Requisito temático de Ciberseguridad

¿Qué son los requisitos temáticos?

Los Requisitos Temáticos son un componente esencial del Marco Internacional de Prácticas Profesionales®, que también incluye las Normas Globales de Auditoría Interna™ y las Guías Globales. El Instituto de Auditores Internos, como organismo normativo de la profesión de auditoría interna, exige estos Requisitos Temáticos obligatorios como complemento de las Normas Globales de Auditoría Interna, que sirven como autoridad para las prácticas requeridas descritas y referenciadas en los Requisitos Temáticos.

Los requisitos temáticos proporcionan una estructura para los temas globales auditados frecuentemente que suelen ser de mayor riesgo y de naturaleza generalizada. Aunque las Normas se aplican a todos los servicios de auditoría interna prestados, un requisito temático debe considerarse como un requisito obligatorio adicional que debe cumplirse cuando ese tema es el objeto de un encargo de auditoría interna.

Los requisitos temáticos deben aplicarse, a nivel de entidad u organización, a los temas que tienen un impacto en toda la organización. Los auditores internos deben estar familiarizados con los requisitos temáticos y estar preparados para aplicarlos cuando el tema se incluya en sus planes anuales de auditoría, o si ese tema específico es el objeto de un encargo de auditoría interna. Los elementos de los requisitos temáticos deben ser evaluados al determinar el alcance del encargo. Deben documentarse y conservarse pruebas de que se ha realizado la evaluación y el tratamiento del tema. Los trabajos que incluyan cualquier aspecto del tema en cuestión deben evaluar los requisitos relevantes para el encargo o documentar por qué los requisitos específicos no son aplicables. En el Apéndice B se proporciona una herramienta para ayudar a los auditores internos a explicar los motivos para incluir o excluir requisitos.

¿Por qué son necesarios los requisitos temáticos?

La aplicación de los requisitos temáticos tiene por objeto reforzar la pertinencia permanente de la función de auditoría interna en el cambiante panorama global de los riesgos y aumentar el valor de los servicios de auditoría interna en todas las industrias y sectores. El cumplimiento de los requisitos temáticos ayudará a los auditores internos a aumentar la calidad y la coherencia de los trabajos.

Los requisitos temáticos están estructurados para proporcionar orientación para la realización de servicios de auditoría interna en tres áreas: gobierno, gestión de riesgos y procesos de control. Cada área incluye:

- Requisitos, que son obligatorios y cubren los objetivos esenciales de la organización.
- Consideraciones, que no son obligatorias, pero sirven como mejores prácticas para evaluar el diseño y la implementación de los objetivos de la organización. Las consideraciones, que figuran en el Apéndice A, deben utilizarse simplemente como ejemplos para validar los requisitos.

La conformidad con los requisitos temáticos se evaluará en las evaluaciones de calidad. Para demostrar la conformidad en la preparación de una revisión de calidad, los auditores internos deben utilizar la herramienta proporcionada como Apéndice B para indicar la conformidad con cada requisito o para explicar por qué no se logró la conformidad.

Requisito temático de Ciberseguridad

Evaluación y valoración de la eficacia de los procesos de gobierno, gestión de riesgos y control de la ciberseguridad

La ciberseguridad protege los activos de información de una organización frente a usuarios no autorizados, interrupciones, alteraciones o destrucción, y refuerza el entorno general de control para reducir el riesgo. Los ciberataques pueden tener repercusiones directas e indirectas a menudo importantes, ya que los ordenadores, las redes, los programas, los datos y la información sensible son componentes críticos de la mayoría de las organizaciones. Dado que las organizaciones dependen, en gran medida, de los recursos de tecnologías de la información, tener claramente definidos un plan de ciberseguridad, objetivos, riesgos inherentes y controles eficaces debe ser una prioridad para la dirección o gerencia operativa.

Este requisito temático proporciona un enfoque coherente y exhaustivo para evaluar el diseño y la aplicación de los procesos de gobierno, gestión de riesgos y control de la ciberseguridad.

GOBIERNO: Evaluación y valoración dela gobierno de la ciberseguridad

Requisitos:

Al realizar un trabajo de auditoría interna que incluya objetivos de ciberseguridad en su alcance, los auditores internos deben evaluar si los procesos de gobierno de la organización abordan adecuadamente la ciberseguridad. Los auditores internos deben evaluar si:

A. Se establecen y actualizan periódicamente las políticas y procedimientos relacionados con los procesos de gestión de riesgos de ciberseguridad, incluida la promoción de prácticas que refuercen el entorno de control basadas en marcos ampliamente adoptados (NIST, COBIT y otros).

B. Las funciones y responsabilidades que soportan los objetivos de ciberseguridad de la organización están claramente establecidas y esas funciones son desempeñadas por personas con los conocimientos, habilidades y capacidades necesarias.

C. Las actualizaciones de los objetivos, estrategias, riesgos y controles de mitigación en materia de ciberseguridad se comunican periódicamente al consejo.

