Texto

Descripción generada automáticamente

**FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**TITULO DEL PROYECTO:**

Informe de Auditoría de Tecnologías de Información para evaluar los sistemas de información en la empresa Importaciones RGZ EIRL

**AUTOR (ES):**

Mondragon Fernandez Alex

Calderon Burga Ivan Adriano

Yarango Farro Darwin Orlando

Castañeda Jimenez Franklin Roger

**CURSO:**

Auditoria de tecnologías de la información

**DOCENTE:**

Ing. Quinteros Gonzales Hermes Marino

**Pimentel 2024**

**ÍNDICE**

[**1.** **Origen de la auditoria** 3](#_Toc183879068)

[**2.** **Objetivos** 3](#_Toc183879069)

[**2.1.** **Objetivo general** 3](#_Toc183879070)

[**2.2.** **Objetivos específicos** 3](#_Toc183879071)

[**3.** **Periodo a examinar** 3](#_Toc183879072)

[**4.** **Antecedentes de la empresa** 3](#_Toc183879073)

[**4.1.** **Descripción** 3](#_Toc183879074)

[**4.2.** **Misión** 4](#_Toc183879075)

[**4.3.** **Visión** 4](#_Toc183879076)

[**4.4.** **Giro del negocio:** 4](#_Toc183879077)

[**4.5.** **Datos de la empresa** 4](#_Toc183879078)

[**4.6.** **Organigrama** 5](#_Toc183879079)

[5](#_Toc183879080)

[**4.7.** **Modelo del negocio** 5](#_Toc183879081)

[**5.** **Antecedentes del área de TI** 5](#_Toc183879082)

[**5.1.** **Descripción** 6](#_Toc183879083)

[**5.2.** **Misión:** 6](#_Toc183879084)

[**5.3.** **Visión:** 6](#_Toc183879085)

[**5.4.** **Organigrama** 6](#_Toc183879086)

[**5.5.** **Modelo de negocio** 7](#_Toc183879087)

[**5.6.** **Servicios/procesos auditar** 7](#_Toc183879088)

[**5.6.1.** **Servicio a auditar** 7](#_Toc183879089)

[**5.6.3.** **Procesos de del servicio a auditar** 7](#_Toc183879090)

[**5.7.** **Diagramas de flujo de cada proceso.** 8](#_Toc183879091)

[**6.** **Metodología para realizar la auditoria** 10](#_Toc183879092)

[**6.1.** **Etapa 1: Planeación de la auditoría de Tecnologías de la Información.** 10](#_Toc183879093)

[**6.2.** **Etapa 2: Ejecución de la auditoría de Tecnologías de la Información** 11](#_Toc183879094)

[**6.3.** **Etapa 3: Dictamen de la auditoría de Tecnologías de la Información** 12](#_Toc183879095)

[**7.** **Normativas aplicables a la auditoría** 13](#_Toc183879096)

[**8.** **Herramientas de recolección de datos** 14](#_Toc183879097)

[**9.** **Documentos a solicitar** 14](#_Toc183879098)

[**10.** **Software para realizar la auditoría** 15](#_Toc183879099)

[**11.** **Avance de cronograma ejecutado en la auditoria.** 16](#_Toc183879100)

[**12.** **Hallazgos** 17](#_Toc183879101)

[**13.** **REFERENCIAS** 23](#_Toc183879102)

1. **Origen de la auditoria**

La necesidad de llevar a cabo una auditoría del sistema de información en la empresa Importaciones RGZ surge de la creciente importancia de garantizar la calidad integridad y seguridad de los datos que maneja la organización, para respaldar adecuadamente las operaciones y servicios críticos es fundamental que el sistema sea confiable y eficiente, esta auditoría busca identificar áreas de mejora, asegurar el cumplimiento de las normativas vigentes optimizar el uso de recursos y fortalecer la seguridad de la información garantizando así una eficiencia operativa óptima y facilitando la toma de decisiones basadas en datos precisos y actualizados.

1. **Objetivos** 
   1. **Objetivo general**

* Realizar una auditoría del sistema de información en la empresa “Importaciones RGZ EIRL”, para evaluar su calidad, seguridad y cumplimiento normativo, identificando mejoras y optimizando recursos tecnológicos.
  1. **Objetivos específicos**
* Verificar la documentación técnica del sistema de información, asegurando que sea completa y actualizada.
* Evaluar el rendimiento y funcionalidad del software mediante pruebas específicas.
* Brindar retroalimentación de mejora en el sistema​ en base a los hallazgos dados

1. **Periodo a examinar**

La auditoría en la empresa Importaciones RGZ EIRL se realizará durante el mes de noviembre del presente año, se programarán dos visitas a lo largo del mes:

* Primera visita: del 1 al 15 de noviembre.
* Segunda visita: del 16 al 30 de noviembre.

1. **Antecedentes de la empresa**
   1. **Descripción**

Importaciones RGZ EIRL es una empresa especializada en la venta minorista de productos textiles y calzado en comercios especializados, fue fundada en 2018 y formalizada en 2021 la empresa ha crecido de manera significativa para adaptarse a las demandas del mercado, estableciendo una estructura organizativa sólida y actualmente cuenta con departamentos clave como Recursos Humanos, encargado de la contratación y gestión de personal, Finanzas que supervisa la contabilidad y tesorería, el Área de Compras que gestiona la adquisición tanto nacional como de importación y el Área de Almacén responsable del inventario y almacenamiento seguro de productos, además el Área de Ventas que incluye la sede principal y una sucursal garantiza la distribución y atención al cliente de manera efectiva.

Para optimizar sus operaciones, Importaciones RGZ EIRL también ha implementado un robusto sistema de TI en el Área de Sistemas de Información que incluye software especializado para la gestión de inventarios, ventas y soporte técnico, este sistema permite a la empresa mantener un flujo de información preciso y en tiempo real facilitando la toma de decisiones y asegurando un alto nivel de servicio al cliente en todas sus operaciones.

* 1. **Misión**
* Proveer productos de calidad que satisfagan las necesidades de nuestros clientes acompañados de un servicio amable y eficiente para fortalecer nuestra relación con ellos.
  1. **Visión**
* Expandir nuestra capacidad operativa para atender a más clientes y asegurar una distribución eficiente de nuestros productos en diversas partes de Chiclayo.
  1. **Giro del negocio:**
* Venta al por mayor y menor de productos como mercería, joyería, juguetes, artículos deportivos y artículos para el hogar
  1. **Datos de la empresa**
* Tienda con ventanas grandes

  Descripción generada automáticamente con confianza mediaNombre de la empresa: Importaciones RGZ E.I.R.L.
* RUC: 20609367386
* Dirección Legal: Manuel Pardo Nro. 141 Otr. Mercado Modelo.
* Distrito / Ciudad: Chiclayo

Ilustración 1: Ubicación - Google maps

* 1. **Organigrama**

Diagrama

Descripción generada automáticamente

Ilustración 2: Organigrama general - Elaboración propia

* 1. Escala de tiempo

     Descripción generada automáticamente **Modelo del negocio**

Ilustración 3: Modelo de negocio - Elaboración propia

1. **Antecedentes del área de TI** 
   1. **Descripción**

El área de TI específicamente el departamento de Sistemas de Información y Soporte Técnico tiene como objetivo principal asegurar la operatividad continua de los sistemas informáticos de la organización, así mismo proporciona soporte técnico a los usuarios y se encarga de optimizar los procesos de gestión de información para garantizar la eficiencia operativa, además implementa tecnologías que permiten la toma de decisiones basadas en datos en tiempo real y promueven la seguridad y protección de la información de la empresa.

