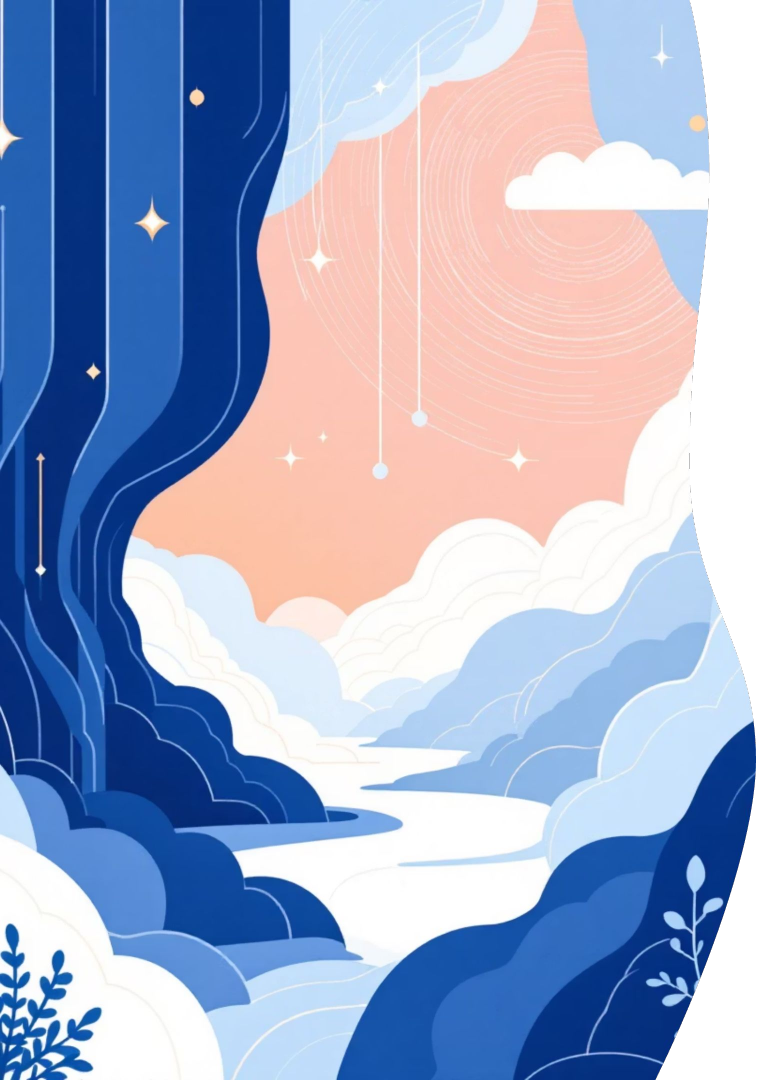


Auditoría al Ciclo de Vida del Software

Integrantes:

- Medina Vertiz Yerson Yassir
- Ore Gonzales Diego Isaac
- Rodriguez Santiago Luis Gerardo
- Rivera Velazco Mauricio Gabriel

Auditoría al Ciclo de Vida del Software

La auditoría revisa todas las etapas del software, desde su concepción hasta su retiro, para asegurar que cada fase cumpla con normas y buenas prácticas.

Requisitos y Diseño

Verifica la correcta recopilación de necesidades y la estructura del sistema.

Programación y Pruebas

Asegura estándares de codificación, control de versiones y validación del software.

Implementación y Mantenimiento

Revisa los procedimientos de despliegue, actualización y gestión de incidentes.

https://drive.google.com/drive/folders/1g7yPzHfJxx4YMjerykFGG0eQgMzGd-dZ?usp=sharing

Fundamentos de la Auditoría

La auditoría se basa en normas, criterios y procedimientos formales para garantizar una revisión objetiva y profesional.

Normas y Estándares

Guías como ISO 12207, ISO 27001, COBIT, ITIL y ISO 9001 definen cómo deben ser los procesos.

Metodología de Auditoría

Un procedimiento estructurado que incluye planificación, recolección de evidencias, evaluación, documentación e informe.

