Ciberseguridad

Topical Requirement

Requisito Temático

Guía de usuario

The Institute of
Internal Auditors

Contenido

Resumen de los Requisitos Temáticos

Los Requisitos Temáticos son un componente esencial del Marco Internacional para la Práctica Profesional (International Professional Practices Framework®), junto con las Normas Globales de Auditoría Interna (Global Internal Audit Standards™) y las Guías Globales. El Instituto de Auditores Internos requiere que los Requisitos Temáticos sean utilizados conjuntamente con las Normas Globales de Auditoría Interna, las cuales proporcionan la base autorizada de las prácticas requeridas. Las referencias a las Normas aparecen a lo largo de esta guía como una fuente de información más detallada

Los requisitos temáticos formalizan cómo los auditores internos abordan las áreas de riesgo prevalentes para promover la calidad y la coherencia dentro de la profesión. Los requisitos temáticos establecen una base y proporcionan criterios relevantes para la realización de servicios de aseguramiento relacionados con el tema de un requisito temático (Norma 13.4 Criterios de evaluación). La conformidad con los requisitos temáticos es obligatoria para los servicios de aseguramiento y recomendada para la evaluación durante los servicios de asesoramiento. Los requisitos temáticos no pretenden abarcar todos los aspectos potenciales que deben tenerse en cuenta al realizar encargos de aseguramiento, sino más bien proporcionar un conjunto mínimo de requisitos que permitan una evaluación coherente y fiable del tema.

Los requisitos temáticos están claramente vinculados al Modelo de las Tres Líneas del IIA y a las Normas Globales de Auditoría Interna. La gobernanza, la gestión de riesgos y los procesos de control son los principales componentes de los requisitos temáticos que se ajustan a la Norma 9.1 Comprender los procesos de gobierno, gestión de riesgos y control. En referencia al Modelo de las Tres Líneas, la gobernanza se vincula al Consejo/órgano de gobierno, la gestión de riesgos se vincula a la segunda línea, y los controles o procesos de control se vinculan a la primera línea. Mientras que la dirección está representada tanto en la primera como en la segunda línea, la función de auditoría interna se representa en la tercera línea como un proveedor de aseguramiento independiente y objetivo, que informa al Consejo/órgano de gobierno (Principio 8 Supervisión del Consejo)

Aplicabilidad, riesgo y criterio profesional

Los requisitos temáticos deben cumplirse cuando las funciones de auditoría interna realicen encargos de aseguramiento sobre temas para los que exista un requisito temático o cuando se identifiquen aspectos del requisito temático en otros encargos de aseguramiento.

Como se describe en las Normas, la evaluación del riesgo es una parte importante de la planificación del Director de Auditoría Interna. Determinar los encargos de aseguramiento a incluir en el plan de auditoría interna requiere evaluar las estrategias, objetivos y riesgos de

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

la organización al menos anualmente (Norma 9.4 Plan de Auditoría Interna). Al planificar encargos individuales de aseguramiento, los auditores internos deben evaluar los riesgos relevantes para el encargo (Norma 13.2 Evaluación de riesgos del Encargo).

Cuando el tema de un Requisito Temático se identifica durante el proceso de planificación de auditoría interna basada en riesgos y se incluye en el plan de auditoría, entonces los requisitos descritos en el Requisito Temático deben ser utilizados para evaluar el tema dentro de los compromisos aplicables. Además, cuando los auditores internos realicen un encargo (incluido o no en el plan) y surjan elementos de un Requisito Temático, deberá evaluarse la aplicabilidad del Requisito Temático como parte del encargo. Por último, si se solicita un encargo que no estaba originalmente en el plan e incluye el tema, debe evaluarse la aplicabilidad del Requisito Temático.

