**AUDITORÍA DONATELLO**

**YONATHAN NICOLAY JOYA GONZÁLEZ**

**LINO ALFONSO MESA AFRICANO**

**JONATHAN CAMILO FERRUHO ESPITIA**

**UNIVERSIDAD PEDAGIGICA Y TECNOLOGICA DE COLOMBIA**

**INGENIERIA DE SISTEMAS Y COMPUTACIÓN**

**TUNJA**

**2017**

**AUDITORÍA DONATELLO**

**YONATHAN NICOLAY JOYA GONZÁLEZ**

**LINO ALFONSO MESA AFRICANO**

**JONATHAN CAMILO FERRUHO ESPITIA**

**PRESENTADO A:**

**JUAN JOSE CAMARGO VEGA**

**UNIVERSIDAD PEDAGIGICA Y TECNOLOGICA DE COLOMBIA**

**INGENIERIA DE SISTEMAS Y COMPUTACIÓN**

**TUNJA**

**2017**

Contenido

[1. Objetivo general del proyecto 4](#_Toc499194044)

[2. Información general de la empresa 4](#_Toc499194045)

[3. Información general del departamento de sistemas 5](#_Toc499194046)

[4. Censo a nivel de software y hardware 5](#_Toc499194047)

[5. Plano centro de computo 6](#_Toc499194048)

[6. Censo de la documentación 7](#_Toc499194049)

[7. Selección del módulo a auditar 8](#_Toc499194050)

[8. Metodologia Selección del módulo a auditar 10](#_Toc499194051)

[9. Descripción del módulo seleccionado 10](#_Toc499194052)

[10. Flujograma 11](#_Toc499194053)

[11. Descripción de los procesos significativos del Módulo de Facturación 12](#_Toc499194054)

[12. Diseño de archivos y bases de datos 12](#_Toc499194055)

[13. Diseño de entradas y salidas 13](#_Toc499194056)

[14. Guías de evaluación de control interno 13](#_Toc499194057)

[15. Hoja de evaluación de controles 19](#_Toc499194058)

[16. Matriz análisis de riesgo 22](#_Toc499194059)

[17. Deficiencias y recomendaciones 25](#_Toc499194060)

[18. Carta de recomendaciones 25](#_Toc499194061)

# Objetivo general del proyecto

Realizar la auditoría de los sistemas de cómputo de la empresa **Donatello** en la cual se implementa el uso del software licenciado **SAI OPEN** en su versión **9.0.0** seleccionado como aplicación prioritaria para su evaluación de acuerdo con la relevancia que posee, en las principales operaciones de la empresa.

# Información general de la empresa

* **NOMBRE:** Donatello
* **UBICACIÓN:** Calle 33 # 8-33 Mesopotamia (Tunja, Boyacá).
* **MISIÓN:** Somos una empresa enfocada en la prestación de servicios de alimentos propios de un salón de onces, esforzándonos en la calidad del producto, servicio y el bienestar de nuestros clientes.
* **VISIÓN:** Con el favor de Dios queremos llegar a ser en el mediano plazo una empresa con presencia en varios puntos del departamento de Boyacá y a largo plazo estar presentes en varios departamentos de Colombia.
* **OBJETIVOS DE LA EMPRESA:**

Estandarización de nuestros productos y servicios.

Terminar el desarrollo de los productos que solicita el mercado.

Desarrollar e implementar el plan legal del proceso de extensión de la empresa como franquicia.

* **ORGANIGRAMA GENERAL**:

Diagrama 1. Organigrama general

**PROPIETARIO**

**ADMINISTRADOR**

**GENERAL**

**GERENCIA GENERAL DE INFORMÁTICA**

**JEFE DE PUNTO**

**AUXILIAR DE COCINA**

**AUXILIAR DE**

**MESA**

# Información general del departamento de sistemas

Actualmente Donatello cuenta con un departamento de sistemas pequeño debido a que las necesidades requeridas no son de gran envergadura, este departamento se encuentra organizado de la siguiente forma:

Diagrama 2. Organigrama departamento de sistemas

**ADMINISTRADOR**

**GENERAL**

**GERENCIA GENERAL DE INFORMÁTICA**

**SOPORTE Y MANTENIMIENTO**

# Censo a nivel de software y hardware

**Hardware:**

* **Computador de escritorio Compaq SR5420LA:**

Processor: AMD Athlon (tm) II X4 620 Processor 2.60 GHz

Memoria RAM: 4.00 GB

Disco Duro: 500 GB

Conexión Red: Ethernet

Mouse: si

Teclado: si

Monitor: Samsung (21 pulgadas)

Puertos USB: 5

Unidad de DVD: si

* **Impresora Térmica De Recibos Epson TN-T20**
* **Cajón Monedero Metálico SAT Con Conexión RJ11**

**Software:**

* **Sistema Operativo:** Windows 7 profesional Service Pack 1 (64 Bits)
* **Microsoft Office 2010**
* **Adobe Reader version 8.0**
* **Chrome Versión 62.0.3202.94**
* **SAI OPEN versión 9.0.0**

|  |  |
| --- | --- |
| EQUIPO | SOFTWARE |
| Computador de escritorio Compaq SR5420LA | Sistema operativo Windows 7 SP1 |
| Microsoft Office 2010 |
| Google Chrome Versión 62.0.3202.94 |
| SAI OPEN Versión 9.0.0 |
| Adobe Reader Versión 8.0 |
| Impresora TérmicaTN-T20 | Controlador integrado basado en arquitectura Linux x86 |
| Cajón Monedero Metálico SAT | NA |

