CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°5

OPERACIONES DE SEGURIDAD

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°5: Operaciones de Seguridad.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, Marzo 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

INTRODUCCIÓN A LAS OPERACIONES DE CIBERSEGURIDAD

La operación en ciberseguridad requiere de la adopción de procesos y buenas prácticas que posibiliten la gestión de amenazas y vulnerabilidades de manera transversal en los activos de información de las organizaciones, siendo fundamental para alcanzar adecuados niveles de protección la adopción de procesos relacionados a la gestión de vulnerabilidades, gestión del cambio, gestión de la configuración, gestión de la disponibilidad, controles frente a código malicioso, la protección de registros, entre otros.

Nota Importante

Estrictamente hablando, **Seguridad de la Información y Ciberseguridad** son dos conceptos diferentes.

La **"Seguridad de la Información"** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **"Ciberseguridad"** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de "Seguridad de la Información y Ciberseguridad", pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de "Seguridad de la Información", "Ciberseguridad" o el acrónimo "SIC" como sinónimos para mejorar la comprensión lectora.

Muchas de las brechas de seguridad existentes y materializadas en diversos ataques en Servicios Públicos surgen de las debilidades en las operaciones de ciberseguridad, siendo en consecuencia una labor de aseguramiento fundamental para el Auditor Interno Gubernamental.
El dominio proporcionará un nivel de desarrollo específico para la auditoría a las operaciones de Ciberseguridad abordando los principios y componentes claves en la materia, desde los procesos claves, contextos de riesgos, elementos de controles, roles, responsabilidades, entre otros, siendo un elemento clave de evaluación la integración con los procesos tecnológicos de la organización y su alineamiento con la gestión de riesgo institucional.

Objetivo General

Evaluar la adopción de buenas prácticas en operaciones y procesos claves en materias de seguridad y ciberseguridad otorgando el aseguramiento al cumplimiento normativo y las mejores prácticas en la materia.

Para cumplir con este objetivo, este dominio considerará los siguientes temas:

- ✓ **Gestión de los Cambios de TI**
- ✓ **Gestión de la Configuración**
- ✓ **Gestión de Vulnerabilidades**

NOTA

Los procesos operativos de seguridad son variados e incluyen de forma total o incidental: Gestion de Incidentes, Gestion de Riesgos, Gestion de la Continuidad, Gestion de Amenazas, Gestion de Vulnerabilidades, Monitoreo Continuo, Hardening, Pentesting, y un largo etcétera. Esta guía tiene como alcance tres procesos comunes, donde la aplicación de controles de seguridad permite alcanzar hitos base en seguridad.
Las siguientes GASIC abordarán otros procedimientos operativos de seguridad, revísalas en el repositorio oficial.

Capítulo 2

GESTIÓN DE LOS CAMBIOS EN LAS TECNOLOGÍAS DE LA INFORMACIÓN

2.1 GESTIÓN DE LOS CAMBIOS TI

Según ITIL, un cambio es "la adición, modificación o eliminación de cualquier cosa que pueda tener un efecto directo o indirecto en los servicios". En su forma más simple, cualquier cambio en la infraestructura de TI de una organización que pueda afectar las operaciones de la organización se denomina cambio de TI. Esto incluye el reemplazo de impresoras, proyectores, servidores y más.

Fuente: ITIL v4

La mala gestión de los cambios, para una organización de TI, puede manifestarse como:

01 **Cambios “Sorpresa”**

02 **La Ocurrencia de Incidentes Después de un Cambio**

03 **Un Elevado Número de Cambios Urgentes**

Las organizaciones deben agilizar la gestión del cambio y evitar la burocracia innecesaria mediante el uso del proceso completo de gestión del cambio sólo para un pequeño número de cambios (conocidos como cambios normales). La eficacia y la eficiencia de la Gestión del Cambio pueden mejorarse, por ejemplo, mediante la:

Creación	De modelos de cambio para cambios recurrentes.
Descentralización	De la aprobación de cambios para cambios estándar.
División	Dividir los cambios más grandes en cambios más pequeños que conllevan menos riesgo.
Uso	De comprobaciones, pruebas e implementación automatizadas.

Para que este control se lleve a cabo satisfactoriamente, el proceso de Gestión del Cambio debe procurar:

Reutilizar	Métodos y procedimientos estandarizados.
Registrar	Todos los cambios
Considerar	Los riesgos e impactos en el negocio.

Tipos de Cambios

Cambios Estándar

Cambios preautorizados y de bajo riesgo que siguen un procedimiento bien conocido. Se puede predefinir una lista de cambios estándar; cualquier cambio que no forme parte de esta lista debe tratarse como un cambio normal.

Ejemplos: Actualización de un Parche - Sustitución de una impresora

Cambios Normales

Todos los demás cambios que no son cambios estándar o cambios de emergencia se consideran cambios normales. La parte que requiere el cambio normalmente enviará una solicitud de cambio (RFC) a Gestión de cambios. La Gestión del Cambio registrará, analizará y aprobará (o rechazará) el Cambio.