El juicio profesional desempeña un papel clave en la aplicación del Requisito Temático. Las evaluaciones de riesgo impulsan las decisiones de los Directores de Auditoría Interna sobre qué compromisos incluir en el plan de auditoría interna (Norma 9.4 Plan de Auditoría Interna). Adicionalmente, los auditores internos utilizan su juicio profesional para determinar qué aspectos serán cubiertos dentro de cada trabajo (Normas 13.3 Objetivos y Alcance del trabajo, 13.4 Criterios de evaluación, y 13.6 Programa de trabajo). El Apéndice A "Ejemplos de Aplicación Práctica" describe cómo los auditores internos determinan si el Requisito Temático es aplicable.

Deberán conservarse pruebas de que se ha evaluado la aplicabilidad de cada uno de los requerimientos del Requisito Temático, incluida una justificación de la exclusión de cualquier requisito. La conformidad con el Requisito Temático debe documentarse utilizando el juicio profesional del auditor, tal como se describe en la norma 14.6, Documentación de los trabajos..

Aunque el Requisito Temático de Ciberseguridad proporciona una base de procesos de control a tener en cuenta, las organizaciones que evalúan el riesgo de ciberseguridad como muy alto pueden necesitar evaluar aspectos adicionales.

Si un Director de Auditoría Interna determina que la función de auditoría interna no tiene los conocimientos necesarios para llevar a cabo trabajos de auditoría sobre un tema del Requisito Temático, el trabajo puede ser subcontratado (Normas 3.1 Competencia, 7.2 Cualificaciones del Director de Auditoría Interna, 10.2 Gestión de los recursos humanos). Incluso en este caso, la externalización no exime a la función de auditoría interna de su responsabilidad de cumplir con los requisitos temáticos. El Director de Auditoría Interna mantiene la responsabilidad última de garantizar la conformidad. Además, si el Director de Auditoría Interna determina que los recursos de auditoría interna son insuficientes, el Director de Auditoría Interna debe informar al Consejo sobre el impacto de la insuficiencia de recursos y cómo se abordará cualquier déficit de recursos (Norma 8.2 Recursos).

Rendimiento, documentación e informes

Al aplicar los Requisitos Temáticos, los auditores internos también deben ajustarse a las Normas, realizando su trabajo de acuerdo con el Dominio V: Desempeño de los Servicios de Auditoría Interna. Las normas del dominio V describen la planificación de los trabajos

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

(Principio 13 Planificar eficazmente los trabajos), la realización de los trabajos (Principio 14 Ejecución de los trabajos) y la comunicación de los resultados de los trabajos (Principio 15 Comunicar las conclusions del trabajo y monitorear los planes de acción).

La cobertura del requisito temático puede documentarse en el plan de auditoría interna o en los papeles de trabajo del trabajo, basándose en el juicio profesional de los auditores. Uno o más encargos de auditoría interna pueden cubrir los requisitos. Además, puede que no todos los requisitos sean aplicables. Deben conservarse pruebas de que se ha evaluado la aplicabilidad del Requisito Temático, incluida una justificación que explique cualquier exclusión

La herramienta opcional del Apéndice C puede utilizarse como referencia y para documentar el trabajo que realizan los auditores internos

Aseguramiento de laCalidad

Las Normas exigen que el Director de Auditoría Interna desarrolle, implemente y mantenga un Programa de Aseguramiento y Mejora de la Calidad que abarque todos los aspectos de la función de auditoría interna (Norma 8.3 Calidad). Los resultados deben comunicarse al Consejo y a la Alta Dirección. Las comunicaciones deben informar sobre la conformidad de la función de auditoría interna con las Normas y el logro de los objetivos de desempeño.

La conformidad con los requisitos temáticos se evaluará en las evaluaciones de calidad. Para preparar una revisión de calidad, los auditores internos pueden utilizar la herramienta que figura en el Apéndice C.