Tabla 1. Matriz Hardware vs Software

# Plano centro de computo

Vista general del establecimiento:

6 m



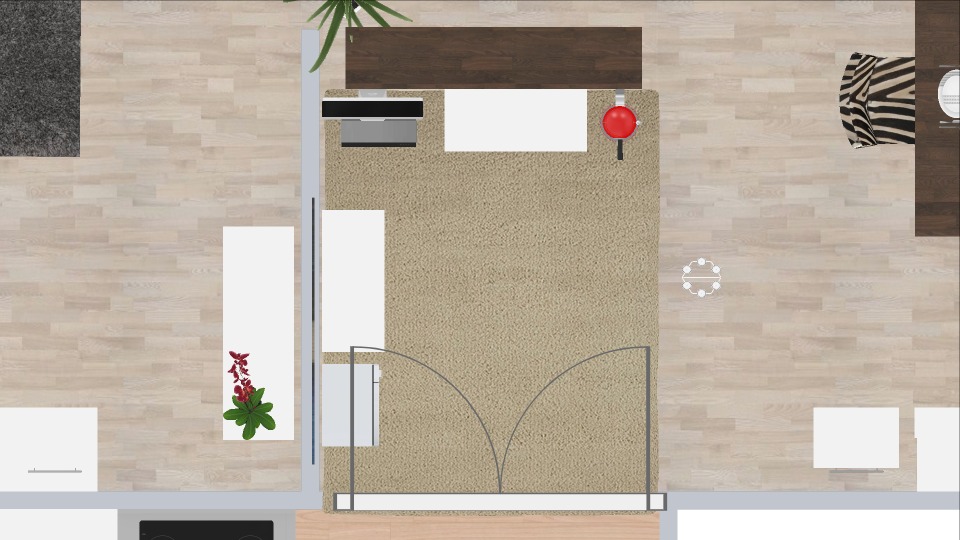
3 m

2 m

Diagrama 3. Plano del establecimiento

Vista del área de facturación:

Es necesario mencionar que el computador se encuentra a una distancia de 30 cm de la impresora y de la caja registradora, además que se encuentra cerca de una máquina de café y un microondas.



120 cm

95 cm

30 cm

30 cm

Diagrama 4. Plano área de facturación



Diagrama 5. Representación 3D de la ubicación de los dispositivos de computo

# Censo de la documentación

La documentación en los aplicativos es indispensable para la prevención de errores y solución de los mismos, además esta brinda una guía de fácil acceso para capacitar al personal en caso de existir dudas en el funcionamiento del aplicativo, por esta razón se presenta a continuación el censo de la documentación respectiva de cada uno de los softwares utilizados en Donatello.

|  |  |  |  |
| --- | --- | --- | --- |
| APLICACIÓN | MANUAL DE USUARIO | MANUAL DE LA OPERACIÓN | MANUAL DE ERRORES |
| **SAI OPEN** | No hay manual de usuario fisco, sin embargo, la aplicación cuanta un módulo de ayuda. | NA | NA |
| **Microsoft Office** | No hay manual de usuario fisco, sin embargo, la aplicación cuanta un módulo de ayuda, y un sistema para solución de errores en línea. | SI | SI |

Tabla 2.Censo de la documentación

# Selección del módulo a auditar

A continuación, se presenta la metodología con el respectivo ponderado para cada criterio utilizada para la selección del módulo a auditar, esta metodología es sugerida por el Ingeniero Juan José Camargo Vega.

* **Criticidad = VALOR FACTOR 1 \* VALOR FACTOR 2 …\* VALOR FACTOR 12**

|  |  |  |
| --- | --- | --- |
| FACTORES | CRITERIOS | PUNTAJE |
| **1.** | Importancia de las cifras  ( )% de activos controlados  ( )% de pasivos controlados  Resultado = (1 + %) |  |
| **2.** | Importancia de los archivos que actualizan:  ( ) Actualiza uno o más archivos clave para la operación de la empresa  ( ) No actualiza archivos clave | **1.25**  **1.00** |
| **3.** | Horas de computador utilizadas actualmente  ( ) Diez Horas  ( ) Entre 10 y 100 Horas  ( ) Entre 100 y 500 Horas  ( ) Entre 500 y 1000 Horas  ( ) Entre 1000 y 10000 Horas  ( ) Más de 10000 | **1.00**  **1.10**  **1.20**  **1.30**  **1.40**  **1.50** |
| **4.** | Requerimientos legales que satisface  ( ) Ninguno  ( ) Uno  ( ) Dos  ( ) Más de dos | **1.00**  **1.25**  **1.50**  **1.75** |
| **5.** | Importancia administrativa de los informes que produce  ( ) No se utilizan para toma de decisiones  ( ) Se utilizan para toma de decisiones | **1.00**  **1.50** |
| **6.** | Relación con otras aplicaciones importantes  ( ) No tiene enlace clave con otras aplicaciones  ( ) Tiene enlace clave con otras aplicaciones | **1.00**  **1.25** |
| **7.** | Rol que juega el control de las operaciones  ( ) No tiene elementos de control importantes  ( ) Tienen elementos de control importantes  ( ) Es de vital importancia para el control operacional | **1.00**  **1.50**  **2.00** |
| **8.** | Participación de los usuarios en el diseño del sistema  ( ) Alta  ( ) Media  ( ) Baja | **1.00**  **1.50**  **2.00** |
| **9.** | Vulnerabilidad del fraude  ( ) Alta  ( ) Media  ( ) Baja | **1.00**  **1.50**  **2.00** |
| **10** | Importancia financiera de la aplicación  ( ) Produce cifras para aceptar los estados financieros  ( ) No produce cifras para afectar los estados financieros | **2.00**  **1.00** |
| **11.** | Edad de la aplicación en años, desde que entró en producción  ( ) Uno o menos  ( ) Entre uno y Cinco  ( ) Más de cinco | **1.00**  **1.50**  **2.00** |
| **12.** | Expectativas de vida de la aplicación  ( ) Próxima a remplazarse  ( ) No está próxima a remplazarse | **1.00**  **1.50** |