Cambios de Emergencia

Cambios que deben implementarse inmediatamente, por ejemplo, para resolver un incidente mayor. Esencialmente, seguirá el mismo proceso que los cambios normales, pero se adaptará a la situación de emergencia. Si el CAB no puede reunirse rápidamente, se recurrirá al ECAB, que tiene el nivel de autoridad necesario para tomar decisiones. Las pruebas deben llevarse a cabo tanto como sea posible, y la documentación de los datos de cambio y configuración puede completarse más adelante.

Ejemplos: Resolver un incidente importante - Implementar un parche de seguridad urgente.

¿Quién aprueba y es responsable de los cambios?

Change Advisory Board (CAB)

- ***Grupo de personas que asesora al Gestor de Cambio en la evaluación, priorización y programación de Cambios.***
- ***Esta junta generalmente está compuesta por representantes de todas las áreas dentro de la organización de TI, el negocio y terceros, como proveedores.***

Emergency Change Advisory Board (ECAB)

- ***Un subconjunto de la CAB que toma decisiones sobre Cambios de Emergencia de alto impacto.***
- ***Los miembros del ECAB pueden decidirse en el momento en que se convoca una reunión, y depende de la naturaleza del cambio de emergencia.***

2.2 RIESGOS ASOCIADOS A LA GESTIÓN DEL CAMBIO

Riesgos Generales	Riesgos Emergentes	Riesgos Relacionados a Terceros
• Incumplimiento de los objetivos de negocio. • Las deficiencias que pueden resultar en un cumplimiento inconsistente o resultados negativos de auditoría. • Desgaste del personal de TI bien calificado debido a la frustración por los resultados de baja calidad. • Sistemas de mala calidad, pueden obstaculizar la productividad de los empleados o frustrar a los clientes. • Perder la oportunidad de proporcionar productos y servicios innovadores o más eficientes. • Interrupciones y trabajos no planificados. • No realizar un análisis de amenazas o probar e implementar los parches necesarios, que pueden introducir nuevas vulnerabilidades de seguridad críticas o reintroducir vulnerabilidades anteriores. • No involucrar adecuadamente a la organización en la junta de aprobación de cambios (CAB) en el proceso de aprobación de cambios, aumentando la posibilidad de que el cambio pueda afectar la finalización de una actividad comercial crítica. • Cambios en el sistema que no satisfacen las necesidades del propietario del proceso, lo que resulta en variados errores de procesamiento, pérdida de tiempo debido al retrabajo y más resultados negativos.	• Aplicaciones en distribuciones Cloud y la manera cómo se aplican los cambios a aquellas aplicaciones que admiten infraestructura, que son fuentes de riesgo de terceros. • Aplicaciones de dispositivos móviles y cómo se aplican los cambios al hardware, los sistemas operativos y las aplicaciones. • BYOD - Si los cambios son administrados por una organización o los propietarios individuales del dispositivo.	• Muchos proveedores producen un informe sobre sus controles a nivel de sistema y a nivel de organización entidad, que puede ofrecer varios niveles de garantía. La obtención y evaluación de estos informes puede ser necesaria para el cumplimiento normativo de la organización. • Los procesos sólidos de gestión del cambio pueden ayudar a una organización a mantener el cumplimiento de las regulaciones nuevas o ampliadas. Las actividades que abordan el impacto potencial de los cambios en el cumplimiento normativo deben incluirse dentro de los pasos de evaluación de riesgos y aprobación de unidades de negocio del proceso de cambio.

Fuente: GTAG IT Change Manangement: Critical for Organization Success

La gestión de los cambios de TI presenta una serie de riesgos, que no necesariamente se asocian a la explotación de una vulnerabilidad o a la inyección de Malware. Estos riesgos, cuando se manifiestan en incidentes, afectan la Confidencialidad, Integridad o Disponibilidad de los activos de información de la Organización. En general, se pueden distinguir tres tipos de riesgos: Generales, Emergentes y aquellos que provienen por terceros.

2.3 BENEFICIOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN

La gestión del cambio de TI es un proceso esencial para garantizar que cualquier modificación en los sistemas, aplicaciones, infraestructuras o procesos se realice de manera controlada y estructurada. Cuando se trata de seguridad de la información, la gestión del cambio adquiere una relevancia aún mayor. La implementación de controles de seguridad de la información promueven:

01 **Reducción de Riesgos**
Al seguir un proceso estructurado de gestión del cambio, se pueden identificar y evaluar los riesgos asociados con un cambio propuesto antes de su implementación. Esto permite tomar medidas preventivas y reducir la probabilidad de incidentes de seguridad.

02 **Documentación y Trazabilidad**
La gestión del cambio requiere la documentación detallada de cada cambio propuesto, aprobado e implementado. Esto proporciona una trazabilidad completa, lo que es esencial para las auditorías y revisiones de seguridad.

03 **Reducción de Interrupciones**
Al planificar y probar los cambios de manera adecuada, se minimiza el impacto en los usuarios y se reduce la probabilidad de interrupciones no planificadas, que podrían exponer a la organización a vulnerabilidades de seguridad.

04 **Evaluación de Impacto**
Antes de implementar un cambio, se realiza una evaluación de impacto para determinar cómo afectará a otros sistemas o procesos. Esto asegura que no se introduzcan nuevas vulnerabilidades o debilidades en el entorno de TI.

