

**CASIG 5 – Operaciones de Ciberseguridad**

**Preguntas de Auditoría**

**Establecer y Mantener un Proceso de Configuración Seguro**

**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

Un proceso de configuración seguro reduce las superficies de ataque y asegura que los sistemas y dispositivos de la organización operen bajo configuraciones que protejan contra vulnerabilidades y accesos no autorizados. Además, los dispositivos de red y cualquier otro equipo crítico deben tener un proceso de configuración separado y seguro, y los cambios en el sistema deben ser probados en un entorno separado antes de ser aplicados al entorno operativo, lo cual permite identificar y mitigar riesgos de seguridad o privacidad.

**1.1 Establecimiento de Configuraciones de Seguridad Mínima**  
El proceso de configuración seguro exige una serie de configuraciones de seguridad mínimas para todos los activos de la organización. Estas configuraciones incluyen el bloqueo automático de sesiones tras un periodo definido de inactividad (máximo de 15 minutos para sistemas operativos y 2 minutos para dispositivos móviles), la desinstalación de servicios innecesarios, y la gestión cuidadosa de cuentas predeterminadas como root y administrador, mediante su deshabilitación o inhabilitación. Además, el proceso define que los activos deben estar configurados para usar servidores DNS confiables, idealmente controlados por la empresa o acreditados externamente. La seguridad de los dispositivos móviles se refuerza con configuraciones de bloqueo automático y capacidades de borrado remoto para proteger la información en caso de pérdida o robo. Esta serie de medidas asegura que los activos de la organización mantengan una configuración mínima de seguridad que reduzca el riesgo de exposición.

**1.2 Auditoría y Revisión Continua del Proceso de Configuración**  
La auditoría se enfoca en identificar funciones, puertos, protocolos y servicios innecesarios que podrían representar un riesgo y asegurar que estos elementos sean eliminados o desactivados. Adicionalmente, se generan registros de auditoría de manera automática para cada acción de cumplimiento, lo cual facilita la revisión y permite una supervisión detallada del cumplimiento de la configuración segura en los activos. Estas actividades de auditoría y revisión continua refuerzan la seguridad de la configuración, asegurando que los sistemas y dispositivos se mantengan alineados con los estándares de protección de la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Establecer y mantener un proceso seguro de la configuración para los activos de la empresa (dispositivos de usuarios, incluidos portátiles y móviles; dispositivos no informáticos/IoT; and servers) y software (Sistemas operativos y aplicaciones) 2. Establecer y mantener un proceso de configuración seguro para dispositivos de red 3. Analizar los cambios en el sistema en un entorno de prueba separado antes de la implementación en un entorno operativo, buscando impactos de seguridad y privacidad debido a fallas, debilidades, incompatibilidad o malicia intencional |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Defina el proceso de gestión de configuración para que exija, por lo menos, los siguientes configuraciones mínimas de seguridad:    1. Configurar el bloqueo automático de sesiones en los activos de la empresa después de un período definido de inactividad. Para los sistemas operativos de propósito general, el período no debe exceder los 15 minutos. Para dispositivos móviles de usuario final, el período no debe exceder los 2 minutos    2. Desinstale o deshabilite los servicios innecesarios en los activos y el software de la empresa, como un servicio de uso compartido de archivos, un módulo de aplicación web o una función de servicio    3. Administre cuentas predeterminadas en activos y software de la empresa, como root, administrador y otras cuentas de proveedores preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o inutilizarlas.    4. Configurar servidores DNS confiables en activos empresariales. Las implementaciones de ejemplo incluyen: configurar activos para usar servidores DNS controlados por la empresa y/o servidores DNS acreditados externamente.    5. Aplicar el bloqueo automático de dispositivos en portátiles y dispositivos móviles    6. Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revise y actualice la documentación anualmente, o cuando ocurran cambios significativos en la empresa que puedan causar un impacto a esta salvaguarda 2. Revisar el sistema para identificar funciones, puertos, protocolos, software y servicios innecesarios y/o no seguros. |
| 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. Generar automáticamente registros de auditoría de las acciones de cumplimiento. |