D. Las partes interesadas relevantes (por ejemplo, el liderazgo, las operaciones, los proveedores estratégicos y otros) se comprometen a debatir la mejor manera de establecer y mejorar los procesos de gestión de riesgos de ciberseguridad.

E. Se comunican al consejo los recursos necesarios (como liderazgo, presupuesto, talento, *hardware*, *software* y formación) para ejecutar eficazmente los procesos de gestión de riesgos de ciberseguridad.

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

Requisitos:

Al realizar un trabajo de auditoría interna que incluya objetivos de ciberseguridad en su alcance, los auditores internos deben evaluar si los procesos de gestión de riesgos de la organización abordan adecuadamente la ciberseguridad. Los auditores internos deben evaluar si:

A. Se establece un proceso de gestión de riesgos para toda la organización que incluye la identificación, el análisis y la gestión de los riesgos relacionados con la tecnología y la seguridad de la información, centrándose específicamente en los riesgos de ciberseguridad y en cómo dichos riesgos pueden afectar a la capacidad de alcanzar los objetivos de la organización.

B. Los procesos de gestión de riesgos de ciberseguridad son llevados a cabo por un equipo interfuncional que incluye la dirección de tecnologías de la información, la gestión de riesgos de toda la organización, los aspectos jurídicos, el cumplimiento normativo, otros directivos (operaciones, contabilidad, finanzas y otros) e implica a partes externas (vendedores, proveedores de servicios subcontratados, proveedores, clientes y otros), según proceda.

C. Se han establecido políticas y procedimientos de gestión de riesgos de ciberseguridad que se actualizan periódicamente, incluida la promoción de prácticas que refuerzan los procesos de gestión de riesgos de ciberseguridad basados en marcos de gestión de riesgos ampliamente adoptados, guías autorizadas u otras mejores prácticas.

D. La rendición de cuentas y la responsabilidad, con respecto a la gestión de los riesgos de ciberseguridad, están establecidas y se ha identificado a una persona o equipo que supervisa y comunica periódicamente cómo se están gestionando los riesgos de ciberseguridad, incluidas las necesidades de recursos para mitigar los riesgos y la identificación de riesgos de ciberseguridad emergentes que no se habían identificado previamente.

E. Se establece un proceso para elevar rápidamente cualquier riesgo de ciberseguridad (emergente o previamente identificado) que alcance niveles inaceptables sobre la base de las directrices de gestión de riesgos establecidas por la organización o para cumplir con los requisitos legales y/o reglamentarios aplicables.

F. La gestión de riesgos de ciberseguridad incluye la coordinación entre la seguridad de la información, el departamento jurídico, el de cumplimiento y otros directivos para identificar y cumplir todas las obligaciones legales y contractuales, como leyes y reglamentos. Tanto el estado del cumplimiento como del incumplimiento de los requisitos aplicables se comunica periódicamente dentro de la organización.

G. Se establece un proceso para identificar y gestionar los riesgos de ciberseguridad relacionados con terceros. Los vendedores, proveedores y otros proveedores de procesos y/o servicios externalizados están obligados contractualmente a implantar controles de ciberseguridad eficaces que protejan adecuadamente la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización a los que tienen acceso terceros.

H. Las políticas y procesos relacionados con la clasificación, conservación, destrucción y encriptación de datos se diseñan adecuadamente y se despliegan con eficacia para proporcionar un enfoque sistemático que garantice un registro completo y preciso de los datos y proteja la confidencialidad y privacidad de la información sensible.

I. Se establece un proceso de comunicación de los riesgos operativos de ciberseguridad para garantizar el conocimiento por parte de la dirección o gerencia operativa y los empleados. Todos los problemas, diferencias, deficiencias o fallos de control se comunican al consejo de administración y a la dirección o gerencia operativa, y el estado de las medidas correctoras se supervisa estrechamente y se notifica. Los incumplimientos de las políticas de ciberseguridad se identifican, investigan, notifican y corrigen a su debido tiempo.

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

Requisitos:

Al realizar una auditoría interna que incluya objetivos de ciberseguridad en su alcance, los auditores internos deben evaluar si los procesos de control de la organización abordan adecuadamente la ciberseguridad. Los auditores internos deben evaluar si la organización:

A. Prioriza los controles de ciberseguridad y garantiza que el presupuesto y los recursos relacionados (como personal, *software*, herramientas y otros) se asignan para maximizar los beneficios esperados.

B. Garantiza que los controles de ciberseguridad funcionen de forma que promuevan la consecución de los objetivos de ciberseguridad de la organización y la resolución oportuna de los problemas.

C. Proporciona formación suficiente al personal responsable de las operaciones de ciberseguridad.

D. Ha desarrollado políticas y procedimientos suficientes para gestionar todos los aspectos de las operaciones de ciberseguridad y los controles relacionados.

