Ciberseguridad

Topical Requirement

Requisito Temático

The Institute of
Internal Auditors

Requisito Temático Ciberseguridad

El Marco Internacional de Prácticas Profesionales (International Professional Practices Framework®) comprende las Normas Globales de Auditoría Interna (Global Internal Audit Standards™), los Requisitos Temáticos y la Guía Global. Los Requisitos Temáticos son obligatorios y deben utilizarse junto con las Normas, que proporcionan la base autorizada para las prácticas requeridas.

Los requisitos temáticos proporcionan expectativas claras para los auditores internos mediante el establecimiento de una base mínima para la auditoría de temas específicos de riesgo. El perfil de riesgo de la organización puede requerir que los auditores internos consideren aspectos adicionales sobre los temas.

La conformidad con los Requisitos Temáticos aumentará la consistencia con la que se realizan los servicios de auditoría interna y mejorará la calidad y confiabilidad en los servicios y resultados de auditoría interna. En última instancia, los Requisitos Temáticos elevan la profesión de auditoría interna.

Los auditores internos deben aplicar los Requisitos Temáticos en conformidad con las Normas Globales de Auditoría Interna. La conformidad con los Requisitos Temáticos es obligatoria para los servicios de aseguramiento y recomendada para los servicios de asesoramiento.

El requisito temático es aplicable cuando el tema es uno de los siguientes:

A. El objeto de un trabajo incluido en el plan de auditoría interna.
B. Identificado durante la ejecución de un trabajo.
C. El objeto de una solicitud de trabajo no figura en el plan de auditoría interna original.

Deben documentarse y conservarse pruebas de que se ha evaluado la aplicabilidad de cada requisito del requisito temático. Es posible que no todos los requisitos individuales se apliquen en todos los trabajos; si se excluyen requisitos, deberá documentarse y conservarse una justificación. La conformidad con los requisitos temáticos es obligatoria y se evaluará durante las evaluaciones de calidad.

Para más información, consulte la Guía del Usuario del Requisito Temático de Ciberseguridad.

Ciberseguridad

El Instituto Nacional de Normas y Tecnología (NIST) define la ciberseguridad como "La capacidad de proteger o defender el uso del ciberespacio de los ciberataques". La ciberseguridad es un subconjunto de la seguridad general de la información, que el NIST define como "la protección de la información y los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, con el fin de proporcionar confidencialidad, integridad y disponibilidad".

La ciberseguridad reduce el riesgo reforzando el entorno general de control y protegiendo los activos de información de una organización contra el acceso no autorizado, la interrupción, la alteración o la destrucción. Los ciberataques pueden provocar impactos directos e indirectos, a menudo significativos, ya que los ordenadores, las redes, los programas, los datos y la información sensible son componentes críticos para la mayoría de las organizaciones.

Evaluación y valoración de los procesos de gobernanza, gestión de riesgos y control de la Ciberseguridad

Este Requisito Temático proporciona un enfoque coherente y exhaustivo para evaluar el diseño y la implementación de la gobernanza, la gestión de riesgos y los procesos de control de la ciberseguridad. Los requisitos representan una base mínima para evaluar la ciberseguridad en una organización.

GOBERNANZA: Evaluación y valoración de la gobernanza de la ciberseguridad

Requisitos:

Los auditores internos deben evaluar lo siguiente en relación con la gobernanza de la ciberseguridad de la organización:

- **A.** Se establecen y actualizan periódicamente una estrategia y unos objetivos formales de ciberseguridad. Las actualizaciones sobre la consecución de los objetivos de ciberseguridad se comunican periódicamente y son revisadas por el Consejo, incluidos los recursos y las consideraciones presupuestarias para apoyar la estrategia de ciberseguridad.
- **B.** Se establecen y actualizan periódicamente políticas y procedimientos relacionados con la ciberseguridad para reforzar el entorno de control.
- **C.** Se han establecido funciones y responsabilidades que respaldan los objetivos de ciberseguridad, y existe un proceso para evaluar periódicamente los conocimientos, competencias y capacidades de las personas que desempeñan estas funciones
- **D.** Las partes interesadas se comprometen a debatir y actuar sobre las vulnerabilidades existentes y las amenazas emergentes en el entorno de la ciberseguridad. Entre las partes interesadas se incluyen la Alta Dirección, operaciones, gestión de riesgos, recursos humanos, legal, cumplimiento, proveedores y otros.

