Universidad De Guayaquil

Facultad de Ciencias Matemáticas y Físicas

Carrera de Ingeniería en Software

Asignatura: Construcción de Software

PLAN DE MANTENIMIENTO

Proyecto

Sistema de control de Ferromundo

**Grupo C**

**Integrantes**

* Chiriguaya Alvarez Erick Antonio
* Castro Cañizares Bryan Anderson
* Chilan Roca Jostin Javier
* Villalva Rios Ariel Andres

**Objetivos**

**Objetivo General**

El objetivo general de este plan de mantenimiento para el sistema de control de ventas de FerroMundo es garantizar la disponibilidad, confiabilidad, seguridad y eficiencia continua del sistema a lo largo del tiempo, asegurando que cumpla con las necesidades operativas y comerciales de la ferretería de manera efectiva.

**Objetivos Específicos**

1. **Seguridad del Sistema:**

* Asegurar que el sistema esté protegido contra vulnerabilidades de seguridad.
* Minimizar los riesgos de pérdida de datos y garantizar la integridad de la información.

1. **Rendimiento Optimizado:**

* Mantener un rendimiento óptimo del sistema para garantizar tiempos de respuesta eficientes.
* Identificar y abordar cuellos de botella y mejoras en el rendimiento.

1. **Disponibilidad Continua:**

* Implementar estrategias de copias de seguridad para garantizar la disponibilidad continua de datos.
* Minimizar el tiempo de inactividad no planificado y maximizar la disponibilidad del sistema.

1. **Cumplimiento Normativo:**

* Garantizar que el sistema cumpla con todas las normativas y regulaciones locales y sectoriales aplicables.
* Prepararse para auditorías y revisiones normativas de manera proactiva.

1. **Actualizaciones Funcionales:**

* Implementar actualizaciones que mejoren y amplíen las funcionalidades del sistema.
* Asegurar que el sistema siga siendo relevante y cumpla con las necesidades cambiantes del negocio.

1. **Capacitación Continua:**

* Proporcionar capacitación continua a los usuarios para garantizar un uso eficiente del sistema.
* Mantener a los usuarios informados sobre nuevas funcionalidades y cambios en los procedimientos.

1. **Retiro de Funcionalidades Obsoletas:**

* Identificar y eliminar funcionalidades obsoletas o no utilizadas.
* Optimizar la arquitectura del sistema para mantener la simplicidad y eficiencia.

1. **Adaptabilidad a Cambios:**

* Asegurar que el plan de mantenimiento sea lo suficientemente flexible para adaptarse a cambios en las tecnologías y requisitos comerciales.
* Garantizar que el sistema pueda evolucionar para satisfacer futuras necesidades.

**Etapas del plan de mantenimiento**

* Evaluación del sistema.

Comprende en el análisis exhaustivo del sistema para identificar las áreas de mejora, detectar posibles problemas o errores, evaluar la eficiencia y la efectividad de las operaciones, y determinar si se están cumpliendo los objetivos.

* Capacitación de Usuarios.

Implica proporcionar formación y capacitación a los usuarios del sistema con el fin de garantizar y comprender su funcionamiento, así puedan aprovechar al máximo sus características y sepan cómo utilizarlo de manera efectiva.

* Actualizaciones y Mejoras.

Incluye la implementación de actualizaciones de software, parches de seguridad, correcciones de errores y mejoras funcionales para mantener el sistema actualizado y funcionando de manera óptima. También puede implicar la adición de nuevas características según las necesidades identificadas.

* Auditorías y Revisiones.

Se realizan inspecciones periódicas para verificar la integridad, la seguridad y el cumplimiento de estándares establecidos en el sistema. Esto puede incluir auditorías de seguridad, revisiones de código, evaluaciones de rendimiento, entre otros.

* Retiro de Funcionalidades Obsoletas.

Se identifican y eliminan las funcionalidades o características del sistema que se han vuelto obsoletas, poco utilizadas o que ya no son compatibles con los estándares actuales o muy complejas para los usuarios. Esto ayudara a simplificar el sistema y mantenerlo más eficiente.