1. **Preguntas de Auditoría para Establecer y Mantener un Proceso de Configuración Seguro**

|  |
| --- |
| Temática: Proceso de Solicitudes de Cambio |
| La organización debe asegurar que las solicitudes de cambio se gestionen adecuadamente desde su creación hasta su implementación, que se evalúen en función de su impacto en la seguridad de la información y otros aspectos críticos, y que se documenten de manera completa y precisa. En este proceso el auditor puede verificar que se sigan los protocolos adecuados, que se tomen decisiones informadas sobre la autorización de cambios y que se mantenga un registro adecuado de todas las solicitudes y cambios implementados. Este proceso se debe encontrar documentado e incluir las siguientes actividades:   * + - * Crear y registrar una solicitud de cambio (RFC)       * Revisar RFC       * Valorar y evaluar el cambio       * Autorizar el cambio, compilación y prueba       * Coordinar la creación y prueba de cambios       * Autorizar la implementación de cambios       * Coordinar la implementación del cambio       * Revisar y cerrar el registro de cambios.   Este levantamiento puede incluir análisis específicos tales como: 3.1.1 ****Crear y registrar una solicitud de cambio (RFC):****  * ¿Se ha implementado un procedimiento efectivo para la creación y registro de solicitudes de cambio (RFC) que incluya la información necesaria, como descripción del cambio, justificación, impacto previsto y prioridad? * ¿Se verifica que todas las RFC sean registradas de manera oportuna y de acuerdo con el procedimiento establecido? * ¿Existe un mecanismo para rastrear y documentar el estado actual de todas las RFC, incluyendo su fecha de creación y las actualizaciones correspondientes? * ¿Se requiere la identificación de los responsables de la RFC, incluyendo aquellos que solicitan el cambio y aquellos que deben aprobarlo? * ¿Se asegura que las RFC contengan información suficiente para permitir una revisión adecuada y una evaluación inicial del cambio propuesto? * ¿Se realiza una revisión de calidad de las RFC para asegurar que cumplen con los estándares de documentación y contenido requeridos?   **3.1.2 Revisar RFC:**   * + - ¿Existe un proceso formal y documentado para revisar las RFC que incluye una evaluación inicial de su validez y coherencia?     - ¿Se asegura que las RFC sean revisadas por un equipo o individuo competente que evalúe su factibilidad y su alineación con los objetivos y estrategias organizativas?     - ¿Se verifica que las RFC sean revisadas en función de su prioridad y que se tomen medidas adecuadas para las RFC críticas y de alta prioridad?     - ¿Las RFC revisadas incluyen una evaluación de riesgos preliminar y un análisis de impacto para ayudar en la toma de decisiones sobre la aprobación?     - ¿Se documentan las revisiones realizadas a las RFC, incluyendo los resultados de la revisión y las acciones recomendadas?     - ¿Se asegura que todas las RFC sean comunicadas de manera adecuada a los interesados relevantes y que se mantenga un registro de dicha comunicación?   **3.1.3 Valorar y evaluar el cambio:**   * + - ¿Se realiza una evaluación de riesgos de los cambios propuestos como parte del proceso de valoración y evaluación?     - ¿Se asegura que la valoración de los cambios se base en criterios claros, como la seguridad de la información, la continuidad del negocio y los requisitos regulatorios?     - ¿Las evaluaciones de cambios incluyen una revisión de sus posibles impactos en sistemas, procesos, recursos y personal?     - ¿Se verifica que se establezcan evaluaciones de impacto adecuadas para los cambios de alta complejidad o riesgo?     - ¿Se documenta la evaluación de cada cambio, incluyendo la identificación de riesgos y la justificación para la aprobación o rechazo?     - ¿Se involucra a los expertos técnicos y a los responsables de la seguridad de la información en el proceso de valoración y evaluación de los cambios?   **3.1.4 Autorizar el cambio, compilación y prueba:**   * ¿Existe un proceso formal y documentado para autorizar cambios, que incluye la designación de personas autorizadas para aprobar cambios? * ¿Las autorizaciones de cambios se basan en la evaluación de impacto y riesgo previamente realizada? * ¿Se asegura que las aprobaciones sean registradas y documentadas, incluyendo las fechas de autorización? * ¿Se verifica que se hayan establecido criterios de compilación y pruebas para cada cambio y que estos sean adecuados para su naturaleza y complejidad? * ¿Existe un proceso de coordinación eficiente para la compilación y pruebas de cambios, que incluye la asignación de recursos y la programación de actividades? * ¿Se documentan los resultados de las pruebas de cambios, incluyendo cualquier problema o desviación identificada?   **3.1.5 Coordinar la creación y prueba de cambios:**   * ¿Se asegura que la creación y prueba de cambios se lleve a cabo de manera planificada y coordinada, minimizando conflictos y riesgos? * ¿Existe una comunicación efectiva entre los equipos responsables de la creación y prueba de cambios, así como con otras partes interesadas? * ¿Se verifica que se cumplan los plazos establecidos para la creación y prueba de cambios? * ¿Existe una revisión independiente de los cambios antes de su implementación para garantizar su calidad y conformidad? * ¿Se asegura que se resuelvan de manera adecuada y oportuna los problemas identificados durante la creación y prueba de cambios?   **3.1.6 Autorizar la implementación de cambios:**   * ¿Existe un proceso formal y documentado para autorizar la implementación de cambios, que incluye la revisión de los resultados de las pruebas y la evaluación final del cambio? * ¿Las autorizaciones de implementación se basan en la satisfacción de los criterios de aceptación previamente establecidos? * ¿Se asegura que las aprobaciones de implementación sean registradas y documentadas de manera adecuada? * ¿Existe una revisión final de la documentación y los resultados de las pruebas antes de la autorización de implementación? * ¿Se verifica que se comuniquen de manera efectiva las autorizaciones de implementación a los equipos responsables y otros interesados? * ¿Se documentan los planes de implementación, incluyendo los pasos específicos a seguir y las fechas programadas?   **3.1.7 Coordinar la implementación del cambio:**   * **¿**Se garantiza que la implementación de cambios se coordine de manera efectiva, considerando las interdependencias y minimizando posibles conflictos? * ¿Se verifica que se asignen los recursos necesarios para la implementación y que estén disponibles según lo planificado? * ¿Se asegura que se siga el plan de implementación y que se registren los progresos y desviaciones? * ¿Se documentan los resultados de la implementación, incluyendo cualquier incidente o problema que surja durante este proceso?   **3.1.8 Revisar y cerrar el registro de cambios:**   * ¿Existe un proceso formal para revisar y cerrar los registros de cambios, que incluye la verificación de que los cambios se han implementado de acuerdo con los planes y aprobaciones? * ¿Se verifica que se hayan completado todos los pasos de implementación y que no haya elementos pendientes? * ¿Las revisiones incluyen la comparación de los resultados de implementación con los criterios de aceptación previamente definidos? * ¿Se documentan las revisiones realizadas y los resultados obtenidos? * ¿Se asegura que los registros de cambios sean cerrados de manera oportuna y de acuerdo con los procedimientos establecidos? * ¿Existe una comunicación efectiva de los resultados de la revisión y el cierre de los registros de cambios a todas las partes interesadas pertinentes? |

