DIÁRIO DA REPÚBLICA

2.ª série
N.º 118
22-06-2026

PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

Regulamento n.º 756/2026

Sumário: Regulamento de execução do Regime Jurídico da Cibersegurança, aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro.

Regulamento do Regime Jurídico da Cibersegurança

O Decreto-Lei n.º 125/2025, de 4 de dezembro, aprovou o Regime Jurídico da Cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União, sendo aplicável às entidades essenciais, importantes e públicas relevantes, com o enquadramento e delimitações previstas no mesmo regime jurídico.

Em consequência, o mesmo Regime Jurídico da Cibersegurança prevê a necessidade de estabelecer, através de regulamento, os termos da aplicação de algumas das suas disposições, nomeadamente quanto às regras de funcionamento da plataforma eletrónica (n.º 7 do artigo 8.º); às medidas de cibersegurança mínimas e níveis de conformidade determinadas do Quadro Nacional de Referência para a Cibersegurança (n.os 2 e 5 do artigo 14.º); às medidas de cibersegurança mínimas e níveis de conformidade a adotar pelas entidades essenciais e entidades importantes (n.º 5 do artigo 26.º); à gestão do risco residual (n.º 1 do artigo 29.º); à comunicação do relatório anual (n.º 2 e 4 do artigo 30.º); à indicação do responsável de cibersegurança (n.º 3 do artigo 31.º); à indicação da pessoa ou pessoas que compõem a equipa que asseguram as funções de ponto de contacto permanente (n.º 3 do artigo 32.º); à determinação das medidas de cibersegurança que devem ser cumpridas por parte das entidades públicas relevantes (n.º 2 do artigo 33.º); às comunicações entre as entidades com o Centro Nacional de Cibersegurança, ou com as autoridades nacionais setoriais de cibersegurança, incluindo as notificações obrigatórias e voluntárias de informações pertinentes de incidentes (artigos 40.º a 45.º e n.º 2 do artigo 83.º); e às notificações eletrónicas realizadas pelas autoridades de cibersegurança competentes às entidades registadas na plataforma eletrónica (n.º 2 do artigo 72.º).

Considerando as diversas matérias dependentes, na sua aplicação, de regulamento a aprovar pelo Centro Nacional de Cibersegurança (CNCS) optou-se, numa lógica de simplificação regulamentar, por incluí-las num único documento normativo.

Nesses termos, no âmbito das competências que lhe são cometidas e de acordo com os seus poderes e funções como Autoridade Nacional de Cibersegurança, o CNCS procedeu à elaboração do projeto de Regulamento, o qual foi submetido a consulta pública, nos termos do artigo 101.º do Código de Procedimento Administrativo, através do Aviso n.º 5146/2026/2, de 10 de março, publicado no *Diário da República*, 2.ª série, n.º 48 e aprovado pelo seu subdiretor-geral do Gabinete Nacional de Segurança e coordenador do Centro Nacional de Cibersegurança, por despacho de 27 de fevereiro de 2026. O mesmo projeto de Regulamento foi, ainda, sujeito à audição prévia das demais autoridades de cibersegurança competentes.

Findo o prazo de consulta pública, foram recebidas 57 pronúncias. Atento os contributos recebidos e de acordo com a fundamentação estabelecida no relatório da consulta pública, o projeto de Regulamento em consulta pública foi objeto das alterações que se entenderam como oportunas e pertinentes de acordo com as sugestões realizadas. A fundamentação da análise realizada pelo CNCS e das decisões tomadas consta do relatório da consulta pública, que se encontra publicado no sítio institucional do CNCS na Internet. Este relatório contém referência a todos os contributos recebidos, bem como o resultado da apreciação que reflete o entendimento sobre os mesmos e os fundamentos das opções tomadas pelo CNCS. O projeto final de Regulamento, acompanhado da respetiva nota justificativa fundamentada, foi submetido à aprovação do Coordenador do Centro Nacional de Cibersegurança a 16 de junho de 2026.

Assim, por força e em cumprimento do disposto no artigo 3.º e no n.º 4 do artigo 4.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, na redação atual, que aprova a orgânica do Gabinete Nacional de Segurança e nos termos do n.º 7 do artigo 8.º, do n.º 2 do artigo 14.º, da alínea e) do n.º 1 do artigo 20.º, do n.º 5 do artigo 26.º, do n.º 1 do artigo 29.º, do n.º 3 do artigo 31.º, do n.º 3 do artigo 32.º, do n.º 2 do artigo 33.º, do n.º 6 do artigo 40.º e dos artigos 45.º, 72.ºe 83.º do Regime Jurídico da Cibersegurança, aprovado em anexo ao Decreto-Lei n.º 125/2025, de 4 de dezembro, e ao abrigo das competências que me foram delegadas através da alínea a) do n.º 1 do Despacho n.º 8875/2025, de 17 de julho, publicado no *Diário da República*, 2.ª série, n.º 145, aprovo, nos termos e com a fundamentação já referida, o seguinte Regulamento para as matérias nele previstas.

17 de junho de 2026. — O Coordenador do Centro Nacional de Cibersegurança, Lino Santos.

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

1 — O presente Regulamento aprova:

a) As regras de funcionamento da plataforma eletrónica, nomeadamente quanto ao procedimento de auto-identificação e respetiva qualificação das entidades, nos termos do n.º 7 do artigo 8.º do Regime Jurídico da Cibersegurança;

b) As regras das notificações obrigatórias de incidentes de cibersegurança ou notificações voluntárias de informações pertinentes, previstas no n.º 6 do artigo 40.º e no artigo 45.º do Regime Jurídico da Cibersegurança;

c) As regras relativas às comunicações entre entidades e a autoridade de cibersegurança competente, nomeadamente do Relatório Anual, do Responsável de Cibersegurança, do Ponto de Contacto Permanente, nos termos do artigo 83.º do Regime Jurídico da Cibersegurança;

d) O Quadro Nacional de Referência de Cibersegurança (QNRCS) que consta no Anexo I ao presente Regulamento, nos termos do n.º 2 do artigo 14.º do Regime Jurídico da Cibersegurança;

e) As regras para a produção da Matriz de Risco enquanto variável que permite definir os níveis de conformidade e respetivas medidas de cibersegurança mínimas a adotar pelas entidades essenciais e importantes e que consta do Anexo II ao presente Regulamento, nos termos da alínea e) do n.º 1 do artigo 20.º e do n.º 5 do artigo 26.º do Regime Jurídico da Cibersegurança;

f) As regras relativas à gestão dos riscos residuais, nos termos do n.º 1 do artigo 29.º do Regime Jurídico da Cibersegurança;

g) Os níveis de conformidade e respetivas medidas de cibersegurança mínimas, obrigatórias para as entidades essenciais e importantes e os critérios de verificação que as entidades devem considerar, que constam do Anexo III ao presente Regulamento e que advêm do QNRCS, nos termos do n.º 5 do artigo 26.º do Regime Jurídico da Cibersegurança;

h) As regras relativas à comunicação do responsável de cibersegurança e do ponto de contacto permanente, nos termos do n.º 3 do artigo 31.º e do n.º 3 do artigo 32.º do Regime Jurídico da Cibersegurança;

i) As medidas de cibersegurança obrigatórias para as entidades públicas relevantes, consoante a sua qualificação como A ou B, e os critérios de verificação que as entidades devem observar, e que constam do Anexo IV ao presente Regulamento, nos termos do n.º 2 do artigo 33.º do Regime Jurídico da Cibersegurança.

