

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Informar cambios no autorizados y el estado 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

A través de un proceso riguroso de seguimiento y reporte, es posible identificar rápidamente cualquier discrepancia con respecto a la línea base aprobada, permitiendo que los gestores de cambios actúen con agilidad para mitigar posibles riesgos. Este enfoque fortalece la capacidad de respuesta y facilita la continuidad operativa al asegurar que solo se implementen cambios autorizados en el entorno.

**1.1 Identificación y Reporte de Cambios No Autorizados**  
Para identificar cambios no autorizados, todos los ajustes de configuración deben estar vinculados con solicitudes de cambio previamente aprobadas, lo cual facilita la detección de discrepancias. Una vez que se detecta un cambio no autorizado, es crucial notificar a los gestores de cambios para que puedan tomar medidas correctivas. Además, se deben identificar y cumplir con los requisitos de reporte de todas las partes interesadas, incluyendo detalles sobre el contenido, frecuencia y medio de los informes, a fin de mantener una comunicación clara y efectiva.

**1.2 Monitoreo del Estado de Configuración y Mejora de la Comunicación**  
Es importante monitorear continuamente el estado de los elementos de configuración (CIs), comparando sus cambios con las líneas de referencia establecidas para asegurar la precisión y consistencia. Indicadores cuantitativos, como el número de cambios no autorizados y el porcentaje de precisión en los cambios de estado, permiten medir el rendimiento y la efectividad de la gestión de configuración. Además, se deben mejorar los mecanismos y tiempos de comunicación para reportar cambios no autorizados de manera ágil, reduciendo el tiempo de respuesta ante posibles riesgos. Utilizar mecanismos automatizados para mantener la vigencia e integridad de la línea base de configuración contribuye a una gestión eficaz y reduce los riesgos asociados a la alteración no controlada de los sistemas.

**1.3 Auditoría de Cambios No Autorizados y Estado de Configuración**  
Desde la perspectiva de auditoría, es crucial revisar la efectividad de los controles implementados para identificar y gestionar cambios no autorizados en el estado de configuración. La auditoría se centra en evaluar la precisión de los informes generados, la agilidad en la notificación de cambios no autorizados a los gestores de cambios, y la efectividad de los indicadores cuantitativos de rendimiento, como el porcentaje de precisión en los cambios de estado de los CIs. La auditoría también verifica el cumplimiento de los requisitos de reporte a todas las partes interesadas y el uso de mecanismos automatizados para asegurar la integridad de la línea base de configuración. Esta supervisión garantiza que las medidas de gestión de cambios contribuyan efectivamente a mantener un entorno de TI controlado y seguro, alineado con las políticas y procedimientos organizacionales.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Relacionar todos los cambios de configuración con las solicitudes de cambio aprobadas para identificar los cambios no autorizados. 2. Informar sobre cambios no autorizados a los gestores de cambios. 3. Identificar los requisitos de reporte de todas las partes interesadas, incluyendo el contenido, la frecuencia y el medio. Producir informes conforme a los requisitos identificados. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Identificar los cambios de estado de los CIs y compararlos con las líneas de referencia |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Establecer indicadores cuantitativos específicos para la medición del desempeño y rendimiento de esta actividad, tales como: 2. Número de cambios no autorizados identificados 3. Porcentaje de precisión en los cambios de estado de los CIs en comparación con las líneas de referencia |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mejorar los mecanismos, medios y frecuencias de la comunicación, y disminuir el tiempo en que los cambios no autorizados riesgosos son comunicados |
| 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. Mantener la vigencia, integridad, precisión y disponibilidad de la línea base de configuración de los sistemas utilizando mecanismos automatizados. |

1. **Preguntas de Auditoría para Evaluar la notificación de cambios no autorizados y el Estado de Configuración**

|  |
| --- |
| Temática: Identificación y Reporte de los cambios no autorizados |
| La identificación y el reporte de cambios no autorizados permiten a las organizaciones detectar rápidamente alteraciones indebidas en sus sistemas de TI. Este proceso involucra el uso de herramientas de monitoreo y detección para rastrear continuamente las configuraciones y alertar sobre cualquier desviación de las líneas base establecidas. Una vez identificado un cambio no autorizado, es crucial reportarlo de manera efectiva para que se tomen las acciones correctivas adecuadas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo verifica la organización que cada cambio de configuración esté vinculado a una solicitud de cambio aprobada? * ¿Existen mecanismos automatizados para comparar los cambios realizados con las solicitudes de cambio aprobadas? * ¿Qué protocolo se sigue cuando se detecta un cambio de configuración que no está relacionado con una solicitud aprobada?   + ¿Se mantiene un registro histórico de todas las solicitudes de cambio y su estado (aprobado/rechazado)? * ¿Cómo se asegura que las solicitudes de cambio aprobadas son las únicas que se implementan en el sistema? * ¿Qué mecanismo o proceso se utiliza para informar a los gestores de cambios sobre modificaciones no autorizadas? * ¿Existe un protocolo de respuesta o acción inmediata cuando se informa de un cambio no autorizado? * ¿Se mantiene un registro de todos los informes de cambios no autorizados y las acciones tomadas al respecto? * ¿Con qué frecuencia se revisan y analizan los informes de cambios no autorizados para identificar patrones o áreas de mejora? * ¿Se proporciona formación o concienciación al personal sobre la importancia de seguir el proceso de gestión de cambios y las consecuencias de realizar cambios no autorizados? |