E. Garantiza que la dirección o gerencia operativa disponga de los recursos necesarios para mantenerse informada sobre los problemas de ciberseguridad emergentes de las nuevas tecnologías, identificar oportunidades para mejorar las operaciones y comprender cómo pueden desplegarse mejor los esfuerzos de ciberseguridad para incidir en metas y objetivos organizativos más amplios.

F. Integra adecuadamente la ciberseguridad en el ciclo de vida de desarrollo de sistemas para aplicaciones empresariales, incluidos los programas informáticos y las aplicaciones adquiridas o desarrolladas a medida.

G. Ha incluido la ciberseguridad en la gestión del *hardware* (como portátiles, ordenadores de sobremesa, dispositivos móviles).

H. Ha implantado controles eficaces en relación con el soporte de *hardware* de producción, como la configuración, la aplicación de parches, el soporte de la gestión de acceso de usuarios y la supervisión de la disponibilidad y el rendimiento. La organización ha evaluado tanto la adecuación del diseño como la eficacia operativa de estos controles.

I. Optimiza los controles relacionados con la red en lo que respecta a su segmentación, el uso y la colocación de cortafuegos, las conexiones limitadas a redes y/o sistemas externos y el uso de tecnologías preventivas y detectivas, como los sistemas de detección/prevención de intrusiones.

J. Ha implantado controles eficaces en torno a los servicios comunes de comunicación de escritorio, como el correo electrónico, los navegadores de Internet, las videoconferencias, la mensajería y los protocolos de intercambio de archivos.

K. Ha implantado controles adecuados de prestación de servicios para garantizar que las siguientes áreas están integradas con la supervisión de la ciberseguridad: gestión de cambios, servicio/ayuda y administración de dispositivos de usuario final.

L. Ha implantado controles de seguridad física adecuados para proteger de ataques los centros de información de alto riesgo (como centros de datos, centros de operaciones de red y centros de operaciones de seguridad).

M. Ha implantado controles de respuesta a incidentes y de recuperación.

Normas relacionadas:

3.1 Competencia
4.2 Debido cuidado profesional
9.1 Comprender los procesos de gobierno, gestión de riesgos y control
9.4 Plan de auditoría interna
12.3 Supervisión y mejora del desempeño en los trabajos
13.1 Comunicación durante el trabajo
13.2 Evaluación de riesgos del trabajo
13.3 Objetivos y alcance del trabajo
13.4 Criterios de evaluación
13.5 Recursos del trabajo
13.6 Programa de trabajo
14.1 Recopilación de información para el análisis y evaluación
14.2 Análisis y potenciales conclusiones del trabajo
14.3 Evaluación de los hallazgos
14.4 Recomendaciones y planes de acción
14.5 Conclusiones del trabajo
14.6 Documentación de los trabajos
15.1 Comunicación final del trabajo
15.2 Confirmar la implementación de recomendaciones o planes de acción

Guías Globales de Auditoría Tecnológica (GTAG) relacionadas:

Evaluación del riesgo de ciberseguridad: el modelo de las tres líneas
Auditoría de aplicaciones de negocio
Auditoría de la respuesta a ciberincidentes y recuperación
Auditoría de operaciones de ciberseguridad: Prevención y detección
Auditoría de la gestión de identidad y acceso
Auditoría del gobierno de TI
Auditoría de la informática móvil
Auditoría de la gestión de redes y comunicaciones

Apéndice A. Consideraciones

Consideraciones para cada requisito de gobierno:

