

ESQUEMA DE CERTIFICAÇÃO QNRCS

Perfil de Certificação RJC

Versão Preliminar

Índice

1. Introdução 3
2. Destinatários 3
3. Âmbito de aplicação para a lista de critérios de auditoria 3
Presunção de cumprimento das medidas de cibersegurança do RJC através da certificação 4
Níveis de garantia do Perfil de Certificação RJC 4
4. Critérios de auditoria de certificação do EC QNRCS – Perfil de Certificação RJC. 5
4.1. Medidas mínimas de cibersegurança – Anexo III do Regulamento n.º 756/2026 7
4.1.1. Objetivo: GOVERNAR 7
4.1.2. Objetivo: IDENTIFICAR 16
4.1.3. Objetivo: PROTEGER 22
4.1.4. Objetivo: DETETAR 33
4.1.5. Objetivo: RESPONDER 38
4.1.6. Objetivo: RECUPERAR 41
4.2. Outras medidas resultantes do Regime Jurídico da Cibersegurança 43
5. Critérios para a declaração de certificação EC QNRCS – Perfil de Certificação RJC 45
6. Classificação da informação 45
7. Divulgação e publicação 45
8. Revisão e atualização 45
9. Histórico de revisões 45

Versão Preliminar

1. Introdução

A presente versão do EC QNRCS introduz o conceito de "perfil de certificação", entendidos como conjuntos de requisitos, medidas e controlos de cibersegurança desenvolvidos para responder às características, necessidades, níveis de risco ou obrigações regulamentares aplicáveis a um determinado grupo de organizações ou contexto específico. Esta abordagem permite assegurar uma aplicação proporcional e adequada dos requisitos de certificação, promovendo simultaneamente a flexibilidade, a simplicidade de adoção e a evolução contínua do EC através da criação de novos perfis.

Foi assim criado o Perfil de Certificação RJC, que se destina à demonstração da conformidade com os requisitos estabelecidos pelo Regime Jurídico da Cibersegurança (RJC), incluindo em matéria de medidas mínimas de cibersegurança, permitindo que as entidades abrangidas possam recorrer à certificação como mecanismo de presunção de cumprimento.

As medidas e respetivos critérios de verificação definidas no presente Perfil de Certificação RJC constituem a lista de critérios de auditoria de certificação que os organismos de certificação (OC) utilizarão para sustentação das constatações de conformidade ou não conformidade.

2. Destinatários

O Perfil de Certificação do RJC destina-se, primordialmente, às organizações abrangidas pelo RJC que pretendam beneficiar da presunção de cumprimento do RJC, designadamente, através da avaliação da conformidade da implementação das medidas do nível de garantia correspondente ao nível de conformidade do RJC a que estão legalmente obrigadas, ou superior.

Poderá ser também adotado por organizações fora do âmbito do RJC e que queiram efetuar a certificação como uma forma de aderir voluntariamente ao ecossistema de cibersegurança estabelecido pelo RJC. Para estas, o presente perfil de certificação estabelece, para além das medidas mínimas de cibersegurança definidas no nível para o qual se candidatam, um conjunto de requisitos adicionais, originários dos normativos e regulamentos aplicáveis às entidades abrangidas pelo RJC, para que possam também tirar partido das vantagens da certificação e elevarem o seu nível de maturidade em cibersegurança.

3. Âmbito de aplicação para a lista de critérios de auditoria

O Quadro Nacional de Referência para a Cibersegurança (QNRCS) aprovado pelo Centro Nacional de Cibersegurança (CNCS) é considerado um instrumento nacional de referência para a identificação das normas, padrões e boas práticas existentes em matéria de gestão da Cibersegurança.

O presente anexo tem por objetivo a avaliação da implementação das medidas mínimas de cibersegurança previstas no RJC e nos instrumentos regulamentares associados, que derivam do QNRCS, bem como a avaliação do cumprimento de requisitos regulamentares adicionais estabelecidos no RJC e legislação associada.

Nesse sentido, o âmbito de aplicação do Perfil de Certificação RJC corresponde à implementação das medidas mínimas de cibersegurança definidas em cada nível de conformidade do RJC, bem como outras especificadas no presente Anexo, de acordo com o prescrito no RJC. Isto quer dizer que todas as medidas mínimas de cibersegurança descritas no presente anexo para um determinado nível têm de ser implementadas e

Versão Preliminar

respetivamente evidenciada a sua implementação perante o OC para que a organização candidata obtenha a certificação.

Para organizações fora do âmbito do RJC e que queiram efetuar a certificação como uma forma de aderir voluntariamente ao ecossistema de cibersegurança estabelecido pelo RJC, mantém-se esta obrigação de implementar e evidenciar a implementação de todas as medidas mínimas de cibersegurança definidas no nível de garantia para o qual se candidatam. No entanto, o âmbito das atividades da organização em que as medidas devem ser aplicadas poderá ser restringido, recomendando-se, ainda assim, que sejam incluídas as atividades mais relevantes para a prestação dos serviços considerados essenciais para a organização. Para as organizações neste enquadramento, o âmbito da aplicação das medidas deve ser identificado de acordo com o disposto na secção "Delimitação do contexto de atividade aplicável e decisão de exclusão de medidas do QNRCS" do EC QNRCS, devendo o âmbito ser descrito na Declaração de Aplicabilidade, conforme preconiza o EC QNRCS.

Presunção de cumprimento das medidas de cibersegurança do RJC através da certificação

Determina o RJC que as organizações por aquele abrangidas poderão beneficiar da presunção do cumprimento das medidas de cibersegurança nele previstas, caso se certifiquem no EC QNRCS, de acordo com o Artigo 27.º do Regulamento n.º 756/2026. Tal presunção será devidamente tida em conta pelo CNCS para efeitos de gestão das suas atividades de Supervisão.

Para que as organizações abrangidas pelo RJC beneficiem da presunção de cumprimento das medidas de cibersegurança, deverão obter a certificação no nível de garantia correspondente ao nível de conformidade do RJC a que estão legalmente obrigadas, ou superior (nível determinado conforme o disposto no Artigo 28.º do Regulamento n.º 756/2026). Sendo a certificação uma atividade voluntária, a organização abrangida pelo RJC poderá na mesma optar por certificar-se, caso assim o deseje, num nível de garantia inferior ao do correspondente nível de conformidade do RJC a que está legalmente obrigada, mas nessa situação não haverá lugar a presunção de cumprimento das medidas de cibersegurança do RJC através da certificação.

Devido à natureza da aplicação da presunção de cumprimento, as entidades abrangidas pelo RJC que pretenda beneficiar desta ferramenta, têm de implementar e evidenciar a implementação de todas as medidas de cibersegurança definidas no nível de conformidade do RJC a que estão legalmente obrigadas, ou superior, em todas as atividades da entidade. Não se lhes aplicam, portanto, o disposto nas secções "Delimitação do contexto de atividade aplicável e decisão de exclusão de medidas do QNRCS", "Declaração de Aplicabilidade" e "Alteração do âmbito". A implementação de uma medida específica poderá ser dispensada por motivo superveniente (por exemplo, pode não ser materialmente aplicável), competindo ao OC avaliar a pertinência do pedido, em função da situação da organização e das evidências apresentadas que o fundamentem, e decidir pela dispensa.

Níveis de garantia do Perfil de Certificação RJC

Em alinhamento com a abordagem de classificação das entidades abrangidas pelo RJC, assente na matriz de risco prevista no artigo 28.º do Regulamento n.º 756/2026, e com o previsto genericamente no EC QNRCS, as medidas de cibersegurança do Perfil de Certificação RJC encontram-se organizadas em três níveis de garantia: Básico, Substancial e Elevado.

Versão Preliminar

Estes níveis de garantia refletem diferentes graus de maturidade e robustez das capacidades de cibersegurança das organizações, sendo a respetiva conformidade objeto de avaliação no âmbito das auditorias de certificação realizadas pelos organismos de certificação (OC) competentes.

O nível de garantia selecionado pela organização deverá ter em conta o seu contexto e ter por base, entre outros, as capacidades e as necessidades de cibersegurança, inferidas do processo de análise e gestão dos riscos, acrescido do esforço, do custo de efetivação das medidas, da repercussão a atingir com a certificação, bem como outros fatores que lhe possam ser exclusivos. Todas as organizações candidatas deverão também considerar eventuais requisitos legais adicionais a que estejam obrigadas em matéria de cibersegurança.

Recomenda-se que a determinação do nível de garantia assente numa análise dos riscos, realizada de acordo com uma metodologia adequada à natureza da organização. Esta análise deverá considerar, entre outros aspetos, os ativos a proteger, as ameaças e vulnerabilidades relevantes, os impactos potenciais decorrentes de incidentes de cibersegurança e o contexto interno e externo da organização. O resultado desta avaliação permite enquadrar a organização no nível de garantia mais adequado, assegurando que os requisitos e medidas de certificação são proporcionais para mitigar os riscos identificados.

Específico para as organizações abrangidas pelo RJC que pretendam beneficiar da presunção de cumprimento das medidas de cibersegurança do RJC, tal exposto na secção anterior, deverão obter a certificação no nível de garantia correspondente ao nível de conformidade do RJC a que estão legalmente obrigadas, ou superior. A determinação do nível de garantia aplicável é efetuada com base na matriz de riscos definida no regime, a qual considera fatores como a criticidade dos serviços prestados, a dependência de sistemas de informação e comunicação, o potencial impacto de incidentes de cibersegurança, e consequentemente do resultado da qualificação da organização. O nível de garantia resultante desta avaliação serve de referência para a seleção do nível de garantia adequado e para a definição dos requisitos a cumprir.