Concepto de Auditoría

Una evaluación independiente, objetiva y documentada, basada en evidencia, no en opiniones.

Evaluación de Procesos y Controles

Se analiza si los procesos internos y los controles implementados funcionan y cumplen las normativas, garantizando seguridad y eficiencia.

El Auditor Evalúa:

- Documentación y seguimiento de procesos.
- Seguridad y eficiencia de los procesos.
- Existencia de controles para prevenir errores.
- Capacitación del personal y cumplimiento de políticas.

Controles Revisados:

- Políticas de contraseñas y roles.
- Logs y registros de actividad.
- Control de versiones y revisión de código.
- Controles de acceso físico a servidores.

Integridad de Datos y Eficiencia de Recursos

Este punto se centra en la calidad de la información y el rendimiento del sistema, evitando gastos innecesarios y fallas.

Integridad de Datos

Los datos deben ser correctos, consistentes, completos y accesibles solo para autorizados.

- Respaldos y restauraciones.
- Controles de acceso y validaciones.
- Registro de modificaciones y encriptación.

Eficiencia de Recursos

Evalúa el uso óptimo de recursos tecnológicos para evitar saturación y lentitud.

- Uso adecuado de almacenamiento y licencias.
- Mantenimiento de equipos.
- Sistemas que no consuman recursos excesivos.

Normas, Buenas Prácticas y Políticas de Seguridad

La auditoría se fundamenta en normas internacionales y políticas internas para asegurar la seguridad y el cumplimiento.

1

Normas Internacionales

ISO 27001 (seguridad), ISO 20000 (servicios TI), ISO 12207 (ciclo de vida), COBIT (control de TI).

2

Políticas de Seguridad

Reglas internas sobre contraseñas, acceso autorizado, protección de datos, antivirus y manejo de incidentes.

Se verifica que estas políticas estén actualizadas y se cumplan rigurosamente.

Gestión de Riesgos y Controles

La auditoría identifica riesgos potenciales y evalúa la eficacia de los controles para mitigarlos, proponiendo mejoras.

Tipos de Riesgos

- Técnicos (fallas, vulnerabilidades).
- Humanos (mala manipulación).
- Operativos (procesos deficientes).
- Externos (ataques, desastres).

Tipos de Controles

- Preventivos (firewalls, autenticación).
- Detectivos (logs, monitoreo).
- Correctivos (restauración de backups, parches).

Guía de Auditoría y Checklists

Estos documentos estructuran el proceso de auditoría, asegurando que no se omita ningún aspecto importante.

1

Guía de Auditoría

Define el alcance, normas, métodos de recolección de evidencias, herramientas, fechas y responsables.

2

Checklists

Listas de verificación basadas en normas para evaluar políticas, seguridad, accesos, procesos y documentación.

Informe Final de Auditoría

El informe final es el producto clave de la auditoría, presentando hallazgos, análisis y recomendaciones para la mejora continua.

Contenido del Informe

Incluye hallazgos, criterios, evidencias, análisis, impacto, recomendaciones, prioridad y plazos.

Impacto

Ayuda a la organización a mejorar sus procesos, seguridad y calidad del sistema.

El Ciclo de Vida del Software y su Auditoría

https://drive.google.com/drive/folders/1olXIFKEM1nmz9z1L1QA5T7BwXUNn3S9Z

Fundamentos del Ciclo de Vida del Software (SDLC)

Fases Estructuradas

Un conjunto de etapas organizadas y bien definidas para guiar el desarrollo de software, desde la concepción hasta la implementación y el mantenimiento.

Calidad y Conformidad

Garantiza el orden en el proceso, la calidad del producto final y el cumplimiento de los requisitos establecidos al inicio del proyecto.

Base para Auditorías

Proporciona un marco sólido para aplicar revisiones y evaluaciones en cada fase, asegurando la adherencia a los estándares y las buenas prácticas.

Modelo en Cascada: La Aproximación Clásica

Un Enfoque Secuencial Riguroso

El modelo en cascada, popularizado por Pressman (2005), propone un flujo lineal y secuencial, donde cada fase debe completarse antes de pasar a la siguiente.