* 1. **Misión:**
* Garantizar la operatividad continua y segura de los sistemas informáticos ofreciendo soporte técnico eficaz y optimizando la gestión de la información para una mayor eficiencia en la organización.
  1. **Visión:**
* Ser el pilar tecnológico de la organización reconocido por la implementación de sistemas seguros y el soporte técnico confiable que impulsan la toma de decisiones en tiempo real
  1. Diagrama

     Descripción generada automáticamente**Organigrama**

Ilustración 4: Organigrama TI - Elaboración propia

* 1. Escala de tiempo

     Descripción generada automáticamente con confianza media**Modelo de negocio**

Ilustración 5: Modelo de negocio TI - Elaboración propia

* 1. **Servicios/procesos auditar** 
     1. **Servicio a auditar**
     2. **Servicio**
* **Sistema de información**

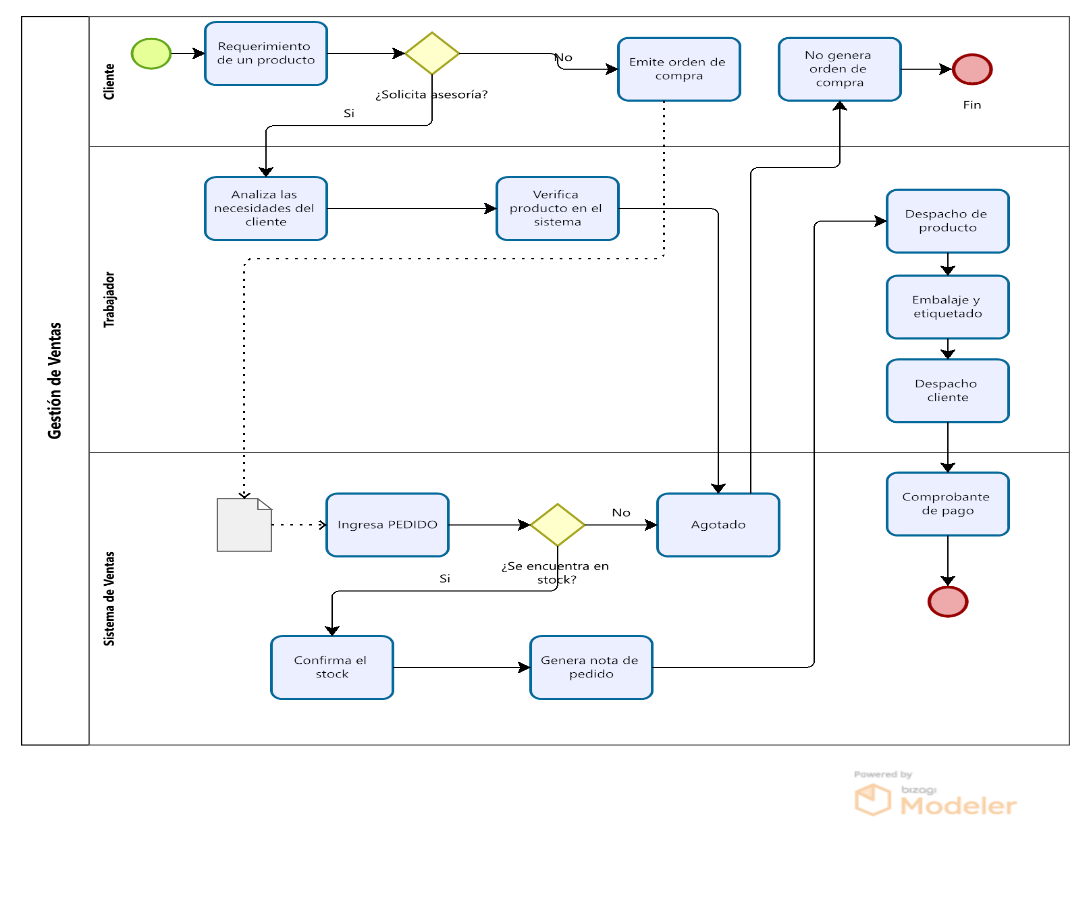
El sistema de información de la empresa Importaciones RGZ EIRL se va a auditar debido a la necesidad de asegurar la calidad integridad y seguridad de los datos que maneja la organización, el sistema soporta procesos críticos como la gestión de inventarios, ventas y relaciones con proveedores que son fundamentales para el funcionamiento y la competitividad de la empresa.

* + 1. **Procesos de del servicio a auditar**
* **Gestión de Almacén:** Garantiza que el inventario esté siempre actualizado y disponible optimizando los recursos y evitando tanto excesos como faltantes de productos, a través de la auditoría se evalúa la precisión y eficiencia del control de inventarios.
* **Proceso de Ventas:** Asegura que todas las transacciones de venta, desde el registro hasta la facturación se manejen de manera precisa y en cumplimiento con la normativa.
* **Gestión de Proveedores:** Facilita la relación y el flujo constante con los proveedores asegurando que los materiales o productos se reciban en tiempo y forma, de este modo la auditoría de este servicio ayuda a identificar riesgos en la cadena de suministro y asegurar que los acuerdos con proveedores se cumplan de manera efectiva y segura.
* **Soporte Técnico:** Proporciona el soporte necesario para que los sistemas de información funcionen sin interrupciones asegurando disponibilidad y rendimiento, la auditoría revisa la efectividad de este servicio, garantizando que se realicen mantenimientos preventivos y que se dé una respuesta rápida.
  1. **Diagramas de flujo de cada proceso.**
* **Gestión de Almacén**