2 — Os anexos ao presente Regulamento, e dos quais constam as matérias previstas nos números anteriores, fazem parte integrante do mesmo com igual valor jurídico.

Artigo 2.º

Âmbito de aplicação

1 — O presente Regulamento aplica-se às entidades essenciais, importantes e públicas relevantes, nos termos e com os limites previstos no Regime Jurídico da Cibersegurança.

2 — O presente Regulamento é aplicado pela autoridade de cibersegurança competente, sendo a mesma entendida nos termos da alínea b) do artigo 2.º do Regime Jurídico da Cibersegurança e na alínea b) do artigo 3.º deste Regulamento.

Artigo 3.º

Definições

Para efeitos do disposto no presente Regulamento e sem prejuízo das definições previstas no artigo 2.º do Regime Jurídico da Cibersegurança, entende-se por:

a) «Regime Jurídico da Cibersegurança», aprovado em anexo ao Decreto-Lei n.º 125/2025, de 4 de dezembro;

b) «Autoridade de cibersegurança competente» — O Centro Nacional de Cibersegurança (CNCS), ou, quando aplicável, a autoridade nacional setorial de cibersegurança competente nos termos da alínea a) do n.º 2 do artigo 15.º do Regime Jurídico da Cibersegurança, sem prejuízo das reservas de competência exclusiva de entidades públicas com responsabilidades em matéria de investigação criminal, de produção de informações e de ciberdefesa;

c) «Níveis de Conformidade» — Sistema de classificação, graduado com os níveis básico, substancial e elevado, do qual resultam as medidas de cibersegurança mínimas que devem ser cumpridas pelas entidades abrangidas pelo Regime Jurídico da Cibersegurança, a partir da matriz de risco aprovada pelo presente Regulamento;

d) «Critérios de Verificação» — Evidências factuais, documentais ou técnicas da aplicação de medidas de cibersegurança, previstas nos anexos III e IV ao presente Regulamento;

e) «Plataforma eletrónica» — A plataforma prevista, entre outros, no n.º 7 do artigo 8.º do Regime Jurídico da Cibersegurança;

f) «Área reservada» — Área digital de acesso reservado disponibilizada na plataforma eletrónica, prevista no n.º 4 do artigo 72.º do Regime Jurídico da Cibersegurança;

g) «Autenticação segura» — Os mecanismos de autenticação digital segura resultantes, nomeadamente, do Cartão de Cidadão, Chave Móvel Digital ou outros que sejam reconhecidos como equivalentes em território nacional;

h) «Registo provisório» — O registo criado em consequência do preenchimento do formulário de autoidentificação e válido até à notificação da qualificação da entidade;

i) «Registo definitivo» — A consolidação do registo provisório quando se confirme que a entidade está inserida no âmbito de aplicação material, subjetivo e territorial do Regime Jurídico da Cibersegurança e é qualificada nos termos dos artigos 6.º e 7.º do mesmo regime.

CAPÍTULO II

Plataforma eletrónica

SECÇÃO I

Registo e Funcionalidade Plataforma

Artigo 4.º

Finalidades e Funcionalidades da plataforma

1 — A plataforma eletrónica prevista no n.º 7 do artigo 8.º do Regime Jurídico da Cibersegurança, desenvolvida e gerida pelo CNCS, visa, através do recurso a meios digitais, simplificar e agilizar os procedimentos de registo das entidades e dos meios de comunicação e notificação entre as entidades abrangidas pelo Regime Jurídico da Cibersegurança com a autoridade de cibersegurança competente.

2 — Têm acesso à plataforma eletrónica, o CNCS, enquanto Autoridade Nacional de Cibersegurança, as demais autoridades de cibersegurança competentes, previstas na alínea a) do n.º 2 do artigo 15.º do Regime Jurídico da Cibersegurança e outras autoridades competentes, para os efeitos previstos no mesmo Regime.

3 — A plataforma eletrónica tem, designadamente, as seguintes funcionalidades:

a) A identificação e registo das entidades, nos termos dos nos n.os 1 e 6 do artigo 8.º do Regime Jurídico da Cibersegurança;

b) A tramitação do procedimento de qualificação de entidades e respetiva notificação, nos termos dos n.os 2 a 5 e 8 do artigo 8.º do Regime Jurídico da Cibersegurança;

c) A comunicação do relatório anual, nos termos dos n.os 2 e 4 do artigo 30.º do Regime Jurídico da Cibersegurança;

d) A comunicação do responsável de cibersegurança e do ponto de contacto permanente, nos termos do n.º 3 do artigo 31.º e dos n.os 2 e 3 do artigo 32.º do Regime Jurídico da Cibersegurança;

e) A notificação de incidentes de cibersegurança e a notificação voluntária de informações pertinentes, nos termos dos n.os 1 e 6 do artigo 40.º e do artigo 45.º do Regime Jurídico da Cibersegurança;

f) A notificação de incidentes de cibersegurança, simultaneamente, à autoridade de cibersegurança competente e às autoridades especiais de cibersegurança, nos termos do n.º 7 do artigo 40.º do Regime Jurídico da Cibersegurança;

g) A divulgação de informação, pela autoridade de cibersegurança competente, sobre a ocorrência de um incidente significativo, nos termos do artigo 51.º do Regime Jurídico da Cibersegurança;

h) As notificações eletrónicas realizadas pelas autoridades de cibersegurança competentes para a prática dos atos da sua competência às entidades registadas, nos termos do n.º 2 do artigo 72.º do Regime Jurídico da Cibersegurança;

i) A concretização de qualquer outra comunicação a que as entidades estejam obrigadas por força do Regime Jurídico da Cibersegurança, nos termos do artigo 83.º do Regime Jurídico da Cibersegurança.

4 — A plataforma eletrónica deve permitir, ainda, a notificação simultânea a outras entidades competentes, nomeadamente em matéria criminal ou de proteção de dados pessoais, em respeito pelos respetivos regimes jurídicos, através de soluções de interoperabilidade, a definir por protocolo entre as entidades em causa, nos termos do n.º 7 do artigo 40.º do Regime Jurídico da Cibersegurança.

5 — A plataforma eletrónica assegura a emissão de recibo de entrega sempre que as entidades submetam ou comuniquem quaisquer elementos, informações ou documentos através da sua conta de entidade, nos termos legalmente aplicáveis.

