Borrador para consulta pública
Requisito Temático de Resiliencia Organizacional

El Marco Internacional para la Práctica Profesional® del IIA comprende las Normas Globales de Auditoría Interna™, los Requisitos Temáticos y las Guías Globales. 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 tratados.

La conformidad con los Requisitos Temáticos aumentará la consistencia con la que se prestan los servicios de auditoría interna y mejorará la calidad y fiabilidad 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 en cuestión responde a una de las siguientes situaciones:

1. Es objeto de un trabajo incluido en el Plan de Auditoría Interna.
2. Se ha identificado durante la ejecución de un trabajo.
3. Es objeto de una solicitud de trabajo que 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 sean aplicables en todos los trabajos; si se excluyen requisitos, debe documentarse y conservarse una justificación. La conformidad con los Requisitos Temáticos es obligatoria y se evaluará durante las Evaluaciones de Calidad.

Para obtener más información, consulte la Guía de usuario del Requisito Temático de Resiliencia Organizacional.

Resiliencia Organizacional

La resiliencia organizacional se define como la "habilidad de una organización para absorber y adaptarse en un entorno cambiante", según la norma ISO 22316:2017, Seguridad y resiliencia - Resiliencia organizacional - Principios y atributos, publicada por la Organización Internacional de Normalización. La resiliencia organizacional es una cuestión amplia, que abarca importantes elementos estratégicos, operativos, tecnológicos, humanos,

sociales y financieros. La resiliencia organizacional aborda los riesgos que pueden alterar o mermar significativamente la capacidad de una organización para ofrecer sus principales productos y servicios, mantener la confianza de las partes interesadas o cumplir sus objetivos estratégicos. Estos riesgos pueden ser el resultado de acontecimientos repentinos (como catástrofes naturales, ciberataques y conflictos geopolíticos), presiones ambientales prolongadas (como escasez de recursos y crisis de salud pública) o cambios en el contexto externo (como disrupción tecnológica, cambios normativos y erosión de la reputación). Estos riesgos también pueden consistir en cambios graduales o presiones que se acumulan lentamente y que, con el tiempo, comprometen la estabilidad y la capacidad de adaptación de una organización. Este tipo de riesgos incrementales pueden pasarse por alto de forma rutinaria. Para tener éxito, las organizaciones resilientes se anticipan y adaptan a los riesgos, ya sean repentinos o acumulativos.

Entre los factores de riesgo inherentes que elevan la amenaza a la resiliencia figuran la elevada complejidad operativa, las cadenas de suministro globalizadas, las infraestructuras o sistemas de datos centralizados, la disponibilidad limitada de mano de obra, las condiciones volátiles del mercado y la fuerte dependencia de terceros o ubicaciones geográficas críticas. Las organizaciones de sectores de alta fiabilidad o las que operan bajo un intenso escrutinio normativo también pueden enfrentarse a riesgos intrínsecamente mayores, debido al impacto público y a obligaciones de cumplimiento.

Los auditores internos suelen evaluar los procesos y controles de las tecnologías de la información (TI) en torno a la continuidad del negocio y la recuperación de desastres. Un plan de continuidad del negocio detalla los pasos que da una organización para volver a las funciones operativas normales cuando se produce un desastre. Un plan de recuperación de desastres describe cómo protegerán las organizaciones sus sistemas informáticos y datos críticos durante una interrupción. La resiliencia organizacional también requiere planificación estratégica, gestión del riesgo empresarial, liderazgo y cultura eficaces, así como procesos de control en toda la organización. Disponer de procesos de control sólidos para la resiliencia organizacional no sólo permite a las organizaciones anticiparse, prepararse, responder y adaptarse continuamente al cambio, sino que también les permite sobrevivir y prosperar.

Evaluación y valoración de los procesos de Gobierno, gestión de riesgos y control de la Resiliencia Organizacional

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 Resiliencia Organizacional. Los requisitos representan una base mínima para evaluar la resiliencia organizacional.