4. Critérios de auditoria de certificação do EC QNRCS – Perfil de Certificação RJC.

Os quadros seguintes apresentam. para cada objetivo de cibersegurança definido pelo QNRCS a identificação das subcategorias e respetivas medidas de cibersegurança obrigatórias no âmbito do EC QNRSC – Perfil de Certificação RJC. São igualmente incluídos os critérios de verificação obrigatórios que constituem um instrumento de suporte aos OCs nas das auditorias de certificação.

Sendo o objetivo principal do EC QNRCS – Perfil de Certificação RJC. concretizar o descrito no Art.º 27º do Regulamento 756/2026, possibilitando as entidades, que se encontram ao abrigo do RJC, de beneficiar da presunção de cumprimento com o cumprimento das medidas de cibersegurança previstas no RJC mediante a certificação no EC QNRCS, as medidas de cibersegurança listadas no presente anexo são de carácter obrigatório, não estando previstos mecanismos para exclusão da sua aplicação.

O conjunto de medidas aplicáveis às organizações que pretendem obter a certificação depende do nível de garantia à qual se candidatam (Básico, Substancial ou Elevado). Estes níveis são cumulativos, o que significa que as organizações que pretendam obter a certificação nos níveis de garantia Substancial ou Elevado devem assegurar igualmente a implementação das medidas de cibersegurança exigidas para os níveis de garantia inferiores.

Versão Preliminar

Para além das presentes medidas, a organização deverá ainda fazer cumprir os restantes requisitos apresentados pelo EC QNRCS, não estando estes presentes neste anexo.

Caso uma entidade em âmbito do RJC já certificada solicite a redução do nível de garantia do seu certificado, a alteração poderá ser efetuada através do procedimento definido para o efeito. Contudo, sempre que o novo nível de garantia pretendido seja inferior ao nível de conformidade que resulta da matriz de risco aplicável à entidade, esta deixa de beneficiar da presunção de cumprimento das medidas de cibersegurança associada ao nível de garantia que lhe seria exigível. Para as restantes organizações aplicam-se apenas os critérios gerais do EC QNRCS a este respeito.

Versão Preliminar

4.1. Medidas mínimas de cibersegurança – Anexo III do Regulamento n.º 756/2026

4.1.1. Objetivo: GOVERNAR

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
GR.CO	GR.CO-1	Missão, visão, estratégia e objetivos	N/A	• Definição, priorização e comunicação da estratégia de gestão dos riscos, a missão, visão e objetivos da organização • Definição das prioridades em matéria de cibersegurança	N/A	N/A	• Registo documentado da missão, visão, estratégia de gestão do risco e objetivos no âmbito da cibersegurança e respetivas prioridades	N/A
	GR.CO-3	Requisitos legais e regulamentares	• Identificação e aplicação dos requisitos legais e regulamentares relativos à cibersegurança	N/A	N/A	• Evidência da gestão quotidiana da organização que demonstre o cumprimento dos requisitos e obrigações legais de cibersegurança aplicáveis à organização	N/A	N/A
	GR.CO-4	Posicionamento no sector	• Identificação dos serviços críticos da organização dos quais as partes interessadas externas dependem	• Classificação, priorização e integração no processo de gestão dos riscos dos serviços críticos da organização dos quais as	N/A	• Registo documentado da identificação dos serviços críticos dos quais as partes	• Registo do processo de gestão dos riscos que contempla os serviços críticos das quais as partes interessadas	N/A

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
				partes interessadas dependem		interessadas externas dependem	externas dependem, incluindo a definição de critérios para a classificação e priorização dos serviços críticos	
	GR.CO-5	Requisitos de resiliência	• Identificação e registo dos requisitos necessários para garantir o suporte dos serviços críticos	• Implementação de mecanismos de redundância, garantindo a disponibilidade dos serviços críticos • Definição, aprovação e implementação de um Plano de Continuidade de Negócio contendo planos e tempos de resposta para a recuperação dos serviços críticos e respetivos processos	• Execução de testes ao Plano de Continuidade de Negócio	• Registo documentando da identificação dos requisitos de resiliência necessários para garantir o suporte dos serviços críticos	• Evidencia técnica da implementação de mecanismos de redundância que garantam a disponibilidade dos serviços críticos. • Plano de Continuidade de Negócio aprovado e implementado e que contenha a definição dos tempos necessários para a recuperação de cada serviço critico e respetivos processos	• Evidência da execução de testes ao Plano de Continuidade de Negócio
	GR.CO-6	Papel na cadeia logística	• Identificação, documentação, classificação e priorização dos serviços críticos externos dos quais a organização depende • Comunicação às partes interessadas a identificação dos serviços críticos externos, respeitando o	N/A	N/A	• Registo da identificação, e da comunicação dos serviços críticos externos dos quais a organização depende. • Registo do processo de gestão dos riscos que contempla os serviços críticos externos dos quais a organização depende, incluindo a definição de critérios para a classificação e	N/A	N/A

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			princípio da necessidade de saber • Inclusão dos serviços críticos externos identificados na gestão dos riscos			priorização destes serviços.		
GR.GR	GR.GR-1	Apetite e tolerância ao risco	N/A	• Definição, registo, aprovação, revisão regular e comunicação interna, do apetite e tolerância ao risco da organização	N/A	N/A	• Registo documentado e aprovado da definição do apetite e tolerância ao risco. • Registo da comunicação às partes interessadas internas do apetite e tolerância ao risco	N/A
	GR.GR-2	Processo de gestão do risco	• Identificação, aprovação, gestão e atualização regular dos processos de gestão dos riscos de cibersegurança	• Inclusão dos processos de gestão dos riscos de cibersegurança na estratégia transversal da gestão dos riscos da organização	N/A	• Evidência da gestão quotidiana que demonstre a implementação das várias fases de gestão de riscos da cibersegurança	• Evidência de gestão quotidiana que demonstre a implementação das várias fases de gestão dos riscos da cibersegurança nos processos transversais de gestão dos riscos da organização	N/A
	GR.GR-3	Estratégia de tratamento	N/A	• Definição e comunicação às partes interessadas da estratégia de tratamento do risco da organização	N/A	N/A	• Registo documentado da estratégia de tratamento do risco e da sua comunicação às partes interessadas.	N/A

Versão preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
	GR.GR-4	Comunicação dos riscos	N/A	• Criação de um canal de comunicação interno, para partilha de informação sobre os riscos de cibersegurança, com os órgãos de gestão, direção e administração e restantes áreas relevantes.	N/A	N/A	• Canal interno de comunicação usado para a partilha de riscos de cibersegurança	N/A
	GR.GR-5	Metodologia para gestão do risco	N/A	• Definição de uma metodologia para a gestão dos riscos de cibersegurança que permita identificar, registar, calcular, categorizar e priorizar os riscos de cibersegurança	• Definição, aprovação e implementação de uma Política de Gestão dos Riscos de Cibersegurança	N/A	• Registo da metodologia de gestão dos riscos de cibersegurança	• Política de Gestão dos Riscos de Cibersegurança aprovada e implementada
GR.FR	GR.FR-1	Plano de melhoria	• Disponibilização, pelos órgãos de gestão, direção e administração, dos recursos necessários para a melhoria contínua da cibersegurança	N/A	N/A	• Plano de Melhoria Contínua de Cibersegurança com medidas, prazos e recursos a afetar, aprovado pelos órgãos de gestão, direção e administração	N/A	N/A
	GR.FR-2	Alocação de recursos	N/A	• Alocação suficiente e proporcional de recursos à gestão do risco de cibersegurança, às funções, responsabilidades e políticas da organização	N/A	N/A	• Registo do planeamento das atividades em matéria de cibersegurança a curto ou médio prazo • Evidência da gestão quotidiana que demonstre a alocação dos recursos para a	N/A

Versão preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
							gestão do risco de cibersegurança	
	GR.FR-3	Funções e responsabilidades	N/A	• Documentação, aprovação e comunicação das funções, responsabilidades e autoridades de cibersegurança dentro da organização	N/A	N/A	• Registo documentado e aprovado das funções, responsabilidades e autoridades em matéria de cibersegurança e da sua comunicação às partes interessadas	N/A
	GR.FR-4	Política de uso aceitável	• Definição de uma Política de Uso Aceitável, abrangente para toda a organização, que defina as regras para a utilização segura e responsável dos seus ativos. • Disponibilização da Política de Uso Aceitável ao pessoal aquando da sua entrada	• Definição e implementação de medidas de cibersegurança associadas à gestão dos recursos humanos, aplicável no recrutamento, durante o contrato e após o seu término	N/A	• Política de Uso Aceitável aprovada e implementada • Registo da tomada de conhecimento da Política de Uso Aceitável pelo pessoal aquando da sua entrada	• Registo das medidas de cibersegurança para a gestão de recursos humanos, desde a entrada até à saída do pessoal	N/A
GR.PP	GR.PP-1	Políticas de cibersegurança	• Definição, documentação, atualização periódica da Política de Cibersegurança • Aprovação da Política de Cibersegurança pelos órgãos de gestão, direção e administração	• Definição, aprovação e implementação da Política de Classificação e Gestão de Dados	N/A	• Política de Cibersegurança, aprovada pelos órgãos de gestão, direção e administração • Registos da comunicação interna da Política de Cibersegurança	• Política de Classificação e Gestão de Dados aprovada e implementada	N/A

