la mecánica.

## **Amenazas:**

Cambios en las regulaciones gubernamentales sobre emisiones o seguridad de las motocicletas que podrían afectar la demanda de ciertos repuestos.

Crisis económicas que reduzcan las ventas, debido a la baja economía de los clientes.

Incremento en los costos de importación debido a cambios en políticas comerciales.

Aparición de nuevas tecnologías que puedan hacer obsoletos ciertos repuestos.

Posibles eventos de vandalismo o robos que afecten la seguridad del local y el inventario.

Auditoria Física

## **Plan de Auditoría**

**Alcance de la auditoría**

La auditoría física abarcará los siguientes aspectos:

Inventario físico de los repuestos en stock: Se contará y registrará la existencia física de todos los repuestos en stock.

Inspección de los repuestos: Se evaluará la condición física de los repuestos para identificar productos dañados, obsoletos o vencidos.

Verificación de las existencias en tránsito: Se verificará la existencia de repuestos en tránsito y se conciliará con los registros contables.

Verificación de los activos fijos: Se verificará la existencia y estado de los activos fijos relacionados con el inventario, como estanterías, vitrinas, herramientas, etc.

Verificación del efectivo y equivalentes de efectivo: Se verificará la existencia y conciliación del efectivo en caja y en bancos.

**Programación de la auditoría**

Tabla Programación de auditoría física

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Actividades** | **Semanas** | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Planificación |  |  |  |  |  |  |  |  |  |
| Ejecución |  |  |  |  |  |  |  |  |  |
| Evaluación de los resultados. |  |  |  |  |  |  |  |  |  |
| Elaboración del informe de auditoría. |  |  |  |  |  |  |  |  |  |
| Presentación y explicación del informe de auditoría. |  |  |  |  |  |  |  |  |  |

**Descripción de cronograma**

Planificación: Definición del alcance de la auditoría, Revisión de la documentación contable y de los procedimientos de control interno, Elaboración del programa de auditoría.

Ejecución: Inventario físico de los repuestos en stock, Inspección de los repuestos, Verificación de las existencias en tránsito, Verificación de los activos fijos, Verificación del efectivo y equivalentes de efectivo, Aplicación de pruebas de controles.

Evaluación de los resultados: Análisis de los resultados de las pruebas de auditoría, Identificación de diferencias o inconsistencias, Obtención de explicaciones de la gerencia, Evaluación del riesgo de control interno, Realización de pruebas sustantivas de transacciones.

Elaboración del informe de auditoría: Redacción del informe de auditoría, Revisión del informe de auditoría por parte del equipo de auditoría y el auditor líder.

Presentación del informe de auditoría: Presentación del informe de auditoría a la gerencia de la empresa.

## **Lista de verificación**

**Criterios del auditor**

Cumplimiento Normativo: Adherencia a leyes, regulaciones y normativas aplicables en la gestión de inventarios y ventas de repuestos para motos.

Políticas Internas: Aplicación de políticas y procedimientos de gestión de inventarios, control de calidad y revisión de repuestos.

Estándares de la Industria: Seguimiento de mejores prácticas y estándares de calidad y seguridad en la gestión de repuestos para motos.

Objetivos Organizacionales: Alcance de los objetivos de inventario, nivel de servicio al cliente y rentabilidad establecidos por la empresa.

Control Interno: Efectividad de los controles en la recepción, almacenamiento, despacho y registro de repuestos, incluyendo la segregación de funciones y la validación de transacciones.

Seguridad y Cumplimiento: Medidas de seguridad física y cumplimiento con políticas de salud y seguridad en el manejo y almacenamiento de repuestos.

Sostenibilidad y Responsabilidad Social: Prácticas sostenibles en la gestión de inventarios y compromiso con la ética y responsabilidad social corporativa.

**Objetivo del auditor**

Verificar la existencia, estado, propiedad y valor del inventario de repuestos para motos de la empresa MotoRepuestos, al 27 de abril de 2024 con el fin de emitir una opinión sobre la confiabilidad de los registros contables relacionados con el inventario.

## **Hallazgos**

**Descripción del hallazgo**

"Durante la auditoría física del inventario de repuestos para motos, se identificó una discrepancia entre los registros contables y la cantidad física contada para el repuesto (Bujia pulsar220/200 NS rg6ch original), en el almacén. Según los registros, debería haber 100 unidades, pero se encontraron solo 80 unidades durante el conteo físico."