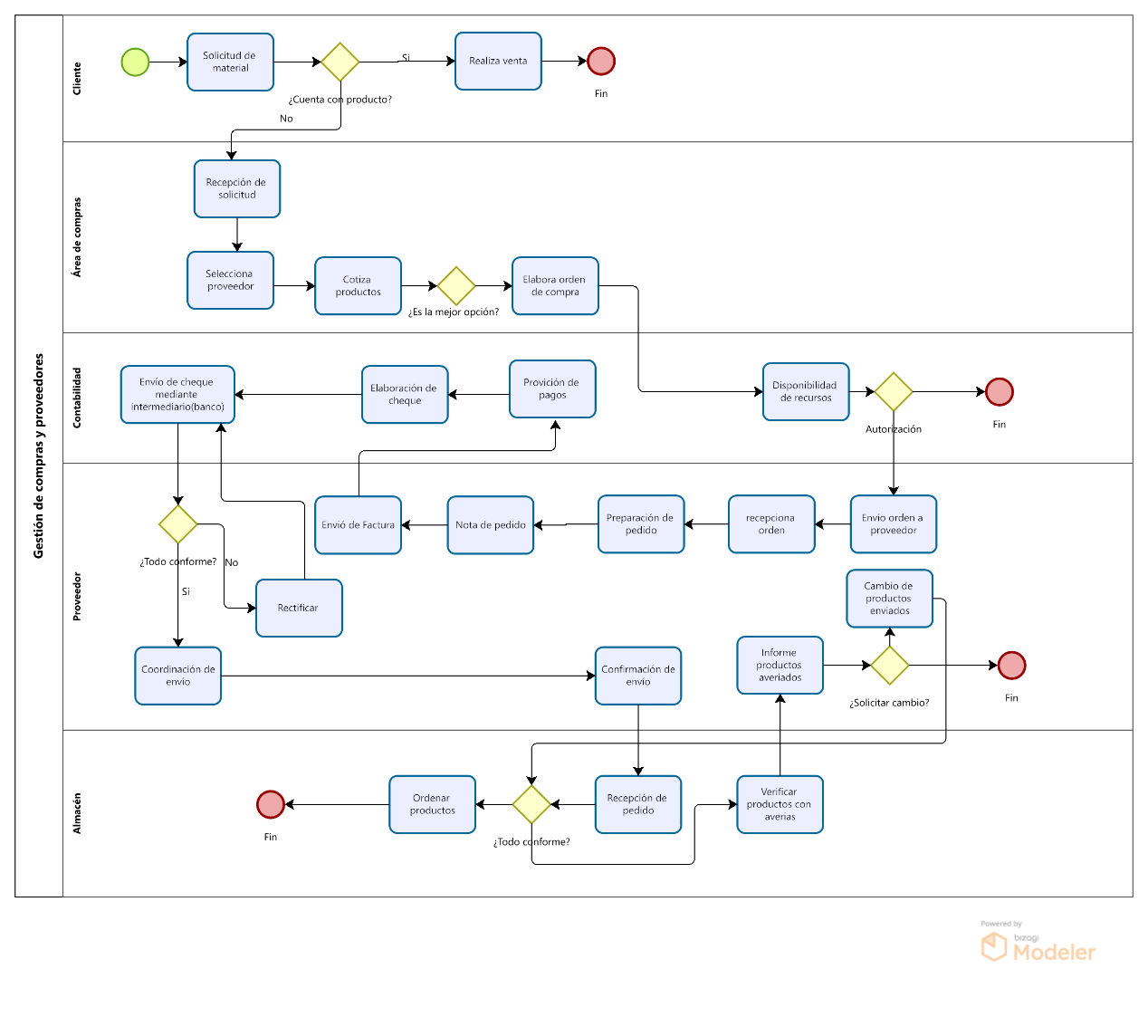
**Gestión de Almacén**

* **Proceso de venta**



**Proceso de Ventas**

* **Gestión de proveedores**



**Gestión de Proveedores**

* Diagrama

  Descripción generada automáticamente**Soporte Técnico**

1. **Metodología para realizar la auditoria**
   1. **Etapa 1: Planeación de la auditoría de Tecnologías de la Información.**

En esta etapa, se definen los objetivos y el alcance de la auditoría se identifican los puntos críticos y se establece un cronograma detallado, además se recaba información preliminar para comprender los sistemas de TI y los riesgos asociados. Se diseñan planes y programas de trabajo, se asignan recursos y se seleccionan los métodos, herramientas e instrumentos necesarios. Esta etapa busca asegurar que la auditoría cubra todos los aspectos relevantes y minimice cualquier impacto en las operaciones de la empresa durante la ejecución.

|  |  |  |
| --- | --- | --- |
| Qué hacer | Orden | Cómo hacerlo |
| Establecer objetivos recopilar datos y evaluar riesgos | Identificar el origen de la auditoría. | Revisar la razón principal y el contexto que motiva la auditoría. |
| Realizar una visita preliminar al área que será evaluada. | Observar procesos y entrevistar al personal clave. |
| Establecer los objetivos de la auditoría. | Definir metas claras alineadas con las necesidades del negocio. |
| Determinar los puntos que serán evaluados en la auditoría. | Seleccionar procesos y áreas críticas a evaluar. |
| Elaborar planes, programas y presupuestos para realizar la auditoría. | Crear cronograma, asignar recursos y estimar costos. |
| Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría. | Elegir técnicas y herramientas específicas para el análisis. |
| Asignar los recursos y sistemas computacionales para la auditoría. | Designar al equipo y asegurar disponibilidad de tecnología. |

* 1. **Etapa 2: Ejecución de la auditoría de Tecnologías de la Información**

En esta etapa, se lleva a cabo todas las actividades programadas en el plan de auditoría, implica aplicar los instrumentos y herramientas seleccionados, realizar las evaluaciones prácticas, recopilar evidencias, identificar desviaciones en los sistemas o procesos de TI y documentar los hallazgos, además, se elabora un dictamen preliminar que es discutido con las áreas involucradas para asegurar su validez y objetividad. Finalmente, se integra el conjunto de papeles de trabajo como respaldo de todo el proceso.

|  |  |  |
| --- | --- | --- |
| Qué hacer | Orden | Cómo hacerlo |
| Realizar las acciones planificadas para ejecutar la auditoría | Realizar las acciones programadas para la auditoría. | Implementar las actividades definidas en el plan de auditoría siguiendo el cronograma establecido. |
| Aplicar los instrumentos y herramientas para la auditoría. | Usar herramientas seleccionadas (software, cuestionarios, plantillas) para evaluar sistemas y procesos. |
| Identificar y elaborar los documentos de desviaciones encontradas. | Registrar hallazgos relevantes en informes preliminares con evidencia de las desviaciones detectadas. |
| Elaborar el dictamen preliminar y presentarlo a discusión. | Preparar un informe inicial con los hallazgos, discutirlo con las áreas responsables y solicitar retroalimentación. |
| Integrar el legajo de papeles de trabajo de la auditoría. | Consolidar todos los registros, documentos y evidencias obtenidos durante la auditoría para su análisis posterior |

* 1. **Etapa 3: Dictamen de la auditoría de Tecnologías de la Información**

La tercera etapa se concentra en la preparación del informe final de la auditoría. Después de haber completado la recopilación de datos y la evaluación de los sistemas de TI, se analiza toda la información obtenida para elaborar un informe detallado con las situaciones detectadas, las desviaciones y las áreas de mejora. A continuación, se elabora el dictamen final, que sintetiza los hallazgos y ofrece recomendaciones basadas en la auditoría realizada. Finalmente, el informe se presenta a la alta dirección o a los responsables correspondientes para su revisión y discusión, lo que puede generar acciones correctivas o planes de mejora, para crear una guía práctica de implementación de mejoras en Importaciones RGZ EIRL.

|  |  |  |
| --- | --- | --- |
| Qué hacer | Orden | Cómo hacerlo |
| Elaborar y presentar el informe final de auditoría | Analizar la información y elaborar un informe de situaciones detectadas. | Examinar los hallazgos y desviaciones, analizando la gravedad y el impacto de los problemas encontrados. |
| Elaborar el dictamen final. | Redactar un informe claro y estructurado con los resultados definitivos de la auditoría, incluyendo recomendaciones. |
| Presentar el informe de auditoría. | Presentar el dictamen final a la alta dirección y a las partes responsables para su revisión y toma de decisiones. |

1. **Normativas aplicables a la auditoría**

Las normativas aplicables a la auditoría de TI en Importaciones RGZ EIRL proporcionan un marco esencial para evaluar la seguridad, eficiencia y cumplimiento del sistema de información, estas normas como ISO/IEC 27001 y COBIT aseguran que la empresa implemente controles sólidos para proteger la información crítica garantizando la confidencialidad, integridad y disponibilidad de los datos, además normas como ISO/IEC 20000 e ISO 22301 ayudan a fortalecer la calidad de los servicios de TI y la continuidad del negocio permitiendo a Importaciones RGZ EIRL estar preparada para gestionar interrupciones imprevistas. Cumplir con la Ley de Protección de Datos Personales también es crucial para salvaguardar los derechos de los usuarios y cumplir con la regulación vigente estableciendo así una base sólida para la confianza y transparencia en el manejo de la información.