Ventaja: Claridad en las fases y documentación exhaustiva.

Limitación: Poca flexibilidad para adaptarse a cambios una vez iniciadas las etapas posteriores.

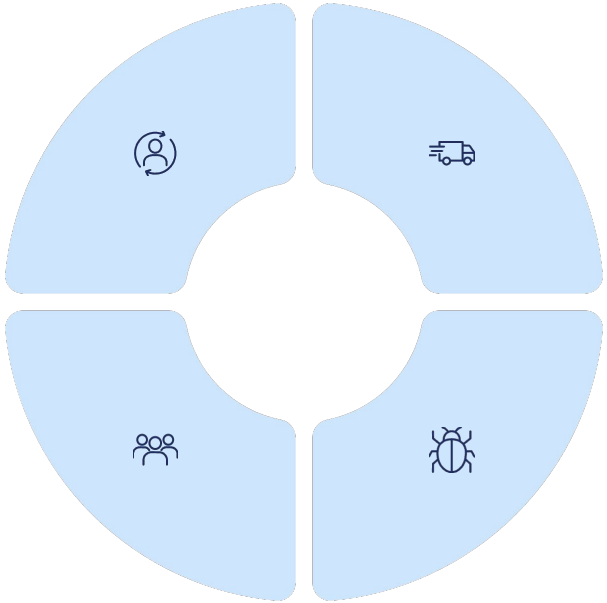
Metodologías Ágiles: Flexibilidad y Adaptación

Desarrollo Iterativo

Se basa en ciclos cortos de desarrollo, con entregas continuas y mejora incremental del producto.

Auditoría en Sprints

La auditoría se enfoca en la disciplina de los sprints, la efectividad de las retrospectivas y el cumplimiento de los principios ágiles.



Entregas Frecuentes

Prioriza la entrega temprana y constante de valor al cliente, mediante lanzamientos parciales y funcionales.

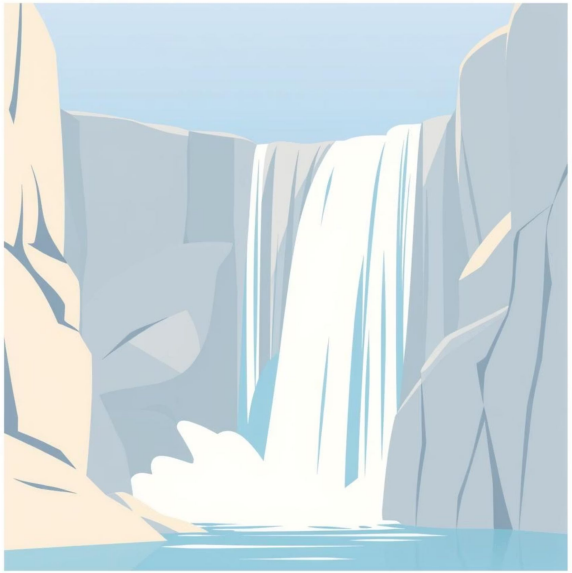
Respuesta al Cambio

Permite una adaptación rápida y eficiente a los cambios de requisitos o prioridades del negocio.

Las metodologías ágiles como Scrum o Kanban, fomentan la colaboración, la autoorganización y la rápida respuesta a los cambios.

Cascada vs. Ágil: Un Contraste Esencial

Modelo en Cascada



Rigidez Estructural: Proceso lineal y poco tolerante a cambios tardíos.

Control Documental: Énfasis en la documentación exhaustiva en cada fase.

Predictibilidad: Mayor predictibilidad en costos y tiempos si los requisitos son estables.

Metodologías Ágiles

Flexibilidad Adaptativa: Capacidad de ajustarse a requisitos cambiantes durante el desarrollo.

Colaboración Continua: Interacción constante entre el equipo y los stakeholders.

Entrega de Valor: Enfoque en la entrega de incrementos funcionales de software.

La auditoría evalúa la conformidad con la metodología elegida, asegurando que se sigan sus principios y procesos definidos.