6 — O CNCS disponibiliza na plataforma eletrónica um instrumento de apoio às entidades de modo a aferirem se estão incluídas no âmbito de aplicação do Regime Jurídico da Cibersegurança e a respetiva qualificação.

7 — Sem prejuízo do número anterior, as informações e orientações previstas na solução automatizada e informativa não constituem autovinculação administrativa, nem dispensam o preenchimento do formulário de autoidentificação quando obrigatório, nos termos do n.º 1 do artigo 8.º do Regime Jurídico da Cibersegurança.

Artigo 5.º

Disponibilização da plataforma eletrónica

1 — A plataforma eletrónica prevista no presente Regulamento respeita os princípios previstos no n.º 2 do artigo 14.º do Código do Procedimento Administrativo, nomeadamente quanto ao controlo e rastreabilidade de acessos, sendo disponibilizada em língua portuguesa e em língua inglesa.

2 — Para os efeitos previstos no número anterior, a plataforma assegura que as entidades acedem à informação sobre as operações realizadas pelos utilizadores associados aos perfis com acesso à conta de entidade, nomeadamente:

a) Operações efetuadas;

b) identificação do utilizador associado a cada operação;

c) data e hora de execução das mesmas.

3 — O CNCS garante a identificação correta e fiável das entidades e respetivos representantes através de mecanismo de autenticação digital segura, nos termos legalmente aplicáveis.

4 — O CNCS mantém e gere a informação em matéria de segurança e integridade na plataforma como sistema de informação seguro, em conformidade com as disposições respeitantes à segurança de informação classificada no âmbito nacional e no âmbito das organizações internacionais de que Portugal é parte.

Artigo 6.º

Identificação e acesso à plataforma eletrónica

1 — A plataforma eletrónica permite a criação de uma conta por entidade e respetiva área reservada, com um registo e dados de acesso únicos.

2 — O CNCS, enquanto entidade gestora da plataforma, define uma política de utilização segura relativa aos mecanismos de registo e atualização dos respetivos dados, garantindo, nomeadamente:

a) O elevado nível de qualidade dos dados de autenticação, nomeadamente alertando os utilizadores para o nível de segurança associado aos métodos de autenticação;

b) Que os dados de autenticação são exigíveis a cada acesso à respetiva conta de utilizador;

c) Que as entidades, enquanto mantiverem o registo ativo na plataforma, podem definir e atualizar os dados e respetivos dados de acesso;

d) Mecanismos de bloqueio ou cessação automática de acessos;

e) A dispensa de informação já disponível na plataforma eletrónica, em cumprimento do princípio da declaração única.

3 — O acesso à plataforma pode ser feito sem registo ou autenticação prévios nos casos legalmente previstos, nomeadamente para acesso a conteúdos, informações, ferramentas de apoio à decisão ou notificações voluntárias de informações pertinentes.

4 — Os requisitos de autenticação segura, para os efeitos do n.º 2 do artigo 12.º do presente Regulamento, são definidos mediante instrução técnica, prevista no n.º 3 do mesmo artigo.

5 — As entidades com registo definitivo na plataforma eletrónica podem permitir o acesso à respetiva conta de entidade, para além do representante legal, ao responsável de cibersegurança ou à pessoa ou pessoas que assegurem as funções de ponto de contacto permanente.

6 — As permissões associadas aos perfis para acessos do representante legal, do responsável de cibersegurança e do ponto de contacto permanente são definidas pelo CNCS, enquanto gestor da plataforma eletrónica.

Artigo 7.º

Mecanismos de autenticação e legitimidade de representação

1 — As entidades autenticam-se na plataforma eletrónica, nomeadamente, através dos respetivos representantes legais, com recurso a sistema de identificação eletrónico com nível de garantia elevado, nos termos do n.º 2 do artigo 84.º do Regime Jurídico da Cibersegurança, nomeadamente, Cartão de Cidadão ou Chave Móvel Digital e com possibilidade de utilização de certificação de determinado atributo profissional, através do Sistema de Certificação de Atributos Profissionais, nos termos da Lei n.º 7/2007, de 5 de fevereiro, e da Lei n.º 37/2014, de 26 de junho.

2 — As entidades, para os efeitos previstos no número anterior, podem fazer-se representar através dos meios legalmente admissíveis, nomeadamente por mandato.

3 — Para os efeitos previstos no número anterior, a plataforma eletrónica assegura, quando necessário, as soluções tecnológicas ou um mecanismo de submissão de documento comprovativo, da constituição de mandato ou atribuição de poderes específicos de representação, devendo o mesmo documento revestir a forma legalmente exigível para o negócio ou ato jurídico correspondente.

4 — A plataforma eletrónica assegura, quando disponível e nos termos legalmente previstos, a reciprocidade de meios de autenticação em uso em território nacional, mas gerados ou emitidos em estado da União Europeia.

5 — O CNCS assegura que a plataforma eletrónica admite os mecanismos autenticação adequados quando a entidade se faça representar por pessoa estrangeira e esta não disponha dos mecanismos de autenticação previstos no presente artigo.

6 — O representante legal, antes de cessar funções, assegura na plataforma a identificação de novo representante legal para a entidade.

7 — Sem prejuízo do número anterior, na impossibilidade de o representante legal proceder à indicação de novo representante legal, a entidade remete, por correio eletrónico para o endereço indicado na plataforma eletrónica, pedido de substituição de representante legal.

Artigo 8.º

Autoidentificação

1 — A autoidentificação das entidades essenciais, importantes e públicas relevantes, com vista à sua qualificação, resulta do preenchimento de formulário(s) eletrónico(s) disponível(eis) na plataforma eletrónica, do(s) qual(is) devem constar os dados estritamente necessários à respetiva qualificação das entidades, nos termos conjugados dos artigos 6.º e 7.º e do n.º 1 do artigo 8.º do Regime Jurídico da Cibersegurança, designadamente:

a) Nome da entidade em causa;

b) Número de identificação fiscal;

c) Se aplicável, o(s) setor(es) e subsetor(es) pertinentes referidos nos anexos I ou II ao Regime Jurídico da Cibersegurança;

d) Tipo de entidade, nos termos e para os efeitos do artigo 3.º e dos anexos I e II ao Regime Jurídico da Cibersegurança;

e) Estabelecimento, nos termos e para os efeitos do artigo 4.º do Regime Jurídico da Cibersegurança;

f) Endereço e dados de contacto atualizados, incluindo os endereços de correio eletrónico; e

g) Se aplicável, uma lista dos Estados-Membros da União Europeia em que prestam serviços abrangidos pelo âmbito de aplicação do Regime Jurídico da Cibersegurança;

h) Número de trabalhadores, nos termos do artigo 2.º do Anexo III ao Regime Jurídico da Cibersegurança;

i) Se aplicável, o volume de negócios anual ou balanço total anual;

j) A adesão ao serviço público de notificações eletrónicas previsto no Decreto-Lei n.º 93/2017, de 1 de agosto, na sua redação atual, quando tenha ocorrido.