05 **Validación Post-Implementación**
Después de implementar un cambio, se realiza una revisión para asegurarse de que se haya llevado a cabo según lo planeado y que no haya introducido problemas de seguridad no previstos.

06 **Capacidad de Reversa**
En caso de que un cambio introduzca problemas de seguridad o no funcione como se esperaba, la gestión del cambio proporciona mecanismos para revertir o corregir el cambio rápidamente.

2.4 ROL DE LA AUDITORÍA EN LA GESTIÓN DE LOS CAMBIOS DE TI

Un proceso de gestión del cambio eficaz y eficiente es un servicio esencial que permite a la organización alcanzar sus metas. La actividad de auditoría interna puede confirmar la existencia y adecuación del proceso de gestión del cambio y puede garantizar que los controles que respaldan el proceso estén diseñados de manera adecuada y funcionen correctamente.

Al llevar a cabo una auditoría o revisión del proceso de gestión del cambio, los auditores internos deben obtener información suficiente, confiable, pertinente y útil para lograr los objetivos del compromiso. Esto podría implicar recopilar datos fundamentales (por ejemplo, informes de cambios autorizados) y corroborar información (por ejemplo, informe de cambios en producción a partir de controles detectives, conciliaciones de cambios en producción con cambios autorizados e información sobre interrupciones del sistema).

La auditoría juega un papel fundamental en la gestión del cambio, ya que:

- Verifica que se sigan las políticas y procedimientos establecidos.
- Asegura que los cambios no comprometan la seguridad de la información.
- Evalúa la eficacia del proceso de gestión del cambio
- Proporciona recomendaciones para mejorar el proceso.

Las áreas generales en las que los auditores internos pueden proporcionar valor organizacional incluyen:

- Mantenerse al día sobre el liderazgo de los procesos de gestión de cambios y parches de TI y recomendar que la organización adopte los que correspondan.
- Demostrar cómo la gestión efectiva del cambio puede ayudar a la empresa a cosechar los beneficios de una mejor gestión de riesgos, una mayor efectividad y menores costos.
- Ayudar a la administración a identificar enfoques prácticos y efectivos para la gestión del cambio.
- Participar como miembros sin derecho a voto de la junta de aprobación de cambios.
- Comprender el proceso seguido por la organización para mantenerse al día sobre la disponibilidad de parches, así como las prácticas de implementación implementadas

Fuente: GTAG IT Change Manangement: Critical for Organization Success

Capítulo 3

GESTIÓN DE LA CONFIGURACIÓN

3. GESTIÓN DE LA CONFIGURACIÓN

La gestión de la configuración (CM) se puede definir como "Asegurar que la infraestructura, las aplicaciones y cualquier otro recurso relacionado con TI estén configurados de manera adecuada y coherente, y que cualquier cambio en estas configuraciones se gestione de forma controlada , antes de realizar cualquier cambio en un elemento de configuración". Es esencial que se someta a un proceso de revisión y aprobación.

Los cinco pilares de la implementación de CM, según el proceso IEEE 12207.2 de la IEEE 12207 son:

- ***Planificación:*** *Un documento formal y un plan para guiar el programa de CM que incluye elementos tales como:*
  - *Personal*
  - *Responsabilidades y recursos*
  - *Requisitos de formación*
  - *Directrices para reuniones administrativas, incluida una definición de procedimientos y herramientas*
  - *Procesos de línea de base*
  - *Control de configuración y contabilidad de estado de configuración*
  - *Convenciones de nomenclatura*
  - *Auditorías y revisiones*
  - *Requisitos de CM del subcontratista/proveedor*

- ***Identificación de Configuración:*** *Consiste en establecer y mantener líneas de base, que definen la arquitectura del sistema o subsistema, los componentes y cualquier desarrollo en cualquier momento. Es la base por la cual los cambios en cualquier parte de un sistema se identifican, documentan y luego rastrean a través del diseño, desarrollo, pruebas y entrega final. CI establece y mantiene incrementalmente la base actual definitiva para la contabilidad del estado de configuración (CSA) de un sistema y sus elementos de configuración (CI) a lo largo de su ciclo de vida, hasta su eliminación.*

- ***Control de Configuración:*** *Incluye la evaluación de todas las solicitudes y propuestas de cambio, y su posterior aprobación o desaprobación. Cubre el proceso de control de modificaciones al diseño, hardware, firmware, software y documentación del sistema.*

- ***Reportería del Status:*** *Incluye el proceso de registrar e informar descripciones de elementos de configuración (por ejemplo, hardware, software, firmware, etc.) y todas las desviaciones de la línea de base durante el diseño y la producción. En caso de sospecha de problemas, la verificación de la configuración de línea de base y las modificaciones aprobadas se pueden determinar rápidamente.*

- ***Verificación y Auditoría de la Configuración:*** *una revisión independiente del hardware y el software con el fin de evaluar el cumplimiento de los requisitos de rendimiento establecidos, las normas militares comerciales y apropiadas, y las líneas de base funcionales, asignadas y del producto. Las auditorías de configuración verifican que la documentación de configuración del sistema y del subsistema cumple con las características de rendimiento funcional y físico antes de su aceptación en una línea base arquitectónica.*

Fuente: ISO/IEC 12207

3.1 RIESGOS Y BENEFICIOS ASOCIADOS A LA GESTIÓN DE CONFIGURACIONES

La adecuada configuración de estos sistemas es esencial para el triunfo de tu organización. La configuración es la que permite que los sistemas (servidores, redes, sistemas operativos, centros de datos, archivos de configuración, activos de TI, entre otros) funcionen correctamente. Es vital gestionarla con precisión y monitorear las modificaciones de configuración para garantizar su rastreabilidad; de lo contrario, tu negocio y tus usuarios finales podrían enfrentar interrupciones del sistema, violaciones de datos y fugas de información.