Auditoría Integral en el Ciclo de Vida

Verificación por Fase

Asegura el cumplimiento y la calidad en cada etapa del desarrollo, desde la planificación hasta la implementación.

Detección de Brechas

Identifica desviaciones en requisitos, diseño, codificación, pruebas y mantenimiento, mitigando riesgos.

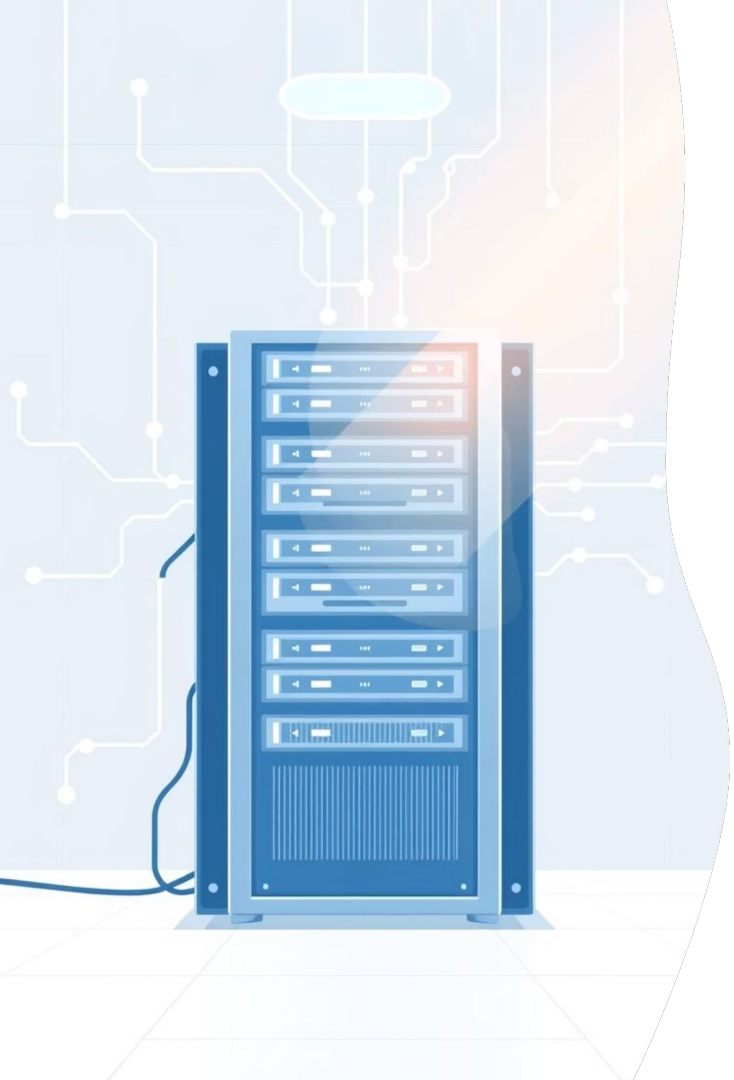
Guías y Checklists

Utiliza herramientas estandarizadas para medir la calidad, productividad y eficiencia de los procesos.

Una auditoría efectiva es clave para garantizar la robustez, seguridad y funcionalidad del software.

Normas y Marcos de Referencia en la Auditoría de Software

La auditoría de software se apoya en estándares internacionales y marcos de referencia para evaluar y mejorar los procesos.



ISO 27001:2013 - Gestión de Seguridad de la Información

Desarrollo Seguro

Aplica controles específicos para asegurar la protección de datos e información sensible a lo largo de todo el ciclo de vida del software.

- Confidencialidad
- Integridad
- Disponibilidad

Estándar Global

Norma internacional para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La auditoría valida que las políticas de seguridad se implementen y mantengan de manera efectiva, reduciendo vulnerabilidades.

CMMI y COBIT: Madurez y Gobierno de TI

CMMI: Madurez de Procesos

El Modelo de Capacidad y Madurez Integrado evalúa la madurez de los procesos de desarrollo de software, desde un nivel inicial hasta la optimización continua.