**Severidad del Hallazgo**

"La discrepancia identificada en el inventario del repuesto (Bujia pulsar220/200 NS rg6ch original) representa un riesgo medio para la empresa, ya que podría afectar la precisión de los registros de inventario y la satisfacción del cliente. Se recomienda realizar un análisis detallado para determinar la causa raíz e implementar controles adicionales para prevenir futuras discrepancias."

**Causa Raíz Identificada**

Falta de procedimientos adecuados de control y monitoreo de inventarios, lo que ha llevado a errores en el registro y seguimiento de las unidades recibidas, almacenadas y despachadas.

**Acción Correctiva Propuesta**

Implementar un sistema de gestión de inventarios automatizado con controles y validaciones adicionales para mejorar la precisión y la integridad de los registros de inventario.

## **Plan de acción**

Tabla Cronograma de plan de acción para los hallazgos

|  |  |  |  |
| --- | --- | --- | --- |
| **Acciones a tomar** | **Responsable** | **Fecha límite** | **Status** |
| Implementación del Sistema Automatizado de Gestión de Inventario | Gerente de Logística | 30/06/2024 | Pendiente |
| Capacitación del personal | Coordinador de Capacitación | 15/07/2024 | Pendiente |
| Revisión y Actualización de Procedimientos | Gerente de Operaciones | 31/07/2024 | Pendiente |
| Monitoreo y Seguimiento Continuo | Supervisor de Inventario | 15/08/2024 | Pendiente |
| Revisión y Evaluación del Plan de Acción | Director de Operaciones | Trimestralmente | Pendiente |

**Descripción del plan de acción**

Implementación del sistema automatizado de gestión de inventario: Evaluación, selección e implementación de un sistema de gestión de inventarios automatizado que incluya controles y validaciones adicionales para mejorar la precisión y la integridad de los registros.

Capacitación del personal: Capacitación y formación del personal involucrado en la gestión de inventarios sobre los nuevos procedimientos y herramientas del sistema automatizado.

Revisión y Actualización de Procedimientos: Revisión y actualización de los procedimientos de control y monitoreo de inventarios para incorporar las mejores prácticas y controles adicionales identificados.

Monitoreo y seguimiento continuo: Implementación de un plan de monitoreo y seguimiento continuo del inventario para identificar y corregir proactivamente cualquier discrepancia o irregularidad.

Revisión y Evaluación del Plan de Acción: Revisión periódica del progreso y los resultados del plan de acción, evaluando la efectividad de las acciones implementadas y realizando ajustes según sea necesario.

Auditoria de Base de Datos

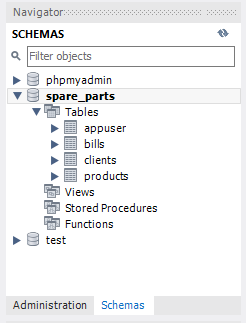
# Información General

## Fecha de la auditoría: 26 de abril de 2024

## Auditor: Edinson Fabián Guzmán Ladino

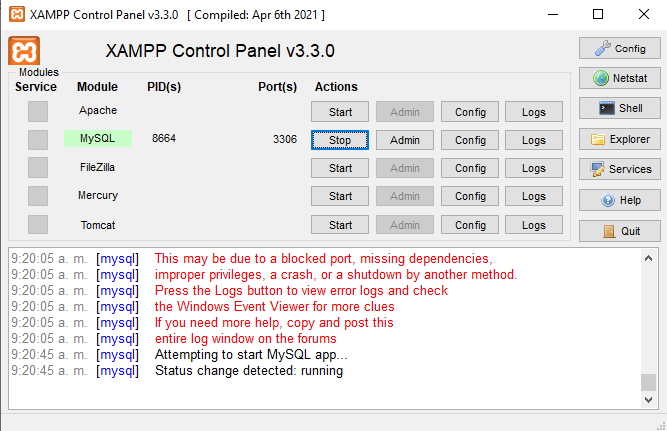
## Base de datos auditada: La empresa MotoRepuestos Cumaral cuenta con una base de datos llamada ‘spare\_parts’ en ella se encuentran 4 tablas llamadas: appuser, bills, clients y products.

Ilustración Base de datos y tablas usadas en la empresa



## Servidor: La empresa hace uso de la herramienta Open Source llamada ‘XAMPP’ para el uso de la plataforma de gestión de bases de datos MySQL Worbench. De esta manera se crea un servidor local en el computador base, pues no está conectado en red.