Ciberseguridad

La ciberseguridad es un tema amplio relacionado con la mayoría de los aspectos tecnológicos de cualquier organización. Además de la tecnología de la información, la ciberseguridad suele formar parte de los procesos empresariales, lo que exige que los auditores internos evalúen los riesgos relacionados con la ciberseguridad a la hora de planificar, determinar el alcance y ejecutar los trabajos de aseguramiento.

El Instituto Nacional de Normas y Tecnología (NIST), que forma parte del Departamento de Comercio de EE.UU., define la ciberseguridad como "La capacidad de proteger o defender el uso del ciberespacio de los ciberataques". El Requisito Temático de Ciberseguridad se centra en el perímetro externo que las organizaciones aseguran para mitigar los riesgos de usuarios no autorizados y amenazas cibernéticas maliciosas. 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 contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción con el fin de proporcionar confidencialidad, integridad y disponibilidad."

Entre los requisitos del Requisito Temático de Ciberseguridad se incluyen:

- Gobernanza: objetivos y estrategias básicos de ciberseguridad claramente definidos que respalden los objetivos, políticas y procedimientos de la organización.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- Gestión de riesgos: procesos para identificar, analizar, gestionar y supervisar las ciberamenazas, incluido un proceso para escalar los ciberriesgos con prontitud.
- Controles: procesos de control establecidos por la dirección y evaluados periódicamente para mitigar el ciberriesgo.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Consideraciones

Los auditores internos pueden utilizar las siguientes consideraciones como ayuda para su evaluación de los requisitos del Requisito Temático de Ciberseguridad. Estas consideraciones, que hacen referencia a los requisitos, son ilustrativas pero no obligatorias. Los auditores internos deben basarse en su juicio profesional para determinar qué incluir en sus evaluaciones.

Consideraciones sobre la gobernanza

Para evaluar cómo se aplican los procesos de gobernanza a los objetivos de ciberseguridad, los auditores internos pueden revisar:

A. Plan estratégico y objetivos de ciberseguridad formalizados y documentados, incluyendo pruebas de que el consejo revisa periódicamente (generalmente trimestralmente) las actualizaciones de ciberseguridad proporcionadas por el responsable de la función de seguridad de la información, como el director de seguridad de la información (CISO). Las pruebas pueden incluir informes sobre:
   - Supervisar la consecución de los objetivos estratégicos.
   - Necesidades presupuestarias para apoyar las metas y objetivos de ciberseguridad.
   - Centrarse en los riesgos y los controles internos, incluidos los avances en la corrección.
   - Indicadores clave de rendimiento (KPI) para medir el éxito.
   - Recursos humanos necesarios para contratar, formar y desarrollar al personal de ciberseguridad.

B. Políticas, procedimientos y otra documentación relevante utilizada para gestionar los procesos de ciberseguridad, incluyendo:
   - Políticas revisadas y actualizadas al menos una vez al año. Los nuevos riesgos cibernéticos pueden requerir revisiones y actualizaciones más frecuentes.
   - Un proceso para determinar si las políticas y procedimientos son suficientes para respaldar las operaciones de ciberseguridad.
   - Marcos ampliamente adoptados (NIST, COBIT y otros) para reforzar los procesos de ciberseguridad y los controles internos.

C. Funciones y responsabilidades que apoyen la consecución de los objetivos de ciberseguridad, incluida una estructura que garantice que la función de ciberseguridad dependa de un nivel de la organización que tenga suficiente visibilidad para lograr el apoyo de la organización.
   - Un proceso para evaluar periódicamente los conocimientos, competencias y habilidades del personal que desempeña funciones de ciberseguridad.

D. Pruebas del compromiso con las partes interesadas pertinentes (por ejemplo, la alta dirección, operaciones, gestión de riesgos, recursos humanos, jurídico,

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

cumplimiento, proveedores estratégicos y otros), incluida la comunicación sobre los riesgos cibernéticos existentes y emergentes y las vulnerabilidades potenciales conocidas. Las pruebas de comunicación pueden incluir actas de reuniones, informes o correos electrónicos.