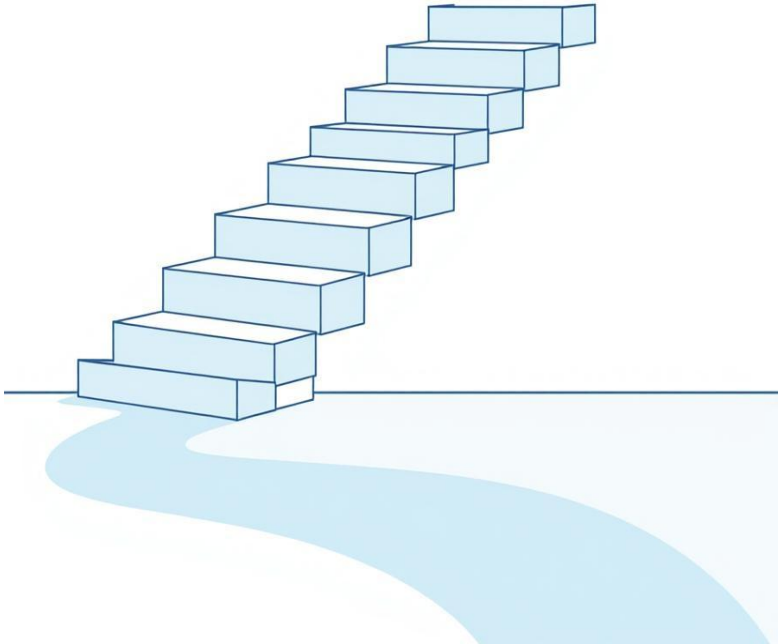
- Mide el nivel de capacidad actual.
- Recomienda áreas de mejora.

COBIT: Gobierno y Control de TI

Marco de referencia para la gobernanza y gestión de TI, que permite a las organizaciones alinear sus objetivos de TI con los del negocio.

- Define procesos y objetivos de control.
- Alinear TI con la estrategia empresarial.

La auditoría utiliza CMMI para diagnosticar la capacidad del equipo de desarrollo y COBIT para asegurar que las inversiones en TI generen valor y gestionan riesgos.



ITIL e ISO: Gestión de Servicios y Calidad

ITIL: Gestión de Servicios de TI

Biblioteca de Infraestructura de Tecnologías de la Información, un marco de buenas prácticas para la gestión de servicios de TI, enfocándose en el ciclo de vida del servicio.

- Gestión de incidentes y problemas.
- Gestión de cambios y liberaciones.

Estas normas son fundamentales para auditar no sólo los procesos, sino también la calidad final del producto de software.

ISO 19011 y 25000: Directrices de Auditoría y Calidad

ISO 19011 proporciona directrices para la auditoría de sistemas de gestión, mientras que ISO 25000 (SQuaRE) especifica los requisitos para la evaluación de la calidad del software.

- Funcionalidad, fiabilidad y usabilidad (ISO 25000).
- Directrices para realizar auditorías (ISO 19011).

Definiendo el Control Interno y su Aplicación

¿Qué es el Control Interno?

Es el conjunto de medidas, políticas y procedimientos diseñados para proteger los procesos de desarrollo contra errores, fraudes y desperdicios. Se fundamenta en marcos como **COBIT 2019** para la gobernanza de TI, **ISO/IEC 27001:2013** para la gestión de seguridad de la información, y **CMMI-DEV v2.0** para la mejora de procesos. Su objetivo es asegurar la integridad, confidencialidad y disponibilidad de la información y los sistemas.

Aplicación Estratégica en el Ciclo de Vida del Software

El control interno se integra en cada etapa del desarrollo del software, desde la concepción hasta el mantenimiento, asegurando la calidad y seguridad conforme a estándares internacionales.

Análisis de Requisitos

Validación y documentación clara de necesidades del usuario, aplicando los procesos de requisitos de **ISO/IEC 12207:2017** y considerando las directrices de seguridad de **NIST SP 800-64**.