Ilustración Software usado para conexión a base de datos



Versión del SGDB: MySQL Workbench 8.0

# Objetivo de la auditoría

* Evaluar el cumplimiento de la normas y políticas de seguridad de la información.
* Identificar riesgos y vulnerabilidades en la base de datos.
* Verificar la eficiencia y el rendimiento de la base de datos.
* Validar la integridad de los datos.

# Alcance de la auditoría

Estructura de la base de datos: Revisión de la arquitectura y diseño de la base de datos, incluidas tablas, índices, procedimientos almacenados y funciones.

Seguridad de la base de datos: Análisis de los controles de acceso, roles de usuario, políticas de contraseñas y auditoría de accesos.

# Metodología de la auditoría

* Entrevistas al personal
* Revisión de la estructura de base de datos
* Evaluación del rendimiento
* Documentación de hallazgos

# Hallazgos de la auditoría

1. Riesgo de pérdida total de datos en la empresa.

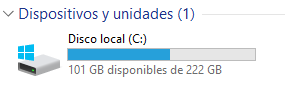
Descripción del hallazgo: La empresa no cuenta con un servidor externo para el almacenamiento de los datos, pues como se ha descrito anteriormente, se hace uso de un servidor local creado en el mismo computador base de la empresa.

## Severidad del hallazgo: Alta

## Impacto del hallazgo: El primer gran riesgo que se presenta en este hallazgo es la pérdida total de los datos almacenados debido a que estos se están almacenando en el disco duro del computador. Si por alguna razón el disco duro llega a sufrir un daño irreparable, toda esta información se perderá, pues además de que no se está realizando ningún tipo de almacenamiento en la nube, tampoco se realiza un backup de la información en otro lugar.

El otro riesgo que se presenta al almacenar toda la información en el mismo computador es que este tiene una limitación muy baja y cuando se llene tendrá que ser reemplazado y toda esa información igualmente corre el riesgo de perderse. La capacidad total de almacenamiento es de 200GB y hasta el momento se han usado la mitad.

Ilustración Capacidad de almacenamiento del computador base



## Recomendaciones: Se recomienda urgentemente tomar medidas correctivas en cuanto a la forma de almacenamiento de los datos en la empresa, lo idea en este caso sería empezar a usar un servicio de almacenamiento en la nube, teniendo en cuenta que la cantidad de datos será cada vez mayor y el sistema debe de ser escalable, de esta manera se podrá empezar a usar otro equipo en la empresa sin depender de que la información esté almacenada en un solo sitio y esto mejorará además, la eficiencia en la atención al usuario cuando se pueda congestionar por el aumento de clientes o cuando se quiera abrir una nueva sede en otro lugar.

1. Incorrecta distribución de acciones en los roles existentes en la base de datos.

## Descripción del hallazgo: En la base de datos existen dos roles de usuario: ‘Administrador’ y ‘Vendedor’. Cada rol puede realizar ciertas acciones en el sistema, pues al iniciar sesión en cada uno de estos, se puede ver un panel diferente como aparece en las siguientes imágenes.

Ilustración Panel de Administrador



Ilustración Panel de Vendedor



El error encontrado en la auditaría realizada se basa en la incorrecta distribución de algunas de estas acciones, por ejemplo, en el panel de Vendedor se tiene acceso a las opciones de añadir y modificar productos. Esta acción debería de ser exclusiva de los Administradores del sistema, pues un empleado con el rol de vendedor no debería de tener la función de modificar el inventario registrado en la base de datos, las funciones propias de este rol deberían ser consultar y vender los productos.