Consideraciones sobre la gestión de riesgos

Para evaluar cómo se aplican los procesos de gestión de riesgos a los objetivos de ciberseguridad, los auditores internos pueden revisar:

A. Cómo evalúa y gestiona la organización los riesgos de ciberseguridad, incluyendo cómo las amenazas y vulnerabilidades son:
   - Inicialmente identificadas e informadas.
   - Analizadas para evaluar el riesgo para la consecución de los objetivos de la organización.
   - Mitigadas, incluyendo planes de acción para reducir el riesgo a un nivel aceptable.
   - Supervisadas, incluyendo un plan de información continua hasta que las amenazas se hayan resuelto por completo.

B. Cómo obtiene la organización información periódica sobre la gestión de riesgos de ciberseguridad de las áreas funcionales, tales como: tecnología de la información (TI), gestión de riesgos empresariales, recursos humanos, legal, cumplimiento, operaciones, contabilidad y finanzas. Se puede utilizar un equipo de ciberseguridad interfuncional o un comité directivo de TI para obtener información.

C. Cómo ha asignado la organización la responsabilidad sobre la gestión de los riesgos de ciberseguridad a un individuo o equipo
   - La(s) persona(s) responsable(s) debe(n) comunicar periódicamente (trimestralmente, mensualmente o cuando sea necesario) las actualizaciones continuas de los riesgos de ciberseguridad a toda la organización y también puede(n) incluir las necesidades de recursos para las estrategias de mitigación de riesgos.

D. Los procesos de escalado de los riesgos de ciberseguridad, incluyendo cómo se evalúa, asigna y prioriza el nivel de amenaza o riesgo. La revisión puede incluir la identificación de los:
   - Niveles de riesgo definidos por la organización -como alto, moderado y bajo- con explicaciones detalladas de cada nivel de riesgo y los procedimientos de escalamiento para cada categoría de riesgo.
   - Lista de riesgos de ciberseguridad identificados actualmente y estado de mitigación de cada evento de riesgo.
   - Requisitos legales, reglamentarios y de cumplimiento aplicables.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- Impacto de los riesgos financieros y no financieros (por ejemplo, reputación).

E. El proceso para comunicar los riesgos de ciberseguridad a la dirección y a los empleados, incluyendo:
   - Formación periódica (al menos una vez al año) sobre ciberseguridad para los empleados, tales como campañas de phishing simuladas y sin previo aviso para comprobar y realizar un seguimiento de la concienciación de la organización.
   - Actualizaciones sobre la corrección de los problemas de ciberseguridad existentes, con fechas de finalización previstas.
   - Supervisión del incumplimiento que incluye actualizaciones para el Consejo y la Alta Dirección.
   - Reevaluar las amenazas cuando cambien el apetito de riesgo y la tolerancia al riesgo de la organización.

F. Procesos que la organización ha implementado en relación con la respuesta ante incidentes y la recuperación, que incluyen:
   - Un plan documentado que se revisa y actualiza a medida que las operaciones de la organización cambian con el tiempo. El plan debe incluir:
     - Cómo se detectan y notifican los incidentes.
     - Cómo se contienen los incidentes para evitar daños mayores.
     - Cómo se recuperará y responderá la organización para reanudar las operaciones.
     - Cómo se analizará el incidente para identificar las lecciones aprendidas y cómo prevenir sucesos similares en el futuro.
   - Pruebas periódicas (al menos una vez al año) (ejercicios teóricos) y comunicación de los resultados a la Alta Dirección y a las partes interesadas. Las pruebas pueden dar lugar a planes de acción.