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

A. Políticas, procedimientos y otra documentación relevante utilizada por la organización para gestionar las responsabilidades diarias de ciberseguridad, incluyendo:
    1. Documentación clara, concisa, coherente y actualizada periódicamente, idealmente a medida que se identifican nuevos riesgos de ciberseguridad y al menos una vez al año.
    2. Procedimientos relacionados con la identificación, el análisis, la resolución y la notificación de brechas u otras pérdidas de datos sensibles.
    3. Documentación sobre cómo la dirección o gerencia operativa garantiza que las políticas y procedimientos son suficientes para respaldar las operaciones de ciberseguridad.
B. Funciones y responsabilidades creadas por el consejo para apoyar la consecución de la estrategia de ciberseguridad, incluida una estructura de informes que garantice que la ciberseguridad se informa a un nivel de la organización que tenga suficiente visibilidad para lograr el apoyo de la organización.
C. Materiales presentados al consejo sobre estrategia, objetivos, riesgos y controles de ciberseguridad, incluido el análisis de si:
    1. La frecuencia de la comunicación es adecuada, lo ideal es que sea trimestral y que la presente el responsable de la función de seguridad de la información; por ejemplo, un director de sistemas de información.
    2. La información presentada es clara, concisa y coherente; los riesgos y controles se comunican de manera que el consejo pueda comprenderlos fácilmente.
    3. Se incluyen indicadores clave de rendimiento u otras métricas/estadísticas importantes de ciberseguridad.
    4. Cuando procede, la dirección o gerencia operativa recibe las aportaciones del consejo y las pone en práctica, comunicando al consejo el estado de los cambios.
D. Pruebas de las comunicaciones relacionadas con la ciberseguridad de la dirección o gerencia operativa con las partes interesadas pertinentes (por ejemplo, liderazgo, operaciones, proveedores estratégicos y otros), incluido que la información comunicada sea clara, concisa, coherente y adaptada a la audiencia de las partes interesadas:
    1. Empleados.
    2. Vendedores, proveedores, prestadores de servicios subcontratados y terceros.
    3. Clientes.
    4. Socios estratégicos.
E. El análisis y la comunicación de las necesidades de recursos por parte de la dirección o gestión operativa, incluyendo:
    1. Entender cómo se identifican las diferencias y qué métricas clave se utilizan para anticipar los cambios en los requisitos.
    2. Cómo trabaja la dirección o gerencia operativa con recursos humanos para analizar las necesidades de talento en ciberseguridad.
    3. Cómo analiza la dirección o gerencia operativa los inventarios actuales de *hardware* y *software* y determina si se necesitan inversiones adicionales para apoyar las iniciativas de ciberseguridad.
    4. Si los auditores internos revisan cómo la dirección o gerencia operativa establece y actualiza los materiales de formación en ciberseguridad e identifica las lagunas, incluyendo la garantía de que la formación cubre los objetivos, riesgos y controles de ciberseguridad emergentes.

Consideraciones para cada requisito de gestión de riesgos:

Para evaluar los aspectos requeridos de la gestión de riesgos de ciberseguridad, los auditores internos pueden revisar:

A. Cómo identifica inicialmente la dirección o gerencia opearativa los riesgos de ciberseguridad, incluyendo:
    1. Entender qué personal es responsable tanto de las amenazas diarias a las que se enfrenta la organización como de los riesgos emergentes con la comunidad de seguridad de la información.
        a. Determinar si estas personas tienen la experiencia profesional relacionada y la formación necesaria para reconocer y elevar eficazmente las amenazas al equipo más amplio de gestión de riesgos.
    2. Identificar las aplicaciones informáticas o los proveedores en los que confía la dirección o gerencia operativa para identificar los riesgos de ciberseguridad.
    3. Documentación relacionada con el proceso de gestión de riesgos de ciberseguridad, incluyendo:
        a. Actas de reuniones.
        b. Acciones derivadas.
        c. Listas de asistentes o miembros del equipo.
        d. Investigación posterior al incidente/análisis de la causa raíz.

B. La forma en que la dirección o gerencia operativa identifica o nombra a los miembros del equipo de gestión de riesgos y los fundamentos o cualificaciones empresariales correspondientes utilizados para evaluar la pertenencia a dicho equipo. Examinar las pruebas de la participación periódica en debates sobre riesgos de ciberseguridad con las partes externas pertinentes.

C. El proceso que la organización utiliza para establecer y actualizar periódicamente las políticas y procedimientos relacionados con la gestión de riesgos de ciberseguridad, que puede incluir:
    1. Una revisión y aprobación anual de las políticas y procedimientos.
    2. Comprensión de cómo la organización garantiza el cumplimiento de sus políticas y procedimientos de gestión de riesgos y la manera en que se forma al personal en la ejecución de las políticas y procedimientos.
        a. Comprensión de qué marcos o directrices autorizadas utiliza la dirección o gerencia operativa para gestionar los riesgos de ciberseguridad (NIST, COBIT y otros) y la forma en que la organización confirma la adhesión a los marcos elegidos.

D. La(s) persona(s) responsable(s) de la ejecución de la gestión de riesgos de ciberseguridad, incluyendo la garantía de que su formación profesional, experiencia, cualificaciones y credenciales son apropiadas para gestionar los riesgos y amenazas a la seguridad de la información. Verificar que la persona responsable está situada en un nivel dentro de la organización que le permite dar visibilidad a los riesgos de ciberseguridad y comunicarlos de manera eficaz.

E. Los procesos que utiliza la organización para elevar y comunicar los riesgos de ciberseguridad, incluyendo cómo se evalúa, asigna y prioriza el nivel de amenaza o riesgo. Verificar que la organización ha definido niveles de riesgo, tales como alto, moderado, bajo, incluyendo una explicación detallada para cada nivel de riesgo y procedimientos para elevar cada categoría de riesgo. Revisar el listado de riesgos de ciberseguridad actuales identificados y el estado de mitigación de cada evento.

F. El proceso que utiliza la organización para garantizar el cumplimiento de toda la normativa aplicable en materia de ciberseguridad, incluyendo:
    1. Cómo afectan a la organización las normativas propuestas o adoptadas recientemente.
    2. Si existe un inventario de la normativa aplicable que se supervisa, actualiza y sobre el que se informa periódicamente para garantizar el conocimiento de la organización.
        a. Para cualquier elemento de incumplimiento, verificar que la dirección o gerencia operativa es consciente de los riesgos asociados, incluso mediante informes periódicos.