|  |
| --- |
| Temática: Adopción de los requisitos de reporte las partes interesadas |
| La adopción de requisitos de reporte a las partes interesadas asegura la transparencia y la comunicación efectiva dentro de una organización en lo que respecta a la gestión de cambios y el estado de configuración de los sistemas de TI. En este proceso se establecen protocolos claros sobre cuándo, cómo y a quién se deben informar los cambios en la configuración, especialmente aquellos no autorizados, y el estado general de la configuración.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se identifican y documentan los requisitos específicos de las partes interesadas para informes sobre cambios no autorizados y estados de configuración?   + Revisar la documentación o protocolos donde se establecen los requisitos de reporte. Las actas de reuniones o comunicaciones con las partes interesadas pueden ser útiles.   + ¿Se dispone de un mecanismo o herramienta que permita generar informes automatizados sobre cambios no autorizados y estados actuales de configuración? * ¿Con qué frecuencia se generan y distribuyen estos informes, y se ajusta esta frecuencia a las necesidades y requisitos de las partes interesadas?   + Revisar registros o historiales de informes generados y distribuidos en el pasado.   + Comparar con los requisitos establecidos para determinar la coherencia.   + Entrevistar a las partes interesadas para entender sus expectativas en cuanto a la frecuencia de los informes. * ¿Cómo se verifica que el contenido de los informes refleje de manera * precisa y fidedigna los cambios no autorizados detectados y los estados actuales de configuración?   + Comparar informes generados con registros reales de cambios y configuraciones para verificar su precisión. * ¿Se realiza una revisión o validación de los informes sobre cambios no autorizados y estados de configuración antes de su distribución para asegurar que cumplen con los requisitos y expectativas de las partes interesadas?   + Revisar el proceso o protocolo de revisión y validación de informes.   + Identificar quiénes son los responsables de esta revisión y entrevistarlos para entender el proceso en detalle.   + Solicitar evidencia de revisiones anteriores, como comentarios, correcciones o aprobaciones |

|  |
| --- |
| 3.3 Temática: Medición y mejora continua |
| La medición y mejora continua en el contexto de la gestión de la configuración y el reporte de cambios no autorizados implica establecer métricas claras para evaluar la eficacia de los procesos de detección, reporte y respuesta a cambios no autorizados, así como el cumplimiento de los requisitos de reporte a las partes interesadas. Al analizar estas métricas regularmente, las organizaciones pueden identificar áreas de mejora, ajustar sus procedimientos y políticas de acuerdo con las lecciones aprendidas y las tendencias emergentes en el panorama de amenazas, y optimizar la eficiencia operativa.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización utiliza métricas relevantes y específicas para la identificación de áreas de mejora? Algunos ejemplos de indicadores pueden ser:   + Número de cambios no autorizados identificados   + Porcentaje de precisión en los cambios de estado de los CIs en comparación con las líneas de referencia * ¿Se asignan responsabilidades claras para llevar a cabo estas acciones?   + ¿Se realiza un seguimiento efectivo de la implementación y el impacto de las acciones? * ¿Las áreas de mejora identificadas resultan en acciones correctivas y preventivas documentadas?   + ¿Qué acciones ha implementado la organización para mejorar los mecanismos de comunicación respecto a cambios no autorizados?   + Revisar cualquier documentación o protocolo actualizado relacionado con la comunicación de cambios no autorizados.   + Entrevistar al equipo de comunicaciones o al equipo encargado de la gestión de cambios para entender las mejoras implementadas. * ¿Cómo ha optimizado la organización los medios utilizados para comunicar cambios no autorizados riesgosos?   + Evaluar los diferentes canales de comunicación utilizados (correo electrónico, sistemas de alerta, notificaciones, etc.) y cómo se han adaptado o mejorado.   + Solicitar ejemplos o registros de comunicaciones recientes para evaluar su efectividad. * ¿Se ha establecido una frecuencia específica o se ha modificado la existente para la comunicación de cambios no autorizados?   + Comparar con registros históricos para determinar si ha habido un cambio en la frecuencia de comunicación. |