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			• Inclusão na Política de Cibersegurança a atribuição de funções e responsabilidades em cibersegurança. • Divulgação interna da Política de Cibersegurança					
	GR.PP-2	Plano de resposta a incidentes	• Definição, aprovação, implementação e atualização do Plano de Resposta a Incidentes, incluindo a atribuição e identificação de funções e responsabilidades	N/A	N/A	• Plano de Resposta a Incidentes aprovado, implementado e atualizado	N/A	N/A
	GR.PP-3	Plano de recuperação de desastres	N/A	• Definição, aprovação, implementação e atualização do Plano de Recuperação de Desastres, incluindo a atribuição e identificação de funções e responsabilidades	N/A	N/A	• Plano de Recuperação de Desastres aprovado, implementado e atualizado	N/A
GR.SP	GR.SP-2	Quadro de ameaças	N/A	N/A	• Revisão e atualização regular da estratégia de gestão dos riscos de cibersegurança, garantindo a sua adaptação e cobertura dos requisitos e riscos organizacionais	N/A	N/A	• Evidência de que a organização tem atualizado o quadro de ameaças e que revê e adapta a estratégia de gestão dos riscos em conformidade
	GR.SP-3	Desempenho da gestão dos riscos	N/A	N/A	• Definição e implementação de	N/A	N/A	• Registo da definição de mecanismos para avaliar

Versão preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
					mecanismos de avaliação do desempenho da gestão dos riscos de cibersegurança			o desempenho da gestão dos riscos de cibersegurança
GR.CA	GR.CA-1	Política de Gestão de Riscos da Cadeia de Abastecimento	N/A	N/A	• Definição, aprovação, implementação, revisão e atualização da Política de Gestão de Riscos da Cadeia de Abastecimento e do respetivo procedimento	N/A	N/A	• Política e procedimento de Gestão de Riscos da Cadeia de Abastecimento aprovados, implementados e atualizados
	GR.CA-3	Riscos da cadeia de abastecimento	N/A	• Identificação, aprovação, correta gestão e atualização periódica dos riscos de cibersegurança associados à cadeia de abastecimento • Inclusão dos processos de gestão dos riscos de cibersegurança da cadeia de abastecimento nos processos transversais de cibersegurança e de gestão dos riscos da organização	N/A	N/A	• Registo documentado da identificação, aprovação, gestão e atualização dos riscos de cibersegurança associados à cadeia de abastecimento	N/A
	GR.CA-5	Contratos com fornecedores	N/A	• Definição e integração de requisitos de cibersegurança, incluindo os meios de partilha de informação sensível, nos contratos e outros acordos a celebrar com fornecedores	• Integração nos contratos e outros acordos com fornecedores disposições legais que permitam a avaliação contínua da cibersegurança dos fornecedores e a	N/A	• Modelos de contratos/acordos contendo cláusulas específicas de requisitos de cibersegurança	• Modelos de contratos/acordos contendo cláusulas específicas que permitam a avaliação contínua da cibersegurança dos fornecedores e a

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
					correção de eventuais falhas identificadas			correção de eventuais falhas identificadas
	GR.CA-6	Avaliação de fornecedores	N/A	N/A	• Condução de processos de devida diligência, sempre que possível, antes de serem estabelecidas relações contratuais com fornecedores, com o objetivo de minimizar a exposição ao risco	N/A	N/A	• Registo dos processos de devida diligência realizados antes da contratação
	GR.CA-7	Execução da avaliação do risco da cadeia de abastecimento	• Execução de avaliações do risco da cadeia de abastecimento pelo menos uma vez por ano ou sempre que relevante	• Mitigação dos riscos identificados durante o processo de avaliação do risco da cadeia de abastecimento	• Realização de avaliações da cibersegurança dos seus fornecedores em conformidade com o nível de exigência requerido	• Registo documentado das avaliações do risco da cadeia de abastecimento	• Registo das medidas de mitigação aplicadas face aos riscos identificados durante o processo de avaliação do risco da cadeia de abastecimento	• Registo da avaliação de cibersegurança dos fornecedores em conformidade com o nível de exigência requerido, nomeadamente: certificados valido no âmbito do Selo de Maturidade Digital; Relatórios de auditorias realizadas; Resultados de testes realizados no âmbito da cibersegurança
	GR.CA-8	Partes interessadas ao Plano de Resposta a	N/A	• Identificação do pessoal-chave dos fornecedores a incluir nas atividades previstas nos Plano de Resposta a Incidentes e	• Inclusão do pessoal-chave dos fornecedores nos seus exercícios e testes dos Plano de Resposta a Incidentes e	N/A	• Registo da inclusão do pessoal-chave dos fornecedores nas atividades previstas nos Plano de Resposta a Incidentes e no Plano de	• Registo de testes e exercícios ao Plano de Resposta a Incidentes e Plano de Recuperação de Desastres com a

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
		Incidentes e no Plano de Recuperação de Desastres		Plano de Recuperação de Desastres	Plano de Recuperação de Desastres		Recuperação de Desastres	inclusão do pessoal-chave dos fornecedores

Versão Preliminar

4.1.2. Objetivo: IDENTIFICAR

Categoria	Sub Categoria		Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
IG.GA	ID.GA-1	Inventário de recursos físicos	• Inventário atualizado dos equipamentos e demais recursos físicos geridos ou detidos pela organização	N/A	• Ferramenta de suporte à gestão de equipamentos e os demais recursos físicos	• Inventário atualizado de equipamentos e recursos físicos	N/A	• Evidência técnica da ferramenta de inventariação e de suporte à gestão de equipamentos e os demais recursos físicos
	ID.GA-2	Inventário de recursos lógicos	• Inventário, documentado e atualizado, de recursos lógicos que incluía plataformas de software e aplicações que são geridas ou detidas pela organização	N/A	• Ferramentas ou aplicações de suporte à gestão de recursos lógicos	• Inventário atualizado de recursos lógicos	N/A	• Evidência técnica da ferramenta de inventariação e de suporte à gestão de recursos lógicos
	ID.GA-3	Redes e fluxos	N/A	• Diagramas de rede e sistemas que demonstrem a topologia da rede • Mapa dos fluxos de comunicação entre os sistemas internos	• Mapa dos fluxos de comunicação externos, e os mesmos devem ser documentados, devidamente aprovados e atualizados	N/A	• Diagramas de rede e sistemas e de fluxos de comunicação internos	• Diagramas de rede e sistemas e de fluxos de comunicação externos aprovados e atualizados
	ID.GA-4	Inventário de serviços externos	• Inclusão no inventário de ativos os serviços prestados por fornecedores que a organização utiliza e depende	N/A	N/A	• Inventário de ativos que inclua os serviços prestados por fornecedores que a organização utiliza e depende	N/A	N/A

Categoria	Sub Categoria		Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
	ID.GA-5	Classificação de ativos	• Classificação dos ativos de acordo com a sua criticidade e valor dos mesmos	N/A	N/A	• Registo da classificação dos ativos de acordo com a sua criticidade e valor	N/A	N/A
	ID.GA-6	Identificação e classificação de dados e metadados	N/A	N/A	• Identificação e classificação dos dados e respetivos metadados tratados pela organização, em concordância com a Política de Classificação e Gestão de Dados	N/A	N/A	• Registo da identificação e classificação dos dados e respetivos metadados, de acordo com a Política de Classificação e Gestão de Dados
	ID.GA-7	Atualizações de segurança e manutenção	• Realização de atualizações de segurança regulares nos sistemas e aplicação de *patches* adequados nas aplicações e sistemas da organização • Aplicação de controlos compensatórios, em função do risco, consoante a impossibilidade da aplicação de atualizações de segurança • Execução de manutenção periódica dos equipamentos e demais recursos físicos existentes	• Definição, aprovação e implementação de uma Política de Gestão do Ciclo de Vida de Ativos, garantindo que são implementadas as medidas necessárias para gerir a perda, má utilização, dano ou roubo de ativos • Planeamento, execução e registo de manutenções preventivas e as reparações dos componentes críticos dos sistemas, de acordo com a Política de Gestão do Ciclo de Vida de Ativos	N/A	• Evidência técnica das atualizações de segurança e aplicação de *patches* nas aplicações e sistemas • Evidência técnica de aplicação de controlos compensatórios, que sejam aplicados de acordo com uma análise de risco, na eventual impossibilidade de realização de atualizações de segurança e de aplicação de *patches* • Registo da execução de manutenções de equipamentos e demais recursos físicos • Registo da aprovação das ações de	• Política de Gestão do Ciclo de Vida de Ativos aprovada e implementada • Registo documentado do planeamento das ações de manutenção e reparações de componentes críticos dos sistemas, em conformidade com a Política de Gestão do Ciclo de Vida de Ativos	N/A