Gobierno

Requisitos:

Los auditores internos deben evaluar los siguientes aspectos del gobierno de la resiliencia organizacional:

A. El Consejo establece y documenta una estrategia formal de resiliencia organizacional, con objetivos que se alinean con, y respaldan, la misión y la visión de la organización. La estrategia aborda los elementos operativos, tecnológicos y financieros necesarios para resistir y continuar las operaciones en medio de crisis, disrupciones y emergencias, así cómo recuperarse y adaptarse posteriormente. La estrategia se ajusta al planteamiento general de la organización en materia de gestión de riesgos y se comprueba y actualiza periódicamente.

B. Las actualizaciones sobre la consecución de la estrategia y los objetivos de resiliencia de la organización se comunican periódicamente al Consejo para su revisión, garantizando que la resiliencia esté integrada en la supervisión estratégica, los procesos de planificación a largo plazo y la cultura de la organización, incluidas las consideraciones presupuestarias y de recursos necesarias para apoyar las actividades empresariales críticas.

C. Se han identificado los procesos operativos, tecnológicos y financieros críticos relacionados con la resiliencia de la organización. Se han establecido políticas y procedimientos para los procesos críticos, que se revisan periódicamente y se actualizan, en caso necesario, para reforzar el entorno de control.

D. Se establece una estructura de mando del incidente, que incluye jerarquías de toma de decisiones, protocolos de comunicación y escalada, así como funciones y responsabilidades de liderazgo y operativas. La estructura se utiliza para supervisar y apoyar el establecimiento de objetivos de resiliencia organizacional.

E. Se establece un proceso para reevaluar periódicamente las competencias de las personas que desempeñan funciones críticas en los procesos de resiliencia. Existe un plan de sucesión que identifica los puestos clave y los posibles candidatos a sustituirlos.

F. Se establece un proceso para implicar a las partes interesadas internas y externas pertinentes en la identificación, el análisis y la respuesta a las vulnerabilidades existentes y las amenazas emergentes que podrían afectar a la consecución de los objetivos de resiliencia de la organización. Las partes interesadas pueden incluir la alta dirección, operaciones, gestión de riesgos, TI, cadena de suministro/aprovisionamiento, instalaciones, recursos humanos, finanzas, jurídico, cumplimiento, relaciones públicas, proveedores críticos, clientes, reguladores y otros.

GESTIÓN DE RIESGOS:

Requisitos:

Los auditores internos deben evaluar los siguientes aspectos de la gestión del riesgo de resiliencia organizacional:

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 que podrían alterar las operaciones. La estrategia de gestión de riesgos para la resiliencia organizacional se comunica a toda la organización y se revisa periódicamente.

B. Los riesgos relacionados con la resiliencia organizacional se evalúan y gestionan periódicamente en toda la organización. La evaluación y gestión de riesgos puede incluir las siguientes áreas: operaciones, gestión de riesgos empresariales, TI, cadena de suministro/aprovisionamientos, instalaciones, recursos humanos, finanzas, jurídico, cumplimiento, regulación, relaciones públicas, proveedores críticos, reputación, riesgos emergentes y otros.

C. Se establece la rendición de cuentas y la responsabilidad de la gestión del riesgo de resiliencia organizacional. Se identifica una persona o un equipo para supervisar e informar periódicamente sobre cómo se están gestionando los riesgos de resiliencia organizacional, incluidos los recursos necesarios para mitigar los riesgos e identificar las amenazas emergentes para la resiliencia de la organización.

D. Se establece un proceso para supervisar los niveles de riesgo de resiliencia organizacional (emergentes o previamente identificados) y escalar rápidamente aquellos que alcancen un nivel considerado inaceptable, según lo definido por las directrices de gestión de riesgos y la tolerancia al riesgo establecidas por la organización o los requisitos legales y regulatorios aplicables. Se consideran los impactos financieros y no financieros del riesgo de resiliencia organizacional.

