

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Establecer la Política de Gestión de Configuración**

**Competencias Básicas del Auditor**

**1. Conocimiento en Sistemas de Información y Arquitecturas de TI:** Un auditor debe comprender cómo funcionan los sistemas de información, incluyendo hardware, software, redes y bases de datos. Debe estar familiarizado con las arquitecturas de TI más comunes y cómo se interconectan sus componentes.

**2.Entendimiento de Estándares y Marcos de Ciberseguridad:** Es esencial que el auditor conozca y comprenda los estándares y marcos de referencia en ciberseguridad, como ISO 27001, NIST SP 800-53 y CIS Controls. Estos proporcionan las mejores prácticas y directrices para la gestión de la configuración y otros aspectos de la ciberseguridad.

**3.Habilidades en Herramientas de Auditoría y Análisis:** El auditor debe ser competente en el uso de herramientas específicas de auditoría que permitan evaluar y analizar configuraciones, detectar vulnerabilidades y validar la conformidad con las políticas y estándares establecidos.

**4.Conocimiento en Gestión de Cambios y Control de Versiones:** Dado que la gestión de la configuración implica cambios constantes, el auditor debe entender cómo se gestionan, aprueban y documentan estos cambios. Además, debe conocer sistemas de control de versiones para rastrear y validar las modificaciones en los CIs.

**5.Competencia en Evaluación de Riesgos y Análisis de Impacto:** El auditor debe ser capaz de identificar y evaluar riesgos asociados con configuraciones inadecuadas o no autorizadas. Además, debe poder determinar el impacto potencial de cualquier desviación o vulnerabilidad en la seguridad y operatividad del sistema.

# Visión General

El establecimiento de políticas claras para la gestión de la configuración permite estructurar los procesos operativos de manera eficiente y alineada con las regulaciones aplicables. Estas políticas proporcionan una base para definir responsabilidades, coordinar entre entidades organizativas y garantizar el cumplimiento normativo en la administración de cambios y configuraciones críticas.

**1.1 Implementación de la Política de Gestión de Configuración**

Para lograr una aplicación eficaz, es necesario desarrollar y documentar una política integral que abarque el propósito, alcance, roles y compromisos de la administración. La política debe incluir procedimientos detallados que respalden su implementación y controles asociados, asegurando que se asignen responsables para supervisar su desarrollo y difusión. Es imprescindible que estas políticas sean compatibles con las leyes y estándares vigentes, estableciendo un marco que facilite la coordinación entre las áreas de la organización.

**1.2 Auditoría y Actualización Continua**

Desde el punto de vista de auditoría, se debe verificar que la política documentada se aplique de manera uniforme y que los procedimientos definidos sean efectivos para prevenir configuraciones indebidas o no autorizadas. La auditoría debe enfocarse en la revisión de registros que evidencien el cumplimiento de los controles, así como en la periodicidad y calidad de las actualizaciones realizadas. La designación de responsables claros y la existencia de un plan de revisión continua garantizan que las políticas se mantengan vigentes y alineadas con las necesidades organizativas y normativas actuales.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Desarrollar, documentar y difundir en la organización una política de gestión de configuración que aborde el propósito el alcance, los roles, las responsabilidades, el compromiso de la administración, la coordinación entre las entidades organizativas y el cumplimiento. 2. Asegurar que la política de gestión de la configuración es consistente con las leyes, directivas, regulaciones, políticas, estándares y pautas aplicables |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir procedimientos para facilitar la implementación de la directiva de administración de configuración y los controles de administración de configuración asociados. 2. Designar a un responsable para gestionar el desarrollo, la documentación y la difusión de la política y los procedimientos de gestión de la configuración |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar y actualizar la política y los procedimientos actuales de gestión de la configuración |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. |  |

1. **Preguntas de Auditoría para Establecer la Política de Gestión de Configuración**

|  |
| --- |
| Temática: Objetivos y Alcance de la Política de Gestión de Cambios |
| Los objetivos y alcance de la política de gestión de cambios establecen las metas fundamentales y los límites dentro de los cuales se aplicará la política de gestión de configuración en una organización. Esta sección define claramente lo que la política pretende lograr, como asegurar la estabilidad, seguridad y confiabilidad de los entornos de TI a través de la gestión controlada de cambios en las configuraciones de sistemas y aplicaciones. Además, detalla los sistemas, procesos y actores específicos que están sujetos a la política, garantizando que todos los involucrados comprendan sus roles y responsabilidades.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La política de gestión de cambios establece claramente el objetivo principal de proteger el negocio y otros servicios mientras se realizan cambios necesarios? * ¿Se asegura que los cambios implementados estén alineados con los requisitos de servicio acordados con los clientes y, al mismo tiempo, optimicen los costos? * ¿La política de gestión de cambios establece la contribución al cumplimiento de requisitos legales, contractuales y regulatorios? * ¿Se han implementado medidas para reducir los cambios fallidos y minimizar la interrupción del servicio, los defectos y la repetición del trabajo? * ¿Existe un enfoque proactivo para reducir la cantidad de cambios no autorizados, contribuyendo a una disminución en la interrupción del servicio y en el tiempo de resolución de incidentes relacionados con cambios? |