|  |  |  |
| --- | --- | --- |
| Normativa | Descripción | Aplicación en la Auditoría |
| ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información (SGSI) | Define los requisitos para implementar y mejorar un sistema de gestión de seguridad de la información. | Revisar políticas y procedimientos de seguridad (acceso, contraseñas, respaldo). Evaluar controles que protejan la confidencialidad, integridad y disponibilidad de datos. |
| COBIT (Control Objectives for Information and Related Technology) | Marco de gobierno de TI para alinear objetivos de TI con los estratégicos de la empresa. | Evaluar si los procesos de TI soportan los objetivos del negocio y gestionan adecuadamente riesgos y recursos en el sistema de información. |
| ISO/IEC 20000 - Gestión de Servicios de TI | Normativa de gestión de servicios de TI enfocada en la calidad de servicios y mejora continua. | Verificar procedimientos de soporte técnico y mantenimiento para asegurar calidad y continuidad en el servicio del sistema de información. |
| ISO 22301 - Gestión de Continuidad del Negocio | Establece requisitos para la continuidad del negocio en caso de interrupciones. | Revisar planes de respaldo y recuperación de datos ante incidentes para asegurar que los datos críticos y la operación puedan continuar en caso de fallo. |
| Ley de Protección de Datos Personales | Regula el tratamiento adecuado de datos personales (aplicable según la legislación del país). | Verificar el cumplimiento en el manejo de datos personales, asegurando consentimiento, medidas de seguridad, y derecho de acceso y rectificación de los datos de usuarios. |

1. **Herramientas de recolección de datos**

* **Entrevistas:** Realizar entrevistas con los responsables de cada área (Recursos Humanos, Finanzas, Compras, Almacén y Ventas) para comprender cómo interactúan con el sistema de TI.
* **Cuestionarios y encuestas:** Diseñar cuestionarios dirigidos a los usuarios finales del sistema, tales como empleados de ventas, almacén y finanzas.
* **Observación directa:** Observar directamente cómo los empleados utilizan el sistema en sus actividades diarias.
* **Revisión de documentación:** Examinar la documentación técnica del sistema de TI, incluyendo manuales, procedimientos operativos y registros de mantenimiento.
* **Grupos focales:** Organizar grupos focales con empleados de distintas áreas (como finanzas, compras, almacén) para discutir los puntos fuertes y débiles del sistema de TI.
* **Auditoría física:** Inspeccionar físicamente los equipos de TI, como servidores, estaciones de trabajo y dispositivos de almacenamiento, para evaluar su estado físico y su capacidad para manejar la carga de trabajo. verificar el cumplimiento de las normativas de seguridad y la correcta disposición de los equipos.
* **Revisión de procesos operativos:** Analizar los flujos de trabajo entre departamentos y cómo el sistema de información apoya esas actividades.

1. **Documentos a solicitar**

|  |  |  |
| --- | --- | --- |
| **Documento** | **Propósito** | **Importancia** |
| Políticas de seguridad de la información | Establecer directrices para proteger la información y los activos de la organización. | Esencial para cumplir con normativas y estándares, y para proteger la información sensible. |
| Documentación de control de accesos y permisos | Definir y gestionar quién tiene acceso a qué recursos y en qué condiciones. | Crucial para prevenir accesos no autorizados y asegurar la integridad y confidencialidad de la información. |
| Políticas de uso de contraseñas | Establecer requisitos para la creación, almacenamiento y gestión de contraseñas. | Importante para proteger las cuentas de usuario y prevenir accesos no autorizados. |
| Manual de operación del sistema | Proporcionar instrucciones detalladas para la configuración, uso y mantenimiento del sistema. | Vital para asegurar que el sistema funcione correctamente y que los usuarios puedan operarlo de manera efectiva. |

1. **Software para realizar la auditoría**

Para realizar una auditoría de TI eficiente y precisa en Importaciones RGZ EIRL es esencial contar con herramientas especializadas que permitan automatizar la recopilación y análisis de datos, identificar vulnerabilidades y facilitar la elaboración de informes detallados, estas herramientas optimizan cada fase de la auditoría desde las pruebas de seguridad hasta la documentación de hallazgos y la gestión del plan de acción permitiendo que el equipo auditor obtenga resultados confiables y visualice de manera clara los riesgos y mejoras necesarias. A continuación, se detallan los softwares recomendados para apoyar en cada etapa del proceso de auditoría.

|  |  |  |
| --- | --- | --- |
| Software | Función en la Auditoría | Descripción de Uso |
| Nmap | Escaneo de Red y Detección de Servicios | Herramienta de escaneo de red que puede identificar servicios y vulnerabilidades en servidores web. |
| SQLMap | Detección de Vulnerabilidades de Inyección SQL | Herramienta automatizada para detectar y explotar vulnerabilidades de inyección SQL en aplicaciones web. |
| Metasploit | Simulación de Ataques de Seguridad | simular ciberataques y evaluar la robustez de la seguridad en el sistema de información. |
| oswap zap | Escaneo de Vulnerabilidades en Servidores Web | escaneo de vulnerabilidades para servidores web, que identifica problemas de configuración y seguridad. |
| DirBuster | Fuerza Bruta en Directorios y Archivos | Herramienta para realizar ataques de fuerza bruta en directorios y archivos ocultos en servidores web. |
| Hydra | Ataques de Fuerza Bruta en Autenticación | Herramienta para realizar ataques de fuerza bruta en protocolos de autenticación, como HTTP, FTP, SSH, etc. |
| Speed test | Medir velocidad de internet de subida y baja | Herramienta web que sirve para medir la velocidad de internet en una red |

1. **Avance de cronograma ejecutado en la auditoria.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fase** | **Actividad** | **Fecha de Inicio** | **Fecha de Finalización** |
| **Etapa 1:** | Definir alcance y objetivos de la auditoria | 5 de noviembre | 7 de noviembre |
| Elaboración de herramientas de recolección de información | 8 de noviembre | 11 de noviembre |
| Evaluación de riesgos asociados al sistema web | 12 de noviembre | 13 de noviembre |
| Elaboración del plan de auditoría para el sistema web | 14 de noviembre | 15 de noviembre |
| **Etapa 2:** | Evaluación de la gestión de inventarios mediante el sistema web | 26 de noviembre | 27 de noviembre |
| Evaluación del proceso de ventas a través del sistema web | 28 de noviembre | 29 de noviembre |
| Evaluación de seguridad de la información (acceso a datos, políticas de seguridad, protección de contraseñas, firewalls, etc.) | 2 de diciembre | 3 de diciembre |
| **Etapa 3:** | Identificación de deficiencias en el sistema web | 4 de diciembre | 5 de diciembre |
| Evaluación de impacto y clasificación de riesgos | 6 de diciembre | 7 de diciembre |
| Elaboración de informe final de auditoria | 8 de diciembre | 10 de diciembre |

1. **Hallazgos**

* **Hallazgo 1:**

Se puede observar en la imagen es que la conexión de internet tiene una velocidad de descarga de 238.53 Mbps y una velocidad de subida de 317.49 Mbps. Además, el ping es de 18 ms. Estos valores indican una conexión de alta velocidad, especialmente la velocidad de subida, que es notablemente alta. Para corroborar lo antes mencionado, se utilizó la herramienta web de speedtest.com para realizar un test de velocidad a la conexión y una revisión detallada de los contratos existentes con los proveedores de Internet.