2 — Para os efeitos do número anterior, o registo de nomes de domínio de topo, bem como as entidades que sejam prestadores de serviços de DNS, prestadores serviços de registo de nomes de domínio, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados, fornecedores de redes de distribuição de conteúdos, prestadores de serviços geridos, prestadores de serviços de segurança geridos, bem como dos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, asseguram o seu registo na plataforma eletrónica, fornecendo, adicionalmente, os seguintes elementos:

a) O endereço do respetivo estabelecimento principal e dos outros estabelecimentos legais que possui na União Europeia ou, caso não esteja estabelecida na União, do representante designado que tenha estabelecimento no território nacional;

b) Contactos atualizados, incluindo endereços de correio eletrónico;

c) Os Estados-Membros onde presta serviços.

3 — No momento do preenchimento do formulário de autoidentificação é criado um registo provisório por entidade, independentemente do número de setores ou subsetores de atividade, que permite o acompanhamento do procedimento de qualificação.

4 — Para além dos dados requeridos nos números anteriores e quando não consiga obtê-los através dos mecanismos de interoperabilidades previstos no n.º 1 do artigo 87.º do Regime Jurídico da Cibersegurança, a autoridade de cibersegurança competente pode solicitar, por uma única vez, após o preenchimento do formulário, informações ou documentos adicionais para comprovar um determinado dado ou grupo de dados.

5 — A plataforma eletrónica garante a identificação de erros ou falta de preenchimento, que, a existirem, deverão ser corrigidos antes da submissão final do formulário.

6 — Após a submissão, é gerado um recibo comprovativo correspondente à auto-identificação da entidade, acompanhado da data e hora da submissão.

Artigo 9.º

Qualificação de entidades

1 — A decisão de qualificação observa os critérios previstos nos artigos 4.º, 6.º, 7.º e 9.º, bem como os trâmites e formalidades previstos nos n.ºs 4 e 5 do artigo 8.º, todos do Regime Jurídico da Cibersegurança, quando aplicáveis.

2 — Após a auto-identificação prevista no artigo anterior, as entidades são notificadas pela autoridade de cibersegurança competente, na plataforma eletrónica e por correio eletrónico, para se pronunciarem quanto ao projeto de decisão de qualificação, no prazo de 10 dias úteis, nos termos do artigo 121.º e seguintes do Código do Procedimento Administrativo para audiência dos interessados.

3 — A audiência dos interessados deve ser realizada na plataforma eletrónica, através de campo disponibilizado para o efeito.

4 — Decorrido o prazo para a audiência dos interessados sem que haja pronúncia das entidades ou após a sua apreciação pela autoridade de cibersegurança competente, é proferida decisão final de qualificação, a notificar às entidades através da plataforma eletrónica.

5 — A notificação final de qualificação contém, ainda, quando aplicável, a indicação do nível de conformidade e as respetivas medidas de cibersegurança obrigatórias aplicáveis à entidade notificada.

6 — O disposto no número anterior não obsta que a autoridade de cibersegurança competente notifique a entidade que procedeu à respetiva autoidentificação de que está fora do âmbito de aplicação ou do não preenchimento dos requisitos de qualificação previstos no n.º 7 do artigo 3.º e nos artigos 4.º, 6.º e 7.º do Regime Jurídico da Cibersegurança.

7 — Nos casos em que a entidade que se autoidentificou esteja fora do âmbito de aplicação do Regime Jurídico da Cibersegurança, é extinto o registo provisório previsto no n.º 3 do artigo 8.º do presente Regulamento, no prazo máximo de 90 dias, sem prejuízo da conservação, por outros meios e pelo tempo que se afigure necessário para o efeito, do formulário de autoidentificação e da respetiva notificação de exclusão, pela autoridade de cibersegurança competente.

8 — Sem prejuízo do número anterior, mediante decisão do CNCS e após pedido fundamentado da entidade, podem ser conservados os registos de entidades que estejam fora do âmbito de aplicação do Regime Jurídico da Cibersegurança para efeitos de acesso a informações, funcionalidades ou comunicações disponibilizadas pela plataforma eletrónica.

9 — O parecer das autoridades nacionais setoriais de cibersegurança a que se refere o n.º 4 do artigo 8.º do Regime Jurídico da Cibersegurança é submetido na plataforma eletrónica pelas referidas autoridades, competindo ao CNCS disponibilizar os mecanismos de acesso para o efeito.

10 — As entidades podem reagir à decisão final de qualificação nos termos gerais de Direito e através da plataforma eletrónica, nomeadamente através dos meios impugnatórios e prazos previstos no Código do Procedimento Administrativo.

11 — A qualificação das entidades pode ser alterada ou atualizada a qualquer momento, por decisão da autoridade de cibersegurança competente, com fundamento na alteração das circunstâncias ou das características das entidades, nos termos dos critérios previstos nos artigos 6.º e 7.º do Regime Jurídico da Cibersegurança.

12 — A alteração ou atualização da qualificação prevista no número anterior é notificada nos termos definidos no presente Regulamento, quando a entidade esteja registada na plataforma eletrónica ou, na sua ausência, por via postal.

Artigo 10.º

Registo definitivo na plataforma

1 — Após a notificação da qualificação das entidades, nos termos dos artigos anteriores, o registo provisório na plataforma eletrónica é consolidado em definitivo, podendo a autoridade de cibersegurança competente notificar as entidades para a prestação das informações ou dados que não constem do formulário de autoidentificação e que sejam obrigatórios nos termos do artigo 35.º do Regime Jurídico da Cibersegurança.

2 — As entidades financeiras abrangidas simultaneamente pelo Regime Jurídico da Cibersegurança, pelo Regulamento (UE) 2022/2554 e pela Lei n.º 73/2025, de 23 de dezembro, após o seu registo e qualificação nos termos dos artigos anteriores, realizam as comunicações e notificações respeitantes à resiliência operacional digital do setor financeiro, incluindo as relativas a incidentes severos relacionados com TIC e a ciberameaças significativas, às autoridades competentes designadas nos termos da legislação especial aplicável.

3 — As entidades financeiras devem assegurar as obrigações previstas no Regime Jurídico da Cibersegurança e nos termos do presente Regulamento, em matéria de designação do Responsável de Cibersegurança, ponto de contacto permanente e notificação de incidentes, sem prejuízo dos mecanismos de cooperação, interoperabilidade e partilha de informação das autoridades especiais de cibersegurança com o CNCS legalmente previstos.

Artigo 11.º

Atualização permanente da informação

Os dados e informações submetidos na plataforma eletrónica são da responsabilidade da respetiva entidade, devendo esta mantê-los permanentemente atualizados.