|  |
| --- |
| Temática: Eficiencia de la Política de Gestión de Cambios |
| La eficiencia de la política de gestión de cambios se refiere a la capacidad de la política para facilitar cambios seguros, oportunos y efectivos dentro de la infraestructura de TI, minimizando al mismo tiempo las interrupciones y maximizando el valor para la organización. Esta eficiencia se mide por la rapidez con la que se pueden implementar los cambios sin comprometer la seguridad, la precisión en la alineación de los cambios con los objetivos empresariales y de seguridad, y la minimización del impacto negativo en las operaciones diarias. Una política eficiente debe equilibrar la necesidad de agilidad y adaptabilidad en un entorno tecnológico en constante cambio con la imperativa necesidad de mantener la integridad y seguridad de los sistemas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La política de gestión de cambios respalda la entrega rápida de cambios para cumplir con los plazos comerciales establecidos? * ¿Se realiza un seguimiento efectivo de los cambios a lo largo de su ciclo de vida y de los activos de los clientes relacionados? * ¿Contribuye la gestión de cambios a estimaciones más precisas de calidad, tiempo y costos de los cambios? * ¿Se evalúan adecuadamente los riesgos asociados a la transición de servicios, ya sea en su introducción o enajenación? * ¿La política de gestión de cambios contribuye a una mejora en la productividad del personal al minimizar las interrupciones causadas por cambios no planificados o de "emergencia"? |

|  |
| --- |
| Temática: Integración y Coordinación de Cambios de la Política de Gestión de Cambios |
| La integración y coordinación de cambios de la política de gestión de cambios asegura que las modificaciones a las políticas y procedimientos de gestión de cambios se realicen de manera armónica con las prácticas y sistemas existentes dentro de la organización. Esta temática enfatiza la importancia de una comunicación efectiva y colaboración entre los departamentos, garantizando que los cambios en la política sean comprendidos, aceptados y aplicados consistentemente a través de todas las áreas relevantes. La integración exitosa implica alinear los cambios de la política con los objetivos estratégicos de la organización, así como con otras políticas y procedimientos de seguridad y operaciones de TI.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La política de gestión de cambios fomenta la creación de una cultura organizacional donde no se toleren los cambios no autorizados? * ¿Se establecen vínculos efectivos entre el proceso de gestión de cambios y los procesos de cambio empresarial, proyectos y stakeholders? * ¿Se garantiza que los cambios generen valor empresarial y que se midan e informen los beneficios para el negocio? * ¿Existe un punto focal único para la gestión de cambios con el fin de minimizar la probabilidad de cambios conflictivos y posibles interrupciones en los entornos compatibles? * ¿Se evita que personas no autorizadas tengan acceso a entornos soportados y se asegura la integridad de los cambios? |

|  |
| --- |
| Temática: Política Contempla Registro y Evaluación de los Cambios |
| Esta parte de la política establece la necesidad de documentar de forma exhaustiva cada cambio propuesto, incluyendo su justificación, el análisis de impacto, las pruebas realizadas y la revisión de los resultados post-implementación. La evaluación rigurosa de los cambios antes de su aprobación y ejecución ayuda a identificar potenciales riesgos y repercusiones, asegurando que las decisiones se tomen con una comprensión completa de sus implicaciones.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La política de gestión de cambios promueve la integración con otros procesos de gestión de servicios para establecer trazabilidad del cambio, detectar cambios no autorizados e identificar incidentes relacionados con el cambio? * ¿Se evalúa el desempeño y riesgo de todos los cambios que impactan la capacidad del servicio? * ¿Se registran y mantienen registros precisos de cambios, configuraciones y lanzamientos e implementaciones? * ¿Se realiza un análisis sistemático del impacto del cambio empresarial en TI? * ¿Se analiza cuidadosamente el impacto de un servicio o cambio de TI en el negocio? * ¿Se notifica de manera efectiva a los afectados sobre los cambios propuestos, planificados e implementados? * ¿Se identifican los problemas que requieren cambios continuos y se gestionan de manera adecuada para evitar interrupciones y garantizar la mejora continua? |