Tabla 3. Metodología para cuantificar la Criticidad

* **Esfuerzo de auditoria requerido = Valor del Factor 13 \* Valor del Factor 14 …\* Valor Factor 16.**

|  |  |  |
| --- | --- | --- |
| FACTORES | CRITERIOS | PUNTAJE |
| **13.** | Cantidad de trabajo anual requerido para dar mantenimiento a las aplicaciones en meses/ hombres  ( ) Menos de uno  ( ) Entre uno y cinco  ( ) Entre cinco y diez  ( ) Entre diez y veinte  ( ) Entre veinte y cien  ( ) Mas de cien | **1,0**  **1,2**  **1,4**  **1,6**  **1,8**  **2,0** |
| **14.** | Numero de programas que compone la aplicación  ( ) 1 a 5  ( ) 6 a 10  ( ) 11 a 20  ( ) 21 a 35  ( ) 35 a 60  ( ) Más de 60 | **1,0**  **1,2**  **1,4**  **1,6**  **1,8**  **2,0** |
| **15.** | Participación de la Auditoria en el diseño del sistema  ( ) Alta  ( ) Madia  ( ) Baja | **1,0**  **1,5**  **2,0** |
| **16.** | Tiempo trascurrido desde la última auditoria  ( ) Menos de un año  ( ) Entre 1 y 2  ( ) Más de 2 | **1,0**  **1,5**  **2,0** |

Tabla 4. Metodología para cuantificar el esfuerzo de auditoria

* **Necesidad de auditoria = Criticidad \* Esfuerzo de Auditoria**

# Metodologia Selección del módulo a auditar

**SAI OPEN** es el software elegido para auditar debido a que este aplicativo presenta mayor riesgo de falla en comparación con Microsoft Office, se detectó que la documentación de esta plataforma es obsoleta, tiene un bajo nivel de calidad que no le brinda al usuario la información necesaria para la solución de sus necesidades. A partir de esta identificación se realiza una comparativa entre los módulos de SAI OPEN acorde a las metodologías establecidas para Auditar sistemas, y poder así seleccionar el módulo con mayor riesgo potencial. A continuación, se menciona una descripción de los módulos con los que cuenta la aplicación y su respectivo puntaje obtenido de acuerdo con: Anexo 1 “Metodología de selección de la aplicación a Auditar”.

|  |  |  |
| --- | --- | --- |
| MÓDULOS | DESCRIPCIÓN DE LOS MÓDULOS | PUNTAJE |
| **Facturación** | En este módulo se presenta la información de la venta: tipo de producto, cantidad, precio, impuestos, precio total de la compra permitiendo imprimir y llevar un registro detallado de las ventas. | 334,12 |
| **Inventario** | En este módulo se guarda el registro de los productos con su respectiva especificación detallada, además permite agregar, eliminar y modificar cada registro | 132,89 |
| **Proveedores** | En este módulo se guarda el registro de los proveedores con su respectiva especificación además de permitir: agregar, eliminar y modificar registros. | 47,46 |
| **Reportes** | Este módulo gestiona todos los tipos de reportes que se generan en la empresa, algunos de ellos son presentados a la DIAN. | 56,95 |

Tabla 5. Resultados de comparación según metodología para selección del módulo a auditar

# Descripción del módulo seleccionado

El módulo de facturación es el seleccionado para auditar, este módulo es el puente de unión y comunicación con los módulos de inventario, proveedores y reportes; la finalidad del módulo es ingresar los datos de compra de cada cliente para poder generar los costos por producto y totales de la venta; una vez realizada la compra, este módulo envía los datos para actualizar el inventario y finalmente imprimir la factura que se le dará al cliente.

A continuación, se realiza una breve descripción de cada una de las funcionalidades del módulo para así identificar sus entradas, salidas y procesos

**EMPLEADO**

1. **CREAR FACTURA**:

**Entrada:** Orden de por parte del empleado para la creación de una nueva Factura al software

**Proceso:** El software consulta el numero de la factura, solicita hora y fecha del sistema

**Salida:** Se abre una ventada con información de la factura y un meno en donde el empleado puede completar la factura

1. **ADICIONAR PRODUCTO**:

**Entrada**: código o nombre del producto y si se desea cantidad, si no se ingresa la cantidad el software por defecto colocara cantidad uno

**Proceso**: buscar el producto en la base de datos, calcular el valor total del producto de acuerdo con la cantidad, descuento e impuestos

**Salida:** si encuentra el producto se agrega su información con especificación de precios a la factura de lo contrario envía un mensaje de error

1. **INGRESAR CLIENTE:**

**Entrada:** nombre o identificación del cliente

**Proceso:** buscar el cliente en la base de datos

**Salida:** si encuentra el cliente se agrega su información a la factura de lo contrario envía un mensaje de error

1. **FINALIZAR COMPRA:**

**Entrada:** Orden de por parte del empleado para la finalización de una nueva Factura al software, además de ingresar la forma de pago

**Proceso:** Calcular valor total de la factura de acuerda a la cantidad de productos, descuentos e impuestos, gestionar forma de pago

**Salida:** Cuenta total de la factura y orden de impresión

1. **IMPRIMIR FACTURA:**

**Entrada:** Orden de impresión

**Proceso:** Adecuar la factura a formato de impresión

**Salida:** Factura impresa

# Flujograma

A continuación, se encuentra el flujograma del módulo de Facturación donde se evidencian los diferentes actores que interviene en las operaciones de este módulo.