SECÇÃO II

Comunicações com as autoridades de cibersegurança

Artigo 12.º

Comunicações com as autoridades de cibersegurança

1 — As entidades essenciais, importantes e públicas relevantes efetuam, através da plataforma eletrónica, todas as comunicações previstas no Regime Jurídico da Cibersegurança, no presente Regulamento ou nos seus anexos, e dirigidas à autoridade de cibersegurança competente, nos termos do n.º 7 do artigo 8.º e do n.º 1 do artigo 83.º do mesmo Regime Jurídico, salvo previsão legal ou regulamentar em sentido contrário.

2 — As comunicações referidas no número anterior podem ser asseguradas por mecanismos automatizados de transmissão de informação, nomeadamente por recurso a interfaces de programação de aplicações (API — application programming interface).

3 — O CNCS disponibiliza, para os efeitos previstos no número anterior, instrução técnica de configuração e utilização de cada um dos interfaces de programação de aplicações.

4 — A plataforma eletrónica assegura que as autoridades nacionais setoriais têm acesso exclusivamente às informações que devam conhecer ou aceder, nos termos do Regime Jurídico da Cibersegurança.

5 — O disposto no n.º 1 do presente artigo aplica-se, igualmente, às comunicações e notificações em matéria de taxas de supervisão, nos termos constantes da portaria prevista no artigo 82.º do Regime Jurídico da Cibersegurança.

Artigo 13.º

Comunicação de documentos

1 — As entidades essenciais comunicam à autoridade de cibersegurança competente, anualmente e através da sua área reservada na plataforma eletrónica, o relatório anual, com os elementos e nos prazos previstos nos n.os 1 e 2 do artigo 30.º do Regime Jurídico da Cibersegurança.

2 — As entidades importantes, sempre que lhes seja solicitado, remetem o seu relatório anual ao CNCS, na sua área reservada na plataforma eletrónica, nos termos previstos nos n.os 1 e 4 do artigo 30.º do Regime Jurídico da Cibersegurança.

3 — O CNCS, ouvidas as autoridades nacionais setoriais de cibersegurança, disponibilizará, na plataforma eletrónica e acessíveis às entidades essenciais e importantes, modelos de utilização obrigatória para a apresentação do relatório anual nos termos do disposto no n.º 5 do artigo 30.º do Regime Jurídico da Cibersegurança.

4 — Quando resultar das medidas de cibersegurança mínimas ou do exercício dos poderes de supervisão nos termos das alíneas f) e g) do n.º 1 do artigo 54.º e das alíneas f) e g) do n.º 2 do artigo 55.º do Regime Jurídico da Cibersegurança, a obrigatoriedade de elaborar e comunicar à autoridade de cibersegurança competente, determinadas informações ou documentos, os mesmos são remetidos através da plataforma eletrónica, nos prazos estabelecidos para o efeito.

Artigo 14.º

Responsável de cibersegurança

1 — As entidades essenciais e importantes comunicam à autoridade de cibersegurança competente, através de formulário disponível na sua área reservada da plataforma eletrónica, a pessoa designada para as funções de responsável de cibersegurança, nos termos e com os prazos previstos nos n.os 3 a 7 do artigo 31.º do Regime Jurídico da Cibersegurança.

2 — Sem prejuízo do disposto no número anterior, nos casos previstos no n.º 4 do artigo 31.º do Regime Jurídico da Cibersegurança, o prazo conta-se a partir da notificação da qualificação da entidade, nos termos do n.º 5 do artigo 8.º do mesmo regime.

3 — A comunicação prevista no n.º 1 contém, nomeadamente, as seguintes informações:

a) Nome do responsável de cibersegurança;

b) Cargo do responsável de cibersegurança;

c) Endereço de correio eletrónico;

d) Número de telefone fixo, se aplicável;

e) Número de telefone móvel;

f) Despacho ou ato de designação do responsável de cibersegurança, se aplicável.

Artigo 15.º

Ponto de contacto permanente

1 — As entidades essenciais e importantes comunicam à autoridade de cibersegurança competente, através de formulário disponível na área reservada da plataforma eletrónica, o ponto de contacto permanente, nos termos e com os prazos previstos nos n.os 2 a 6 do artigo 32.º do Regime Jurídico da Cibersegurança.

2 — Sem prejuízo do disposto no número anterior, nos casos previstos no n.º 4 do artigo 32.º do Regime Jurídico da Cibersegurança, o prazo conta-se a partir da notificação da qualificação da entidade, nos termos do n.º 5 do artigo 8.º do mesmo regime.

3 — A comunicação prevista no n.º 1 contém, nomeadamente, as seguintes informações:

a) Identificação da equipa ou entidade terceira que assume(m) a função de ponto de contacto permanente;

b) Endereço de correio eletrónico principal;

c) Endereço de correio eletrónico alternativo;

d) Número de telefone fixo principal, se aplicável;

e) Número de telefone móvel principal;

f) Número de telefone fixo alternativo, se aplicável;

g) Número de telefone móvel alternativo;

h) Outros contactos alternativos.

Artigo 16.º

Tratamento, conservação e atualização dos dados e respetiva destruição

1 — A autoridade de cibersegurança competente assegura que o tratamento de dados, através da plataforma eletrónica, respeita as regras em matéria de segurança da informação e, quando pessoais, a legislação aplicável em matéria de proteção de dados pessoais, nomeadamente o Regulamento (UE) n.º 679/2016, do Parlamento e do Conselho, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

2 — Para os efeitos previstos no número anterior, a autoridade de cibersegurança competente define e publica no sítio da internet da plataforma eletrónica, uma política de tratamento de dados, sem prejuízo das demais obrigações que lhe sejam atribuídas enquanto responsável pelo tratamento de dados.

3 — Os dados submetidos pelas entidades e registados na plataforma eletrónica serão conservados durante toda a vigência do registo associado às entidades e pelo período de cinco anos após a extinção do mesmo registo, sem prejuízo do disposto nos n.os 2 e 3 do artigo 21.º da Lei n.º 58/2019, de 8 de agosto.

Artigo 17.º

Situações de indisponibilidade técnica

1 — Nos casos em que ocorra uma indisponibilidade técnica da plataforma eletrónica e as entidades não possam aguardar pela disponibilidade da mesma para prática de determinados atos ou submissão de informações, poderão remeter as mesmas para o correio eletrónico da autoridade de cibersegurança competente ou contacto telefónico, disponíveis no sítio da Internet da mesma, nos termos do n.º 3 do artigo 83.º do Regime Jurídico da Cibersegurança.

2 — Caso as entidades pretendam enviar a informação protegida por método criptográfico, podem proteger a informação utilizando a chave pública de PGP, associada ao endereço de correio eletrónico referido no número anterior, identificada nos contactos dos sítios na Internet do CNCS e da plataforma eletrónica.

3 — Os atos praticados ou a informação submetida pelo endereço de correio eletrónico, nos termos dos números anteriores, considera-se validamente submetida no momento de receção da comunicação, devendo a autoridade de cibersegurança competente assegurar resposta automática de confirmação da mesma, bem como a sua integração na área reservada da plataforma quando disponível.