G. El proceso de la organización para gestionar los riesgos de ciberseguridad de terceros. Verificar que los controles de ciberseguridad del proveedor se revisan antes de iniciar una relación comercial y que los contratos incluyen el derecho a revisiones periódicas a lo largo de la relación. Incluir la obtención y el análisis del informe de controles de la organización de servicios del tercero y la verificación de que la organización ha documentado su revisión del informe SOC, que debe incluir la garantía de que se han aplicado las consideraciones de control del usuario. Comprender el enfoque de la dirección o gerencia operativa para determinar si los terceros tienen un entorno de control adecuado que se corresponda con los controles de la organización.
    a. Si se detectan deficiencias en el control de terceros, comprender el proceso que utiliza la dirección o gerencia operativa para asegurarse de que las deficiencias no comprometen la ciberseguridad relacionada con las operaciones, o comprender cómo comunica la organización que se requieren cambios para mantener la relación con el proveedor aplicable, o que potencialmente debe encontrarse un proveedor sustituto.

H. Las políticas y procesos que la organización ha establecido en relación con:
    1. Clasificación de los datos.
    2. Conservación de datos.
    3. Destrucción de datos.
    4. Cifrado.
    5. Gestión de acceso/identidad.
    6. Quién prepara, revisa y actualiza la documentación, que idealmente debería incluir personal jurídico y de cumplimiento para garantizar la conformidad con la normativa aplicable.
    7. Cómo realiza la organización la clasificación de información para garantizar que los datos confidenciales y privados se han identificado y tienen el nivel de protección adecuado, como la limitación del acceso de los usuarios.
    8. Cómo revisa periódicamente la organización el proceso utilizado para clasificar los datos y si el proceso sigue respaldando los objetivos de ciberseguridad de la organización y cumpliendo las políticas de la organización y la normativa aplicable.

I. El proceso de comunicación de los riesgos operativos de ciberseguridad a la dirección o gerencia operativa y a los empleados. Lo ideal sería que esta comunicación se incluyera en la formación periódica sobre ciberseguridad (al menos una vez al año). Comprender el proceso de la dirección o gerencia operativa para comunicar las actualizaciones sobre la remediación existente de los problemas de ciberseguridad junto con las fechas de finalización previstas. Verificar que el incumplimiento se supervisa de cerca y que se proporcionan actualizaciones al consejo y a la alta dirección.

Consideraciones para cada requisito del proceso de control:

Para evaluar los aspectos requeridos de los controles de ciberseguridad, los auditores internos pueden revisar:

A. El proceso de la dirección o gerencia operativa para determinar cómo desplegar los recursos presupuestados para dar soporte al entorno de control de la ciberseguridad, que debe incluir una planificación estratégica anual para garantizar que se dispone de un nivel adecuado de recursos organizativos para cumplir los objetivos de ciberseguridad. Deben revisarse los resultados formales y documentados de la planificación anual y la supervisión periódica de la gestión de los recursos.

B. El proceso de la dirección o gerencia operativa para evaluar periódicamente que los controles de ciberseguridad funcionan de forma que promueven la consecución de los objetivos de ciberseguridad de la organización. Verificar que la dirección o gerencia operativa supervisa la eficacia de los controles y evalúa si los controles existentes están diseñados adecuadamente o si se requieren nuevos controles. En muchas organizaciones, la función de auditoría interna desempeña un papel importante en este proceso, proporcionando garantías sobre el diseño de los controles y si éstos funcionan eficazmente mediante pruebas periódicas (trimestrales, anuales). Verificar los procesos de la dirección o gestión operativa para subsanar las deficiencias de control o abordar las conclusiones de las evaluaciones realizadas por la función de auditoría interna u otros proveedores de garantías (por ejemplo, pruebas de penetración).

C. El proceso de la dirección o gerencia operativa para evaluar las necesidades de formación del personal de ciberseguridad dentro de la organización y cómo se asignan los recursos para impartir la formación adecuada y garantizar que se comprenden y gestionan las nuevas amenazas a la ciberseguridad. Comprender cómo se asegura la dirección o gerencia operativa de que los empleados tienen suficiente formación en ciberseguridad, que puede incluir eventos de formación en directo, instrucción grabada o realización de módulos de formación.

D. El proceso de la organización para crear y actualizar políticas y procedimientos de ciberseguridad y cómo evalúa la dirección o gerencia operativa si dichas políticas y procedimientos son adecuados. Comprender cómo se forma al personal responsable de las operaciones y controles de ciberseguridad en el cumplimiento de las políticas y procedimientos y cómo se evalúa su cumplimiento interno.