Mantenimiento

Control riguroso de cambios y gestión de incidencias, adhiriéndose a los procesos de mantenimiento de **ISO/IEC 12207:2017**, la gestión de riesgos de **ISO/IEC 27001:2013** y las prácticas de mejora continua de **CMMI-DEV v2.0**.

Diseño

Revisión de estándares de arquitectura y seguridad, siguiendo las prácticas de **ISO/IEC 12207:2017**, implementando controles de **ISO/IEC 27001:2013** y garantizando atributos de calidad según **ISO/IEC 25010:2011 (SQuaRE)**.

Codificación

Controles de calidad del código, revisiones por pares y pruebas unitarias, en línea con los procesos de implementación de **ISO/IEC 12207:2017** y las prácticas de desarrollo seguras de **CMMI-DEV v2.0**.

Pruebas

Asegurar cobertura y trazabilidad de casos de prueba, verificando el cumplimiento de los requisitos de calidad y seguridad según **ISO/IEC 25010:2011** y **ISO/IEC 12207:2017**.

https://drive.google.com/file/d/1_qhlwJr-eKYh7J1Tu9Wc8kbW0O-N7cAw/view?usp=sharing

Eficacia vs. Eficiencia en la Auditoría

Eficacia: ¿Se cumplen los objetivos?

- ¿Se completan los requisitos de cada fase del ciclo?
- ¿Los entregables son funcionales y alineados a las expectativas?
- ¿Las pruebas son exitosas y demuestran la calidad del software?

La eficacia se centra en alcanzar los resultados deseados, lo que implica cumplir los principios de gestión de calidad de **ISO 9001:2015**.

Eficiencia: ¿Se utilizan los recursos de forma óptima?

- ¿Los tiempos de entrega son adecuados y competitivos?
- ¿Los costos de desarrollo se mantienen dentro del presupuesto?
- ¿Existe reutilización de componentes y procesos optimizados?

La eficiencia evalúa el uso de recursos para lograr esos resultados, alineándose con los procesos de medición de software de **ISO/IEC 15939:2017**.

Indicadores Clave para Medir Ambas

Productividad del Equipo

Mide la capacidad de entrega y el rendimiento del equipo, utilizando **métricas de velocidad (velocity metrics)** y conforme a las prácticas de **CMMI (Measurement and Analysis Process Area)**.

Calidad del Software

Cuantifica la robustez mediante el **análisis de la densidad de defectos (defect density rates)**, los **porcentajes de cobertura de código (code coverage percentages)** y métricas de calidad definidas por **ISO/IEC 25022:2016**.

Cumplimiento de Plazos

Evalúa la adherencia a los cronogramas definidos, supervisando la desviación respecto a la planificación original y aplicando los procesos de medición de software establecidos por **ISO/IEC 15939:2017**.

La auditoría es crucial para medir ambos aspectos de forma técnica y ofrecer recomendaciones que optimicen el desarrollo de software y aseguren la conformidad con estándares.

Estrategias de Planificación y Ejecución de la Auditoría

Planificación Rigurosa

1

Definir Alcance y Objetivos

Especificar qué fases se auditarán y qué se busca evaluar (calidad, seguridad, cumplimiento).

2

Normas y Metodologías Clave

Utilizar marcos reconocidos: **ISO 19011:2018** para directrices de auditoría, **ISO/IEC 27001:2013 Anexo A** para seguridad en desarrollo, **COBIT 2019** (dominios APO y BAI) para planificación de auditorías, e **ITIL 4** para consideraciones del sistema de valor de servicio.

3

Diseño de la Guía de Auditoría

Crear checklists detallados con preguntas por fase, como: "¿Se documentan los requisitos con trazabilidad?".

Ejecución Detallada

Recolección de Evidencias

- Entrevistas estructuradas con responsables y equipos clave.

Observación directa de procesos de desarrollo y pruebas, aplicando **métodos de muestreo estadístico** para la selección de artefactos.

Revisión exhaustiva de documentación: manuales de usuario, especificaciones de requisitos, planes de prueba, informes de incidentes, código fuente y **registros de auditoría (audit trails)**.
Análisis de **enfoques de auditoría basados en riesgos** para priorizar áreas críticas.