## Severidad del hallazgo: Media

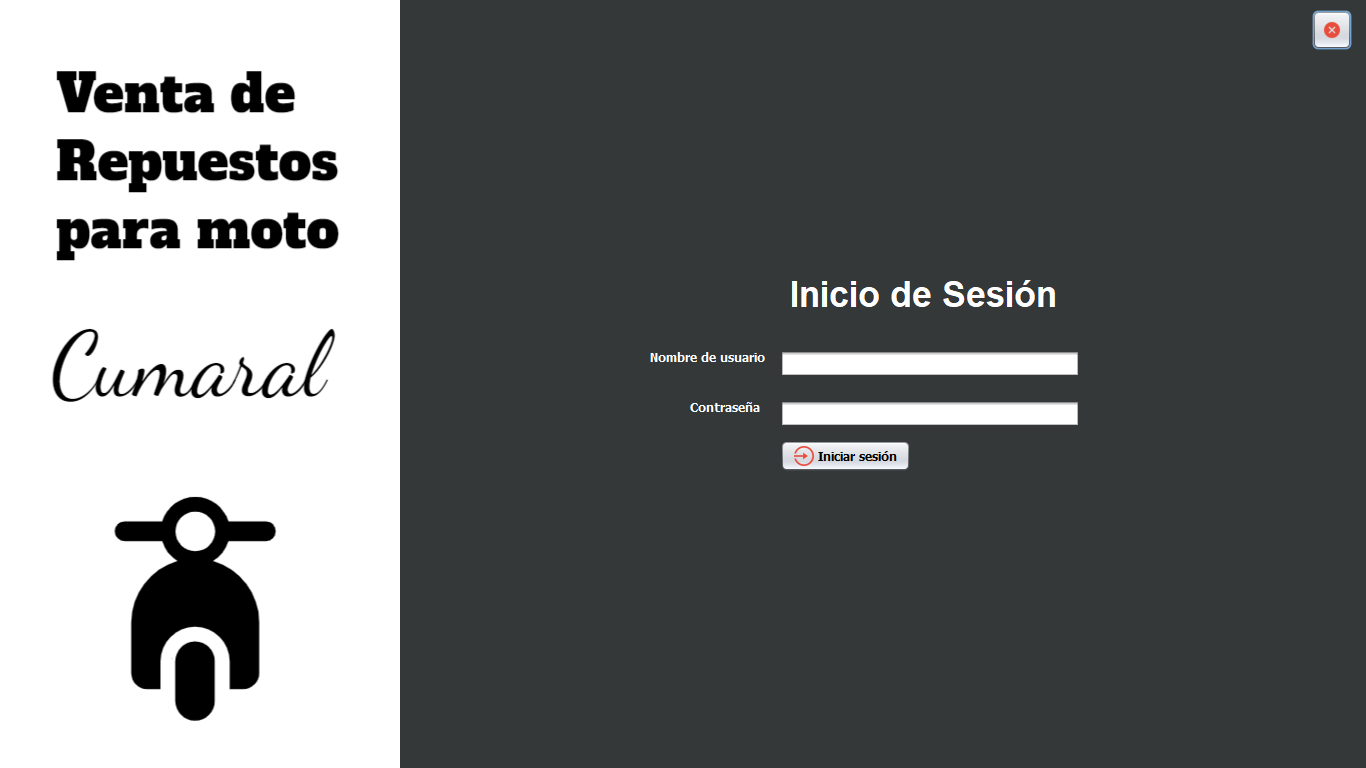
## Impacto del hallazgo: Si se concede al vendedor la opción de modificar inventario y los precios, se puede correr el riesgo de que éste lo altere erróneamente, ya sea intencional o no intencionalmente, esto afecta directamente en el correcto funcionamiento de la empresa, por ejemplo al momento de realizar una venta y consultar el inventario de la base de datos se puede hallar que estos datos son erróneos y no coinciden con el inventario real. Esto puede provocar que se brinde información falsa a los clientes y que el control de inventario sea total o parcialmente incorrecto.

## Recomendaciones: La solución se basa en corregir el acceso a determinadas funciones por parte de cada rol, teniendo en cuenta este y otros aspectos que no se tuvieron en cuenta al momento de crear el software. Así se garantiza la seguridad de los datos y la correcta asignación de funciones entre los trabajadores de la empresa.

1. Función de recuperación de contraseña no implementado.

## Descripción del hallazgo: el sistema no cuenta con una función de recuperación de contraseñas, estos es una mala práctica en el desarrollo de sistemas de software, pues en caso de perder u olvidar la contraseña o usuario de la cuenta, esta se perderá.

Ilustración Interfaz de inicio de sesión al sistema



## Severidad del hallazgo: Baja

## Impacto del hallazgo: En este caso, el impacto del hallazgo no es muy alto, porque si se pierde una cuenta con rol de vendedor, se puede crear otra desde el rol de administrador. Igualmente las cuentas con rol de administrador se crean desde el rol de administrador, el problema principal se presenta cuando solo hay una cuenta de administrador y esta persona olvida sus credenciales de acceso, pues tocará crear nuevamente la cuenta desde la base de datos, así como fue creada principalmente.