4 — Nas circunstâncias excecionais de justo impedimento motivadas por indisponibilidade generalizada de infraestruturas ou plataformas digitais nacionais, nomeadamente por ausência de energia elétrica ou serviço de telecomunicações, as entidades podem praticar os atos, enviar os documentos ou informações assim que restabelecido o regular funcionamento dos serviços afetados.

5 — A plataforma eletrónica assegura informação atempada sobre indisponibilidades de acesso planeadas por motivos técnicos.

Artigo 18.º

Mecanismos de interoperabilidade e acesso a informação

A plataforma eletrónica assegura, quando disponíveis, os mecanismos de interoperabilidade adequados ao tratamento dos dados relevantes para a sua atividade, nomeadamente com outras plataformas ou bases de dados, nos termos do artigo 87.º do Regime Jurídico da Cibersegurança.

SECÇÃO III

Notificações eletrónicas

Artigo 19.º

Notificações eletrónicas às entidades

1 — A autoridade de cibersegurança competente notifica eletronicamente as entidades essenciais, importantes e públicas relevantes, dos atos, decisões ou solicitações que pratique no âmbito das suas competências, nos termos do artigo 72.º do Regime Jurídico da Cibersegurança.

2 — As notificações previstas no número anterior são realizadas para a área reservada das entidades na plataforma eletrónica, gerando uma notificação automática para o endereço de correio eletrónico registado na mesma plataforma e, quando expressamente indicado pelas entidades, para o endereço de correio eletrónico do responsável de cibersegurança.

3 — As notificações eletrónicas devem conter, quando aplicável, os elementos previstos no n.º 2 do artigo 114.º do Código do Procedimento Administrativo, bem como assinatura digital ou certificado eletrónico que assegure a respetiva autenticidade do documento a notificar.

4 — As notificações eletrónicas consideram-se feitas na data da consulta eletrónica da área reservada ou, se esta não ocorrer, no termo do terceiro dia a contar da receção, nos termos do n.º 4 do artigo 72.º do Regime Jurídico da Cibersegurança.

5 — O disposto nos números anteriores não se aplica à citação e à decisão final emitidas em processos contraordenacionais a instaurar ou em curso, que são realizadas por via postal nos termos de Direito aplicável, sem prejuízo da notificação eletrónica dos atos instrutórios no âmbito dos mesmos processos.

6 — A plataforma eletrónica assegura, ainda, a notificação eletrónica às entidades através do serviço público de notificações eletrónicas (SPNE), quando disponível e sempre que se verifique o destinatário a ele tenha aderido, nos termos do Decreto-Lei n.º 93/2017, de 1 de agosto, na redação atual.

7 — Para os efeitos previstos no número anterior, as entidades essenciais, importantes ou públicas relevantes devem indicar, no momento do registo, se aderiram ao SPNE e, em caso afirmativo, se pretendem ser notificadas através do mesmo.

CAPÍTULO III

Notificação de incidentes

Artigo 20.º

Notificação obrigatória de incidentes

1 — As entidades essenciais, importantes e públicas relevantes, quando ocorra um incidente com impacto significativo, submetem à autoridade de cibersegurança competente, através de formulário disponível na área reservada da plataforma eletrónica:

a) Uma notificação inicial, nos termos e com a informação prevista no artigo 42.º do Regime Jurídico da Cibersegurança;

b) Uma notificação de fim do impacto significativo, nos termos e com a informação prevista no artigo 43.º do Regime Jurídico da Cibersegurança;

c) Um relatório final ou intercalar, nos termos e com a informação prevista no artigo 44.º do Regime Jurídico da Cibersegurança;

2 — Sem prejuízo do número anterior, as entidades podem, ainda, submeter, sem necessidade de autenticação na plataforma eletrónica, notificações voluntárias de informações pertinentes nos termos do artigo seguinte.

3 — O impacto de um incidente é definido como significativo:

a) Nos termos do Regulamento de Execução (UE) n.º 2024/2690, de 17 de outubro, para as entidades pertinentes aí previstas;

b) Nos termos gerais previstos na alínea l) do artigo 2.º do Regime Jurídico da Cibersegurança, densificados por via de instrução técnica a aprovar pela Autoridade Nacional de Cibersegurança, para as restantes entidades integradas no âmbito subjetivo do Regime Jurídico da Cibersegurança.

4 — Quando as entidades não consigam proceder às notificações de incidentes, por falta temporária de capacidade operacional própria, em resultado do incidente ou por outro motivo de natureza eminentemente técnica devidamente justificado, a notificação pode ser efetuada, a título excecional, através de correio eletrónico ou telefonicamente, estando os devidos meios de contacto disponibilizados no sítio de internet da autoridade de cibersegurança competente. Nos casos em que a plataforma eletrónica esteja indisponível aquando do envio da notificação, aplicam-se os procedimentos previstos no artigo 17.º do presente Regulamento.

Artigo 21.º

Notificação voluntária de informações pertinentes

1 — Qualquer pessoa singular ou coletiva pode submeter à autoridade de cibersegurança competente e através da plataforma eletrónica, notificações voluntárias de ocorrência de incidentes, ciberameaças, quase incidentes ou vulnerabilidades, nos termos do n.º 1 do artigo 45.º do Regime Jurídico da Cibersegurança.

2 — Para os efeitos previstos no n.º 3 do artigo 45.º do Regime Jurídico da Cibersegurança, a entidade ou pessoa notificante deve, sempre que tenha conhecimento ou acesso à informação, disponibilizar os elementos previstos no n.º 2 do artigo 42.º, no n.º 2 do artigo 43.º e nos n.os 2 e 4 do artigo 44.º do mesmo Regime Jurídico da Cibersegurança.

3 — A autoridade de cibersegurança competente, pode, sempre que necessário, solicitar informações ou elementos adicionais relativamente ao incidente em questão.

4 — A notificação voluntária de informações pertinentes não carece de autenticação ou registo da pessoa singular ou coletiva na plataforma eletrónica.

Artigo 22.º

Tramitação de notificações obrigatórias de incidentes

1 — A plataforma eletrónica assegura a consulta e extração, permanente e atualizada de informação, quando disponível, sobre o estado ou conteúdo das notificações obrigatórias realizadas pelas entidades, sempre que as mesmas tenham sido feitas nas respetivas áreas reservadas, nos termos legalmente previstos.

2 — A plataforma eletrónica assegura, ainda, a possibilidade de associar as diferentes notificações previstas nas alíneas do n.º 1 do artigo 20.º do presente Regulamento, sempre que relacionadas com um mesmo incidente.

3 — A plataforma eletrónica disponibiliza um mecanismo de emissão automatizada de alertas às entidades relativos ao decurso dos prazos previstos nos artigos 42.º a 44.º do Regime Jurídico da Cibersegurança, sempre que tais prazos sejam contabilizáveis pela Autoridade de Cibersegurança Competente.