E. La dirección ha implantado y pone a prueba periódicamente un proceso de respuesta y recuperación en caso de crisis, disrupciones y emergencias. El proceso de respuesta y recuperación ante incidentes incluye la detección, la contención, la recuperación y el análisis posterior al incidente. El planteamiento de respuesta ante incidentes incluye análisis de escenarios y pruebas de estrés periódicas frente a una serie de acontecimientos disruptivos plausibles. Los resultados de estos ejercicios son revisados por el Consejo y la alta dirección, y las acciones de mejora son objeto de seguimiento y se comunican periódicamente. Las recomendaciones son factibles, con propietarios y plazos claros.

CONTROLES

Requisitos:

Los auditores internos deben evaluar los siguientes aspectos de los procesos de control relacionados con la resiliencia de la organización.

A. Se establece un proceso para identificar a los proveedores críticos (suministradores y vendedores) y los niveles mínimos de inventario necesarios para continuar con las operaciones vitales. El proceso incluye el mantenimiento de una lista de proveedores alternativos.

B. Se identifican y clasifican los datos críticos para las operaciones. La clasificación de datos incluye la identificación de dónde residen los datos, quién necesita acceder a ellos, cómo se accede a ellos y si se dispone de copias de seguridad, así como si estas pueden recuperarse durante una emergencia.

C. Se establecen controles informáticos críticos y una supervisión continua para mitigar los riesgos de seguridad de la información (incluidos los riesgos cibernéticos) y garantizar la protección de los datos sensibles durante crisis, disrupciones y emergencias. Los controles y la supervisión continua incluyen inteligencia sobre amenazas en tiempo real y restricción del acceso sólo a usuarios autorizados.

D. Los activos informáticos críticos están inventariados. Incluyen el hardware, el software y los servicios necesarios para dar soporte a las operaciones durante crisis, disrupciones y emergencias.

E. Se establecen planes de continuidad del negocio y de recuperación ante desastres. Los planes incluyen funciones definidas para el personal asignado y los equipos de recuperación. Los planes se ponen a prueba periódicamente (por ejemplo, un "ejercicio de simulación en mesa"), y los resultados de las pruebas, incluidas las oportunidades de mejora, se comunican al Consejo y a la alta dirección.

F. Se establece un proceso para modificar el entorno de trabajo durante crisis, disrupciones y emergencias. Las modificaciones pueden incluir el uso de lugares de trabajo alternativos, como trabajar desde casa o establecer una oficina temporal de forma oportuna y eficaz.

G. Se establece un proceso para supervisar e informar continuamente de las amenazas y vulnerabilidades emergentes relacionadas con la resiliencia organizacional, así como para identificar, priorizar e implementar oportunidades de mejora de las operaciones de resiliencia organizacional. El proceso puede incluir sistemas de denuncia o de recopilación de información sobre riesgos.

H. Se establece un proceso para formar al personal en materia de resiliencia organizacional, garantizando que conozcan las políticas y procedimientos a seguir, así como las medidas a tomar cuando se produzcan crisis, disrupciones y emergencias. El proceso incluye ejercicios de formación en los que se simulan escenarios disruptivos.

I. Se establece un proceso para garantizar que los recursos humanos, tecnológicos y financieros necesarios estén presupuestados y disponibles durante crisis, disrupciones y emergencias. El proceso puede incluir financiación pre-aprobada.

J. Los recursos financieros necesarios para apoyar la resiliencia de la organización se analizan periódicamente y se comunican al Consejo. El análisis incluye la evaluación de la liquidez, la cobertura de seguros y los acuerdos de financiación de contingencias.

K. Se establece un proceso para revisar las crisis, disrupciones y emergencias después de que ocurran, así como analizar las revisiones posteriores a los incidentes a través de un proceso de lecciones aprendidas, incluida la integración de las lecciones en la futura planificación de la resiliencia organizacional.

Acerca del Instituto de Auditores Internos

El IIA es una asociación profesional internacional que cuenta con más de 265.000 miembros en todo el mundo y ha concedido más de 200.000 certificaciones Certified Internal Auditor® (CIA®). Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, formación, investigación y orientación técnica. Para más información, visite www.theiia.org.

Copyright

Septiembre de 2025