Consideraciones sobre el proceso de control

Para evaluar cómo se aplican los procesos de control a los objetivos de ciberseguridad, los auditores internos pueden revisar:

A. Enfoque de la dirección para construir un entorno de control interno de ciberseguridad eficaz, incluyendo:
   - Evaluar y aplicar los controles internos necesarios tanto para mitigar los riesgos elevados como para proteger los datos sensibles, críticos, personales o confidenciales, basándose en el proceso de evaluación de riesgos de la organización.
   - Determinar las necesidades de recursos para mantener los controles clave de ciberseguridad.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- Considerar los controles basados en proveedores como parte del entorno de control, lo que incluye revisar los informes de controles de las organizaciones de servicios (SOC) de los proveedores antes de iniciar la relación comercial y durante toda la vigencia de la misma.
- Comprobación periódica de que los controles de ciberseguridad funcionan de forma que se mitigan los riesgos y se apoya la consecución de los objetivos de ciberseguridad.
- Proceso para subsanar las deficiencias de control interno o abordar las conclusiones de las evaluaciones realizadas por la función de auditoría interna u otros proveedores de aseguramiento (por ejemplo, pruebas de intrusión).

B. El proceso de gestión del talento de la organización para la contratación y formación de profesionales de ciberseguridad, incluyendo cómo la organización identifica oportunidades para aumentar las capacidades de los profesionales de ciberseguridad para apoyar el conocimiento técnico y mejorar la concienciación de la organización sobre problemas emergentes.
   - Algunos ejemplos son la participación en cursos de formación, la implicación en grupos de intercambio de conocimientos y la formación profesional continua, que incluye la obtención de certificaciones relacionadas con la cibernética.

C. El proceso de la dirección para identificar, priorizar, supervisar y notificar las amenazas y vulnerabilidades emergentes en materia de ciberseguridad de forma continua y centrada en las operaciones diarias. La revisión puede incluir que se establezcan procesos para evaluar las amenazas y vulnerabilidades relacionadas con tecnologías nuevas o emergentes, como el uso de inteligencia artificial.

D. Procesos y controles establecidos para gestionar y proteger los activos informáticos a lo largo de su ciclo de vida, incluida la selección, el uso, el mantenimiento y el desmantelamiento de hardware, software y servicios de proveedores. El hardware incluye servidores, equipos de red (como routers o cortafuegos), ordenadores de sobremesa, portátiles, teléfonos móviles, tabletas y periféricos. El software incluye sistemas operativos (como Windows), software de planificación de recursos empresariales, aplicaciones, programas antivirus y otros. Las consideraciones sobre el hardware y software pueden incluir:
   - El uso por parte de la organización del cifrado, software antivirus, gestión de dispositivos móviles, requisitos de contraseñas complejas, redes privadas virtuales (VPN)/red de confianza cero (ZTN) para la autenticación y actualización periódica del firmware.
   - Un proceso de gestión de activos que garantice que el hardware suministrado por la empresa tenga una configuración de seguridad adecuada en el momento de su entrega y se elimine correctamente cuando se retiren los activos.
   - Controles relacionados con las bases de datos, que incluyen limitar el acceso de usuarios y administradores, garantizar el uso de cifrado, la realización de copias de seguridad y pruebas de las bases de datos, y la presencia de fuertes controles de seguridad de la red.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

- Cómo se tienen en cuenta las amenazas o vulnerabilidades de ciberseguridad en el ciclo de vida de desarrollo de sistemas (SDLC).
- El enfoque utilizado por desarrollo, seguridad y operaciones (DevSecOps) para garantizar que el proceso de desarrollo de software, incluyendo la ciberseguridad para identificar vulnerabilidades de forma proactiva.