* **\*Evidencia encontrada**



* **Norma:**
* ISO/IEC 20000-1 - Gestión de servicios de TI: Esta norma describe los requisitos para un sistema de gestión del servicio (SGS). Las velocidades de internet mencionadas pueden ser parte de los requisitos de desempeño y calidad de servicio que una organización debe gestionar y monitorear para garantizar una prestación de servicios efectiva.
* **Hallazgo 2:**

Para la realización del hallazgo hemos utilizado el software oswap zap ya que es unaes una herramienta de seguridad de código abierto diseñada para encontrar vulnerabilidades en aplicaciones web durante el desarrollo y las pruebas de seguridad.

* **\*Evidencia encontrada**



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente**Norma:**

* ISO/IEC 27001:2013 - Sistemas de gestión de seguridad de la información (SGSI).
* Control A.14.1.2: Las aplicaciones deben estar protegidas contra fraudes y ataques. unsafe-inline facilita ataques como la inyección de scripts (XSS).
* Control A.13.1.1: Establece que las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones. Problemas de configuración de dominio cruzado pueden permitir interacciones no seguras entre dominios, comprometiendo la seguridad de la red y la información.
* Control A.14.2.5: Los principios de ingeniería de seguridad en sistemas de información deben ser seguidos para proteger la integridad y la confidencialidad de la información. La falta del encabezado X-Frame-Options puede exponer la aplicación a riesgos de clickjacking, comprometiendo la integridad de la información.
* Control A.12.6.1: Este control requiere la gestión de vulnerabilidades en el suministro de software para asegurar que se conozcan y gestionen los riesgos de seguridad. El uso de bibliotecas de JavaScript con vulnerabilidades conocidas puede exponer la aplicación a riesgos significativos de seguridad.
* Control A.13.2.1: Este control establece que se deben implementar medidas para proteger la confidencialidad, la autenticidad y la integridad de la información. La falta del atributo Secure en las cookies puede comprometer la confidencialidad de la información al transmitirse en conexiones no cifradas.
* **Recomendaciones**
* ISO/IEC 27002:2013 Código de Práctica para Controles de Seguridad de la Información
* Sección 14.2.5: Recomienda seguir principios de diseño seguro. unsafe-inline permite la ejecución de scripts maliciosos.
* Sección 13.1.3: Recomienda la segregación de redes. Una configuración incorrecta de dominio cruzado puede permitir accesos no autorizados a recursos y datos entre dominios, violando el principio de segregación de redes.
* Sección 14.2.2: Establece que la seguridad de los servicios de aplicaciones debe ser gestionada. Una configuración de dominio cruzado incorrecta puede permitir interacciones no seguras con la aplicación, comprometiendo la seguridad del servicio.
* Sección 14.2.8: Esta sección establece que los cambios en los sistemas y software deben gestionarse de manera controlada. Utilizar bibliotecas de JavaScript con vulnerabilidades conocidas puede comprometer la seguridad de la información y la integridad del sistema.
* Sección 10.2.1: Recomienda que la información debe ser protegida adecuadamente mediante métodos de cifrado y otras medidas de seguridad. Las cookies sin el atributo Secure pueden ser interceptadas durante la transmisión, comprometiendo la seguridad de la información transmitida.
* Sección 10.1.1: Recomienda que los sistemas de información deben protegerse contra el acceso no autorizado. La ausencia del atributo SameSite en las cookies puede facilitar ataques CSRF, comprometiendo la seguridad de los sistemas de información.
* Sección 14.1.2: Establece que se deben implementar controles para proteger la confidencialidad de la información en redes y sistemas. La ausencia del encabezado HSTS puede comprometer la confidencialidad al permitir comunicaciones no cifradas que podrían ser interceptadas.
* Sección 15.1.3: Recomienda la protección de la información en sistemas de información. Los comentarios sospechosos en el código pueden revelar detalles técnicos sobre la implementación y posibles puntos débiles, comprometiendo la seguridad de la información.
* **Hallazgo 3:**

La cláusula A.12 de la norma ISO/IEC 27001: Gestión de Incidentes de Seguridad de la Información, establece que una organización debe contar con procedimientos adecuados para manejar incidentes de seguridad de la información. Esto incluye responder a incidentes con acciones destinadas a contener y eliminar sus causas, registrar detalladamente los incidentes, comunicarse con las partes relevantes, analizar las causas y aplicar medidas correctivas y preventivas, así como revisar la eficacia de estas acciones por parte de la alta dirección para fomentar la mejora continua en la gestión de la seguridad de la información.

Durante la auditoría, se identificó que la organización no tiene una política formal de seguridad de la información. Esta política es fundamental para establecer directrices claras y procedimientos destinados a proteger los activos de información, garantizar el cumplimiento de normativas, y mitigar los riesgos asociados con la gestión de datos.

* Recomendaciones:

1. Desarrollo e Implementación de una Política de Seguridad de la Información: Según la Norma ISO/IEC 27001: Cláusula 5.2: Establecer una política de seguridad de la información adecuada al propósito de la organización, comunicada internamente y revisada periódicamente.
2. Realizar Evaluaciones de Riesgos: Según la norma ISO/IEC 27001 - Cláusula 6.1.2: Realizar evaluaciones de riesgos a intervalos planificados y ante cambios significativos.
3. Establecer un proceso de gestión de incidentes: Según la norma ISO/IEC 27001 - Cláusula 16: Establecer procedimientos para gestionar incidentes de seguridad de la información, incluyendo detección, reporte, respuesta y lecciones aprendidas.
4. Capacitar y Concienciar al Personal: Según la norma ISO/IEC 27001 - Cláusula 7.2: Asegurar que el personal tenga la competencia necesaria basada en educación, entrenamiento o experiencia.
5. Establecer Comunicación Interna y Externa: Según la norma ISO/IEC 27001 - Cláusula 7.4: Determinar las necesidades de comunicación interna y externa sobre seguridad de la información.
6. Revisar y Mejorar Continuamente: Según la norma ISO/IEC 27001 - Cláusula 10: Mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

* **Hallazgo 4:**

Se observó la ausencia de plan de respuestas a incidentes

* Normas:

1. Norma ISO 27001-Cláusula 16 (Gestión de Incidentes de Seguridad de la Información): ISO 27001 requiere que las organizaciones establezcan un proceso de gestión de incidentes de seguridad de la información. Esto incluye la identificación, reporte, evaluación, respuesta y aprendizaje de incidentes. La ausencia de un plan de respuestas a incidentes implica el incumplimiento de esta cláusula, lo que puede poner en riesgo la seguridad de la información y la capacidad de la organización para gestionar y mitigar incidentes de manera efectiva.
2. ITIL: Define la gestión de incidentes como un proceso crucial para restaurar el servicio normal lo más rápido posible tras una interrupción, minimizando el impacto en las operaciones del negocio. La ausencia de un plan de respuesta a incidentes significa que no se cumple con las mejores prácticas de ITIL para la gestión de incidentes, lo que puede resultar en tiempos de inactividad prolongados y un impacto negativo en la calidad del servicio.

* Recomendaciones:

Para cumplir con las normas ISO 27001 e ITIL, se recomienda desarrollar un plan formal de respuesta a incidentes que incluya procedimientos para la identificación, reporte, evaluación, respuesta y seguimiento de incidentes, asegurando la alineación con la cláusula 16 de ISO 27001. Capacitar al personal en el manejo de incidentes y realizar simulacros regulares, además de establecer un proceso de gestión de incidentes claro y estructurado según las mejores prácticas de ITIL. Asignar roles y responsabilidades específicas al equipo de respuesta, y monitorear y revisar continuamente el proceso, implementando mejoras basadas en evaluaciones y análisis de incidentes pasados.