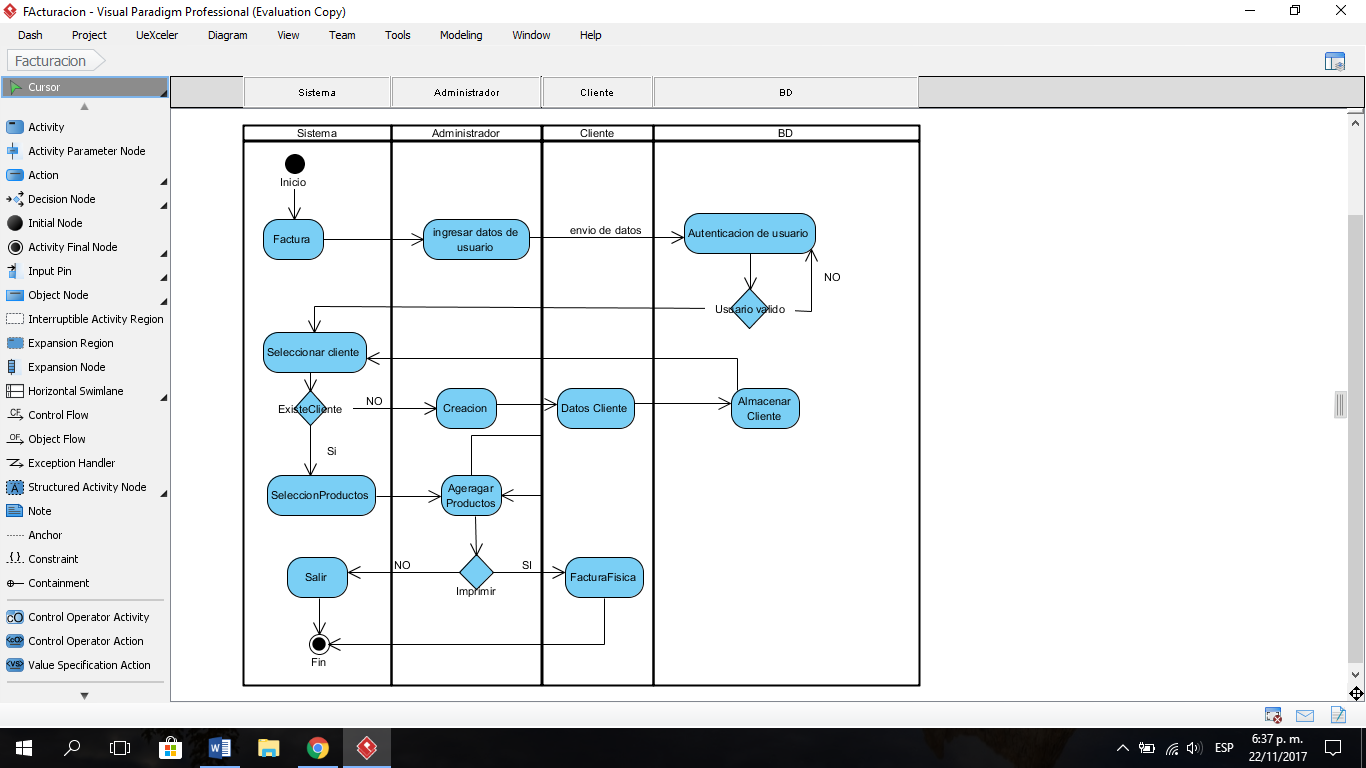


Diagrama 6. Flujograma Módulo Facturación

Véase Anexo 2 “Diagrama Entidad Relación”

# Descripción de los procesos significativos del Módulo de Facturación

**FACTURACIÓN DE VENTA**

**BASE DE DATOS NOVEDADES**

* Agregar datos cliente
* Agregar productos

**MÓDULO**

**INFORMACIÓN INCONSISTENCIAS**

Datos incongruentes

* Documento cliente
* Nombre productos
* Costo producto
* Cantidad
* Fecha de venta
* Intereses
* Descuento

# Diseño de archivos y bases de datos

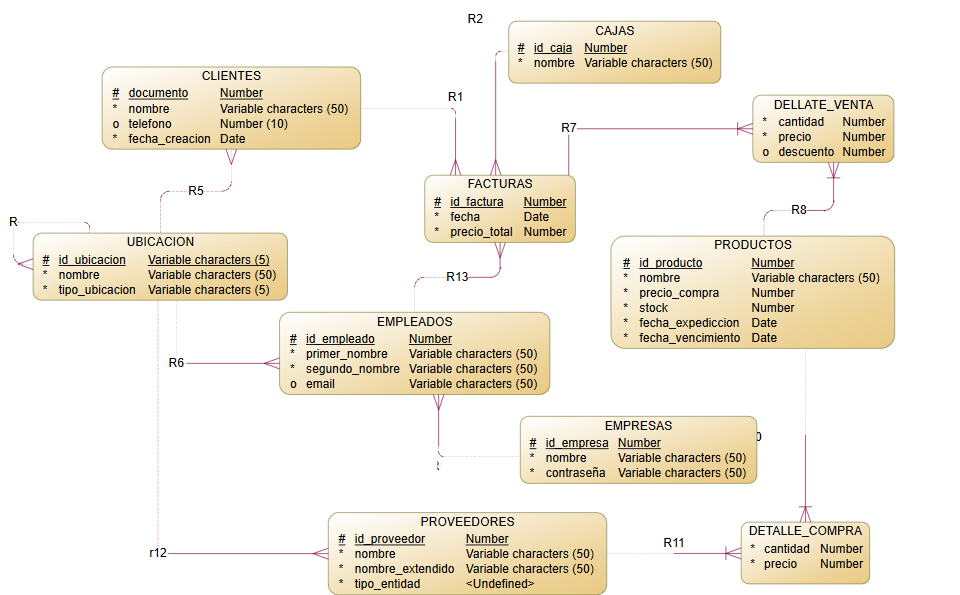
A partir de la observación directa y formatos impresos (Facturas) proporcionados por la empresa se realizó el siguiente diagrama entidad relación: *Véase A*nexo 3 “Diagrama Entidad Relación”.