Categoria	Sub Categoria		Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			• Aprovação das ações de manutenção de software e hardware			manutenção de software e hardware		
	ID.GA-8	Processos de sanitização	N/A	• Inclusão na Política de Classificação e Gestão de Dados, requisitos para a destruição dos dados dos sistemas críticos e informações sensíveis	• Registo da execução dos processos de sanitização físicos e digitais • Registo da execução de testes aos processos de sanitização, garantindo a eficácia da destruição da informação	N/A	• Registo da inclusão de medidas para a destruição dos dados dos sistemas críticos e das informações sensíveis na Política de Classificação e Gestão de Dados	• Registo do processo de sanitização e dos testes realizados
	ID.GA-9	Gestão de alterações	N/A	N/A	• Definição e implementação de regras internas para a gestão de alterações, incluindo processos de avaliação e aprovação prévia de alterações. • Execução de testes às alterações antes da sua implementação nos sistemas operacionais • Realização de atualizações aos seus procedimentos de forma a acompanhar as alterações efetuadas	N/A	N/A	• Registo do processo documentado de gestão de alterações que inclua, pelo menos, a avaliação e aprovação prévia das regras para a realização de alterações • Registo do resultado dos testes e da validação às alterações efetuadas antes da sua implementação em produção. • Evidência de uma gestão do quotidiano que reflita atualizações de procedimentos quando existam alterações
ID.AR	ID.AR-1	Vulnerabilidades identificadas	• Identificação das vulnerabilidades dos ativos da organização	• Aprovação e implementação de uma Política de Monitorização, Identificação	• Ferramentas de identificação e monitorização contínua	• Registo documentado das vulnerabilidades identificadas	• Política de Monitorização, Identificação e Documentação das	• Evidência técnica de ferramentas de identificação e

Categoria	Sub Categoria		Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
				e Documentação das Vulnerabilidades dos seus sistemas críticos • Definição de um processo, incluindo-o na Política	das vulnerabilidades dos ativos • Realização regular de testes de intrusão		Vulnerabilidades aprovada e implementada	monitorização contínua das vulnerabilidades • Registo do resultado da realização regular de testes de intrusão
	ID.AR-4	Probabilidade e impacto das ameaças	• Cálculo e registo, no processo de gestão dos riscos, a probabilidade de concretização de ameaças e avaliação dos respetivos potenciais impactos	N/A	N/A	• Critérios para determinar a probabilidade das ameaças e para a avaliar os potenciais impactos das mesmas	N/A	N/A
	ID.AR-5	Avaliação do risco dos ativos	• Realização de avaliações do risco com base na análise de ameaças, vulnerabilidades, probabilidades e impactos nos processos e em todos os ativos que garantam a continuidade do funcionamento das redes e sistemas de informação que a organização utiliza, incluindo os ativos que garantam a prestação dos serviços críticos	• Realização e documentação das avaliações do risco com base nos critérios definidos na sua metodologia de gestão do risco • Atualização contínua da avaliação do risco	N/A	• Evidência da gestão quotidiana que demonstre realização de avaliações do risco tendo como base a análise de ameaças, vulnerabilidades, probabilidades e impactos nos processos e ativos organizacionais	• Registo documentado da avaliação do risco e respetiva atualização, tendo por base os critérios definidos na metodologia	N/A
	ID.AR-6	Respostas priorizadas aos riscos	• Implementação de controlos de segurança para os riscos identificados	• Identificação, priorização, planeamento, acompanhamento e comunicação das ações em respostas aos ricos	• Inclusão, na estratégia de tratamento dos riscos da organização, de um plano de monitorização, revisão e melhoria	• Evidência técnica da implementação de controlos de segurança para os riscos identificados	• Registo da identificação, priorização, planeamento, acompanhamento e comunicação das respostas aos riscos	• Registo da inclusão de um plano de monitorização, revisão e melhoria contínua, na

Versão preliminar

Categoria	Sub Categoria		Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
					contínua das respostas aos riscos			estratégia de tratamento dos riscos
	ID.AR-7	Tratamento de vulnerabilidades internas e externas	• Tratamento das vulnerabilidades que a organização tenha conhecimento	• Implementação de processos de gestão de vulnerabilidades que incluam processamento, análise e correção de vulnerabilidades de fontes internas e externas • Processo de gestão de vulnerabilidades da organização alinhado com a Instrução Técnica de Divulgação Coordenada de Vulnerabilidades	• Registo, análise e avaliação sistemática das vulnerabilidades identificadas • Implementação de mecanismos automatizados, para divulgação e acompanhamento dos esforços de correção de vulnerabilidades, recolhidas de fontes internas e externas, para as principais partes interessadas	• Registo da identificação e de tratamento das vulnerabilidades	• Registo dos processos de gestão de vulnerabilidades que incluam processamento, análise e correção de vulnerabilidades de fontes internas e externas, o qual deve estar alinhado com a Instrução Técnica de Divulgação Coordenada de Vulnerabilidades	• Registo do resultado da análise e avaliação das vulnerabilidades identificadas • Evidência técnica da implementação de mecanismos automatizados para a divulgação e acompanhamento dos esforços de correção de vulnerabilidades
ID.MC	ID.MC-2	Testes e exercícios de cibersegurança	N/A	N/A	• Identificação de pontos de melhoria dos processos através da realização de testes e exercícios de cibersegurança • Execução de testes e exercícios de cibersegurança com as partes interessadas	N/A	N/A	• Registo da realização de testes e exercícios de cibersegurança, incluindo os efetuados com partes interessadas
	ID.MC-3	Lições aprendidas e melhoria de processos	• Identificação de lições aprendidas através de avaliações pós-incidentes, numa ótica de melhoria dos processos/ procedimentos/	• Inclusão nos planos e processos de gestão de cibersegurança da organização, as melhorias derivadas da monitorização e avaliação periódicas, das	N/A	• Registo documentado das avaliações pós-incidentes, com identificação de lições aprendidas, definição e implementação de melhorias	• Registo das melhorias derivadas da monitorização e avaliação periódicas nos seus planos e processos de gestão de cibersegurança	N/A

Categoria	Sub Categoria		Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			tecnologias como reforço à ciber-resiliência da organização	medidas, controlos e processos de cibersegurança				

Versão Preliminar

4.1.3. Objetivo: PROTEGER

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
PR.GA	PR.GA-1	Ciclo de vida das identidades	• Gestão de identidades e credenciais de dispositivos, serviços e utilizadores • Implementação de uma Política de Palavra-passe e uma Política de Gestão de Identidades, Autenticação e Controlo de Acessos	• Gestão de credenciais dos sistemas são desativadas após um período específico de inatividade, como determinado na Política de Gestão de Identidades, Autenticação e Controlo de Acessos, a menos que isso comprometa o funcionamento seguro dos processos críticos • Monitorização da utilização atípica de credenciais dos sistemas críticos	• Gestão de identidades e credenciais dos dispositivos, serviços e utilizadores através de mecanismos automatizados • Aplicação de autenticação segura nas transações entre sistemas críticos, nomeadamente, a autenticação multifator (MFA), certificados criptográficos, tokens e chaves criptográficas	• Evidência técnica da gestão de identidades e respetivas credenciais de dispositivos, serviços e utilizadores. • Política de Palavra-passe e política de Gestão de Identidades, Autenticação e Controlo de Acessos aprovada e implementada	• Evidência técnica da desativação de credenciais dos sistemas, após o período específico de inatividade definido de acordo com a Política de Gestão de Identidades, Autenticação e Controlo de Acessos • Registo da monitorização contínua dos sistemas críticos quanto à utilização atípica de credenciais dos sistemas	• Evidência técnica de mecanismos automatizados de suporte à gestão de identidades e credenciais dos dispositivos, serviços e utilizadores • Evidência técnica da aplicação de autenticação segura nas transações entre sistemas críticos
	PR.GA-2	Verificação de identidade	N/A	• Implementação de procedimentos de acordo com o estabelecido na Política de Gestão de Identidades, Autenticação e Controlo de Acessos para verificar a identidade dos utilizadores antes de emitir as credenciais que dão acesso aos sistemas da organização	• Garantia de a utilização de credenciais únicas associadas a cada utilizador, dispositivo e processo que interaja com os sistemas críticos da organização • Garantia de que todas as exceções estão documentadas e devidamente aprovadas	N/A	• Registo da implementação de procedimentos de verificação da identidade dos utilizadores, antes da emissão de credenciais	• Evidência técnica da atribuição de credenciais únicas para cada utilizador, dispositivo ou processo que interaja com sistemas críticos da organização • Registo documentado das exceções à Política de Gestão de Identidades,

v 2.0 Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
								Autenticação e Controlo de Acessos e a sua respetiva aprovação
	PR.GA-3	Mecanismos de autenticação	• Implementação de autenticação multifator (MFA) nos acessos remotos e contas privilegiadas	• Realização de uma avaliação do risco das comunicações entre sistemas críticos • Aplicação de mecanismos de autenticação aos utilizadores, dispositivos e outros ativos, adequados e proporcionais ao risco identificado • Implementação de autenticação multifator (MFA) nos seus sistemas críticos	• Enquadramento da comunicação entre os sistemas incluído em acordo entre as entidades participantes (ex: parceiros, fornecedores ou prestadores de serviços, incluindo, serviços de computação em nuvem) • Implementação de autenticação multifator (MFA) em todos os dispositivos e outros ativos de sistemas de informação, quando estes o permitam	• Evidência técnica da implementação de autenticação multifator (MFA) nos acessos remotos e contas privilegiadas.	• Registo da avaliação do risco das comunicações entre sistemas críticos. • Evidência técnica dos mecanismos de autenticação aplicados aos utilizadores, dispositivos e outros ativos. • Evidência técnica da implementação de autenticação multifator (MFA) nos sistemas críticos.	• Modelos de acordos entre a organização e terceiros para comunicação entre sistemas. • Evidência técnica da implementação de autenticação multifator (MFA) em todos os seus dispositivos e outros ativos de sistemas de informação, quando possível.
	PR.GA-4	Afirmações de identidade	N/A	N/A	• As afirmações de identidade são protegidas, transmitidas e verificadas	N/A	N/A	• Evidência técnica da proteção, transmissão e verificação das afirmações de identidade
	PR.GA-5	Política de gestão de identidades, autenticação e controlo de acessos	• Gestão de permissões de acesso dos utilizadores aos sistemas em conformidade com a Política de Gestão de Identidades, Autenticação e Controlo	• Implementação de mecanismos de gestão de acessos aos seus sistemas críticos, incluindo a desativação, a monitorização, a comunicação e a	• Monitorização do contexto em que ocorre a autenticação de utilizadores, e identificação dos acessos realizados através de	• Registo documentado da definição e evidência técnica da gestão de acessos dos utilizadores aos sistemas da organização em conformidade com a	• Evidência técnica da implementação de mecanismos para apoiar a gestão do ciclo de vida dos acessos aos sistemas críticos	• Evidência técnica da aplicação de restrições e monitorização ativa do contexto em que ocorre a autenticação de utilizadores