## Recomendaciones: Implementar la función de recuperación de cuenta y recuperación de contraseña en el sistema para todo los roles y tener como mínimo 2 cuentas de administrador creadas.

# Conclusiones

La auditoría realizada a la base de datos ha permitido conocer el estado general de seguridad de los datos almacenados. De esta manera se ha llegado a la conclusión de que el nivel de seguridad en el manejo de estos es muy bajo y se deben de tomar medidas urgentes para mitigar los riesgos presentados, estos van desde las distintas maneras en las que se puede acceder a la base de datos, hasta la misma forma en la que fue creada y se manipula actualmente.

Cuando se habla de las distintas maneras en las que se puede acceder a la base de datos se hace referencia tanto a la asignación de funciones en los roles como a la seguridad manejada para acceder directamente a esta. La cuestión de la asignación de funciones específicas de roles ya ha sido tratada en la sección de hallazgos. Por otra parte, al hablar de la seguridad manejada para acceder directamente a la base de datos, se hace referencia a la manera en la que se puede acceder al SGBD para manipular completamente la base de datos con sus tablas y registros y no solamente para realizar consultas y agregar inventario así como se puede hacer desde el software de ventas. Esto ocurre porque solamente se utiliza un computador para realizar todas las acciones de la empresa, la base de datos fue creada en este computador y es administrada desde el mismo, no existe un almacenamiento en la nube o un respaldo de información en otro disco, por este motivo, la única seguridad existente para ingresar a manipular la base de datos completa de la empresa es la contraseña de accesos al SGBD, si esta seguridad es vulnerada por alguien externo a la empresa sin autorización o alguien que no pertenezca a la sección administrativa, estará en grave riesgo la integridad de los datos de la empresa.

# Anexos

En esta sección se presentarán las evidencias de los hallazgos encontrados y un posible plan de acción para corregirlos.

Hallazgo: Riesgo en la integridad de los datos.