GESTIÓN DE RIESGOS: Evaluación y valoración de la gestión de riesgos de Ciberseguridad

Requisitos:

Los auditores internos deben evaluar lo siguiente en relación con la gestión de riesgos de ciberseguridad de la organización:

- **A.** Los procesos de evaluación y gestión de riesgos de la organización incluyen la identificación, el análisis, la mitigación y el seguimiento de las amenazas de ciberseguridad y su efecto en la consecución de los objetivos estratégicos.
- **B.** La gestión del riesgo de ciberseguridad se lleva a cabo en toda la organización y puede incluir las siguientes áreas: tecnología de la información, gestión del riesgo empresarial, recursos humanos, legal, cumplimiento, operaciones, cadena de suministro, contabilidad, finanzas y otras.
- **C.** Se establece la rendición de cuentas y la responsabilidad de la gestión de los riesgos de ciberseguridad. Se designa a una persona o a un equipo para que supervise e informe periódicamente sobre la gestión de los riesgos de ciberseguridad, incluidos los recursos necesarios para mitigar los riesgos e identificar las nuevas amenazas de ciberseguridad.
- **D.** Se establece un proceso para escalar rápidamente cualquier riesgo de ciberseguridad (emergente o previamente identificado) que alcance un nivel inaceptable según las directrices de gestión de riesgos establecidas por la organización o los requisitos legales y reglamentarios aplicables. Deben considerarse los impactos financieros y no financieros del riesgo de ciberseguridad.
- **E.** Se establece un proceso para comunicar la concienciación sobre los riesgos de ciberseguridad a la dirección y a los empleados, y para que la dirección revise periódicamente los problemas, brechas, deficiencias o fallos de control, informando y corrigiendo oportunamente
- **F.** La organización ha implantado un proceso de respuesta y recuperación ante incidentes de ciberseguridad que incluye la detección, contención, recuperación y análisis posterior al incidente. El proceso de respuesta y recuperación ante incidentes se prueba periódicamente.

CONTROLES: Evaluación y valoración de los procesos de control de la Ciberseguridad

Requisitos:

Los auditores internos deben evaluar lo siguiente en relación con los procesos de control de la ciberseguridad de la organización:

- **A.** Se establece un proceso para garantizar que existen controles internos y controles basados en proveedores para proteger la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización. Se realizan evaluaciones periódicas para determinar si los controles funcionan de manera que promuevan la

consecución de los objetivos de ciberseguridad de la organización y la rápida resolución de problemas.

B. Se establece un proceso de gestión del talento que incluye la formación para desarrollar y mantener las competencias técnicas relacionadas con las operaciones de ciberseguridad. Este proceso se revisa periódicamente.

C. Se establece un proceso para supervisar e informar continuamente sobre las amenazas y vulnerabilidades emergentes en materia de ciberseguridad y para identificar, priorizar y aplicar oportunidades para mejorar las operaciones de ciberseguridad.

D. La ciberseguridad se incluye en la gestión del ciclo de vida (selección, uso, mantenimiento y desmantelamiento) de todos los activos informáticos, incluidos el hardware, el software y los servicios de proveedores.

E. Se establecen procesos para reforzar la ciberseguridad, incluida la configuración, la administración de dispositivos de usuario final, el cifrado, la aplicación de parches, la gestión de accesos de los usuarios y la supervisión de la disponibilidad y el rendimiento. Se incluyen consideraciones de ciberseguridad en el desarrollo de software (DevSecOps).

F. Se establecen controles relacionados con la red, tales como controles de acceso a la red y segmentación; el uso y colocación de cortafuegos; conexiones limitadas desde y hacia redes externas; red privada virtual (VPN)acceso a red de confianza cero (ZTNA); controles de red en Internet de las Cosas (IoT); y sistemas de detección/prevención de intrusiones (IDS e IPS).

G. Se establecen controles de seguridad de las comunicaciones de punto final para servicios como el correo electrónico, los navegadores de Internet, las videoconferencias, la mensajería, las redes sociales, la nube y los protocolos de intercambio de archivos.

Acerca del Instituto de Auditores Internos

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional que cuenta con más de 255.000 miembros en todo el mundo y ha concedido más de 200.000 certificaciones de Auditor Interno Certificado® (CIA®) en todo el mundo. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite www.theiia.org.

Copyright

Febrero de 2025

The Institute of Internal Auditors

Sede mundial
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, EE.UU.
Teléfono: +1-407-937-1111
Fax: +1-407-937-1101