4 — A ausência ou impossibilidade de emissão automatizada de alertas não dispensa o cumprimento atempado pelas entidades das obrigações previstas no Regime Jurídico da Cibersegurança.

CAPÍTULO IV

Instrumentos Estruturantes

SECÇÃO I

Quadro Nacional de Referência de Cibersegurança

Artigo 23.º

QNRCS

1 — O QNRCS, aprovado no presente Regulamento e constante do Anexo I, é o instrumento nacional de referência para a identificação das normas, padrões e boas práticas existentes em matéria de gestão da Cibersegurança e da Segurança Informação, nos termos do artigo 14.º do Regime Jurídico da Cibersegurança.

2 — O QNRCS é construído e atualizado atendendo aos princípios da prossecução do interesse público, da legalidade, da eficiência, da eficácia e da proporcionalidade, devendo minimizar, sempre que possível, o seu impacto nas atividades públicas, sociais e empresariais das entidades.

3 — As entidades devem considerar o QNRCS visando uma perspetiva de melhoria contínua e evolutiva.

4 — Compete ao CNCS atualizar, pelo menos, de cinco em cinco anos, o QNRCS, nos termos do n.º 2 do artigo 14.º do Regime Jurídico da Cibersegurança.

Artigo 24.º

Âmbito de aplicação subjetivo

1 — As entidades essenciais, importantes e públicas relevantes devem considerar o QNRCS, nos termos dos n.os 3 e 5 do artigo 14.º do Regime Jurídico da Cibersegurança e de acordo com as disposições do presente Regulamento.

2 — Sem prejuízo do número anterior, a autoridade de cibersegurança competente pode recomendar a utilização do QNRCS às entidades que se encontram fora do âmbito de aplicação do Regime Jurídico da Cibersegurança.

3 — As autoridades nacionais setoriais de cibersegurança referidas na alínea a) do n.º 2 do artigo 15.º do Regime Jurídico da Cibersegurança podem ainda adotar normas complementares ao QNRCS, através de regulamento próprio, em articulação com o CNCS, nos termos do n.º 4 do artigo 14.º do referido regime.

Artigo 25.º

Organização e estrutura do QNRCS

1 — O QNRCS é estruturado em função do ciclo de vida da gestão da cibersegurança a realizar pelas entidades, tendo em consideração o fator humano, tecnológico e processual, com especial foco nos processos e procedimentos da gestão dos riscos.

2 — O QNRCS tem a seguinte estrutura, sem prejuízo da sua atualização:

a) Objetivos de cibersegurança;

b) Categorias;

c) Controlos de cibersegurança.

Artigo 26.º

Aplicação conjunta

A aplicação facultativa do QNRCS pelas entidades essenciais e importantes deve ser conjugada com as medidas de cibersegurança mínimas e respetivos níveis de conformidade previstos no anexo III do presente Regulamento.

Artigo 27.º

Certificação voluntária

1 — Nos termos do n.º 3 do artigo 34.º do Regime Jurídico da Cibersegurança, as entidades essenciais e importantes podem beneficiar da presunção de cumprimento das medidas de cibersegurança previstas nos artigos 26.º a 28.º do mesmo regime jurídico e no artigo 30.º do presente Regulamento, quando apresentem à autoridade de cibersegurança competente um certificado emitido por um organismo de certificação devidamente acreditado, nos termos do n.º 3.

2 — Nos termos do n.º 3 do artigo 34.º do Regime Jurídico da Cibersegurança, as entidades públicas relevantes podem beneficiar da presunção de cumprimento das medidas de cibersegurança previstas no artigo 33.º do Regime Jurídico da Cibersegurança e no artigo 30.º do presente Regulamento, quando apresentem à autoridade de cibersegurança competente um certificado emitido por um organismo de certificação devidamente acreditado, nos termos do número seguinte.

3 — A autoridade de cibersegurança competente, e como referido nos números anteriores, pode atestar o cumprimento das medidas de cibersegurança correspondentes ao nível de conformidade ou superior, exigido às entidades certificadas, tal como previsto nos artigos 26.º e 33.º do Regime Jurídico da Cibersegurança, através da certificação em referenciais de cibersegurança na sua versão atualizada, nomeadamente:

a) Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança (EC QNRCS);

b) ISO/IEC 27001, quando o âmbito da certificação abrange integralmente os sistemas de informação e redes associadas aos serviços prestados pela entidade no âmbito do Regime Jurídico da Cibersegurança; c) Para as entidades públicas relevantes, o Documento Normativo Português Especificação Técnica (DNP TS) 4577-1, Maturidade Digital — Selo Digital;

c) Outro esquema devidamente aprovado ou reconhecido pela Autoridade Nacional de Certificação de Cibersegurança.

4 — Os certificados válidos referidos nos n.ºs 1 e 2 do presente artigo são submetidos voluntariamente pelas entidades à autoridade de cibersegurança competente ou sempre que solicitado, através da plataforma eletrónica prevista no presente Regulamento.

5 — O certificado previsto no número anterior, quando relativo ao referencial ISO/IEC 27001 contém a correspondente declaração de aplicabilidade.

6 — Qualquer alteração do certificado, nomeadamente a sua revogação, suspensão, renovação ou alteração de âmbito deve ser comunicada à autoridade de cibersegurança competente, através da plataforma eletrónica prevista no presente Regulamento, no prazo máximo de 72 horas para a revogação, e de 10 dias úteis para a suspensão, renovação ou alteração de âmbito todos os prazos a contar da respetiva alteração.

7 — O CNCS, enquanto autoridade nacional de certificação em cibersegurança, aprova e publica através de instrução técnica, uma matriz de equivalência entre os esquemas de certificação previstos no presente artigo e as medidas de cibersegurança mínimas constantes dos anexos III e IV.

SECÇÃO II

Matriz de Risco

Artigo 28.º

Matriz de Risco

1 — A matriz de risco, aprovada no presente Regulamento e constante do Anexo II, é o quadro referencial que estabelece os valores de risco para o conjunto de cenários de risco que recaem sobre um setor e subsetor de atividade, considerando os ativos comuns, as principais ameaças e vulnerabilidades, nos termos do disposto na alínea m) do artigo 2.º, no n.os 5 do artigo 26.º e no n.º 3 do artigo 53.º do Regime Jurídico da Cibersegurança.

2 — Considerando o setor de atividade, a dimensão da entidade e a matriz de risco definida são determinados os níveis de conformidade e as medidas de cibersegurança mínimas e específicas a adotar que constam do anexo III.

3 — Os valores de risco referidos no n.º 1 são determinados com base no nível de risco associado ao setor ou subsetor a que as entidades pertencem tendo em conta a sua dimensão e com a importância do setor ou subsetor, podendo ser atribuído um de três níveis de conformidade:

a) Básico;

b) Substancial;

c) Elevado.