E. El proceso de la organización para formar adecuadamente al equipo directivo responsable de las operaciones y controles de ciberseguridad para reconocer las tendencias emergentes y proporcionar a sus equipos y a la organización un liderazgo estratégico. Comprender cómo identifica la organización las oportunidades de aumentar las capacidades de la dirección o gerencia operativa para apoyar la concienciación sobre los problemas emergentes, como la participación en la formación y la educación profesional continua.

F. Cómo aborda la organización la ciberseguridad dentro de su ciclo de vida de desarrollo de sistemas, incluidos los siguientes aspectos de control

   1. Planificación: La ciberseguridad se ha identificado como un componente clave a la hora de evaluar los riesgos y analizar las vulnerabilidades potenciales. El alcance y los objetivos de la implantación del *software* deben incluirse a medida que la organización evalúa los controles de ciberseguridad durante la fase de planificación.
   2. Recopilación de requisitos: Los requisitos de ciberseguridad son un componente a la hora de definir los requisitos funcionales, que también deben incluir el cumplimiento de todos los requisitos legales y reglamentarios aplicables.
   3. Diseño: Las consideraciones de ciberseguridad se incluyen como una pieza integral de los requisitos detallados de procesamiento. Los controles deben identificarse en todos los aspectos del diseño a medida que la organización define más formalmente las necesidades del diseño de la arquitectura del sistema (como plataformas, interfaces de usuario, bases de datos y otros).
   4. Desarrollo: La organización ha establecido un entorno seguro y ha definido formalmente un proceso de desarrollo que minimiza las vulnerabilidades cibernéticas (por ejemplo, el acceso limitado de los usuarios al código de desarrollo, la segregación adecuada del entorno de producción, el uso de herramientas aprobadas, la existencia de pistas de auditoría para realizar un seguimiento de las actividades de desarrollo, los requisitos específicos de ciberseguridad para el *software* desarrollado por el proveedor, y otros).
   5. Pruebas: La organización incluye la revisión y evaluación de la ciberseguridad durante la fase de pruebas (por ejemplo, pruebas automatizadas, pruebas de penetración y evaluación de vulnerabilidades). La organización debe ser capaz de ser alertada rápidamente y abordar cualquier vulnerabilidad cibernética identificada a través de las pruebas, lo que incluye una descripción detallada de la vulnerabilidad y qué cambios de código o controles de mitigación se establecieron en respuesta.
   6. Despliegue: A medida que el nuevo *software* se pone en producción, la organización debe supervisar cuidadosamente las posibles amenazas a la ciberseguridad, incluida la garantía de que los usuarios finales han sido formados para utilizar el *software* de una manera que minimice los riesgos de ciberseguridad. La organización debe asegurarse de que se registran y analizan los eventos y errores relacionados con posibles eventos de ciberseguridad.
   7. Mantenimiento: La organización debe asegurarse de que todas las versiones de *software* relacionadas con la seguridad se aplican de manera oportuna y debe tener una comunicación abierta con los proveedores de

software para garantizar que los riesgos y amenazas emergentes se controlan adecuadamente y que los usuarios finales están informados de cualquier vulnerabilidad conocida.

G. Controles que la organización ha establecido para proteger el *hardware* (como ordenadores de sobremesa, portátiles, dispositivos móviles y otros) de los riesgos de ciberseguridad, lo que incluye el uso de cifrado, *software* antivirus, requisitos de contraseñas complejas, redes privadas virtuales o redes de confianza cero para la autenticación, actualización periódica del *firmware* y un proceso de gestión de activos que garantice que el *hardware* proporcionado por la empresa tiene una configuración de seguridad adecuada en el momento de su entrega y su correcta eliminación cuando se retiren los activos.

H. Los controles que la organización ha desplegado para garantizar que el soporte de producción proporciona protección frente a los riesgos de ciberseguridad, que deben incluir que los servidores se parcheen con las versiones de seguridad de manera oportuna para mitigar los riesgos emergentes. Revisar los controles de supervisión implantados para determinar si la disponibilidad y la utilización de recursos funcionan adecuadamente, lo que permite revisar y analizar posibles problemas de ciberseguridad que amenacen el rendimiento. Revisar los 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 controles sólidos de seguridad de la red.

I. Controles relacionados con la red que prevean la segmentación para limitar los riesgos de ciberseguridad derivados de accesos no autorizados. Revisar cómo utiliza la organización los cortafuegos, incluyendo dónde están ubicados y el proceso utilizado para revisar, analizar y restringir el acceso a la red, evitando el acceso no autorizado. Revisar cómo utiliza la organización los sistemas de detección/prevención de intrusiones para prevenir, detectar y recuperarse de ataques de ciberseguridad.

J. Controles que la organización ha establecido en torno a los servicios comunes de comunicación de escritorio, como el uso del cifrado del correo electrónico, la garantía de que las actualizaciones de seguridad del navegador de Internet se aplican de manera oportuna, la configuración de seguridad de la videoconferencia/mensajería (por ejemplo, MS Teams, Zoom y otros) para restringir el uso de determinadas extensiones de archivo (como los archivos .exe) y el uso de la autenticación multifactor para compartir archivos.