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			de Acessos, sendo que essas permissões são revistas periodicamente • Acessos aos dados, informações e tecnologias críticas, atribuídos de acordo com o princípio do menor privilégio • Garantia de que não são atribuídos privilégios de administração por omissão	eliminação de contas de utilizadores • Aplicação do princípio de segregação de funções na gestão de permissões de acesso • Gestão, documentação e revisão regular das atribuições de privilégios elevados a utilizadores	dispositivos, localizações e horários não habituais • Monitorização das atividades realizadas por utilizadores com privilégios elevados	Política de Gestão de Identidades, Autenticação e Controlo de Acessos • Inclusão na Política de Gestão de Identidades, Autenticação e Controlo de Acessos de critérios que garantam a aplicação do princípio do menor privilégio • Registo documentado dos utilizadores com privilégios de administração atribuídos e respetiva aprovação	• Registo da segregação de perfis de administração de ativos críticos em função da lista de papéis, funções e responsabilidades • Registo documentado da atribuição de privilégios elevados a utilizadores	• Evidência técnica da monitorização das atividades realizadas por utilizadores com privilégios elevados
	PR.GA-6	Controlo de acesso físico	• Definição e proteção das zonas de acesso restrito que alojam informação confidencial, e/ou redes e/ou sistemas de informação	• Monitorização do acesso físico a zonas de acesso restrito • Inclusão de medidas para situações de emergência no acesso físico a zonas de acesso restrito	• Proteção física de ativos alojados nas zonas de acesso restrito	• Evidência da definição das zonas de acesso restrito • Evidência da aplicação de medidas para proteção das zonas de acesso restrito	• Registo da monitorização do acesso físico a zonas de acesso restrito. • Registo da definição de medidas para o acesso físico a zonas de acesso restrito a aplicar em situações de emergência	• Evidência técnica da implementação de proteções físicas aos ativos alojados nas zonas críticas
	PR.GA-7	Acessos remotos	• Definição e documentação da lista de utilizadores e dispositivos com permissão para aceder remotamente às redes e sistemas • Implementação de controlos de segurança adequados para proteger as redes e sistemas	• Definição e implementação das restrições de utilização, dos requisitos de ligação e das autorizações de acesso remoto ao ambiente dos sistemas críticos, de acordo com a Política de Gestão de Identidades,	• Monitorização do acesso remoto aos sistemas críticos • Utilização de canais seguros no acesso remoto e ações de manutenção remota, com recurso a mecanismos de encriptação forte e	• Registo documentado dos utilizadores e dispositivos autorizados a aceder remotamente a redes e sistemas da organização • Evidência técnica da implementação de controlos de segurança para proteção adequada	• Evidência técnica da implementação de medidas de segurança para garantir que os acessos remotos ao ambiente dos sistemas críticos da organização cumprem as restrições de utilização, os	• Evidência técnica da recolha e análise dos registos de atividades dos utilizadores em formato remoto aquando do seu acesso aos sistemas críticos da organização • Evidencia da aprovação interna de mecanismos

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			quando acedidos remotamente	Autenticação e Controlo de Acessos • Monitorização das ações realizadas no âmbito de manutenções remotas, para análise de potenciais eventos que coloquem em causa a segurança dos sistemas • Revogação de acessos atribuídos para manutenções remotas, assim que deixem de ser necessários	protocolos seguros aprovados internamente	de ligações remotas aos sistemas da organização	requisitos de ligação e as autorizações definidas • Evidência técnica da monitorização das manutenções remotas, e dos acessos autorizados, atribuídos, e revogados após a conclusão da manutenção	de encriptação forte e protocolos seguros • Evidência técnica da implementação de canais seguros para acesso remoto (incluindo ações de manutenção)
PR.FC	PR.FC-1	Formação em cibersegurança	• Sensibilização periódica e recorrente do pessoal em matéria de cibersegurança	• Realização de ações de formação periódicas para o pessoal para que melhor compreendam as suas funções, responsabilidades e prioridades específicas durante um incidente de cibersegurança, incluindo quais as ações que devem realizar para responder de forma eficaz • Inclusão, nas ações de formação de cibersegurança, da sensibilização e comunicação de ameaças internas, de forma a ajudar o pessoal	• Definição e implementação de indicadores para avaliar a eficácia das ações de sensibilização e formação • Aplicação dos resultados dos indicadores recolhidos, nos seus processos de melhoria contínua	• Registo documentado da participação do pessoal em ações de sensibilização em matéria de cibersegurança	• Registo documentado da participação periódica do pessoal em ações de formação em matérias de cibersegurança	• Registo da definição dos indicadores para avaliar a eficácia das ações de sensibilização e formação, e recolha dos resultados dos mesmos com a respetiva integração em processos de melhoria continua

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
				a reconhecer e responder a potenciais ameaças internas				
	PR.FC-2	Formação em cibersegurança na gestão de topo	• Formações periódicas em matéria de cibersegurança para os membros dos órgãos de gestão, direção e administração	• Definição, implementação e atualização periódica de plano estruturado de ações de formação em matéria de cibersegurança para colaboradores com funções especializadas em cibersegurança	N/A	• Registo documentado da participação periódica dos membros dos órgãos de gestão, direção e administração em ações de formação em matéria de cibersegurança.	• Registo documentado da definição do Plano de sensibilização e formação para pessoal com funções especializadas em cibersegurança, e da respetiva execução do mesmo	N/A
PR.SD	PR.SD-1	Proteção dos dados armazenados	N/A	• Implementação de controlos de verificação da integridade da informação, do software e firmware para detetar alterações não autorizadas aos dados por si armazenados • Restrição da utilização de suportes de armazenamento amovíveis, em conformidade com a Política de Uso Aceitável	• Proteção das informações dos seus sistemas críticos, consideradas críticas/sensíveis, enquanto estiverem armazenadas, utilizando mecanismos criptográficos	N/A	• Evidência técnica da implementação de controlos de verificação da integridade da informação do software e firmware • Evidência técnica da configuração da restrição da utilização de suportes de armazenamento amovíveis	• Evidência técnica da implementação de controlos de segurança, e de mecanismos criptográficos, para proteção da informação armazenada nos sistemas críticos e que seja considerada crítica/sensível
	PR.SD-2	Proteção dos dados em trânsito	• Implementação de controlos para garantia de confidencialidade e integridade de	N/A	• Implementação de controlos de segurança que garantam a confidencialidade e integridade da informação em trânsito, consoante a sua	• Evidência técnica da implementação de mecanismos criptográficos para os dados em trânsito.	N/A	• Evidência técnica da implementação dos controlos de segurança para proteção dos dados em trânsito, de acordo com a classificação, e em

Versão preliminar

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			transmissão de dados aprovada pela gestão		classificação, para todos os fluxos de dados e interfaces de comunicação para o exterior, de acordo com a Política de Classificação e Gestão de Dados, incluindo quando há recurso a suportes de armazenamento amovíveis. Qualquer exceção à política é devidamente registada			conformidade com a Política de Classificação e Gestão de Dados, inclusive nos fluxos de dados e interfaces de comunicação para o exterior
	PR.SD-3	Proteção contra exfiltração de dados	N/A	N/A	• Adoção de controlos de segurança adequados para monitorizar os sistemas críticos nas fronteiras externas e nos pontos críticos internos, para evitar acessos e atividades não autorizadas, incluindo exfiltração de dados	N/A	N/A	• Evidência técnica da implementação de controlos de segurança adequados para monitorizar os sistemas críticos nas fronteiras externas e nos pontos críticos internos, para evitar acessos e atividades não autorizadas, incluindo exfiltração de dados.
	PR.SD-4	Proteção de dados em utilização	N/A	N/A	• Implementação de controlos de segurança para proteger os sistemas críticos ou limitar o impacto de ataques de negação de serviço	N/A	N/A	• Evidência técnica da implementação de controlos de segurança para proteger os sistemas críticos ou limitar o impacto de ataques de negação de serviço