Para minimizar los riesgos de ciberseguridad y optimizar las operaciones, muchas empresas utilizan una base de datos de gestión de configuración (CMDB), un plan de gestión de configuración y un administrador (o gestor) de configuración para garantizar una gestión de configuración exitosa.

Mantener registros precisos del estado de tus sistemas es fundamental, y establecer una línea base para un atributo puede garantizar que los procesos de control de cambios de configuración sean efectivos. Por ello, el control de versiones es esencial para toda infraestructura de TI. Esto facilita la gestión de proyectos, la administración de activos y los procesos de auditoría, así como el desarrollo y depuración de software.

What Is Configuration Management and Why Is It Important? – UpGuard Team

Algunos beneficios asociados a la correcta gestión de la configuración son:

01 Reducción del riesgo de interrupciones y brechas de seguridad a través de la visibilidad y el seguimiento de los cambios en sus sistemas.

02 Reducción de costes al tener un conocimiento detallado de todos los elementos de su configuración, evitando la duplicación inútil de sus activos tecnológicos.

03 Experiencia mejorada para sus clientes y personal interno al detectar y corregir rápidamente configuraciones incorrectas que podrían afectar negativamente al rendimiento.

04 Control estricto de sus procesos mediante la definición y aplicación de políticas y procedimientos formales que rigen la identificación de activos, la supervisión del estado y la auditoría.

05 Mayor agilidad y resolución de problemas más rápida, lo que le permite proporcionar una mayor calidad de servicio y reducir los costos de ingeniería de software.

06 Gestión eficiente de cambios al conocer su configuración de línea base y tener la visibilidad para diseñar cambios que eviten problemas.

07 Restablecimiento más rápido del servicio.

08 Mejor gestión de versiones y contabilidad de estado clara.

3.2 PRINCIPALES COMPONENTES DE LA GESTIÓN DE LA CONFIGURACIÓN

La gestión de la configuración (CM) se puede definir como “Asegurar que la infraestructura, las aplicaciones y cualquier otro recurso relacionado con TI estén configurados de manera adecuada y coherente, y que cualquier cambio en estas configuraciones se gestione de forma controlada , antes de realizar cualquier cambio en un elemento de configuración”. Es esencial que se someta a un proceso de revisión y aprobación.
COBIT 2019 destaca la necesidad de un proceso formal de control de cambios para garantizar que solo se implementen cambios autorizados.

¿Qué es ITIL?

ITIL es un conjunto de prácticas para la gestión de servicios de tecnología de la información que se centra en alinear los servicios de TI con las necesidades de las empresas. Originalmente desarrollado por la Oficina de Comercio del Gobierno del Reino Unido, ITIL ha evolucionado a lo largo de los años y es considerado el estándar de facto para la gestión de servicios de TI en muchas partes del mundo.

Estos son los subprocesos de ITIL Configuration Management:

01 **Identificación de la Configuración**

Definir y mantener la estructura subyacente del CMS, llamado Modelo de Configuración, de modo que sea capaz de contener toda la información sobre los Elementos de Configuración. Esto incluye especificar los atributos que describen los tipos de CI y sus subcomponentes, así como determinar sus interrelaciones.

02 **Control de Configuración**

Asegurar que no se agreguen o modifiquen elementos de configuración sin la autorización requerida, y que dichas modificaciones se registren adecuadamente en el CMS.

Nota: ITIL Configuration Control se ocupa principalmente de revisar las modificaciones al Sistema de Gestión de Configuración (CMS), para asegurarse de que la información almacenada en el CMS esté completa y que la modificación haya sido realizada por una parte autorizada. Otros procesos también apoyan los objetivos del Control de configuración: La identificación de la configuración define quién está autorizado para realizar ciertos cambios en el CMS. En un sentido más amplio, la gestión de cambios y la gestión de versiones con sus procedimientos definidos también ayudan a garantizar que no se produzcan cambios no autorizados.

03 **Verificación y Auditoría de la Configuración**

Realizar comprobaciones periódicas, asegurando que la información contenida en el CMS sea una representación exacta de los elementos de configuración (CI) realmente instalados en el entorno de producción en vivo.

3.2.1 BASE DE DATOS DE CONFIGURACIÓN

ITIL especifica el uso de un sistema de gestión de configuración (CMS) o una base de datos de gestión de configuración (CMDB) como un medio para lograr las mejores prácticas de la industria para la gestión de la configuración. Las CMDB se utilizan para realizar un seguimiento de los elementos de configuración (CI) y las dependencias entre ellos, donde los CI representan las cosas en una empresa que vale la pena rastrear y administrar, como, entre otras, computadoras, software, licencias de software, bastidores, dispositivos de red, almacenamiento e incluso los componentes dentro de dichos elementos.