Diagrama 7. Diagrama entidad relación

# Diseño de entradas y salidas

# Guías de evaluación de control interno

* **Origen de Transacciones**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Revisión de documentación | Se verifica los documentos que van a ser registrados. | X |  |  |
| Firmas autorizadas | Todos los documentos fuentes llevan una firma para facilitar su rastreo. |  | X |  |
| Identificación de planillas | Se enumeran las planillas para evitar duplicados. | X |  |  |
| Retención de documentos fuente | Los documentos contienen la fecha en que fueron recibidos. |  |  | X |
| Acceso controlado a los documentos | Se limita el acceso a los documentos exclusivamente al personal autorizado. | X |  |  |
| Responsabilidad de la corrección de errores | Los errores serán corregidos por parte de la persona que los cometió. | X |  |  |
| Planillas homogéneas | Las planillas se ajustan a las necesidades del usuario. | X |  |  |

*Tabla 4. Fuente: Elaboración propia*

* **Entrada de datos:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Restricción de acceso a los dispositivos de entrada | Se hacen controles de acceso físico a los dispositivos del sistema que se utilizan para la entrada de datos. |  | X |  |
| Control de documentos de ingreso al sistema | Los documentos al momento de su entrada al sistema deben provenir de un área autorizada. | X |  |  |
| Validación sistematizada de los datos | El sistema permite validar los datos que son ingresados. |  | X |  |
| Entrenamiento del personal de operación | Se realiza un entrenamiento para el personal de operación. | X |  |  |
| Soporte de ayuda de formularios | En el ingreso de los datos, la aplicación debe tener mensajes de ayuda, con el fin de facilitar los ingresos de estos y advertir sobre algún error cometido, indicando la clase de error. |  | X |  |
| Atajos del sistema | Se brinda alternativas de ingreso de datos al sistema para mejorar su desempeño en la entrada de los datos | X |  |  |
| Restringir el acceso de los usuarios | Se restringe el acceso a los usuarios de acuerdo con las funciones de cada cargo, disminuyendo el riesgo de que personas no autorizadas puedan leer, modificar, adicionar, eliminar datos. | X |  |  |
| Correcta inclusión de los datos | Se busca que las entradas sean lo más sencillas y están diseñadas de forma que se limiten los datos incorrectos. |  | X |  |
| Evaluar la capacidad en el desempeño de las funciones | Se evalúa las habilidades y el cumplimiento de las funciones por parte de los operadores que interactúan con el sistema. | X |  |  |
| Supervisión de las transacciones | Se hace una verificación de la razonabilidad de los datos tanto manual como en la aplicación. | X |  |  |

*Tabla 5. Fuente: Elaboración propia*

* **Comunicación:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Verificación lógica de las terminales | Se realiza una verificación lógica de las terminales autorizadas para el ingreso al sistema |  |  | X |
| Seguridad de acceso al sistema red | Existe una gestión redes de telecomunicación entre dependencias. |  | X |  |
| Emplear módems de respaldo | Se usan módems de respaldo en los terminales. |  |  | X |
| Registrar errores que se presentan en las terminales | Se registra el tipo de error, hora, fecha, el terminal, el nombre del operador y el número de veces que se presenta el fallo. |  |  | X |
| Guías de procedimientos para la corrección de errores | Se encuentran contenidos los pasos en una guía, para cuando se presentan errores el usuario los interprete y corrija |  | X |  |
| Protocolos de cifrado de datos | Existen políticas de seguridad para todo el circuito de comunicación de datos. |  | X |  |
| Prueba a los equipos y programas. | Se someten a pruebas rigurosas las terminales para corroborar la comunicación de datos. |  | X |  |

*Tabla 5. Fuente: Elaboración propia*

* **Procesamiento de datos:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Código de transacción | Se utiliza códigos de identificación para indicar el tipo de documento | X |  |  |
| Programar revisiones periódicas | Se planifican comprobaciones periódicas por parte de personal especializado a la aplicación a nivel de bases de datos y tiempos de respuesta del sistema |  | X |  |
| Rotación de funciones | Se realiza cambios periódicos de las funciones que realizan los operadores. |  | X |  |
| Capacitación en las funciones | Se ofrecen capacitaciones o elementos instructivos para el cumplimiento de las funciones. | X |  |  |
| Lista de registros pendientes | Se mantiene un registro de los datos que están pendientes por procesar. |  | X |  |