Versão preliminar

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
	PR.SD-5	Cópias de segurança	• Realização regular de cópias de segurança de dados críticos para garantir a continuidade de negócio • Armazenamento das cópias de segurança num sistema distinto do dispositivo no qual os dados originais estão alojados	• Definição, aprovação e implementação de uma Política de Cópias de Segurança que inclua regras internas formais para a realização das cópias de segurança • A organização verifica e testa regularmente a disponibilidade e integridade das cópias de segurança, de forma independente ao ambiente protegido • Definição e implementação de um esquema de redundância aplicado às cópias de segurança • As cópias de segurança são mantidas em locais distintos e protegidas segundo os mesmos mecanismos de segurança dos dados originais	• O processo de verificação das cópias de segurança é implementado em conformidade com os restantes processos, políticas e planos em matéria de cibersegurança (nomeadamente, o Plano de Continuidade de Negócio e o Plano de Resposta a Incidentes) • Separação das cópias de segurança dos sistemas críticos, nomeadamente, de sistemas operativos, configurações e aplicações, das cópias de segurança de informações críticas	• Evidência técnica da execução regular de cópias de segurança, e armazenamento num sistema distinto do dispositivo no qual os dados originais estão alojados	• Política de Cópias de Segurança aprovada e implementada. • Evidência técnica da verificação e de testes regulares, de acordo com a periodicidade definida na Política de Cópias de Segurança, da integridade das cópias de segurança. • Evidência técnica da implementação de um esquema de redundância das cópias de segurança, e seu armazenamento em local distinto e protegido	• Registo de um processo de verificação das cópias de segurança em conformidade com os restantes procedimentos, planos e políticas da organização • Evidência técnica do armazenamento em locais separados, das cópias de segurança dos sistemas críticos e das informações críticas
PR.SP	PR.SP-1	Configuração base de redes e sistemas de informação	• Manutenção de uma configuração base de redes e sistemas de informação que incorpora os princípios de segurança	• Desenvolvimento, documentação e manutenção atualizada de uma configuração base de segurança das suas redes e sistemas de informação	• Configuração dos sistemas críticos com base no princípio de funcionalidades mínimas e desativação de todos os protocolos, portos e serviços desnecessários (*hardening*)	• Registo da configuração base aplicada nos diferentes sistemas e componentes de rede da organização	• Evidencia técnica das configurações base de segurança das redes e sistemas de informação	• Evidência técnica da aplicação do princípio da funcionalidade mínima e desativação de todos os protocolos, portos e serviços desnecessários, aquando da configuração

Versão

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
					• Implementação de controlos de segurança que sigam os princípios "deny-all" e "permit by exception"			das redes e sistemas da organização • Evidência técnica da implementação de controlos alinhados com os princípios de segurança de "deny-all" e "permit by exception"
	PR.SP-2	Segregação de ambientes	• Recolha, armazenamento, proteção e revisão dos *logs* dos ativos efetuadas regularmente • A definição dos períodos de retenção dos *logs* tem em conta a análise do risco dos sistemas e das atividades bem como o princípio da proporcionalidade	• Os *logs* dos ativos são sincronizados utilizando uma fonte interna de relógio sincronizada com uma fonte de relógio oficial	• Assegurar que as falhas no processamento de *logs* nos seus sistemas geram alertas • A capacidade de retenção e registo de *logs* é revista periodicamente e ampliada sempre que necessário • Gestão de *logs* gerados por sistemas críticos são armazenados em sistema autónomo	• Evidência técnica da recolha, armazenamento e análise regular dos logs dos sistemas da organização • Evidência técnica da diferenciação dos tempos de retenção dos *logs* de acordo com o risco dos sistemas e das atividades	• Evidencia técnica da sincronização temporal dos *logs* dos ativos	• Evidência técnica de alarmística para situações de falha de processamento de *logs* • Evidências de atualização dos tempos de retenção e registo de *logs* • Evidência técnica do armazenamento de logs gerados por sistemas críticos em sistema autónomo
	PR.SP-3	Software não autorizado	• Impedimento da instalação e execução de software não autorizado • Implementação de tecnologias de filtragem de rede, e-mail e web	N/A	N/A	• Evidência técnica de configuração implementada para impedir a instalação e execução de software não autorizado • Evidência técnica da implementação de tecnologias de filtro de rede, e-mail e web	N/A	N/A

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
	PR.SP-4	Ciclo de vida de desenvolvimento de sistemas e aplicações	N/A	• O ciclo de vida de desenvolvimento de sistemas e aplicações incorpora o princípio de segurança por omissão e princípio de segurança desde a conceção • Em caso de alterações e exceções durante o desenvolvimento de software é efetuada uma análise de impacto na segurança, num ambiente de teste separado, antes da implementação em produção	• Integração de práticas de desenvolvimento seguro e a sua monitorização de desempenho ao longo do ciclo de vida do desenvolvimento de software	N/A	• Evidência técnica da aplicação dos princípios de segurança aplicadas ao ciclo de vida de desenvolvimento de sistemas e aplicações • Registos da gestão de alterações aplicável ao desenvolvimento de software	• Registo dos testes de qualidade de software, respetivas conclusões e acompanhamento da devida integração dos critérios de segurança definidos
PR.RI	PR.RI-1	Integridade das redes de comunicações	• Instalação e configuração de firewalls com regras permanentemente atualizadas, em todas as redes • Proteção da integridade da rede dos sistemas críticos através da incorporação da segmentação e segregação da rede • Configuração segura, gestão e monitorização de todos os pontos de acesso a redes sem fio, de forma a prevenir acessos não autorizados	• Identificação, documentação e controlo das ligações entre os componentes do sistema e limitação das ligações externas aos sistemas críticos, para proteger a integridade da rede e dos sistemas críticos • Implementação de dispositivos e tecnologias de proteção para monitorizar e controlar as ligações e comunicações nos limites externos e nos principais limites internos dos sistemas críticos	• Implementação de servidores proxy autenticados para o encaminhamento de tráfego de comunicações entre os sistemas críticos e as redes externas • Implementação de controlos de segurança e de tolerância a falhas em dispositivos e tecnologias de proteção • A organização controla e monitoriza os fluxos de dados dos sistemas críticos	• Evidência técnica da instalação e ativação de *firewalls* em todas as redes da organização • Evidência técnica da segmentação e segregação das redes • Evidência técnica da configuração segura dos pontos de acesso a redes sem fio da organização, da sua gestão e monitorização	• Diagrama de redes da organização com referência à sua segmentação dos sistemas críticos. Demonstração das configurações para bloqueio de ligações não autorizadas aos sistemas críticos • Evidência técnica da monitorização de rede das ligações e comunicações aos sistemas críticos	• Evidência técnica da implementação de servidores proxy para a comunicação entre os sistemas críticos e redes externas • Evidência técnica da implementação de controlos de segurança para a tolerância a falhas dos dispositivos e tecnologias de proteção • Evidência técnica da monitorização dos fluxos de dados dos sistemas críticos

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			e assegurar a integridade da rede					
	PR.RI-2	Segregação de Ambientes	N/A	• Isolamento do(s) ambiente(s) de desenvolvimento e teste do(s) ambiente(s) de produção	N/A	N/A	• Evidência técnica da separação de ambientes de desenvolvimento, teste e de produção.	N/A
	PR.RI-3	Segurança Física	N/A	N/A	• Implementação de dispositivos de deteção de incêndios que se ativam e notificam automaticamente o(s) colaborador(es) indicado(s) em caso de incêndio • Testes periódicos à eficácia dos controlos de segurança aplicados aos ambientes físicos	N/A	N/A	• Evidência técnica da implementação de dispositivos de deteção e notificação automática de incêndios • Evidência técnica da implementação de dispositivos de deteção contra ameaças naturais e registo da realização periódica de testes
	PR.RI-4	Resposta a Disrupções	N/A	• Implementação de controlos adequados de resposta, em tempo útil, a eventuais disrupções às normais operações, em conformidade com o Plano de Continuidade de Negócios estabelecido • Existência de mecanismos que assegurem a disponibilidade dos sistemas críticos, através	N/A	N/A	• Evidência técnica da implementação de controlos adequados que permitam a resposta a disrupções de acordo com o Plano de Continuidade de Negócio. • Evidência técnica da implementação de redundâncias técnicas nos sistemas críticos	N/A

Categoria	Sub Categoria	Contextualização da Medida	Requisitos de implementação incrementais por níveis de garantia:			Evidências incrementais obrigatórias por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
				de soluções de balanceamento de carga e redundâncias dos sistemas				
	PR.RI-5	Planeamento de Capacidade	N/A	• Planeamento e disponibilização da capacidade adequada, para o volume normal, atual e futuro, dos recursos que processam informação dos sistemas críticos, redes, telecomunicações e armazenamento de dados	N/A	N/A	• Registo do planeamento da capacidade dos recursos para o processamento de informações dos sistemas críticos, redes, telecomunicações e armazenamento de dados	N/A

Versão Preliminar

4.1.4. Objetivo: DETETAR

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
DE.MC	DE.MC-1	Monitorização de redes e sistemas	• Instalação, configuração e atualização de soluções de monitorização de tráfego da rede, nomeadamente, através de *firewalls* e proteção contra atividade não autorizada e potencialmente maliciosa	• Monitorização, identificação e bloqueio de comunicações, locais e remotas, não autorizadas às redes e sistemas críticos da organização, removendo conteúdo malicioso	• Monitorização contínua dos sistemas críticos da organização para deteção de eventos e indicadores de potenciais incidentes, acionando, automaticamente, mecanismos de resposta	• Evidência técnica de instalação, configuração e atualização de soluções de monitorização de tráfego da rede e proteção contra atividade não autorizada e potencialmente maliciosa	• Evidência da monitorização, identificação e bloqueio de comunicações não autorizadas e conteúdo/ações malicioso/maliciosas	• Registo de monitorização contínua dos sistemas críticos quanto a potenciais incidentes
	DE.MC-2	Monitorização de ambiente físico	N/A	• Monitorização do ambiente físico para identificar eventos potencialmente adversos	• Monitorização do acesso físico aos sistemas e dispositivos críticos da organização, através do uso de alarmes de intrusão física, equipamento de vigilância e equipas de monitorização independentes	N/A	• Evidência técnica da monitorização do ambiente físico	• Evidência técnica da implementação de alarmes de intrusão física e equipamento de vigilância no acesso físico aos sistemas e dispositivos críticos • Registo de monitorização do acesso físico por equipas independentes
	DE.MC-4	Deteção de código malicioso	• Instalação e atualização continua de ferramentas de monitorização de	N/A	N/A	• Evidência técnica da instalação de ferramentas de monitorização de	N/A	N/A