* **Hallazgo 5:**

Se observó que tiene una Ausencia del plan estratégico

* Normas:

1. ISO 27001 requiere comprender el contexto de la organización (cláusula 4) y establecer objetivos claros para la seguridad de la información. La alta dirección debe demostrar liderazgo y compromiso mediante una política de seguridad y objetivos alineados con la estrategia organizacional (cláusula 5). Además, la planificación debe incluir la gestión de riesgos y oportunidades y el establecimiento de objetivos claros, guiados por un plan estratégico (cláusula 6).
2. ITIL enfatiza la estrategia de servicio para definir visión, misión y objetivos de los servicios de TI. Sin un plan estratégico, la entrega y gestión de servicios carecen de dirección. El diseño, transición y operación de servicios deben alinearse con la estrategia, y la mejora continua necesita esta alineación para ser efectiva.

* Recomendaciones:

Para cumplir con las normas ISO 27001 e ITIL, se recomienda desarrollar e implementar un plan estratégico claro que comprenda el contexto organizacional y defina objetivos claros. La alta dirección debe demostrar liderazgo y compromiso con políticas y objetivos alineados con la estrategia organizacional. La planificación estratégica debe incluir la gestión de riesgos y oportunidades para guiar la implementación y operación de sistemas de gestión y servicios de TI. Además, se debe fomentar la mejora continua para asegurar que todas las iniciativas estén alineadas con la dirección estratégica de la organización.

* **Hallazgo 6:**

**USABILIDAD DEL SISTEMA:**

El sistema es calificado como fácil de usar en general y cumple con la mayoría de las necesidades laborales de los usuarios.

* Normas:
* **ISO 9241-11:2018 (Ergonomía de la interacción humano-sistema - Parte 11: Usabilidad: Definición y conceptos generales)**  
  Esta norma proporciona directrices para medir y evaluar la usabilidad de los sistemas interactivos. Define la usabilidad en términos de efectividad, eficiencia y satisfacción en un contexto de uso específico, asegurando que el sistema sea fácil de usar y satisfactorio para los usuarios.
* Recomendaciones:
* **ITIL Service Design:** El diseño del servicio en ITIL pone un fuerte énfasis en la usabilidad mediante un enfoque centrado en el usuario. Esto asegura que los sistemas de TI se diseñen considerando las necesidades de los usuarios finales, creando sistemas más intuitivos y fáciles de usar.
* **Brechas de Seguridad**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Brecha de Seguridad** | **Descripción** | **Impacto** | **Norma Relacionada** | **Recomendación** |
| Política Formal de Seguridad de la Información | Ausencia de una política formal de seguridad de la información. | Riesgo significativo para la organización en términos de protección de datos y respuesta a incidentes. | ISO/IEC 27001, Cláusula 5.2 | Desarrollar ye implementar una política formal de seguridad de la información. Capacitar al personal sobre la política. |
| Plan de Respuesta a Incidentes | Falta de un plan formal de respuesta a incidentes. | Incremento del riesgo ante la incapacidad de manejar incidentes de seguridad de manera eficiente. | ISO/IEC 27001, Cláusula 16 | Crear y documentar un plan formal de respuesta a incidentes. Realizar simulacros regulares. Asignar roles y responsabilidades claras. |
| Control de Acceso | Control de acceso inadecuado y falta de políticas de backup y recuperación de datos. | Compromiso de la seguridad y disponibilidad de la información crítica. | ISO/IEC 27002, Sección 10.1.1 | Implementar controles de acceso basados en roles. Revisar periódicamente los accesos asignados. Utilizar tecnologías de autenticación robustas. |

1. **REFERENCIAS**

* Alexander, D. (2020). *Transición al ISO/IEC 20000-1:2018*. Obtenido de https://gerenciayproductividad.com/wp-content/uploads/2020/07/14\_Transicion\_al\_ISO\_20000-1\_2018.pdf
* ISO 27001. (2023). *ISO 27001*. Obtenido de https://normaiso27001.es/a12-seguridad-de-las-operaciones/
* *Normas ISO*. (2023). Obtenido de Normas ISO: https://www.normas-iso.com/iso-9001/
* OSTEC. (2016). *ISO 27002: Buenas prácticas para gestión de la seguridad de la información*. Obtenido de https://ostec.blog/es/aprendizaje-descubrimiento/iso-27002-buenas-practicas-gsi/
* *Service Management Institute*. (12 de diciembre de 25023). Obtenido de Service Management Institute: https://news.itsmf.es/iso-19770-una-gran-familia-de-normas-para-la-gestion-de-activos-de-ti/

**Anexos 01:**

**Plantilla: Recolección de Información del Sistema de Información**

**Recolección de Información del Sistema de Información - Sistema Web**

**1. Información General del Sistema**

* + - * **Nombre del Sistema:** Sistema de Gestión Integral de Inventarios y Ventas
      * **Propósito del Sistema Web:** Gestionar y optimizar las operaciones de inventario, ventas, compras y soporte técnico, mejorando la eficiencia operativa y la toma de decisiones basadas en datos precisos y actualizados.
      * **Responsable del Sistema:** Iban Peralez Rosales.
      * **Responsable Auditor:** Grupo 8
      * **Link de sistema:** [**https://app.applikalo.com/login/indexET.html?c=cumbremar**](https://app.applikalo.com/login/indexET.html?c=cumbremar)

**2. Tecnología del Sistema Web**

|  |  |  |
| --- | --- | --- |
| **Elemento Evaluado** | **Datos importantes** | **Observaciones** |
| Servidores | Servidor en la nube | Capacidad de 500 GB |
| Base de Datos | MySQL, versión 7.8 | Base de datos distribuida con replicación activa |
| Lenguaje de Programación | PHP, JavaScript, HTML, CSS | Framework robusto para aplicaciones web escalables |
| Conexiones de Red | Cableada y Wi-Fi, velocidad de 500 Mbps | Estable y segura, conexiones redundantes |

**3. Seguridad del Sistema Web**

|  |  |  |
| --- | --- | --- |
| **Aspecto Evaluado** | **(Cumple/No Cumple)** | **Observaciones** |
| Contraseñas seguras | Cumple | Longitud mínima de 8 caracteres, mezcla de mayúsculas, minúsculas, números y caracteres especiales |
| Políticas de acceso definidas | Cumple | Roles definidos: Administrador, Usuario, Supervisor |
| Permisos según roles de usuario | Cumple | Accesos diferenciados según el perfil del usuario |
| Aplicación de parches de seguridad | cumple | La aplicación de parches de seguridad se realiza, pero con poca frecuencia |
| Vulnerabilidades (XSS, CSRF, ETC) | No Cumple | Problemas detectados en OWASP ZAP (falta de encabezados HSTS Y x-frame-options) |
| Registro de accesos habilitado | No Cumple | Acceso de empleados inactivos no han sido revocados |