Los beneficios de un CMS / CMDB incluyen tener la capacidad para realizar funciones como:

01 Análisis de causa raíz

02 Análisis de Impacto

03 Gestión de cambios

04 Evaluación del estado actual para el desarrollo de estrategias de estado futuro

Los sistemas de ejemplo, identificados como sistemas de gestión de servicios de TI (ITSM), incluyen FreshService, ServiceNow y Samanage. Todos los elementos bajo control de configuración están sujetos a los cinco pilares de una implementación sólida de CM. (Planificación, identificación, reportería del estatus, control de cambios, trazabilidad y auditoría).

3.3 ROL DE LA AUDITORÍA EN LA GESTIÓN DE LAS CONFIGURACIONES

La auditoría de la gestión de configuración de los elementos de TI es esencial para garantizar la integridad, coherencia y seguridad de los sistemas y aplicaciones de una organización. Al supervisar y evaluar regularmente cómo se registran, actualizan y modifican las configuraciones, la auditoría contribuye directamente al logro de los objetivos de la función TI, asegurando que los recursos tecnológicos estén alineados con las necesidades empresariales. Esta alineación y control riguroso no solo minimiza los riesgos asociados con cambios no autorizados o inadecuados, sino que también potencia la eficiencia operativa, facilitando que la organización alcance sus metas estratégicas con éxito.

El objetivo de estas auditorías de configuración es proporcionar lo siguiente:

- ✓ Asegura que el diseño del producto proporcione las capacidades de rendimiento acordadas
- ✓ Valida la integridad de la información de configuración del producto
- ✓ Verifica la coherencia entre un activo de TI y su información de configuración del producto
- ✓ Determina que existen procesos adecuados para proporcionar un control continuo de la configuración
- ✓ Proporciona confianza en que la información de definición del producto está bajo control de configuración

Existen dos principales alcances en la auditoría de la gestión de configuración:

3.3.1 AUDITORÍA DE LA CONFIGURACIÓN FUNCIONAL (FCA)

La Auditoría de Configuración Funcional (FCA) se encarga de inspeccionar las propiedades funcionales del producto, asegurando que se alinee con los requisitos establecidos en su documentación base, los cuales fueron aprobados en las revisiones de diseño preliminares y críticas. Aunque tiene vínculos con la gestión de programas y la ingeniería de sistemas, no se asocia directamente con una auditoría convencional. La FCA se basa en el análisis de datos de prueba del elemento de configuración para confirmar que cumple con las especificaciones de rendimiento del sistema. Además, puede realizarse en conjunto con la Revisión de Verificación del Sistema (SVR).

Por otro lado, una revisión técnica abarca múltiples disciplinas y se orienta a confirmar que el sistema esté preparado para entrar en la etapa de producción, considerando aspectos como costos, tiempos y riesgos. Esta revisión aporta información valiosa que se complementa con la Revisión de Diseño Crítico. Su propósito principal es evaluar el producto final en su configuración de producción, verificando si satisface los requisitos funcionales descritos en las Líneas de Base Funcionales, Asignadas y de Producto. El SVR es crucial para determinar el rendimiento final del producto y contribuye al documento que define la capacidad de producción.

Department of Defense (DoD) Directive 5000.01 "The Defense Acquisition System"

Los elementos que se abordan durante un FCA/SVR son:

- ***Problemas en el diseño continuo, verificación continua, producción, entrenamiento, despliegue, operaciones y soporte.***
- ***Que la verificación es completa.***
- ***La planificación de gestión de riesgos. Que esta se encuentre actualizada y considere riesgos de producción.***
- ***La planificación de los sistemas.***
- ***Cumplimiento de los criterios de éxito.***

3.3.2 AUDITORÍA DE CONFIGURACIÓN FÍSICA (PCA)

Examen físico para verificar que los elementos de configuración (CI) "tal como se construyó" se ajustan a la documentación técnica que define el ítem.

La Auditoría de Configuración Física (PCA) examina la configuración real de un activo de información. Verifica que la documentación de diseño relacionada coincida con el Elemento de Configuración (CI) y confirma que los procesos de fabricación, el sistema de control de calidad, el equipo de medición y prueba, y la capacitación estén adecuadamente planificados, rastreados y controlados. La PCA también se utiliza para verificar que cualquier elemento del CI que fue rediseñado después de la finalización de la Auditoría de Configuración Funcional (FCA) también cumpla con los requisitos de la especificación de rendimiento del CI."

Los elementos que se abordan durante un PCA son:

- *La precisión de la documentación que refleja el diseño del producto.*
- *La validación de los procesos de soporte que se utilizan para producir o mantener los CI.*
- *La verificación de los CI que son rediseñados o implementados después de la FCA.*
- *PCA determina si los activos y sistemas fueron diseñados correctamente.*

Capítulo 4

GESTIÓN DE VULNERABILIDADES

4.1 GESTIÓN DE VULNERABILIDADES

CIS V8 Define la gestión de vulnerabilidades como “Desarrollar un plan para evaluar y dar seguimiento continuo a las vulnerabilidades en todos los activos dentro de la infraestructura de la empresa, con el fin de remediar y reducir la ventana de oportunidad para los atacantes. Monitorear las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades”

¿CIS V8?