**Políticas**

**Actualizaciones de Seguridad**

**Política:** Se realizarán actualizaciones regulares para abordar vulnerabilidades de seguridad identificadas.

**Procedimiento:** Establecer un calendario de actualizaciones de seguridad y realizar pruebas exhaustivas antes de implementarlas en el entorno de producción.

**Política:** Gestión de Acceso y Privacidad de Datos

**Descripción:** Garantizar el control adecuado del acceso a los datos del sistema y la privacidad de la información del cliente.

**Procedimiento:** Implementar políticas de acceso basadas en roles, encriptación de datos y auditorías regulares para verificar y monitorear el acceso.

**Política:** Respaldo y Recuperación de Datos

**Descripción:** Establecer un plan de respaldo robusto para asegurar la recuperación de datos en caso de pérdida o corrupción.

**Procedimiento:** Realizar copias de seguridad periódicas, probar regularmente la recuperación de datos y mantener copias de seguridad fuera del sitio.

**Política:** Cumplimiento de Normativas de Seguridad

**Descripción:** Cumplir con las regulaciones de seguridad y privacidad relevantes para la industria y la localidad.

**Procedimiento:** Mantenerse informado sobre cambios en las normativas, realizar auditorías de cumplimiento y aplicar ajustes según sea necesario.

**Política:** Gestión de Incidentes de Seguridad.

**Descripción:** Establecer un proceso para identificar, reportar y responder a incidentes de seguridad de manera efectiva.

**Procedimiento:** Definir roles y responsabilidades, implementar un sistema de reporte de incidentes y realizar simulacros regulares de respuesta a incidentes.

**Política:** Monitoreo Continuo de Seguridad.

**Descripción:** Implementar un sistema de monitoreo constante para detectar y abordar posibles amenazas de seguridad.

**Procedimiento:** Configurar herramientas de monitoreo, establecer alertas de seguridad y realizar análisis de registros de manera periódica.

**Política:** Evaluación de Vulnerabilidades.

**Descripción:** Identificar y abordar proactivamente las vulnerabilidades del sistema.

**Procedimiento:** Realizar evaluaciones regulares de vulnerabilidades, aplicar parches y actualizaciones de seguridad según sea necesario.

**Política:** Uso Seguro de Contraseñas.

**Descripción:** Garantizar el uso seguro y eficaz de contraseñas para acceder al sistema.

**Procedimiento:** Implementar políticas de complejidad de contraseñas, autenticación de dos factores y realizar auditorías de contraseñas periódicas.

**Política:** Educación y Concienciación en Seguridad

**Descripción:** Fomentar la conciencia de seguridad entre los usuarios y el personal.

**Procedimiento:** Proporcionar entrenamiento regular en seguridad, enviar comunicados sobre buenas prácticas y realizar simulacros de phishing.

**Política:** Evaluación de Seguridad de Terceros

**Descripción:** Evaluar y gestionar los riesgos de seguridad asociados con proveedores y socios externos.

**Procedimiento:** Realizar evaluaciones de seguridad de proveedores, establecer acuerdos contractuales seguros y realizar auditorías regulares.

**Política:** Pruebas de Penetración

**Descripción:** Realizar pruebas de penetración regulares para identificar posibles debilidades en la seguridad del sistema.

**Procedimiento:** Contratar servicios de prueba de penetración, corregir las vulnerabilidades identificadas y actualizar las políticas según los resultados.

Estas políticas adicionales abordan diversos aspectos de la seguridad del sistema y contribuyen a establecer un entorno más seguro y resistente contra posibles amenazas y vulnerabilidades.

**Mantenimiento Preventivo**

**Política:** Se llevarán a cabo tareas de mantenimiento preventivo para evitar problemas potenciales.

**Procedimiento:** Programar revisiones regulares del sistema, realizar limpiezas de base de datos, y optimizar consultas para mejorar el rendimiento.

**Política:** Gestión de Configuración del Sistema

**Descripción:** Controlar y gestionar la configuración del sistema para prevenir configuraciones erróneas o no autorizadas.

**Procedimiento:** Implementar una política de gestión de configuración, mantener registros de cambios y realizar revisiones regulares.

**Política:** Actualización de Documentación del Sistema

**Descripción:** Mantener la documentación del sistema actualizada para reflejar con precisión su configuración y funcionalidades.