**4. Proceso De Control De Incidencias**

|  |  |  |
| --- | --- | --- |
| **Aspecto Evaluado** | **Estado (Cumple/No Cumple)** | **Observaciones** |
| Política de seguridad de la información | No Cumple | La organización no tiene una política formal de seguridad de la información documentada y comunicada. |
| Procedimiento de gestión de incidentes | No Cumple | No se cuenta con un proceso formal para gestionar incidentes de seguridad, incluyendo detección y respuesta de ataques. |
| Evaluación de riesgos periódica | No Cumple | No se han realizado evaluaciones de riesgos a intervalos planificados ni ante cambios significativos. |
| Capacitación sobre seguridad de la información | No Cumple | No se ha implementado un programa formal de capacitación para el personal en temas de seguridad de la información. |
| Registro y seguimiento de incidentes | No Cumple | No existe un registro formal y seguimiento de los incidentes de seguridad, lo que impide análisis adecuados. |
| Revisión de incidentes por la alta dirección | No Cumple | No se han implementado procedimientos para que la alta dirección revise la eficacia de las acciones correctivas. |

**5. Plan de Respuesta contra incidentes:**

|  |  |  |
| --- | --- | --- |
| **Aspecto Evaluado** | **Estado (Cumple/No Cumple)** | **Observaciones** |
| Plan de respuesta a incidentes | No Cumple | La organización no cuenta con un plan formal de respuesta a incidentes, lo que incumple la cláusula 16 de ISO 27001. |
| Procedimientos para identificación y evaluación de incidentes | No Cumple | No se han definido procedimientos claros para la identificación, reporte, evaluación y respuesta ante incidentes. |
| Capacitación del personal en gestión de incidentes | No Cumple | El personal no ha sido capacitado adecuadamente en el manejo y respuesta de incidentes de seguridad de la información. |
| Simulacros y pruebas de respuesta a incidentes | No Cumple | No se realizan simulacros regulares ni se han probado los procedimientos de respuesta a incidentes. |
| Asignación de roles y responsabilidades | No Cumple | No se han asignado roles y responsabilidades específicas al equipo de respuesta a incidentes. |
| Revisión y mejora continua del proceso | No Cumple | No se lleva a cabo un monitoreo ni revisión continua del proceso de respuesta a incidentes para implementar mejoras. |

**6. Proceso de plan estratégico**

|  |  |  |
| --- | --- | --- |
| **Aspecto Evaluado** | **Estado (Cumple/No Cumple)** | **Observaciones** |
| Plan Estratégico de Seguridad de la Información | No Cumple | La organización no cuenta con un plan estratégico que defina objetivos claros y esté alineado con la estrategia general. |
| Contexto organizacional comprendido | No Cumple | No se ha realizado un análisis formal del contexto organizacional según la cláusula 4 de ISO 27001. |
| Liderazgo y compromiso de la alta dirección | No Cumple | La alta dirección no demuestra liderazgo ni compromiso claro con la seguridad de la información, lo que afecta la dirección estratégica. |
| Alineación de objetivos de seguridad con la estrategia organizacional | No Cumple | No se ha establecido una alineación clara entre los objetivos de seguridad de la información y la estrategia organizacional. |
| Gestión de riesgos y oportunidades | No Cumple | No se están gestionando adecuadamente los riesgos y oportunidades relacionados con la seguridad de la información. |
| Mejora continua del proceso estratégico | No Cumple | No se implementa un proceso de mejora continúa alineado con la estrategia organizacional y los objetivos de seguridad. |

**7. Procesos de Operación y usabilidad del Sistema Web**

|  |  |  |  |
| --- | --- | --- | --- |
| **Proceso** | **Datos Importantes** | **Frecuencia (Diario/Semanal/Mensual)** | **Observaciones** |
| Ingreso de datos | Introducción de inventarios, ventas y compras | Diario | Datos ingresados manualmente |
| Generación de reportes | Reportes de ventas, inventario, compras y análisis financieros | Semanal / Mensual | Informes automatizados |
| Respaldo de información | Backup completo de la base de datos y configuraciones del sistema | Diario | Respaldos automáticos en la nube |
| Actualizaciones del sistema | Actualización de versiones y parches de seguridad | Mensual | Sistema actualizado |

**8. Respaldo y Recuperación**

|  |  |  |
| --- | --- | --- |
| **Aspecto Evaluado** | **Estado (Cumple/No Cumple)** | **Observaciones** |
| Frecuencia de respaldos | Cumple | Respaldos automáticos |
| Ubicación de respaldos | Cumple | Almacenamiento en la nube |
| Pruebas de recuperación realizadas | Cumple | Pruebas de recuperación realizadas mensualmente |
| Políticas de respaldo documentadas | Cumple | Políticas de respaldo |

**9. Evaluación del Rendimiento**

|  |  |  |
| --- | --- | --- |
| **Criterio** | **Estado Actual** | **Observaciones** |
| Tiempo de respuesta del sistema | Rápido | Tiempo de respuesta promedio de 2 segundos por operación |
| Disponibilidad (uptime) | Alta | 99.9% uptime garantizado |
| Estabilidad bajo carga | Estable | El sistema soporta más de 200 usuarios simultáneos sin pérdida de rendimiento |

**10. Hallazgos Identificados**

|  |  |  |
| --- | --- | --- |
| **Área o Módulo** | **Problema Detectado** | **Impacto (Alto/Medio/Bajo)** |
| Seguridad | Accesos no revocados a empleados que ya no pertenecen a la empresa | Alto |
| Base de Datos | Espacio de almacenamiento al límite, falta de optimización de queries | Medio |
| Rendimiento | Lento en ciertos reportes debido a consultas no indexadas | Bajo |
| Otros | Interfaces de usuario de algunos módulos no completamente amigables | Medio |