El CIS v8, o "Center for Internet Security Critical Security Controls Version 8", es la octava versión de un conjunto de prácticas recomendadas diseñadas para mejorar la postura de seguridad de las organizaciones al identificar y mitigar las amenazas más comunes en entornos cibernéticos. Estas directrices, desarrolladas por expertos en ciberseguridad de todo el mundo, proporcionan un marco detallado para proteger los sistemas y datos contra las ciberamenazas más prevalentes y potencialmente dañinas.

¿Por qué es importante este control?

Los defensores cibernéticos están siendo constantemente desafiados por los atacantes que buscan vulnerabilidades dentro de su infraestructura para explotar y obtener acceso. Los defensores deben tener información oportuna sobre amenazas disponibles para ellos sobre: actualizaciones de software, parches, avisos de seguridad, boletines de amenazas, etc., y deben revisar regularmente su entorno para identificar estas vulnerabilidades antes de que lo hagan los atacantes. Comprender y gestionar las vulnerabilidades es una actividad continua que requiere un enfoque de tiempo, atención y recursos.

Los atacantes tienen acceso a la misma información y a menudo pueden aprovechar las vulnerabilidades más rápidamente de lo que una empresa puede corregir. Si bien hay una brecha en el tiempo desde que se conoce una vulnerabilidad hasta cuándo se parchea, los defensores pueden priorizar qué vulnerabilidades son las que tienen más impacto para la empresa, o es probable que se exploten primero debido a la facilidad de uso.

Por ejemplo, cuando los investigadores o la comunidad informan sobre nuevas vulnerabilidades, los proveedores deben desarrollar e implementar parches, indicadores de compromiso (IOC) y actualizaciones. Los defensores deben evaluar el riesgo de la nueva vulnerabilidad para la empresa, regresión de pruebas para parches, e instalar los parches.

Fuente: CIS Control v8 – Control 7

4.2 RIESGOS Y BENEFICIOS ASOCIADOS A LA GESTIÓN DE VULNERABILIDADES

La administración de vulnerabilidades es fundamental para cualquier organización que utilice las tecnologías de la información, ya que ofrece protección contra las amenazas conocidas y desconocidas. Con la implementación de un programa de administración de vulnerabilidades, puedes reducir el riesgo de explotación y proteger a la organización de posibles ataques.

Security 101 – What is Vulnerability Management – MICROSOFT

Algunos de los tipos de vulnerabilidades en la ciberseguridad son:

- Contraseñas no seguras
- Configuraciones, estándares o activos no configurados.
- Procedimientos insuficientes de autenticación Por ejemplo, los que no incluyen 2FA y MFA
- Estimaciones de capacidad y disponibilidad erróneas
- Comunicaciones y redes no seguras (No encriptadas)
- Falta de mecanismos de monitoreo y respuesta a incidentes

Hay muchas formas de gestionar vulnerabilidades, pero algunos de los métodos comunes son:

- ✓ Utilizar herramientas de detección para identificar posibles vulnerabilidades antes de que puedan explotarse
- ✓ Restringir el acceso a sistemas y datos confidenciales solo a usuarios autorizados
- ✓ Actualizar periódicamente las revisiones de software y seguridad
- ✓ Implementar firewalls, sistemas de detección de intrusiones y otras medidas de seguridad como protección contra los posibles ataques

Riesgos de no abordar adecuadamente la gestión de vulnerabilidades:

Exposición a Ataques	Si las vulnerabilidades no se identifican y solucionan a tiempo, los atacantes pueden explotarlas para acceder a sistemas y datos.
Interrupciones del Servicio	Al aplicar parches o actualizaciones sin una planificación adecuada, se pueden causar interrupciones no deseadas en los servicios.
Falsos Positivos	Las herramientas de escaneo pueden identificar incorrectamente vulnerabilidades que no existen, lo que puede llevar a esfuerzos innecesarios y distracciones.
Falsos Negativos	No detectar vulnerabilidades reales puede dar una falsa sensación de seguridad, dejando a la organización expuesta a amenazas.
Impacto en el Rendimiento	Algunas herramientas de escaneo pueden afectar el rendimiento de los sistemas al consumir recursos significativos durante su operación.
Conflictos de Software	La aplicación de parches o actualizaciones puede generar incompatibilidades con otros software o configuraciones existentes.
Reputación Dañada	Una gestión inadecuada de vulnerabilidades puede resultar en brechas de seguridad que dañen la reputación de la organización y erosionen la confianza de clientes y socios.

4.3 PRINCIPALES COMPONENTES DE LA GESTIÓN DE LA CONFIGURACIÓN

Existen numerosas herramientas para analizar y verificar la seguridad de los recursos empresariales.
Varias organizaciones han encontrado útiles los servicios comerciales que emplean dispositivos de análisis gestionados a distancia.
Para lograr una uniformidad en la identificación de vulnerabilidades en una organización, es recomendable usar herramientas que relacionen las vulnerabilidades detectadas con esquemas y lenguajes de clasificación de vulnerabilidades, configuración y plataforma, ampliamente reconocidos en el sector.