*Tabla 6. Fuente: Elaboración propia*

* **Almacenamiento y recuperación de datos:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Librerías de documentación | Existen librerías donde se almacenan los archivos y documentos correspondientes al sistema. | X |  |  |
| Librerías electrónicas | Existen librerías en plataformas de servicios en la nube para el almacenamiento de archivos que maneja la empresa. |  | X |  |
| Suministro de una nueva versión del sistema | Se brindan versiones nuevas del sistema, debido a fallos presentadas en la versión actual. |  | X |  |
| Librerías para conservar versiones del sistema | Los archivos de los sistemas se dividen en grupos para efectos de control | X |  |  |
| Clasificación de los archivos | Se organizan los documentos por niveles de importancia de acuerdo con un criterio. |  | X |  |
| Protección con contraseñas | Se protegen ciertos archivos mediante contraseñas. | X |  |  |
| Autorización de cambios | Las modificaciones efectuadas de seguridad son autorizadas antes de que se realice la modificación en el sistema. |  | X |  |
| Inspección de archivos | Se realiza una validación a los archivos críticos por parte de un operador, para descubrir archivos incorrectos o ilógicos |  | X |  |
| Hacer uso de Backups | Los archivos no podrán utilizarse sin antes haber sacado una copia para asegurar la recuperación total del archivo |  | X |  |

*Tabla 7. Fuente: Elaboración propia*

* **Salida de información:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Cotejamiento de la información | Se comparan los informes de salida con respecto a la entrada hecha. | X |  |  |
| Registro de salidas | Los informes emitidos por el sistema se registran de acuerdo con sus características más importantes. | X |  |  |
| Procedimientos para el control de salidas | El manual de sistema establece los procedimientos de salida para cada aplicación, ejemplo rotulo, hora y fecha. |  |  | X |
| Identificación de informes | Los informes contienen: Fecha de preparación, descripción, usuario y número de procesamiento. | X |  |  |
| Destrucción de procesos fallidos | Se hace destrucción de todas las transacciones abortadas para evitar efectos fraudulentos. |  | X |  |
| Suprimir informes no autorizados | Se suprimen los informes que ya no necesita el usuario. |  |  | X |
| Examinar los archivos de errores | Se tiene un archivo de errores independiente para su revisión e informe de errores. |  | X |  |
| Implementar procedimientos para la corrección de errores | Los procedimientos para la corrección de errores están definidos por escrito en el manual de usuario de cada aplicación |  | X |  |
| Seguridad para reportes confidenciales | Los reportes reservados permanecen en lugares confiables. |  | X |  |
| Organización de los reportes de salida | Un grupo independiente analiza la calidad de los controles de salida garantizando él envió de reportes a los usuarios |  |  | X |

*Tabla 8. Fuente: Elaboración propia*

* **Seguridad física:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CONTROL | JUSTIFICACIÓN | SI | NO | NA |
| Dispositivos de seguridad que salvaguarden los bienes de la empresa. | Los equipos del sistema están protegidos por alarmas y cámaras de seguridad que notifiquen acciones fraudulentas. |  | X |  |
| Identificación de los bienes | Se lleva un control de las posesiones de la empresa. | X |  |  |
| Contratar empresa de seguridad privada | El sitio de trabajo se debe encontrar vigilado por personal de seguridad para evitar el ingreso de personas no autorizadas. |  | X |  |
| Mecanismo de seguridad | La empresa se encuentra custodiada por mecanismos de apertura y cierre tales como cerraduras de llave o combinación, electrónicas. | X |  |  |
| Normatividad y rutas de salida | La empresa ofrece capacitación al personal para dar a conocer las medidas de protección, seguridad y vías de escape. | X |  |  |
| Ubicación de los equipos de computo | Los equipos se encuentran ubicados en una zona que no implique riesgo de inundación. | X |  |  |
| Sistemas de alimentación de energía. | Se revisa que todas las conexiones del sistema estén en un estado correcto para su funcionamiento y que no presenten daños que impidan la comunicación. |  | X |  |
| Seguridad de ventanas y puertas | Las ventanas y puertas cuentan con mecanismos de seguridad. | X |  |  |
| Uso de dispositivos de alerta. | La empresa cuenta con detectores de calor, humo e incendios. |  | X |  |
| Implementar extintores adecuados al centro de computo | Se encuentran extintores en el centro de cómputo en caso de incendios, fallos eléctricos o emergencia. |  | X |  |
| Uso de energía auxiliar | Existen fuentes de energía alterna que prevengan la caída del sistema y daños en el mismo. |  | X |  |

*Tabla 9. Fuente: Elaboración propia*

# Hoja de evaluación de controles

* **TRANSACCIONES:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **O1** | Revisión de documentación | Se verifica los documentos que van a ser registrados. |
| **O2** | Firmas autorizadas | Todos los documentos fuentes llevan una firma para facilitar su rastreo. |

*Tabla 10. Fuente: Elaboración propia*

* **ENTRADA DE DATOS:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **E1** | Restricción de acceso a los dispositivos de entrada | Se hacen controles de acceso físico a los dispositivos del sistema que se utilizan para la entrada de datos |
| **E2** | Validación sistematizada de los datos | El sistema permite validar los datos que son ingresados. |
| **E3** | Soporte de ayuda en formularios | En el ingreso de datos, se muestran mensajes de ayuda, que previenen al usuario de cometer error referente a mal uso del sistema. |
| **E4** | Correcta inclusión de los datos | Se busca que las entradas sean lo más sencillas y están diseñadas de forma que se limiten los datos incorrectos. |