E. Procesos utilizados para reforzar la ciberseguridad, incluyendo:
   - Configuración de los parámetros de seguridad para minimizar los riesgos de ciberseguridad.
   - La administración de dispositivos móviles (incluido el uso del correo electrónico y las aplicaciones) está configurada para mitigar los riesgos de ciberseguridad y gestionarse de forma remota si el dispositivo de un usuario se ve comprometido.
   - El uso del cifrado para datos "en reposo", como la información almacenada en un disco duro, o datos "en tránsito", como el cifrado de correos electrónicos.
   - Parchear servidores o software (como un sistema operativo) con las últimas versiones de seguridad.
   - Gestión del acceso de los usuarios, como el uso de autenticación multifactor (MFA) e identificadores de usuario únicos con contraseñas complejas que caducan periódicamente.
   - Controles de supervisión establecidos para determinar si la disponibilidad y la utilización de los recursos funcionan adecuadamente, lo que permite revisar y analizar posibles problemas de ciberseguridad que amenacen al rendimiento.
   - Integración de la ciberseguridad en el SDLC para identificar y abordar las vulnerabilidades de ciberseguridad antes de que el software pase a producción.

F. Controles relacionados con la red que aseguran el perímetro de la organización, incluyendo cómo la organización utiliza:
   - Segmentación de la red.
   - Cortafuegos.
   - Controles de acceso de los usuarios.
   - Limitaciones a las conexiones externas e internas.
   - Controles en torno al Internet de las cosas (IoT) para redes interconectadas.
   - Sistemas de detección/prevención de intrusiones para prevenir, detectar y recuperarse de los ataques a la ciberseguridad.

G. Controles en torno a la seguridad de las comunicaciones de punto final (endpoints) aplicables a servicios como el correo electrónico, los navegadores de Internet, las videoconferencias, la mensajería (Zoom, MS Teams y otros), las redes sociales, la nube y los protocolos de intercambio de archivos. Los controles pueden incluir la restricción del uso de determinadas extensiones de archivo (como los archivos .exe) y la autenticación multifactor para compartir archivos.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Apéndice A. Ejemplos de aplicación práctica

Los siguientes ejemplos describen escenarios en los que sería aplicable el Requisito Temático de Ciberseguridad:

Ejemplo 1: La ciberseguridad se identifica para un trabajo de auditoría interna incluido en el plan de auditoría interna.

Cuando la función de auditoría interna complete su proceso de planificación basado en riesgos e incluya uno o más trabajos sobre ciberseguridad en el plan de auditoría interna, el requisito temático será obligatorio al realizar dichos trabajos. La conformidad puede lograrse incluyendo los requisitos en uno o más encargos del plan de auditoría interna.

La ciberseguridad es un tema amplio, y no todos los requisitos del Requisito Temático pueden aplicarse a todos los trabajos. Cuando los auditores internos apliquen su juicio profesional y determinen que uno o más requisitos del Requisito Temático de Ciberseguridad no son aplicables y, por lo tanto, deben excluirse de un trabajo, los auditores internos deben documentar y conservar la justificación para excluir dichos requisitos. Por ejemplo, la justificación para excluir algunos requisitos podría ser que la función de auditoría interna realiza varios trabajos de ciberseguridad de forma rotatoria o ha determinado que la importancia del riesgo en el trabajo es baja.

Ejemplo 2: Los riesgos de ciberseguridad se identifican durante un trabajo de auditoría que no se centra en la ciberseguridad.

Los auditores internos pueden identificar riesgos de ciberseguridad mientras evalúan un proceso no directamente relacionado con la ciberseguridad. Por ejemplo, los auditores internos pueden estar evaluando el proceso de cuentas por pagar en un trabajo no centrado en la ciberseguridad y no identificar los riesgos de ciberseguridad dentro del alcance al planificar el trabajo. Sin embargo, después de realizar el recorrido inicial, los auditores internos determinan que dichos riesgos deben estar dentro del alcance; por ejemplo, identifican riesgos de ciberseguridad relacionados con la presentación por Internet de una solicitud inicial de orden de compra (Norma 13.2 Evaluación de riesgos del trabajo).