Aplicación de Guías y Evaluación

- Aplicación de preguntas cerradas para verificar la conformidad con los estándares.
- Uso de preguntas abiertas para obtener información cualitativa y percepciones del equipo.

Evaluación sistemática contra normas como **ISO 25000** (calidad de software), **ISO 19011:2018** (directrices de auditoría) y **ISO/IEC 33001:2015** para la evaluación de procesos.

Los resultados esperados son la identificación clara de brechas, riesgos y oportunidades de mejora, sentando las bases para acciones correctivas.

Informe de Auditoría y Recomendaciones

El Informe: Claridad y Evidencia

El informe de auditoría presenta los hallazgos de manera estructurada y basada en evidencias, siguiendo las directrices de **ISO 19011:2018** para la elaboración de informes. Se clasifica por fase del ciclo de vida del software, detallando el grado de cumplimiento frente a las normas y metodologías aplicadas.

Hallazgos: Desglose por fase del ciclo de vida del software, priorizando según impacto (crítico, alto, medio, bajo).

Evidencias: Documentación de respaldo y artefactos verificados para cada observación.

Cumplimiento: Evaluación frente a estándares como la serie **ISO/IEC 25000 (SQuaRE)** para la calidad del software y métodos de evaluación **CMMI (SCAMPI A, B, C)** para la madurez de procesos.

Recomendaciones: Impulsando la Mejora Continua

Las recomendaciones se formulan para abordar los hallazgos, priorizadas por impacto y viabilidad, y se alinean con marcos de remediación y procesos de acción correctiva. Se clasifican como críticas, altas, medias o bajas.

Optimizar Tiempos y Recursos

Implementar métricas de rendimiento basadas en **ISO/IEC 20000-1:2018** para servicios de TI, y refinar la estimación de esfuerzo mediante técnicas como Puntos de Función Ajustados o COCOMO II. (Prioridad: Alta)

Fortalecer Control de Calidad

Establecer un proceso de revisión por pares basado en checklists y un plan de pruebas automatizadas que cubra unitarias, integración y aceptación, asegurando la trazabilidad de requisitos a pruebas. (Prioridad: Crítica)

Adoptar Metodologías Ágiles

Implementar prácticas Scrum/Kanban con iteraciones cortas, ceremonias definidas (planificación, daily, review, retrospectiva) y un backlog priorizado. Capacitar al equipo en roles y responsabilidades ágiles. (Prioridad: Media)

Implementar Seguridad

Integrar el **NIST Cybersecurity Framework**, aplicando controles de seguridad desde la fase de diseño (Security by Design), realizando análisis estáticos y dinámicos de código (SAST/DAST), y gestionando vulnerabilidades. (Prioridad: Crítica)

> La auditoría de control interno no es solo una evaluación, sino una herramienta estratégica de valor agregado que garantiza la calidad, seguridad y eficiencia en el desarrollo de software, impulsando la excelencia operacional.

Mejora Continua y Seguimiento Post-Auditoría

La fase post-auditoría es crucial para transformar los hallazgos en acciones tangibles y sostenibles que impulsen la madurez organizacional. Este capítulo detalla los mecanismos para asegurar que las recomendaciones no solo se implementen, sino que también generen un impacto positivo y medible en el ciclo de vida del desarrollo de software, adhiriéndose a estándares internacionales como ISO 19011:2018 e ISO/IEC 20000-1:2018.

Acciones Correctivas y Preventivas (CAPA)

Implementación sistemática de soluciones para eliminar las causas de las no conformidades detectadas en la auditoría, con un enfoque en la mejora de procesos y la prevención de recurrencias futuras.

Ciclo PDCA

La aplicación del ciclo "Planificar, Hacer, Verificar, Actuar" (PDCA) garantiza una evolución iterativa y constante. Es fundamental para integrar las acciones de mejora en la cultura de desarrollo.

Auditorías de Seguimiento

Procesos periódicos para verificar la efectividad de las CAPA implementadas y la adherencia a los planes de mejora, conforme a las directrices de ISO 19011:2018 para sistemas de gestión.