K. Controles que la organización ha desplegado para mitigar los riesgos de ciberseguridad relacionados con la prestación de servicios, incluyendo:
   1. Garantizar que el proceso de gestión de cambios incluye la consideración de los riesgos de ciberseguridad a la hora de evaluar y aprobar los cambios, así como la respuesta oportuna a los ciberincidentes.
   2. El servicio de asistencia al usuario registra todos los eventos de ciberseguridad comunicados por la organización, garantiza su resolución oportuna y los eleva al miembro adecuado de la dirección o gerencia operativa.
   3. La administración de los dispositivos móviles (como el correo electrónico, las aplicaciones y otros) está configurada para mitigar los riesgos de ciberseguridad y puede gestionarse a distancia si el dispositivo de un usuario se ve comprometido.

L. Controles de seguridad física para proteger la información de alto riesgo, incluidos los riesgos de ciberseguridad. Por ejemplo, garantizar que el acceso de terceros/proveedores sea adecuado y limitar al personal autorizado el acceso físico de los usuarios a los centros de datos, centros de operaciones de red y centros de operaciones de seguridad.

M. Controles que la organización ha implementado en relación con la respuesta y recuperación de incidentes, que deben incluir:
   1. Un plan documentado que se revisa y actualiza a medida que las operaciones de la organización cambian con el tiempo.

2. Pruebas periódicas y comunicación de los resultados a la dirección o gerencia operativa.
3. Determinar si los problemas detectados en las pruebas se solucionan a tiempo.

Apéndice B. Herramienta para documentar la conformidad con los requisitos temáticos

Ciberseguridad - Gobierno

Requisito	Conformidad (Sí / No / Parcial)	Evidencia obtenida o justificación de la exclusión
A. Se establecen y actualizan periódicamente políticas y procedimientos relacionados con los procesos de gestión de riesgos de ciberseguridad, incluida la promoción de prácticas basadas en marcos ampliamente adoptados (NIST, COBIT y otros) que refuerzan el entorno de control.		
B. Las funciones y responsabilidades que apoyan los objetivos de ciberseguridad de la organización están claramente establecidas, y las funciones se desempeñan adecuadamente.		
C. Las actualizaciones de los objetivos, estrategias, riesgos y controles de mitigación en materia de ciberseguridad se comunican periódicamente al consejo.		
D. Las partes interesadas relevantes se comprometen a debatir la mejor manera de establecer y mejorar los procesos de gestión de riesgos de ciberseguridad.		
E. Se comunican al consejo los recursos necesarios (liderazgo, presupuesto, talento, *hardware*, *software*, formación y otros) para ejecutar eficazmente los procesos de gestión de riesgos de ciberseguridad.		

Ciberseguridad - Gestión de riesgos

Requisito	Conformidad (Sí / No / Parcial)	Evidencia obtenida o justificación de la exclusión
A. Establecimiento de un proceso de gestión de riesgos para toda la organización que incluya la identificación, el análisis y la gestión de los riesgos relacionados con la tecnología y la seguridad de la información, centrándose específicamente en los riesgos de ciberseguridad y en cómo dichos riesgos pueden afectar a la capacidad de la organización para alcanzar sus objetivos.		
B. Los procesos de gestión de riesgos de ciberseguridad son llevados a cabo por un equipo interfuncional que incluye la dirección de tecnología de la información, la gestión integral de riesgos de la organización, la dirección jurídica, la dirección de cumplimiento y otras direcciones (por		

Requisito	Conformidad (Sí / No / Parcial)	Evidencia obtenida o justificación de la exclusión
ejemplo, operaciones, contabilidad/finanzas) e involucra a partes externas (vendedores, proveedores, clientes y otros) según proceda.		
C. Se han establecido y se actualizan periódicamente políticas y procedimientos relacionados con la gestión de riesgos de ciberseguridad, incluida la promoción de prácticas que refuercen los procesos de gestión de riesgos de ciberseguridad basados en marcos de gestión de riesgos ampliamente adoptados, guías autorizadas o mejores prácticas.		
D. Se ha establecido la rendición de cuentas y la responsabilidad en relación con la gestión de los riesgos de ciberseguridad y se ha identificado a una persona o equipo que supervisa y comunica periódicamente cómo se están gestionando los riesgos de ciberseguridad, incluidas las necesidades de recursos para mitigar los riesgos y la identificación de riesgos de ciberseguridad emergentes que no se habían identificado previamente.		
E. Se establece un proceso para elevar rápidamente los riesgos de ciberseguridad (emergentes o previamente identificados) que alcanzan niveles inaceptables sobre la base de las directrices de gestión de riesgos establecidas por la organización o para cumplir con los requisitos legales y/o reglamentarios aplicables.		
F. La gestión de los riesgos de ciberseguridad incluye la coordinación entre la seguridad de la información, los aspectos jurídicos, el cumplimiento y otros aspectos de la gestión para identificar y cumplir todas las obligaciones legales y contractuales (leyes, reglamentos). El estado de cumplimiento e incumplimiento de los requisitos aplicables se comunica a la organización periódicamente.		
G. Existe un proceso para identificar y gestionar los riesgos de ciberseguridad relacionados con terceros. Los vendedores, proveedores y otros proveedores de procesos y/o servicios externalizados están obligados contractualmente a implantar controles de ciberseguridad eficaces que protejan adecuadamente la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización a los que tienen acceso.		