Ilustración Plataformas usadas para la Gestión de base de datos

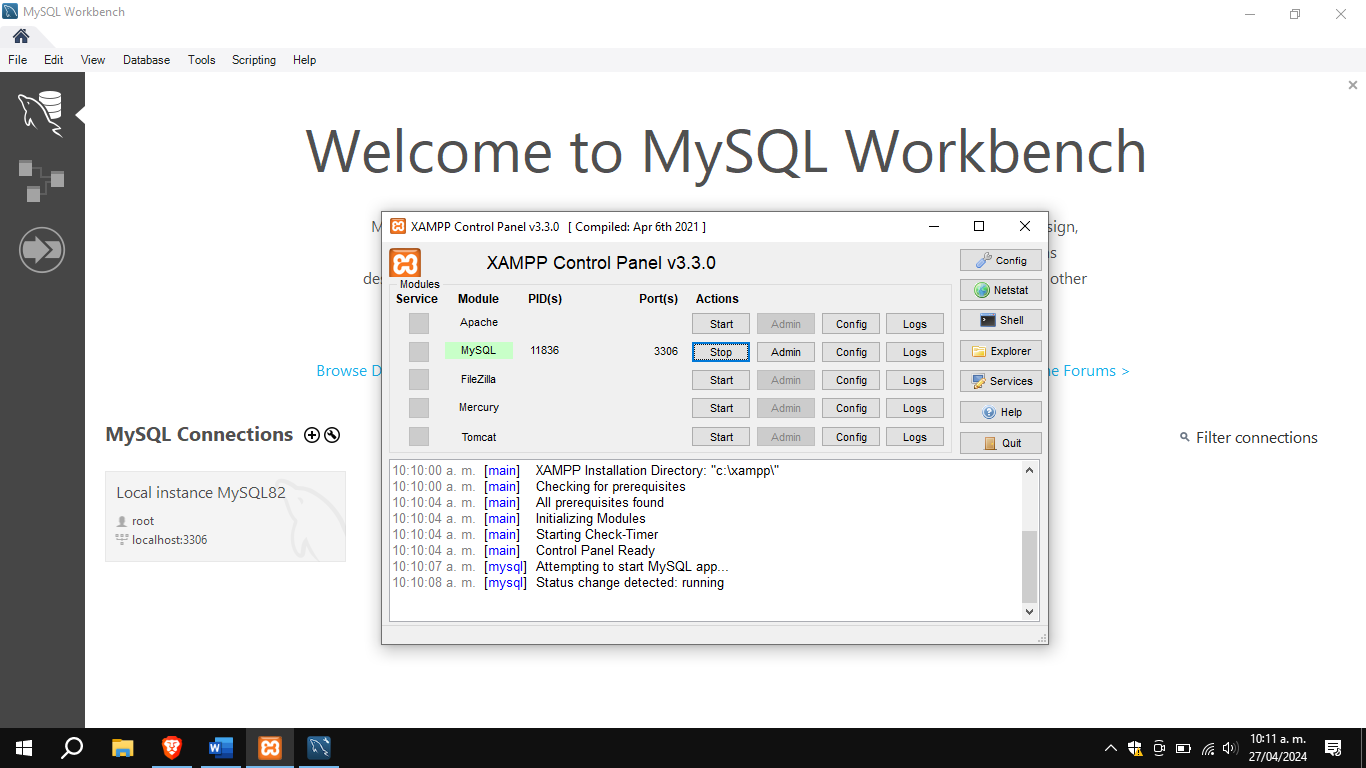
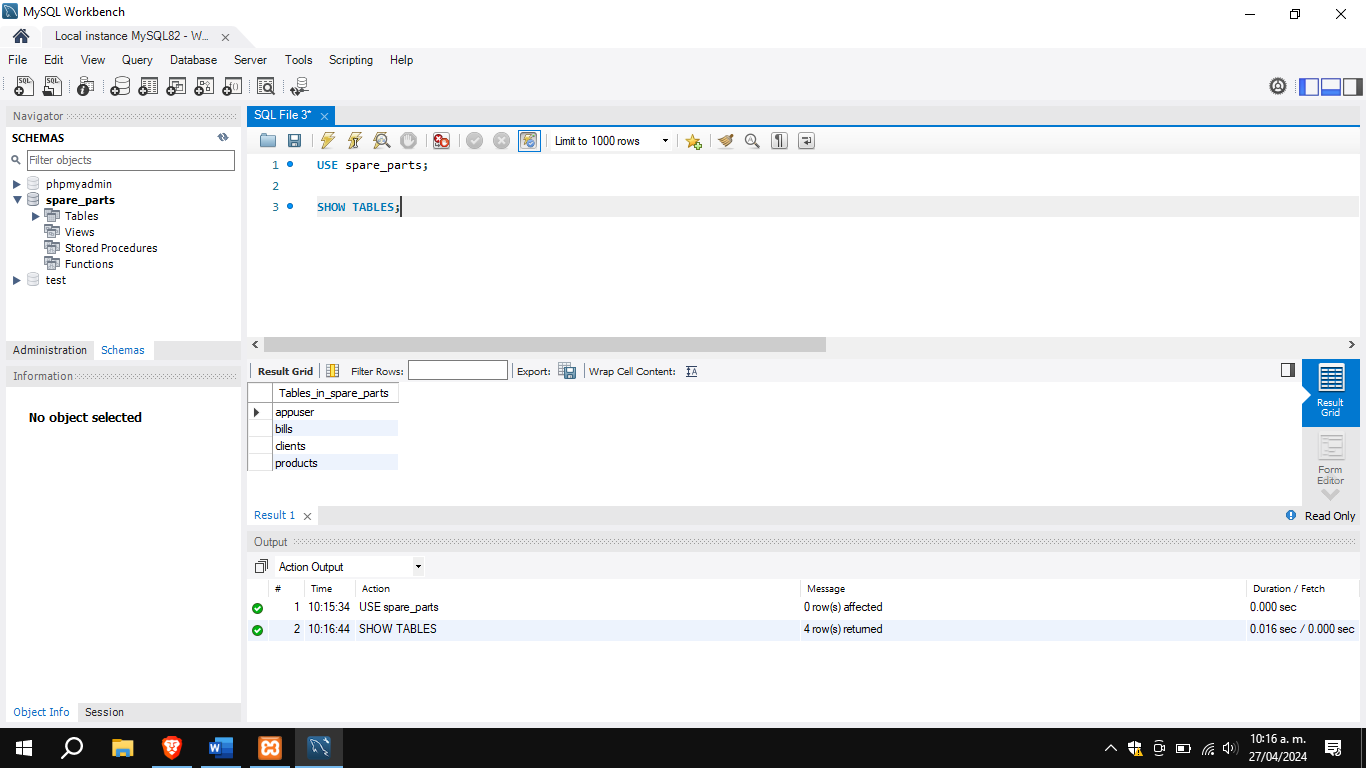