Una vez identificados los riesgos relevantes, los auditores internos deben revisar el requisito temático de ciberseguridad y determinar qué requisitos son aplicables. En este ejemplo, podrían excluir el proceso de gobernanza de la ciberseguridad o el proceso de gestión de riesgos de ciberseguridad. Deben documentar en los papeles de trabajo del trabajo los motivos para excluir los demás requisitos del Requisito Temático l de Ciberseguridad y conservar la documentación.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Ejemplo 3: Se solicita un trabajo de ciberseguridad que no estaba incluido originalmente en el plan de auditoría interna.

Las partes interesadas, como el cCnsejo, la dirección o un regulador, pueden pedir a los auditores internos que realicen evaluaciones de ciberseguridad fuera del plan de auditoría original. Por ejemplo, cuando las organizaciones son objeto de un ciberataque, el Consejo puede solicitar un trabajo de auditoría interna para evaluar los controles de ciberseguridad. El Requisito Temático es aplicable, los requisitos deben ser evaluados, y cualquier exclusión debe ser documentada.

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Apéndice B. Correspondencia con Marcos de referencia

La organización puede tener sus propios esfuerzos de ciberseguridad, utilizando marcos de referencia en gestión de riesgos y gobernanza como COBIT o NIST. Los auditores internos pueden haber desarrollado ya programas de auditoría y procedimientos de pruebas basados en estos marcos. Los auditores internos deben conciliar sus pruebas de controles de ciberseguridad previstas con el Requisito Temático para garantizar una cobertura adecuada. El siguiente cuadro relaciona el Requisito Temático de Ciberseguridad con tres marcos de referencia de uso común: Marco de Ciberseguridad NIST 2.0, COBIT 2019, y NIST 800-53. Estos marcos se han mapeado ya que están disponibles sin coste alguno.

Requisitos de gobernanza	Marco de referencia		
	LCR 2.0 DEL NIST	NIST 800-53	COBIT 2019
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.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Se establecen políticas y procedimientos relacionados con la ciberseguridad, que se actualizan periódicamente y refuerzan el entorno de control.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
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 quienes desempeñan esas funciones.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

D. Las partes interesadas pertinentes 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, las operaciones, la gestión de riesgos, los recursos humanos, el departamento legal, de cumplimiento, los proveedores y otros.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Requisitos para la gestión de riesgos	**LCR 2.0 DEL NIST**	**NIST 800-53**	**COBIT 2019**
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 a la ciberseguridad y su efecto en la consecución de los objetivos estratégicos.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. La gestión del riesgo de ciberseguridad se lleva a cabo en toda la organización, lo que puede incluir las siguientes áreas: tecnología de la información, gestión de riesgos empresariales, recursos humanos, legal, cumplimiento, operaciones, cadena de suministro, contabilidad, finanzas y otras.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Se establece la rendición de cuentas y la responsabilidad sobre la gestión de los riesgos de ciberseguridad y se identifica a una persona o equipo para supervisar e informar periódicamente sobre cómo se están gestionando los riesgos de ciberseguridad, incluidos los recursos necesarios para mitigar los riesgos e identificar las amenazas emergentes de ciberseguridad.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

D. Se establece un proceso para escalar rápidamente cualquier riesgo de ciberseguridad (emergente o previamente identificado) que se eleve a un nivel inaceptable sobre las directrices de gestión de riesgos establecidas por la organización o para cumplir con los requisitos legales y reglamentarios aplicables. Deben tenerse en cuenta los impactos financieros y no financieros del riesgo de ciberseguridad.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Se establece un proceso para comunicar la concienciación sobre los riesgos de ciberseguridad a la dirección y a los empleados, y para la revisión periódica por parte de la dirección de los problemas, brechas, deficiencias o fallos de control con notificación y corrección.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
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.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Requisitos del proceso de control	**LCR 2.0 DEL NIST**	**NIST 800-53**	**COBIT 2019**