**ANEXO 02:**

**INTERFAZ DEL SISTEMA**

* **login**

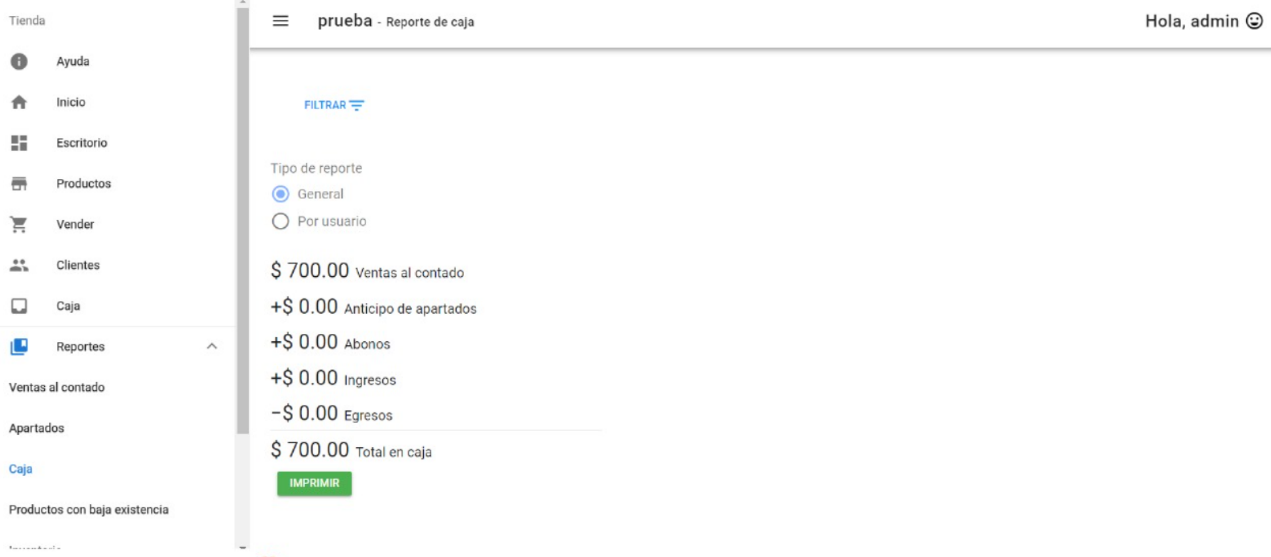
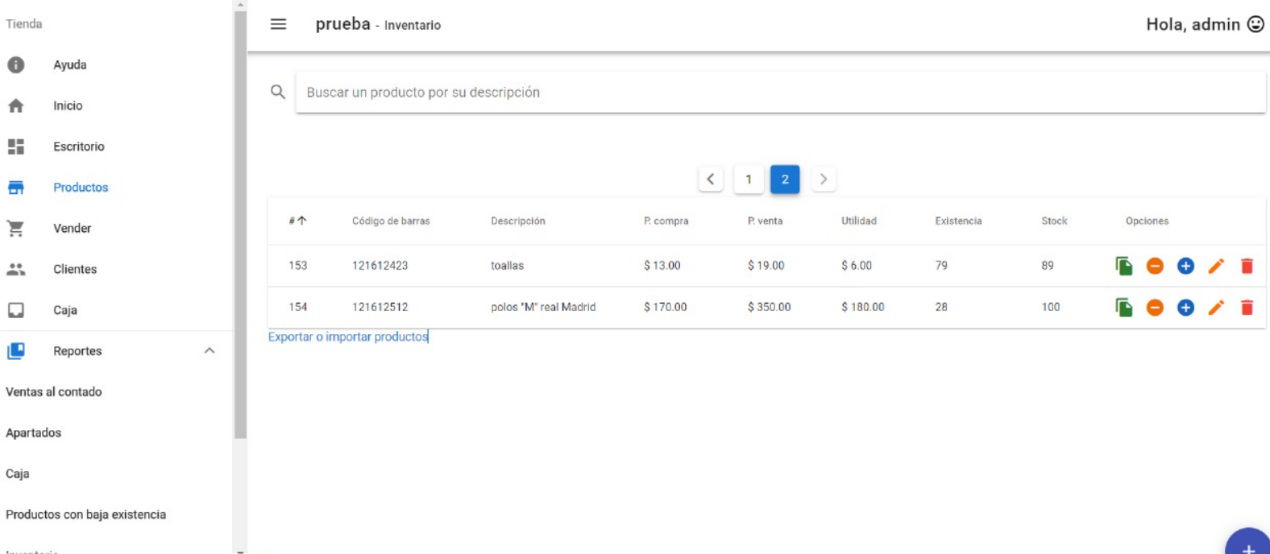
Interfaz de usuario gráfica, Texto, Aplicación

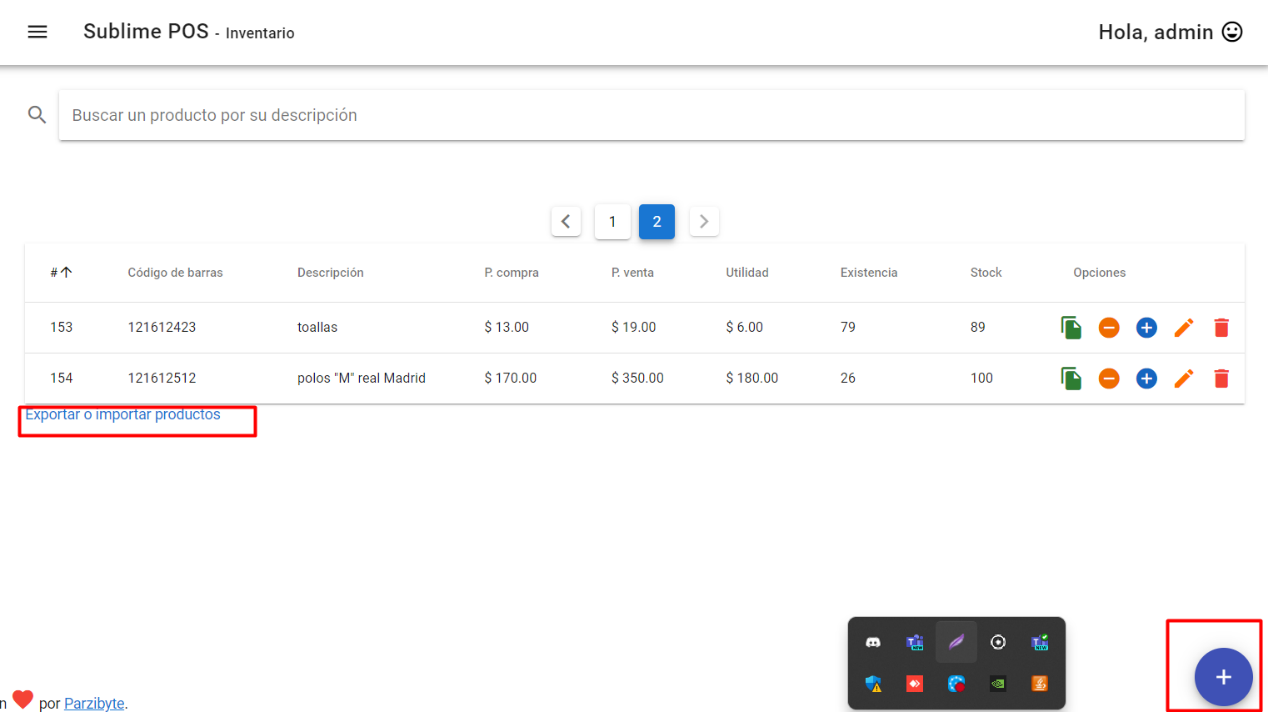
Descripción generada automáticamente

* **Configuraciones**

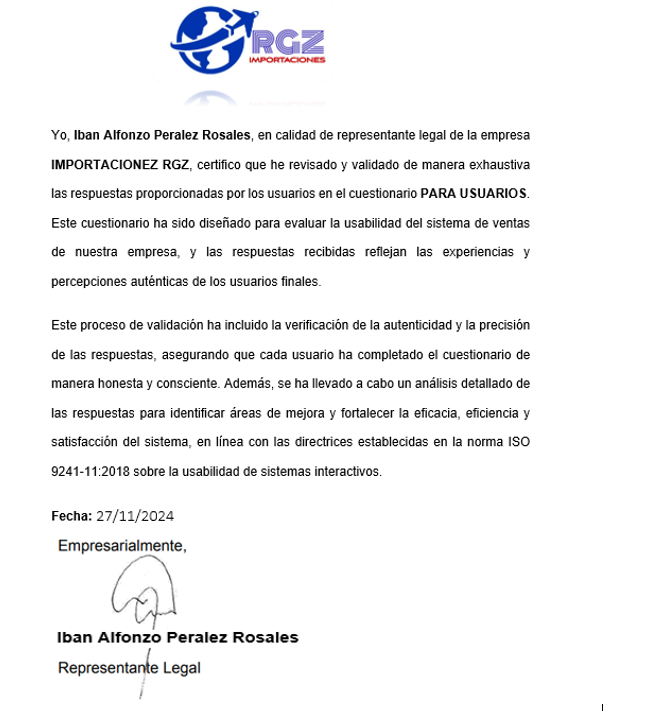
**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**

* **Venta**Gráfico, Gráfico de embudo

  Descripción generada automáticamente**s - Dashborad**
* **Inventario**

**Anexo 3:**

****