*Tabla 11. Fuente: Elaboración propia*

* **COMUNICACIÓN:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **C1** | Seguridad de acceso al sistema red | Existe una gestión redes de telecomunicación entre dependencias. |
| **C2** | Guías de procedimientos para la corrección de errores. | Se encuentran contenidos los procedimientos en una guía, cuando se presentan errores para que el usuario los interprete y corrija. |
| **C3** | Protocolos de cifrado de datos. | Existen políticas de seguridad para todo el circuito de comunicación de datos en el sistema. |
| **C4** | Prueba de los equipos y programas. | Se someten a pruebas rigurosas las terminales para corroborar la comunicación de los datos. |

*Tabla 12. Fuente: Elaboración propia*

* **PROCESAMIENTO DE DATOS:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **P1** | Programar revisiones periódicas | Se planifican comprobaciones periódicas por parte de personal especializado a la aplicación a nivel de bases de datos y tiempos de respuesta del sistema |
| **P2** | Rotación de funciones. | Se realizan cambios periódicos en las funciones que realizan los operadores del sistema. |
| **P3** | Lista de registros pendientes. | Se mantiene un registro de los datos que están pendientes por procesar en él sistema. |

*Tabla 13. Fuente: Elaboración propia*

* **ALMACENAMIENTO Y RECUPERACIÓN DE DATOS:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **A1** | Librerías electrónicas | Existen librerías en plataformas de servicios en la nube para el almacenamiento de archivos que maneja la empresa. |
| **A2** | Suministro de una nueva versión del sistema. | Se brindan versiones nuevas del sistema, si ocurre algún fallo en la versión actual. |
| **A3** | Clasificación de los archivos. | Los documentos son organizados por niveles de acuerdo a su nivel de importancia. |
| **A4** | Autorización de cambios. | Las modificaciones efectuadas, por seguridad pasan por un proceso de autorización antes de llegar a realizar cambios en el sistema. |
| **A5** | Inspección de archivos | Se realiza una validación a los archivos críticos por parte de un operador, para descubrir archivos incorrectos o ilógicos. |
| **A6** | Hacer uso de Backus | Los archivos no podrán utilizarse sin antes haber sacado una copia para asegurar la recuperación total del archivo |

*Tabla 14. Fuente: Elaboración propia*

* **SALIDA DE INFORMACIÓN:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **SI1** | Destrucción de procesos fallidos. | Se eliminan todas las transacciones abortadas para evitar usos y efectos fraudulentos. |
| **SI2** | Examinar los archivos de errores. | Se maneja un archivo de errores independiente, para su revisión periódica e informe de estos. |
| **SI3** | Implementar procedimientos para la corrección de errores. | Los procedimientos para la corrección de errores están definidos por escrito en el manual de usuario de cada parte del sistema. |
| **SI4** | Seguridad para reportes confidenciales | Los reportes reservados permanecen en lugares confiables. |

* **SEGURIDAD FÍSICA:**

|  |  |  |
| --- | --- | --- |
| ID | CONTROL | DESCRIPCIÓN |
| **SF1** | Dispositivos de seguridad que salvaguarden los bienes de la empresa. | Los equipos del sistema están protegidos por alarmas y cámaras de seguridad que notifiquen acciones fraudulentas. |
| **SF2** | Contratar empresa de seguridad privada | El sitio de trabajo se debe encontrar vigilado por personal de seguridad para evitar el ingreso de personas no autorizadas y malintencionadas. |
| **SF3** | Sistemas de alimentación de energía. | Se realizan revisiones de todas las conexiones del sistema para verificar su correcto funcionamiento y detectar posibles fallas o daños que existan. |
| **SF4** | Uso de dispositivos de alerta. | La empresa cuenta con detectores de calor, humo e incendios. |
| **SF5** | Implementar extintores adecuados al centro de cómputo. | Se encuentran extintores en el centro de cómputo, para su uso en caso de incendios, fallos eléctricos o cualquier otra emergencia que lo requiera. |
| **SF6** | Uso de energía auxiliar | Existen fuentes de energía alterna que prevengan la caída del sistema y daños en el mismo. |

*Tabla 15. Fuente: Elaboración propia*

# Matriz análisis de riesgo

* 1. **TRASACCIONES:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELA-CIONADO | CON-FIABILI-DAD |
| Información incompleta en la factura | Se presenta inconsistencias en la información que requiere la factura. | Alto | O1 | Alto |
| Autenticidad de la factura | No se cuenta con la marca registrada que brinde la autenticidad de esta | Alto | O2 | Alto |

*Tabla 16. Fuente: Elaboración propia*

* **ENTRADA DE DATOS:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELA-CIONADO | CON-FIABILI-DAD |
| Confiabilidad de los dispositivos | Manipulación y alteración de los dispositivos que hacen parte del sistema | Alto | E1 | Alto |
| Duplicidad en la entrada en datos | Se presenta duplicidad de información en los campos de ingreso. | Alto | E2 | Alto |
| Datos incompletos en la factura. | El sistema no comprueba la completitud del ingreso de los datos. | Medio | E2 | Medio |
| Uso incorrecto de los campos de ingreso. | No existen mensajes de ayuda que indiquen al administrador o empleado si ha cometido algún error. | Alto | E3 | Media |
| Registros erróneos en la entrada de datos al sistema | El administrador desconoce el formato de los datos para su ingreso. | Alto | E4 | Alto |