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

A. Se establece un proceso que garantiza la existencia de controles internos y controles en proveedores para proteger la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización. Los controles se evalúan periódicamente para determinar si funcionan de manera que promuevan el logro de los objetivos de ciberseguridad de la organización y la resolución oportuna de los problemas.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. Se establece y revisa periódicamente un proceso de gestión del talento para las operaciones de ciberseguridad que incluye oportunidades de formación para desarrollar y mantener las competencias técnicas.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
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.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
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.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. Se establecen procesos para promover la ciberseguridad, incluida la configuración, la administración de dispositivos de usuario final, el cifrado, la aplicación de parches, la gestión del acceso de los usuarios y la supervisión de la disponibilidad y el rendimiento. Se incluyen consideraciones de ciberseguridad en el desarrollo de software (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

F. Se establecen controles relacionados con la red, como controles de acceso a la red y segmentación; el uso y la colocación de cortafuegos; conexiones limitadas desde y hacia redes externas; red privada virtual (VPN)/acceso a red de confianza cero (ZTNA), inclusión de controles de red de Internet de las Cosas (IoT) y sistemas de detección/prevención de intrusiones (IDS e IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Se establecen controles de seguridad de las comunicaciones de punto final en relación con 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.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Apéndice C. Herramienta de documentación opcional

Se espera que los auditores internos ejerzan su juicio profesional para determinar la aplicabilidad de los requisitos, basándose en la evaluación de riesgos y documenten adecuadamente las exclusiones de determinados requisitos. El Requisito Tmático puede documentarse en el plan de auditoría interna o en los papeles de trabajo del trabajo basándose en el juicio profesional del auditor. Uno o más trabajos de auditoría interna pueden cubrir los requisitos. Además, puede que no todos los requisitos sean aplicables. El formulario imprimible que figura a continuación ofrece una opción para documentar la conformidad con el Requisito Temático de Ciberseguridad, pero su uso no es obligatorio.

Ciberseguridad - Gobernanza

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
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 políticas y procedimientos relacionados con la ciberseguridad, que se actualizan periódicamente y refuerzan 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 quienes desempeñan dichas funciones.		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
D. Las partes interesadas pertinentes 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, los proveedores y otros.		

Ciberseguridad - Gestión de riesgos

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
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 de riesgos, recursos humanos, legal, cumplimiento, operaciones, cadena de suministro, contabilidad, finanzas y otras.		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
C. Se establecen la rendición de cuentas y la responsabilidad sobre la gestión de los riesgos de ciberseguridad. Se identifica a una persona o equipo que supervisa e informa periódicamente sobre cómo se están gestionando los riesgos de ciberseguridad, incluidos los recursos necesarios para mitigar los riesgos e identificar las nuevas amenazas a la 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, con información y correcciones oportunas.		
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.		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Ciberseguridad - Procesos de control

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
A. Se establece un proceso para garantizar la existencia de controles internos y controles 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. El proceso se revisa periódicamente.		
C. Se establece un proceso para supervisar e informar continuamente de 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.		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

Requisito	Cobertura ejecutada o justificación de la exclusión	Documentación de referencia
E. Se establecen procesos para promover la ciberseguridad, incluida la configuración, la administración de dispositivos de usuario final, el cifrado, la aplicación de parches, la gestión del acceso 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, como controles de acceso a la red y segmentación; el uso y la ubicación de cortafuegos; conexiones limitadas desde y hacia redes externas; red privada virtual (VPN)/acceso a red de confianza cero (ZTNA), controles de red de 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.		

©2025, The Institute of Internal Auditors. All Rights Reserved.
For individual personal use only.

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 Certified Internal Auditor® (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 www.theiia.org.

Descargo de responsabilidad

El IIA publica este documento con fines informativos y educativos. Este material no pretende dar respuestas definitivas a circunstancias individuales específicas y, como tal, sólo pretende servir de guía. El IIA recomienda buscar asesoramiento experto independiente relacionado directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Copyright

2025 The Institute of Internal Auditors, Inc. Todos los derechos reservados. Para obtener permiso de reproducción, póngase en contacto con .copyright@theiia.org

Febrero de 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101