|  |
| --- |
| Temática: Control de Cambios Relevantes y Cumplimiento Normativo |
| Dentro del marco de establecer y mantener un proceso de configuración seguro, el control de cambios relevantes y el cumplimiento normativo garantiza que todas las modificaciones en los sistemas y aplicaciones no solo sean seguras, sino que también estén alineadas con los requisitos legales y normativos aplicables. Esta temática aborda la necesidad de integrar los procesos de gestión de cambios con las políticas de cumplimiento, asegurando que cada cambio relevante sea evaluado no solo en términos de seguridad, sino también por su impacto en el cumplimiento normativo. Al hacerlo, las organizaciones pueden evitar infracciones que podrían resultar en sanciones, daños a la reputación y otros riesgos legales o financieros.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se garantiza que este proceso de control de cambios mitigue cualquier efecto adverso de los cambios, según sea necesario? * ¿Se controlan los cambios relevantes, como los relacionados con la organización, procesos de negocio, instalaciones de procesamiento de información y sistemas, desde la perspectiva de la seguridad de la información? * ¿Se asegura el cumplimiento de la legislación pertinente, códigos de práctica de la industria, estándares y prácticas organizativas en la gestión de cambios? * ¿Están claramente definidos y documentados los roles y responsabilidades de todas las partes interesadas involucradas en el proceso de cambio? * ¿Se ha establecido la composición de los consejos asesores relevantes, como el Consejo Asesor de Cambios (CAB) y el CAB de Emergencia (ECAB), y se han definido sus funciones y responsabilidades? |

|  |
| --- |
| Temática: Implementación del Cambio |
| La implementación del cambio dentro de un proceso de configuración seguro implica llevar a cabo las modificaciones en la configuración de sistemas, aplicaciones y redes de acuerdo con los planes de cambio aprobados y las líneas base de configuración segura establecidas. Durante la implementación, se debe minimizar el impacto en las operaciones comerciales y asegurar que no se introduzcan nuevas vulnerabilidades en el entorno de TI.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza una revisión formal del riesgo técnico y de negocio asociado con la implementación de cambios, considerando el riesgo en el proceso de planificación? * ¿Se crea un plan de implementación que refleja una estrategia global de implementación, secuencia de pasos, requisitos de recursos, interdependencias, criterios de aceptación y estrategias de transición para el soporte en producción? * ¿Se identifican y documentan los procesos de *fallback* y recuperación en caso de que la implementación tenga problemas? * ¿Existen planes de remediación, incluyendo retrocesos y planes de continuidad del servicio, diseñados para permitir que el proceso comercial continúe en caso de problemas durante la implementación? * ¿Se obtiene el compromiso de los proveedores externos de soluciones para su participación en cada fase de la implementación de cambios? |