Ilustración Acceso al SGBD



### Plan de acción:

1. Realizar un backup de la base de datos en su totalidad.
2. Migrar los datos almacenados en el computador base a un sistema de almacenamiento en la nube como Microsoft SQL Server, PostgreSQL, AWS Aurora, Oracle Database Cloud Service, entre otros. Esto permitirá ahorrar espacio en el computador base, tener siempre un respaldo de los datos, implementar la escalabilidad en el sistema y además crear una flexibilidad para poder acceder a estos desde cualquier lugar.
3. Implementar medidas de seguridad adicionales en el acceso a la base de datos, cómo el uso de medios de autenticación más robustos o de otra manera, administrarla desde otro dispositivo.

Hallazgo: Incorrecta asignación de funciones en el sistema.

Ilustración Panel de vendedor



Ilustración Función de añadir producto - Panel de vendedor



Ilustración Función de modificar productos - Panel de vendedor



### Plan de acción:

1. Retirar las funciones de modificación de inventario del panel de vendedor (excepto la de venta) e implementarlas en el panel de administrador.
2. Realizar un análisis detallado de todas las funciones que se están usando en el sistema y si están implementadas correctamente o no de acuerdo al rol asignado.

Auditoria informática conforme a la Norma ISO 27001

## **• Planificación de la Auditoría:**

El objetivo de la auditoría realizada a la empresa de venta de repuestos es obtener una perspectiva general del estado de seguridad informática de la empresa, haciendo uso de la Norma ISO 27001, estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), esto para poder ofrecer una mejor calidad de servicio a los clientes y asegurar la seguridad de los datos personales de cada usuario.

La planificación implica identificar posibles vulnerabilidades, evaluar la eficacia de los

controles de acceso y verificar el cumplimiento de las regulaciones financieras.

## **• Evaluación de la Conformidad:**

La empresa cuenta con políticas internas de seguridad, cada integrante de la empresa es capacitado inicialmente en cuanto al correcto uso del sistema y en las respectivas medidas del tratamiento de datos, cuestiones como permitir el ingreso o uso del software solamente al personal autorizado y otras medidas de seguridad son consideradas en la empresa seriamente, sin embargo, no cuentan con una documentación formal de estas medidas. No existen registros de auditorias anteriores, pues no se han realizado previamente auditorías de ningún tipo, cada riesgo descubierto es tomado en cuenta como se ha descrito anteriormente en el cuestionario de control interno para el software del sistema.

## **• Ejecución de Pruebas:**

No se han realizado pruebas pentesting al software de la empresa, el sistema se encuentra vulnerable a ciberataques. Por otra parte, el control de acceso es un poco más supervisado, pues continuamente se está revisando que no ingrese personal no autorizado a la empresa e igualmente que nadie manipule el computador de la empresa sin previa autorización. En cuanto al análisis de configuraciones, este ya ha sido descrito anteriormente en el archivo de configuración del computador base. Mediante entrevistas con el personal autorizado para la manipulación del software se ha identificado que cada uno cuenta con un usuario y una contraseña para acceder, igualmente es registrada en una planilla la fecha y hora en que empieza a trabajar cada uno.

## **• Análisis de Resultados:**

En la revisión al sistema de seguridad de la información se han encontrado una gran cantidad de inconsistencias que se categorizan como potencialmente negativas para la seguridad de la información allí almacenada. En el siguiente informe se presentan detalladamente y se propone la respectiva medida de corrección a cada una de ellas.

## **• Elaboración de Informe:**

### Introducción

La presente auditoría informática se ha llevado a cabo con el propósito de evaluar y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de MotoRepuestos Cumaral, empresa dedicada a la venta de repuestos de moto y servicios de reparación y mantenimiento. Esta evaluación se ha realizado en estricta conformidad con los estándares establecidos por la Norma ISO 27001, un marco internacional reconocido que define requisitos para la implementación y mantenimiento de sistemas de gestión de seguridad de la información.