Algunos de estos esquemas son:

1.	Vulnerabilidades y Exposiciones Comunes	(CVE®)
2.	Comunes Enumeración de Configuración	(CCE)
3.	Lenguaje Abierto de Evaluación y Vulnerabilidad	(OVAL®)
4.	Enumeración de Plataforma Común	(CPE)
5.	Sistema de Puntuación de Vulnerabilidad Común	(CVSS)

4.3.1 PROCESO DE GESTIÓN DE VULNERABILIDADES

El ciclo de vida de vulnerabilidades es un proceso que se utiliza para identificar, evaluar y mitigar las vulnerabilidades en los sistemas o sus redes. Consta de varias fases, cada una de las cuales se lleva a cabo de manera secuencial y cíclica para garantizar una protección adecuada contra las vulnerabilidades.

01

Detección y Validación

La primera fase consiste en la detección y validación de vulnerabilidades en los sistemas y redes. Esto se logra mediante herramientas de escaneo, actividades de Red Team, o a través de la consulta de informes de alertas o avisos de seguridad.

02

Análisis

Una vez detectadas y validadas las vulnerabilidades, se lleva a cabo un análisis detallado para evaluar su gravedad y el impacto que pueden tener en el sistema y en los procesos industriales.

03

Notificación

Se notifica a los responsables de la seguridad en entornos operacionales y a los administradores del sistema sobre la existencia de las vulnerabilidades detectadas.

04

Resolución

La fase de resolución implica tomar medidas para mitigar o eliminar las vulnerabilidades detectadas. Esto puede incluir la instalación de parches, la configuración de reglas de seguridad, la implementación de controles de acceso, entre otras medidas.

05

Validación y Cierre

Una vez implementadas las medidas de mitigación, se lleva a cabo una validación para asegurarse de que las vulnerabilidades se han corregido correctamente. Finalmente, se cierra la vulnerabilidad y se actualiza el registro de seguimiento.

Ciclo de vida de las vulnerabilidades en un entorno industrial – INCIBE

4.4 ROL DE LA AUDITORÍA EN LA GESTIÓN DE VULNERABILIDADES

El rol de la auditoría en la gestión de vulnerabilidades es esencial para garantizar que las organizaciones identifiquen, evalúen y gestion en adecuadamente las vulnerabilidades en sus sistemas y aplicaciones. A continuación, se detallan las principales responsabilidades y contribuciones de la auditoría en este ámbito:

Evaluación Independiente	La auditoría proporciona una revisión objetiva e imparcial de los procesos y controles de gestión de vulnerabilidades, asegurando que se sigan las mejores prácticas y políticas establecidas.
Identificación de Brechas	A través de sus evaluaciones, la auditoría puede identificar áreas donde la gestión de vulnerabilidades puede no ser suficiente o donde existen deficiencias en los controles actuales.
Recomendaciones de Mejora	Basándose en sus hallazgos, los auditores pueden proporcionar recomendaciones específicas para fortalecer los procesos y controles de gestión de vulnerabilidades.
Verificación del Cumplimiento	La auditoría verifica que la organización cumpla con las regulaciones y normativas aplicables relacionadas con la gestión de vulnerabilidades, evitando así posibles sanciones.
Validación de Herramientas y Procesos	Los auditores evalúan la eficacia de las herramientas y procesos utilizados para identificar y remediar vulnerabilidades, asegurando que sean adecuados para el entorno y los riesgos de la organización.
Promoción de la Conciencia	La auditoría ayuda a crear conciencia a nivel de dirección y entre los empleados sobre la importancia de la gestión de vulnerabilidades y la necesidad de recursos y formación adecuados.
Seguimiento de Acciones Correctivas	Una vez identificadas las áreas de mejora, la auditoría realiza un seguimiento para asegurarse de que se implementen las acciones correctivas recomendadas.
Documentación y Registro	La auditoría asegura que exista una documentación adecuada de todos los procesos, políticas y procedimientos relacionados con la gestión de vulnerabilidades, así como de los resultados de las evaluaciones y las acciones tomadas.
Colaboración Interdepartamental	La auditoría actúa como un puente entre diferentes departamentos, como TI, seguridad y cumplimiento, facilitando la comunicación y colaboración en temas de gestión de vulnerabilidades.

4.5 CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

Para que el auditor interno pueda aprovechar al máximo esta publicación, es conveniente que se refiera a los instrumentos complementarios: Las preguntas de auditoría temáticas y el modelo de madurez general. Cada GASIC se compone de tres componentes:

Guía de Auditoría de la Seguridad de la Información y Ciberseguridad (GASIC):
Este es el cuerpo teórico y consiste en el marco contextual necesario para que el auditor interno comprenda el alcance y del dominio de seguridad que está evaluando. Es un instrumento con los conceptos fundamentales recopilados de mejores prácticas.

Modelo de Madurez:
Recopila controles desde las mejores prácticas asociadas al tema central de Guía de Auditoría, organiza los controles en una propuesta de madurez y permite al auditor conocer los requisitos que debería evaluar.

Ejemplos de Preguntas de Auditoría:
Complementa el modelo de madurez a través de una serie de preguntas organizadas en varios documentos. Cada documento representa un control que pertenece a uno de los ejes temáticos definidos al interior de la Guía de Auditoría.

