

Apêndice integrativo – Norma de certificação: ISO/IEC 27001 e extensão às diretrizes ISO/IEC 27xxx

Edição: março de 2026

CAPÍTULO 1 - GENERALIDADES

Neste Apêndice são definidos os procedimentos suplementares e/ou substitutivos aplicados pela RINA para a certificação de sistemas de gestão da qualidade, em relação ao que já está definido no Regulamento Geral para a certificação de sistemas de gestão RC/C 40.

A RINA emite a certificação de acordo com os requisitos da norma ISO/IEC 17021-1:2015 e ISO/IEC 27006-1:2024 para Organizações cujo Sistema de Gestão tenha sido reconhecido como conforme a todos os requisitos previstos pela norma:

ISO/IEC 27001:2022 (UNI CEI EN ISO/IEC 27001:2024+A1:2024)

A certificação pode ser integrada às diretrizes:

**ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27035-1, ISO/IEC 27035-2, ISO/IEC 27035-3
ISO/IEC 27701**

CAPÍTULO 2 - NORMA DE REFERÊNCIA / REQUISITOS PARA A CERTIFICAÇÃO

Além do estabelecido no Regulamento Geral para a Certificação de Sistemas de Gestão, para obter a certificação pela RINA, um Sistema de Gestão da Qualidade deve atender inicialmente e ao longo do tempo aos requisitos da norma ISO/IEC 27001, com eventuais integrações às diretrizes, bem como aos requisitos adicionais previstos pelos Organismos de Acreditação (ex.: Circular Técnica ACCREDIA nº 39/2024 ...).

A extensão às diretrizes deve ocorrer com base em uma certificação ISO/IEC 27001 válida, acreditada por um Organismo de Acreditação que seja signatário do acordo de reconhecimento mútuo IAF/MLA (IAF – International Accreditation Forum/MLA - Multilateral Agreements). O escopo da certificação ISO/IEC 27001 deve ser compatível com os processos das Diretrizes cuja integração é solicitada.

Se a organização possuir certificação ISO/IEC 27001 emitida por outro Organismo de Certificação com acreditação MLA, deverá solicitar a transferência da certificação para a RINA antes da extensão às Diretrizes, conforme descrito no capítulo 10 do Regulamento Geral para a certificação de Sistemas de Gestão.

Se a organização não possuir certificação ISO/IEC 27001 emitida por outro Organismo de Certificação com acreditação MLA, deverá solicitar à RINA uma nova certificação.

É permitida a extensão da certificação às diretrizes ISO/IEC 27XXX individualmente, com as exceções descritas a seguir:

- ISO/IEC 27018: a extensão à diretriz ISO/IEC 27018 deve ser sempre precedida pela extensão à ISO/IEC 27017. É permitida a extensão simultânea às diretrizes ISO/IEC 27017 e ISO/IEC 27018.
- ISO/IEC 27035: a extensão à diretriz ISO/IEC 27035 deve sempre compreender as três partes que a compõem.

CAPÍTULO 3 - CERTIFICAÇÃO INICIAL

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

Adicionalmente, aplica-se o seguinte.

As Organizações que desejem obter a certificação de seu Sistema de Gestão de Segurança da Informação e/ou a extensão às diretrizes devem enviar à RINA, além do Questionário Informativo, também o específico ANEXO AO QUESTIONÁRIO INFORMATIVO PARA OFERTA ISO/IEC 27001 (ISMS) e diretrizes ISO/IEC 27XXX, disponível no site www.rina.org, preenchido em todas as suas partes.

Em particular, o Questionário Informativo requer que sejam fornecidas informações sobre:

- Escopo do sistema de gestão de segurança da informação e número de pessoas que nele atuam;
- Datacenters onde estão localizados os servidores que gerenciam o serviço / Sites onde estão localizados ativos críticos;
- Fatores relativos à atividade realizada e à organização;
- Fatores relativos ao ambiente de TI;
- Fatores que podem determinar reduções ou aumentos da duração do tempo de auditoria.

Essas informações devem ser fornecidas por um representante autorizado da organização solicitante.

Se o Sistema de Gestão de Segurança da Informação incluir documentação (procedimentos, registros etc.) classificada como "confidencial" e/ou de qualquer forma não disponível para fins de certificação, a RINA avaliará a existência das condições para prosseguir com o processo de certificação.

Os documentos de certificação podem fazer referência a normas nacionais e internacionais como fonte(s) de controles considerados necessários na Declaração de Aplicabilidade da organização. A referência nos documentos de certificação deve ser indicativa da(s) fonte(s) de controles aplicados na Declaração de Aplicabilidade e não como uma certificação em relação às próprias normas.

CAPÍTULO 4 - MANUTENÇÃO DA CERTIFICAÇÃO

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

CAPÍTULO 5 - RECERTIFICAÇÃO

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

Adicionalmente, aplica-se o seguinte.

Por ocasião da auditoria de recertificação do Sistema de Gestão, prevista a cada três anos, a Organização deve enviar à RINA, além do Questionário Informativo, também o específico **ANEXO AO QUESTIONÁRIO INFORMATIVO PARA OFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX**, disponível no site www.rina.org, preenchido em todas as suas partes, conforme descrito no item 3 deste regulamento.

CAPÍTULO 6 - EXECUÇÃO DAS AUDITORIAS

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

Adicionalmente, aplica-se o seguinte:

O tempo de auditoria on site não deve ser inferior a 70% do tempo total de auditoria.

CAPÍTULO 7 - GESTÃO DOS CERTIFICADOS DE CONFORMIDADE

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

CAPÍTULO 8 - MODIFICAÇÃO DA CERTIFICAÇÃO E COMUNICAÇÃO DE MUDANÇAS

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

CAPÍTULO 9 - PARTICULARIDADES PARA ORGANIZAÇÕES MULTISSITE

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

CAPÍTULO 10 - TRANSFERÊNCIA DE CERTIFICADOS ACREDITADOS

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

Adicionalmente, aplica-se o seguinte.

Caso uma Organização com certificação válida emitida por outro Organismo de Certificação de Sistemas de Gestão, acreditado por um Organismo de Acreditação que seja signatário do acordo de reconhecimento mútuo IAF/MLA, deseje transferir sua certificação para a RINA, deverá enviar à RINA, além do Questionário Informativo, também o específico **ANEXO AO QUESTIONÁRIO INFORMATIVO PARA OFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX**, disponível no site www.rina.org, preenchido em todas as suas partes, conforme descrito no item 3.1 deste regulamento, cópia do certificado do Sistema de Gestão e cópia do documento Declaração de Aplicabilidade cujo referência consta no certificado.

CAPÍTULO 11 - SUSPENSÃO, RESTABELECIMENTO E REVOGAÇÃO DA CERTIFICAÇÃO

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

CAPÍTULO 12 - RENÚNCIA À CERTIFICAÇÃO

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.

CAPÍTULO 13 - CONDIÇÕES CONTRATUAIS

Aplica-se o estabelecido no Regulamento Geral para a certificação de Sistemas de Gestão RC/C 40 e o previsto nas Condições Gerais de Contrato para as atividades de avaliação da conformidade RC/C.17, no Regulamento de disciplina do uso da marca figurativa RINA nos contratos de licença RC/C.50, e no Regulamento Geral para a certificação RINA – Anexo I RC/C.130.