*Tabla17. Fuente: Elaboración propia*

* **COMUNICACIÓN:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELA-CIONADO | CON-FIABILI-DAD |
| Vulnerabilidad del sistema por medio de la red | El no contar con sistema de seguridad que se encargue de evitar estos accesos | Alto | C1 | Alto |
| Presentación de errores desconocidos | No existe un que permitan conocer cómo proceder en caso de un error. | Medio | C2 | Medio |
| Vulnerabilidad de la información. | No existe un cifrado de seguridad que permita mantener la confidencialidad de los datos. | Medio | C3 | Medio |
| Fallas en los equipos y el sistema. | No se hacen el mantenimiento ni revisiones periódicas del funcionamiento de los equipos y programas del sistema. | Alto | C4 | Alto |

*Tabla 18. Fuente: Elaboración propia*

* **PROCESAMIENTO DE DATOS:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELA-CIONADO | CON-FIABILI-DAD |
| Problemas de rendimiento del sistema | No se realiza un mantenimiento adecuado a la aplicación | Medio | P1 | Medio |
| Desconocimiento de registros pendientes por procesar. | No existe un archivo donde se almacenen lo registros pendientes por procesar. | Alto | P3 | Medio |
| Irregularidades en el cumplimiento de funciones | Falta de conocimiento y experiencia para realizar las actividades | Medio | P2 | Medio |

*Tabla 19. Fuente: Elaboración propia*

* **ALMACENAMIENTO Y RECUPERACIÓN DE DATOS:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELA-CIONADO | CON-FIABILI-DAD |
| Perdida de la información | El sistema no permite que la información almacenada se encuentre en la nube solo de manera local | Alto | A1 | Alto |
| Fallas en el sistema por falta de actualizaciones. | No se cuenta con el control de actualización por parte de empresa propietaria del sistema. | Alto | A2 | Medio |
| Desorganización de Archivos | Los archivos que maneja la empresa no son almacenados de acuerdo a su nivel de importancia | Medio | A3 | Medio |
| Alteración en la información del sistema. | No se cuenta con un proceso de autenticación para la realización de esta actividad. | Alto | A4 | Medio |
| La información almacenada es inconsistente. | No se cuenta con la validación de los archivos que permita determinar este aspecto. | Alto | A5 | Alto |
| Fallas del sistema | No se cuenta con copias de seguridad de los archivos que maneja la empresa | Alto | A6 | Medio |

*Tabla 20. Fuente: Elaboración propia*

* **SALIDA DE INFORMACIÓN:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELACIO-NADO | CON-FIABILI-DAD |
| Acciones de fraude con la información generada. | No se cuenta con la eliminación de archivos generados en transacciones abortadas. | Alto | SI1 | Alto |
| Desconocimiento de los errores del sistema. | No se realiza el registro de los errores presentados por el sistema. | Medio | SI2 | Medio |
| Inconsistencias al momento de solucionar los errores del sistema | En la empresa no se cuenta con el manual de usuario ni documentación que permitan dar soluciones a estos problemas presentados | Medio | SI3 | Medio |
| Vulnerabilidad de la información | La información nos es protegida por el sistema de tal forma que es vulnerable a ser alterada. | Alto | SI4 | Alto |

*Tabla 21. Fuente: Elaboración propia*

* **SEGURIDAD FÍSICA:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ERROR POTENCIAL | POSIBLE CAUSA DEL ERROR | RIESGO INHEREN-TE | CONTROL RELA-CIONADO | CON-FIABILI-DAD |
| Alteración y modificación del sistema | No se cuenta con un sistema de alarma que notifique posibles intentos de fraude | Alto | SF1 | Alto |
| Ingreso de personal ajeno a la empresa | La empresa no cuenta con personal de seguridad que evite el ingreso de personas no autorizadas | Alto | SF2 | Alto |
| Fallas en sistema eléctrico y perdida de información. | No se realiza la verificación periódica de las conexiones eléctricas. | Alto | SF3 | Alto |
| Incendio de las instalaciones de la empresa | No se cuenta con alarmas o detectores de humo que den aviso en caso de incendio. | Alto | SF4 | Alto |
| Problemas para apagar un inicio de incendio | El centro de cómputo no cuenta con extintor que permita prevenir la propagación del incendio. | Alto | SF5 | Alto |
| Perdida de información y daños en el sistema | El sistema no cuenta con unas fuentes auxiliares de energía en caso de fallos en la red eléctrica. | Alto | SF6 | Alto |

*Tabla 22. Fuente: Elaboración propia*

# Deficiencias y recomendaciones

|  |  |
| --- | --- |
| DEFICIENCIA | RECOMENDACIONES |
| A los nuevos empleados se les dificulta aprender a manejar el software | Realizar capacitaciones a los empleados y realizar una guía para el manejo del software |
| No se cuenta con respaldo de información | Crear un respaldo de toda la información en la nube u adquirir otro equipo para el respaldo de la empresa |
| No se cuenta con suministro de luz autónoma en caso de que se valla la luz | Adquirir una fuente de luz autónoma para el computador |
| No hay registro de error generados por el sistema o por los empleados | Se recomienda registrar el tipo de error, la hora, la fecha, el empleado y el número de veces que se presenta el fallo |
| El equipo de cómputo está al alcance de cualquier persona lo que podría generar alteración en los datos | Aislar un poco el equipo de cómputo para evitar manipulación no deseada |
| No se cuenta con personal de seguridad que salvaguarde los bienes de la empresa | Se recomienda contratar un servicio de vigilancia. |
| No se cuenta con un cronograma de mantenimiento del sistema | Se recomienda realizar un cronograma para establecer fechas de mantenimiento al sistema |
| No se cuenta con extintores contra incendios especiales en el centro de cómputo | Implementar extintores al centro de cómputo |

# Carta de recomendaciones