La ilustración a continuación presenta esta estructura documental:

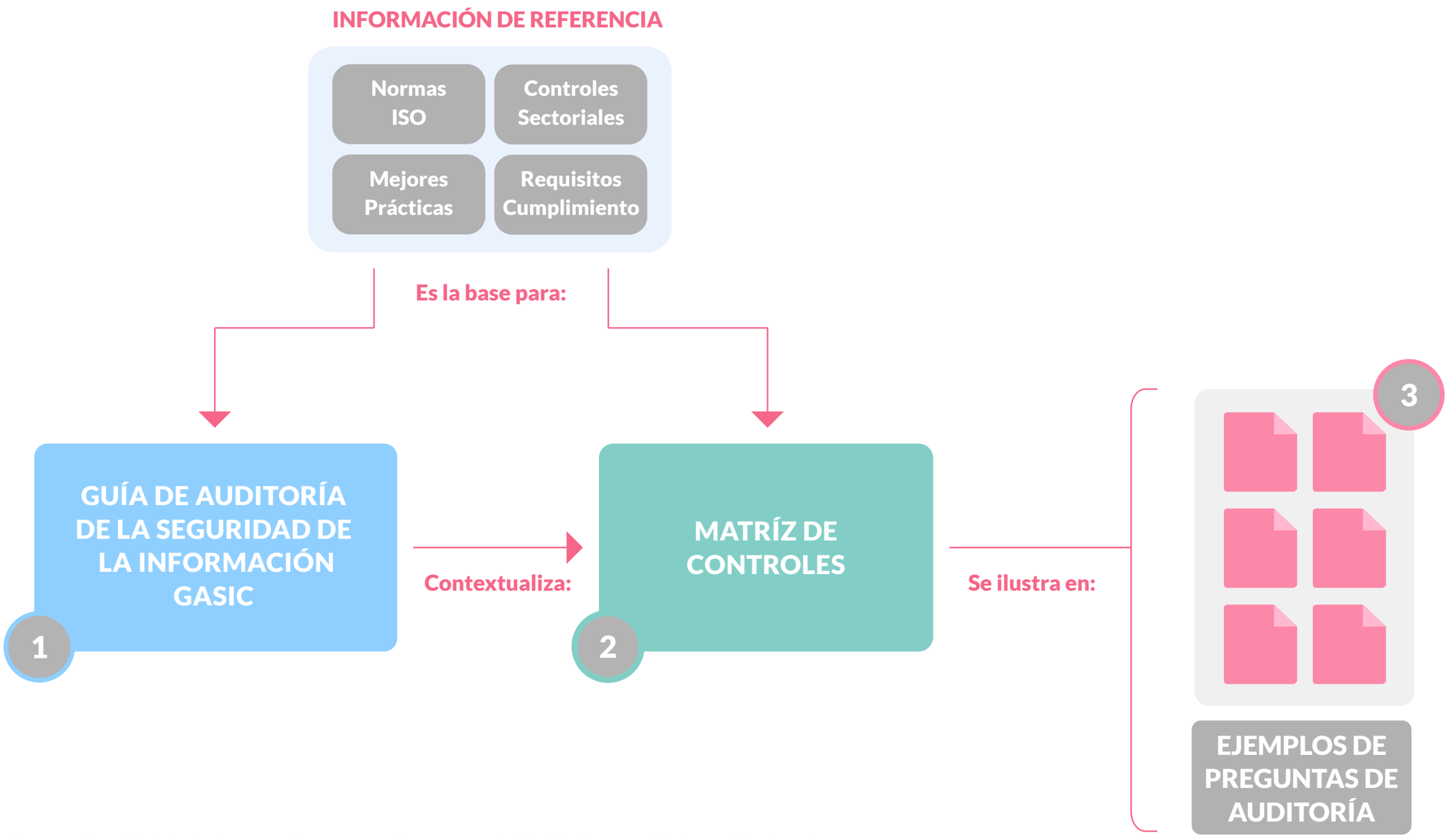

Ilustración n°5. Modo de uso y Estructura Documental GASIC. Fuente: Elaboración Propia

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría y su contexto para tener plena comprensión del tema a trabajar.**

02 **A continuación, puede utilizar el Modelo de Madurez para seleccionar los controles que sean apropiados para la organización. La selección de controles debe estar alineados con:**

a. **La estrategia de la organización.**
b. **Los resultados de la evaluación de riesgos.**
c. **Los requisitos de cumplimiento.**
d. **La estrategia de auditoría interna, expresada en el plan.**

03 **Por último, puede utilizar los documentos de ejemplo para la planificación de las preguntas y pruebas que fuese a realizar. El formato del programa, plan, instrumentos, pruebas y reportería debe ser aquel solicitado en el contexto de cada auditoría, que está fuera del alcance de esta guía.**

NOTA

Los ejemplos de pruebas tienen como propósito ilustrar la forma en la que los requisitos de los marcos que se encuentran en el matriz de controles. El auditor puede elegir utilizar un conjunto de estos ejemplos o diseñar sus propias pruebas para evaluar el nivel de cumplimiento de cada control.

En ningun caso, los ejemplos pretenden ser una lista completa; recuerde, debe contextualizar el ejercicio a la realidad de su organización.