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
			postos cliente (*endpoints*) por forma a detetar atividade maliciosa			postos cliente, e da sua atualização		
	DE.MC-5	Monitorização de aplicações em dispositivos móveis	• Lista de aplicações aprovadas para uso em ativos corporativos • Documentação e aprovação de todas as exceções à lista de aplicações aprovadas • Inclusão, na Política de Uso Aceitável, de critérios para a utilização de dispositivos pessoais no trabalho (BYOD)	• Inclusão de requisitos para a utilização de dispositivos móveis corporativos na Política de Uso Aceitável. • Monitorização do cumprimento dos requisitos de segurança estabelecidos, fazendo este parte, nomeadamente, do processo de gestão de eventos	• Ferramenta centralizada para a gestão da instalação e suporte de software corporativo • Criação de alarmística relativamente à instalação de software indevido e respetiva integração de alarmística na gestão de incidentes	• Registo das aplicações aprovadas para uso em ativos corporativos • Documentação da aprovação das exceções • Registo da inclusão de critérios para a Utilização de Dispositivos Pessoais no Trabalho (BYOD) na Política de Uso Aceitável.	• Registo documentado de inclusão na Política de Uso Aceitável de requisitos para a utilização de dispositivos móveis corporativos e registo da monitorização do cumprimento destes requisitos	• Evidência técnica da ferramenta centralizada de suporte de software • Evidência técnica de alarmística relativamente à instalação de software indevido e integração deste processo de gestão de incidentes
	DE.MC-6	Monitorização de acessos e ligações	N/A	• Monitorização e implementação de mecanismos de proteção para todas as ligações aos sistemas, aplicações ou infraestrutura da organização, efetuadas por fornecedores ou qualquer entidade externa, por forma a detetar eventos	N/A	N/A	• Registo da monitorização de todas as ligações aos sistemas, aplicações ou infraestrutura da organização, efetuadas por fornecedores ou qualquer entidade externa • Registo da avaliação periódica dos prestadores de serviços com acesso às redes e	N/A

Versão final

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
				potencialmente adversos • Realização de avaliações periódicas de conformidade dos prestadores de serviços para com as políticas e procedimentos da organização e os requisitos de segurança previamente definidos em contratos ou acordos			sistemas da organização por forma a garantir o cumprimento dos requisitos de segurança previamente definidos	
	DE.MC-7	Monitorização por eventos potencialmente adversos	N/A	• Monitorização do hardware, software, ambientes em produção e respetivos dados para deteção de eventos potencialmente adversos	• Execução de verificações da integridade do hardware dos sistemas críticos para a deteção eventuais adulterações • Inclusão da capacidade de deteção de adulterações do hardware dos sistemas críticos no Plano de Resposta a Incidente • Implementação de sistema de deteção e alerta de eventos de segurança para identificação de falsos positivos, com vista a uma melhor deteção e	N/A	• Evidência técnica da recolha de eventos potencialmente adversos	• Evidência técnica da monitorização de integridade de hardware dos sistemas críticos • Registo da inclusão da deteção de adulteração de hardware dos sistemas críticos no Plano de Resposta a Incidentes • Evidência técnica da implementação de sistemas de deteção de falsos positivos na deteção e bloqueio de código e atividades maliciosas

Versão Preliminar

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
					bloqueio de código ou atividades maliciosas			
DE.AE	DE.AE-1	Analise de eventos, de alvos e de métodos de ataque	N/A	• Recolha e analise da informação sobre os eventos detetados com o objetivo de filtrar eventos com impacto potencialmente relevante, identificando as respetivas origens, alvos e métodos de ataque	• Implementação de um sistema automatizado para agregação, correlação e análise dos eventos de segurança detetados	N/A	• Evidência técnica da análise da informação sobre os eventos detetados	• Evidência técnica da implementação de sistemas automatizados para agregação, correlação e análise dos eventos de segurança detetados
	DE.AE-2	Coleta de eventos de várias fontes	• Funcionalidade de recolha de eventos de segurança dos sistemas e aplicações ativa • Análise e preservação da informação recolhida através de cópias de segurança, durante um período previamente definido pela organização	N/A	• Integração das diversas fontes e sensores existentes num sistema automatizado para agregação, correlação e análise de eventos de segurança dos ativos críticos da organização • Integração da informação relativa a rastreamento de vulnerabilidades e estatísticas de performance dos sistemas e aplicações da organização num sistema automatizado para agregação, correlação e análise de eventos de segurança	• Evidência técnica da recolha sistemática de eventos • Evidência técnica da preservação da informação da análise de eventos através de cópias de segurança	N/A	• Registo da integração de toda a informação proveniente das diversas fontes e sensores existentes (incluindo rastreamentos de vulnerabilidades e estatísticas de performance dos sistemas e aplicações) para a agregação, correlação e análise dos eventos de segurança dos ativos críticos da organização

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
	DE.AE-3	Impacto dos eventos detetados e gestão do risco	N/A	N/A	• Inclusão, no processo de gestão dos riscos, dos potenciais impactos dos eventos de segurança detetados no normal funcionamento da organização, nas operações, nos ativos ou nas pessoas	N/A	N/A	• Registo documentado da revisão do processo de gestão dos riscos tendo em conta o impacto dos eventos de segurança detetados
	DE.AE-4	Informações sobre eventos adversos	N/A	• Disponibilização das informações sobre eventos adversos ao pessoal autorizado	N/A	N/A	• Registo da disponibilização da informação sobre eventos adversos ao pessoal autorizado	N/A
	DE.AE-6	Declaração de incidentes	• Definição dos limites que determinam quando um evento, conjunto de eventos ou correlação de múltiplos eventos, configura um incidente	N/A	N/A	• Registo da definição dos limites que determinam quando um evento ou correlação de múltiplos eventos configura um incidente	N/A	N/A

Versão Preliminar

4.1.5. Objetivo: RESPONDER

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
RS.GI	RS.GI-1	Execução do plano de resposta a incidente	• Inclusão, no Plano de Resposta a Incidentes, das funções, as responsabilidades e as competências dos envolvidos • Execução do Plano de Resposta a Incidentes durante ou logo após um incidente	• Coordenação das ações de resposta a incidentes com as partes interessadas definidas no Plano de Resposta a Incidentes	N/A	• Registo da inclusão das funções, responsabilidades e competências dos envolvidos no Plano de Resposta a Incidentes	• Registo documentado do planeamento e atualização dos processos de resposta a incidentes que incluam requisitos para escalonamento	N/A
	RS.GI-2	Triagem de incidentes	N/A	• Triagem e validação das notificações de incidentes de acordo com o Plano de Resposta a Incidentes da organização	N/A	N/A	• Registo da triagem e validação das notificações de incidentes	N/A
	RS.GI-3	Categorização e análise de incidentes	N/A	• Categorização de incidentes de cibersegurança de acordo com o nível de gravidade e impacto, e com os critérios de avaliação incluídos no Plano de Resposta a Incidentes • Definição de uma taxonomia de categorização de incidentes	• Inclusão de procedimentos de resposta para os diferentes tipos de incidente definidos na taxonomia de categorização de incidentes, no Plano de Resposta a Incidentes • Implementação de ferramentas automatizadas para apoio à investigação e à avaliação do impacto	N/A	• Registo da categorização de incidentes e a sua classificação, de acordo com a taxonomia de categorização de incidentes	• Registo documentado da inclusão de procedimentos de resposta a diferentes tipos de incidente, no Plano de Resposta a Incidentes • Evidência técnica da implementação de ferramentas automatizadas de apoio à investigação e

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
					de incidentes previamente validados			avaliação do impacto de incidentes
	RS.GI-5	Inicio da recuperação de incidentes	N/A	• Definição e aplicação de critérios para início da recuperação de incidentes	N/A	N/A	• Registo de critérios e evidência da sua aplicação na fase inicial da recuperação de incidentes	N/A
RS.AI	RS.AI-1	Análises forenses	N/A	N/A	• Realização de análises forenses dos artefactos recolhidos para determinar a causa raiz dos incidentes • Existência de mecanismos *on-demand*, internos ou externos para a realização de análises forenses	N/A	N/A	• Registo documentado da realização de análises forenses
	RS.AI-2	Preservação de registos	N/A	N/A	• Documentação e preservação da integridade e proveniência dos registos das ações realizadas durante uma investigação	N/A	N/A	• Registo documentado das ações realizadas durante a investigação dos incidentes
	RS.AI-3	Preservação de dados e metadados	N/A	N/A	• Os dados e metadados dos incidentes são recolhidos e armazenados e a sua autenticidade, exatidão e rastreabilidade são protegidas	N/A	N/A	• Evidência do armazenamento dos dados e metadados dos incidentes e da implementação de mecanismos que garantam a preservação da integridade e

Versão Draft

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Incrementais Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
								proveniência dos mesmos
	RS.AI-4	Avaliação do impacto do incidente	N/A	N/A	• Inclusão dos resultados da análise de incidentes na avaliação de impacto dos mesmos	N/A	N/A	• Registo da inclusão dos resultados da análise das investigações realizadas, na avaliação de impacto do incidente
RS.NC	RS.NC-1	Partilha informação e notificação de incidentes	• Comunicação interna, clara e simples, da ocorrência de incidentes. • Notificação dos incidentes com impacto significativo à autoridade competente, em conformidade com os termos do Regime Jurídico da Cibersegurança	• Partilha de informação sobre incidentes com as partes interessadas externas relevantes dentro do prazo estabelecido no seu Plano de Resposta a Incidentes	N/A	• Evidência da partilha de informações quanto à ocorrência de incidentes	• Registo da partilha de informações sobre incidentes com as partes interessadas externas relevantes	N/A
RS.MI	RS.MI-1	Conter os incidentes	N/A	• Os incidentes são contidos e resolvidos • Registo e documentação das decisões de não contenção e não resolução de incidentes	N/A	N/A	• Evidência dos processos de contenção de incidentes • Registo de decisões tomadas durante o processo de resposta	N/A
	RS.MI-2	Declaração de resolução	N/A	N/A	• Inclusão, no Plano de Resposta a Incidentes, de critérios que permitam declarar a conclusão da resolução do incidente	N/A	N/A	• Registo da inclusão de critérios para declarar a conclusão da resolução do incidente no Plano de Resposta a Incidentes.