**Procedimiento:** Revisar y actualizar la documentación después de cada cambio significativo en la configuración o funcionalidad.

**Política:** Revisión de Logs y Registros

**Descripción:** Monitorear y revisar los registros del sistema para identificar posibles problemas o patrones inusuales.

**Procedimiento:** Establecer protocolos de revisión de registros, configurar alertas para eventos específicos y realizar análisis periódicos.

**Política:** Gestión de Versiones de Software

**Descripción:** Gestionar de manera adecuada las versiones de software para evitar problemas de compatibilidad y asegurar la estabilidad del sistema.

**Procedimiento:** Establecer un proceso de control de versiones, realizar pruebas de compatibilidad y programar actualizaciones planificadas.

**Política:** Evaluación de Desempeño del Hardware

**Descripción:** Monitorizar y evaluar el rendimiento del hardware para anticipar posibles fallos.

**Procedimiento:** Implementar herramientas de monitorización de hardware, programar revisiones periódicas y realizar ajustes según sea necesario.

**Política:** Programación de Mantenimiento Programado

**Descripción:** Planificar y ejecutar tareas de mantenimiento en momentos programados para minimizar el impacto en la operación normal.

**Procedimiento:** Establecer un calendario de mantenimiento, notificar a los usuarios afectados y realizar tareas de mantenimiento en horarios de baja actividad.

**Política:** Pruebas de Estrés y Rendimiento

**Descripción:** Realizar pruebas de estrés y rendimiento para identificar y abordar posibles problemas bajo cargas extremas.

**Procedimiento:** Programar pruebas de estrés regulares, analizar los resultados y realizar ajustes en la capacidad según sea necesario.

**Política:** Actualización de Herramientas de Desarrollo

**Descripción:** Mantener actualizadas las herramientas de desarrollo para aprovechar las mejoras y corregir posibles problemas de compatibilidad.

**Procedimiento:** Establecer un calendario de actualización de herramientas, realizar pruebas antes de la implementación y documentar cambios.

**Política:** Optimización de Procesos de Mantenimiento

**Descripción:** Revisar regularmente los procedimientos existentes para encontrar oportunidades de mejora y eficiencia en las tareas de mantenimiento.

**Procedimiento:** Realizar el funcionamiento adecuado y optimizado de cada uno de los procesos o tareas.

**Política:** Evaluación de Vulnerabilidades de Configuración

**Descripción:** Identificar y corregir posibles vulnerabilidades en la configuración del sistema.

**Procedimiento:** Realizar evaluaciones de vulnerabilidades de configuración, aplicar correcciones y documentar los cambios realizados.

**Política:** Análisis de Tendencias de Problemas

**Descripción:** Analizar tendencias de problemas para anticipar y prevenir posibles fallas recurrentes.

**Procedimiento**: Mantener registros de problemas, analizar patrones y tomar medidas preventivas basadas en los datos recopilados.

**Política:** Adaptación a Tecnologías Emergentes

**Descripción:** Integrar de Nuevas Tecnologías para mayor eficiencia y un mejor funcionamiento

**Procedimiento**: Evaluar, adoptar y adaptar nuevas tecnologías de manera segura y efectiva que permitan un mejor manejo del sistema.

**Política:** Actualización de Normativas

**Descripción:** Actualizar las políticas con las normativas cambiantes en el ámbito de la seguridad informática y protección de datos.

**Procedimiento:** Realizar backups cada cierto tiempo para tener un respaldo de como ha venido funcionando el sistema y que falencias ha tenido.

**Política:** Actualización de Normativas

**Descripción:** Actualizar las políticas con las normativas cambiantes en el ámbito de la seguridad informática y protección de datos.

**Procedimiento:** Realizar backups o un respaldo de las normativas antiguas cada que se actualicen para tener una referencia de como ha venido funcionando el sistema y que falencias ha tenido.

**Política**: Recuperación ante Desastres

**Descripción**: Establecer medidas para recuperar los datos y restablecer las operaciones en situaciones extremas o de desastre.

**Procedimiento**: Realizar simulacros regulares de recuperación ante desastres, probar la eficacia de las copias de seguridad y tener un plan de acción claro para restaurar los sistemas críticos.