El objetivo fundamental de esta auditoría es proporcionar a MotoRepuestos Cumaral una visión detallada y objetiva de la eficacia de su SGSI, identificando posibles brechas de seguridad, evaluando el cumplimiento de las políticas y procedimientos establecidos, y proponiendo recomendaciones específicas para fortalecer la seguridad de la información en consonancia con las mejores prácticas internacionales.

### Resultados de la Auditoria

Falta de documentación formal de las políticas de seguridad: A pesar de que la empresa cuenta con políticas internas de seguridad, carece de documentación formal que respalde estas medidas. No existen dentro de la empresa documentos oficiales que justifiquen las medidas de seguridad tomadas para la protección de datos, ni documentos que registren la creación del software o su uso. En los casi 3 años de la empresa nunca se había llevado a cabo una auditoría de ningún tipo.

Recomendación: Se debe crear la respectiva documentación oficial que justifique la creación e implementación de las políticas de seguridad interna, pues tanto el personal como las personas ajenas a la empresa tendrán pautas establecidas sobre qué pueden y no pueden hacer en esta empresa.

Se debe llevar una documentación formal en cuanto al control de errores o vulnerabilidades encontradas, de preferencia utilizar un formato específicamente para este proceso, en este el personal podrá registrar todas las fallas relacionadas a la seguridad de la información de la empresa y utilizarlo en el respectivo tiempo de correcciones, estas correcciones igualmente deben ser documentadas e indicarse si se logró solucionar completamente el problema descubierto.

Dado que la empresa ya cuenta con casi 3 años de funcionamiento, así no haya tenido un software anteriormente, tendría que haber realizado procesos de auditoría que le permitan tener un mayor control del funcionamiento de la empresa, además de estar registrada ante cámara y comercio y cumplir con todas las obligaciones legales, esto facilitará el proceso de la auditoría informática y brindará por lo tanto mejores resultados.

Vulnerabilidad del software: El software usado en la empresa para el control de inventario, servicios, etc. No es un software muy robusto, por lo tanto presenta vulnerabilidades que pueden ser aprovechadas para realizar ataques informáticos. No se cuenta un sistema robusto de autenticación, cada persona autorizada para manipular el software tiene un usuario y contraseña asignado, con los cuales ingresa al sistema, no existe una función de recuperar contraseña en caso de ser olvidada, no existen criterios establecidos para exigir la creación de contraseñas robustas, por lo que cualquier usuario del sistema se puede crear una contraseña fácil de vulnerar.

Recomendación: En este caso las recomendaciones son netamente acerca del uso del software de la empresa, como se señalaba anteriormente, el software utilizado no es muy robusto, por lo tanto se vuelve más necesario hacer un buen uso del mismo, desde el momento de crear una contraseña, pues el sistema almacena los datos personales de muchos clientes y una forma sencilla de acceder a ellos sería físicamente desde el computador base de la empresa, ya sea cuando alguien deja su sesión iniciada en el computador o cuando establece una contraseña demasiado sencilla como para ser vulnerada con facilidad, se debe implementar en el sistema la exigencia al momento de crear una contraseña, para que esta sea creada en base a criterios establecidos para contraseñas robustas e igualmente capacitar al personal en cuanto a aspectos básicos de seguridad como el almacenamiento de su contraseña, cuando debe ser cambiada, etc.

Se debe implementar igualmente en el sistema un control de logs para poder tener registro en base de datos de la fecha y hora en que ha accedido cada persona al sistema, de esta manera en caso de presentarse algún inconveniente se tendrá un rango específico en el cual realizar la investigación.

En cuanto a la regulación financiera, se presenta un problema al momento de registrar el movimiento financiero de la empresa en su totalidad, pues se encuentra que en el sistema se lleva el registro económico solamente de la venta de los repuestos y no de los servicios realizados de reparación, mantenimiento, o demás servicios prestados, dado que estos servicios también hacen parte de la empresa deben ser registrados en el sistema para lograr una mejor regulación financiera.

### Recomendaciones Finales

Se recomienda implementar de manera diligente las medidas correctivas propuestas y realizar auditorías regulares para mantener un SGSI robusto y adaptado a los estándares de seguridad internacional, como la Norma ISO 27001.

Este informe proporciona una guía detallada para la mejora continua de la seguridad de la información en la empresa MotoRepuestos Cumaral. La implementación efectiva de estas medidas garantizará la protección adecuada de los datos y contribuirá a la confianza de los clientes en la seguridad de los servicios proporcionados.