Versão

4.1.6. Objetivo: RECUPERAR

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
RC.PR	RC.PR-1	Plano de recuperação de incidente	• Definição e execução de procedimentos de recuperação de incidentes, em concordância com o Plano de Resposta a Incidentes	N/A	N/A	• Registo das ações tomadas em resposta a incidentes	N/A	N/A
	RC.PR-3	Verificações de integridade	• Verificação de integridade das cópias de segurança antes da sua utilização no âmbito da recuperação pós-incidente	N/A	N/A	• Registo das ações tomadas em resposta a incidentes, que inclua a verificação da integridade das cópias de segurança	N/A	N/A
	RC.PR-5	Confirmação do estado normal de funcionamento	N/A	• A integridade dos ativos restaurados é verificada, os sistemas e serviços são recuperados e o seu estado de normal funcionamento é confirmado	N/A	N/A	• Registo do processo de verificação da integridade dos ativos, recuperação de sistemas e serviços e confirmação do normal estado de funcionamento	N/A
	PR.RC-6	Fim da recuperação dos incidentes	N/A	• Definição e documentação de critérios para declaração do fim da recuperação dos incidentes	N/A	N/A	• Registo da definição de critérios para a declaração do fim da recuperação do incidente e evidência	N/A

Categoria	Sub Categoria	Contextualização da Medida	Medidas de Cibersegurança Incrementais por níveis de garantia:			Critérios de Verificação Obrigatórios por níveis de garantia:		
			Básico	*Substancial*	*Elevado*	*Básico*	*Substancial*	*Elevado*
							da sua implementação	
RC.CO	RC.CO-1	Implementar um plano de comunicação	N/A	• Comunicação, às partes interessadas internas e externas, das atividades de recuperação e os progressos no restauro do normal funcionamento dos sistemas e aplicações da organização	N/A	N/A	• Registo da comunicação das atividades de recuperação e progresso do restauro, às partes interessadas, internas e externas	N/A
	RC.CO-2	Comunicar a recuperação às partes interessadas	N/A	• Definição e aprovação de métodos de comunicação para partilha de atualizações públicas sobre a recuperação de incidentes	• Implementação de uma estratégia de comunicação de crise como mitigação dos impactos negativos durante uma crise	N/A	• Registo dos procedimentos para a comunicação de atualizações públicas sobre a recuperação de incidentes	• Registo documentado da estratégia de comunicação para situações de crise

Versão preliminar

4.2. Outras medidas resultantes do Regime Jurídico da Cibersegurança

A tabela seguinte lista medidas de cibersegurança adicionais resultantes do RJC, e de caráter obrigatório, de que as organizações deverão também evidenciar o seu cumprimento, independentemente do nível de garantia ao qual se candidatam.

Contextualização da Medida	Medidas de Cibersegurança:	Critérios de Verificação Obrigatórios
Obrigações dos órgãos de gestão, direção e administração	• Aprovação e supervisão, pelos órgãos de gestão, direção e administração, das medidas de gestão dos riscos de cibersegurança	• Evidência da aprovação formal das medidas de gestão dos riscos de cibersegurança pelos órgãos de gestão, direção ou administração • Evidência do acompanhamento do estado de implementação das medidas de gestão dos riscos pelos órgãos de gestão, direção ou administração
Sistema de gestão de riscos de cibersegurança	• Adoção de medidas de cibersegurança com base numa abordagem sistémica de gestão do risco que: abranja todos os riscos da organização, protejam os ativos que suportem a continuidade das redes e dos sistemas de informação e que sejam proporcionais ao nível de risco, à dimensão da organização e ao impacto de potenciais incidentes	• Registo documentado das medidas de cibersegurança adotadas para gerir todos os riscos identificados para todos os ativos que suportem a continuidade das redes e dos sistemas de informação da organização
Gestão do risco residual	• Realização, pelo menos uma vez por ano e após a adoção de medidas de cibersegurança, da análise, avaliação, tratamento e monitorização dos riscos residuais, relativamente aos ativos que suportam as redes, os sistemas de informação e os serviços essenciais • Análise dos riscos tendo em consideração, pelo menos: o histórico de situações extraordinárias ocorridas; o histórico de incidentes e, em especial, de incidentes significativos; o número de utilizadores afetados pelos incidentes; a duração dos incidentes; a distribuição geográfica, no que se refere à zona afetada pelos incidentes; as dependências intersetoriais para efeitos da prestação dos serviços, nomeadamente o setor da energia e infraestruturas digitais	• Evidência documentada da análise, avaliação, tratamento e monitorização dos riscos residuais, realizada anualmente ou após a adoção de medidas de cibersegurança • Evidência documentada da inclusão dos critérios específicos na análise do risco

Versão Preliminar

Contextualização da Medida	Medidas de Cibersegurança:	Critérios de Verificação Obrigatórios
Relatório anual	• Elaboração e manutenção de um relatório anual de cibersegurança, contendo informação sobre as atividades desenvolvidas em matéria de cibersegurança, uma estatística trimestral dos incidentes ocorridos (com indicação do número e tipo de incidentes), uma análise agregada dos incidentes com impacto significativo (incluindo informação sobre: o número de utilizadores afetados pela perturbação do serviço, duração do incidente e distribuição geográfica), as medidas implementadas na sequencia dos incidentes e as oportunidades de melhoria da segurança das redes e dos sistemas de informação	• Evidência documentada e assinada pelo Responsável de Cibersegurança da elaboração do relatório anual contendo, pelo menos, os detalhes exigidos
Lista de ativos publicamente acessíveis	• Elaboração e manutenção de uma lista de ativos diretamente acessíveis publicamente através da Internet, com base no inventário de ativos da organização • Inclusão na lista elaborada das seguintes características: serviço suportado pelo ativo, nome do equipamento/nome do software, modelo/versão, endereço IP (se aplicável), FQDN - *Fully Qualified Domain Names* (se aplicável), fabricante e as dependências existentes entre outros ativos (quando existirem)	• Evidência documentada da lista de ativos diretamente acessíveis publicamente através da Internet • Evidência documentada da inclusão explicita dos detalhes/campos mínimos para cada um dos ativos da lista de ativos diretamente acessíveis publicamente através da Internet e respetivo preenchimento
Responsável de cibersegurança	• Designação formal de um Responsável de Cibersegurança que seja titular dos órgãos de gestão, direção ou administração ou que lhes responda organicamente e de forma direta	• Evidência documentada da designação formal do Responsável de Cibersegurança, aprovada pelos órgãos de gestão, direção ou administração
Notificação de incidentes	• Notificação à Autoridade de Cibersegurança dos incidentes com impacto considerado significativo utilizando os canais oficiais para o efeito, nomeadamente, os previstos no Regime Jurídico de Cibersegurança	• Evidência documentada da notificação à Autoridade dos incidentes com impacto considerado significativo

Versão

5. Critérios para a declaração de certificação EC QNRCS – Perfil de Certificação RJC

A aplicação prática das medidas descritas pelas tabelas anteriores permite ao OC tomar uma decisão de certificação baseada na conjunção de vários fatores, nomeadamente:

- O nível de garantia a que a organização se candidata;
- A conformidade de todas as medidas de cibersegurança no presente anexo, aplicáveis ao nível de garantia selecionado, assim como das medidas referidas no capítulo "4.2. Outras medidas resultantes do Regime Jurídico da Cibersegurança", sendo estas últimas aplicáveis independentemente do nível de garantia à qual a organização se candidata;
- A conformidade com os restantes requisitos do EC QNRCS.

6. Classificação da informação

A Lista de Critérios de Auditoria do EC QNRCS – Perfil de Certificação RJC está classificada como **PÚBLICA**.

7. Divulgação e publicação

Tendo em conta a classificação deste documento, é permitida a sua divulgação não controlada através de qualquer meio de divulgação digital, verbal ou em papel.

A sua publicação será realizada em formato digital PDF/A, no portal do CNCS.

8. Revisão e atualização

A Lista de Critérios de Auditoria do EC QNRCS – Perfil de Certificação RJC será revista e atualizada sempre que se entender relevante para a sua correta interpretação e aplicação.

9. Histórico de revisões

Versão	Data	Modificação	Notas adicionais
Versão 1.0	29/09/2026	Versão inicial para revisão	

Versão Preliminar