Requisito	Conformidad (Sí / No / Parcial)	Evidencia obtenida o justificación de la exclusión
H. Las políticas y los procesos relacionados con la clasificación, la conservación, la destrucción y el cifrado de datos están adecuadamente diseñados y se aplican de forma eficaz para proporcionar un enfoque sistemático que garantice un registro completo y preciso de los datos y proteja la confidencialidad y la privacidad de la información sensible.		
I. Existe un proceso para comunicar los riesgos operativos de ciberseguridad con el fin de garantizar una concienciación adecuada por parte de la dirección o gerencia operativa y los empleados. Los problemas, diferencias, deficiencias y fallos de control se comunican al consejo de administración y a la dirección o gerencia operativa, y el estado de las medidas correctoras se supervisa estrechamente y se comunica. Los incumplimientos de las políticas de ciberseguridad se identifican, investigan, notifican y corrigen a tiempo.		

Ciberseguridad - Procesos de control

Requisito	Conformidad (Sí / No / Parcial)	Evidencia obtenida o justificación de la exclusión
A. Prioriza los controles de ciberseguridad y garantiza que el presupuesto y los recursos relacionados (por ejemplo, personal, *software*, herramientas) se asignan para maximizar los beneficios esperados.		
B. Garantiza que los controles de ciberseguridad funcionen de manera que promuevan la consecución de los objetivos de ciberseguridad de la organización y la resolución oportuna de los problemas que surjan.		
C. Proporciona formación suficiente al personal responsable de las operaciones de ciberseguridad.		
D. Ha desarrollado políticas y procedimientos suficientes para gestionar todos los aspectos de las operaciones de ciberseguridad y los controles relacionados.		
E. Garantiza que la dirección o gerencia operativa disponga de los recursos necesarios para mantenerse informada sobre los problemas de ciberseguridad emergentes de las nuevas tecnologías, identificar oportunidades para mejorar las operaciones y		

Requisito	Conformidad (Sí / No / Parcial)	Evidencia obtenida o justificación de la exclusión
comprender cómo pueden desplegarse mejor los esfuerzos de ciberseguridad para incidir en metas y objetivos organizativos más amplios.		
F. Integra adecuadamente la ciberseguridad en el ciclo de vida de desarrollo de sistemas para aplicaciones empresariales, incluidos los programas informáticos y las aplicaciones adquiridas o desarrolladas a medida.		
G. Ha incluido la ciberseguridad en la gestión del *hardware* (portátiles, ordenadores de sobremesa, dispositivos móviles).		
H. Ha implantado controles eficaces en relación con el soporte de *hardware* de producción, como la configuración, la aplicación de parches, el soporte de la gestión de acceso de usuarios y la supervisión de la disponibilidad y el rendimiento. La organización ha evaluado tanto la adecuación del diseño como la eficacia operativa de estos controles.		
I. Optimiza los controles relacionados con la red en lo que respecta a su segmentación, el uso y la colocación de cortafuegos, las conexiones limitadas a redes y/o sistemas externos y el uso de tecnologías preventivas y detectivas, como los sistemas de detección/prevención de intrusiones.		
J. Ha implantado controles eficaces en torno a los servicios comunes de comunicación de escritorio, como el correo electrónico, los navegadores de Internet, las videoconferencias, la mensajería y los protocolos de intercambio de archivos.		
K. Ha implantado controles adecuados de prestación de servicios para garantizar que las siguientes áreas están integradas con la supervisión de la ciberseguridad: gestión de cambios, servicio/ayuda y administración de dispositivos de usuario final.		
L. Ha implantado controles de seguridad física adecuados para proteger de ataques los centros de información de alto riesgo (como centros de datos, centros de operaciones de red y centros de operaciones de seguridad).		
M. Ha implantado controles de respuesta a incidentes y de recuperación.		

Acerca del Instituto de Auditores Internos

El Instituto de Auditores Internos (IIA) es una asociación profesional que cuenta con más de 245.000 miembros en todo el mundo y ha concedido más de 195.000 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.

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.

Abril de 2024

The Institute of Internal Auditors®

Sede mundial

Instituto de Auditores Internos
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, EE.UU.
Teléfono: +1-407-937-1111
Fax: +1-407-937-1101