4 — Os critérios para a produção da matriz de risco são construídos e atualizados atendendo aos princípios da prossecução do interesse público, da legalidade, da eficiência, da eficácia e da proporcionalidade, devendo minimizar, sempre que possível, o seu impacto nas atividades públicas, sociais e empresariais das entidades.

5 — O CNCS disponibiliza na plataforma eletrónica um glossário de apoio à leitura da Matriz de Risco.

Artigo 29.º

Cenários de Risco

O CNCS emite anualmente, através de instrução técnica, nos termos do n.º 4 do artigo 26.º do Regime Jurídico da Cibersegurança, as orientações relevantes de forma a orientar a política de gestão de riscos da cibersegurança das entidades essenciais e importantes, nomeadamente:

a) Cenários de risco;

b) Vetores de ameaça;

c) Informações quanto aos ativos.

SECÇÃO III

Medidas de Cibersegurança Mínimas e de Execução

Artigo 30.º

Medidas de Cibersegurança Mínimas

1 — As entidades essenciais, importantes e públicas relevantes aplicam, pelo menos, as medidas de cibersegurança mínimas, aprovadas no presente Regulamento e constante dos anexos III e IV, nos termos dos n.os 5 e 6 do artigo 26.º, artigo 27.º e artigo 33.º do Regime Jurídico da Cibersegurança.

2 — As entidades essenciais e importantes sujeitas aos níveis de conformidade substancial e elevado asseguram, ainda, a aplicação das medidas de cibersegurança mínimas dos níveis de conformidade respetivamente inferiores.

3 — As entidades públicas relevantes sujeitas às medidas de cibersegurança previstas para o Grupo A, nos termos definidos no Anexo IV do presente Regulamento, asseguram, igualmente, a aplicação das medidas de cibersegurança mínimas definidas para o Grupo B do mesmo anexo.

4 — Caso as entidades essenciais ou importantes se encontrem em mais do que um nível de conformidade, aplica-se o nível de conformidade que se revelar mais exigente para gerir os riscos que se colocam à segurança das redes e sistemas de informação de acordo com a seguinte ordem descendente:

a) Elevado;

b) Substancial;

c) Básico.

5 — O CNCS pode exigir às entidades essenciais, importantes e públicas relevantes, a obtenção de certificação, nacional, europeia ou internacional, que ateste o cumprimento das medidas de cibersegurança aplicáveis, nos termos do n.º 1 do artigo 34.º do Regime Jurídico da Cibersegurança.

6 — A decisão prevista no número anterior é fundamentada, nomeadamente em função do risco ou essencialidade do serviço ou da entidade, é sujeita a audiência dos interessados nos termos do Código do Procedimento Administrativo e define o prazo de adaptação das entidades, não superior a 24 meses.

7 — Nos termos do n.º 3 do artigo 20.º do Regime Jurídico da Cibersegurança, as autoridades nacionais setoriais ou especiais de cibersegurança podem emitir disposições regulamentares, precedidas de parecer do CNCS, para a adoção de medidas de cibersegurança do setor.

8 — A autoridade de cibersegurança competente pode ainda recomendar, sem caráter vinculativo, a adoção de medidas mínimas de cibersegurança às entidades que se encontram fora do âmbito de aplicação do Regime Jurídico da Cibersegurança.

Artigo 31.º

Gestão do Risco

1 — As entidades essenciais e importantes, procedem, nos termos do n.º 1 do artigo 29.º do Regime Jurídico da Cibersegurança, à análise e gestão periódicas dos riscos e dos riscos residuais, relativos aos ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam, incluindo os ativos que garantam a prestação dos serviços essenciais.

2 — As entidades essenciais e importantes realizam a análise dos riscos com a seguinte periodicidade:

a) Pelo menos uma vez por ano;

b) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que implique uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS.

3 — A análise dos riscos pelas entidades essenciais e importantes deve ter em consideração:

a) O histórico de situações extraordinárias ocorridas;

b) O histórico de incidentes e, em especial, de incidentes com impacto relevante;

c) O número de utilizadores afetados pelos incidentes;

d) A duração dos incidentes;

e) A distribuição geográfica, no que se refere à zona afetada pelos incidentes;

f) As dependências intersetoriais para efeitos da prestação dos serviços;

g) Os elementos constantes da instrução técnica referida no artigo 29.º do presente Regulamento.

4 — As entidades essenciais e importantes realizam ainda a análise do risco residual, após a adoção de medidas de cibersegurança, nos termos do disposto nos n.os 1 e 2 do artigo 29.º do Regime Jurídico da Cibersegurança.

Artigo 32.º

Lista de ativos publicamente acessíveis

1 — Para efeitos de comunicação das gamas de endereços de IP prevista na alínea c) do n.º 1 e alínea d) do n.º 2 do artigo 35.º do Regime Jurídico da Cibersegurança, as entidades essenciais, importantes e públicas relevantes, devem elaborar, manter atualizado e comunicar à autoridade de cibersegurança competente, através da plataforma eletrónica, uma lista de todos os ativos, com base no seu inventário de ativos, que estejam diretamente acessíveis publicamente através da Internet.

a) A lista de ativos acima referida, que constitui informação classificada de grau reservado deve incluir a seguinte informação: Serviço suportado;

b) Nome do equipamento/Nome do *software*;

c) Modelo/Versão;

d) Sistema operativo;

e) *Software* do servidor aplicacional;

f) Endereço IP, se aplicável;

g) Fully Qualified Domain Names (FQDNs), se aplicável;

h) Fabricante;

i) As dependências dos ativos, diretamente acessíveis de forma pública através da Internet, com outros ativos (diretamente acessíveis de forma pública através da Internet ou não), quando existentes.

2 — Para os efeitos da alínea i) do número anterior, existe dependência entre ativos quando a indisponibilidade de um ativo compromete sequencialmente a continuidade da atividade ou utilização de outro ativo.

3 — As entidades devem comunicar à autoridade de cibersegurança competente a lista dos ativos, com a seguinte periodicidade:

a) Na sua versão inicial, até 31 de janeiro do ano seguinte ao ano em que ocorra a notificação prevista no n.º 5 do artigo 8.º Regime Jurídico da Cibersegurança ou no prazo de seis meses após a mesma notificação consoante o que se vença primeiro;

b) Numa versão atualizada, anualmente, a ser entregue simultaneamente com o relatório anual a que se refere o n.º 2 do artigo 30.º do Regime Jurídico da Cibersegurança, quando sejam entidades essenciais;

c) Numa versão atualizada, anualmente, e até ao último dia útil do mês de janeiro, do ano civil seguinte ao qual a mesma se reporta, quando sejam entidades importantes e públicas relevantes.

4 — O CNCS publica uma instrução técnica de apoio à identificação dos ativos essenciais para a prestação dos respetivos serviços e referidos no n.º 1 do presente artigo.

Artigo 33.º

Medidas de Execução

1 — As medidas de execução previstas nos artigos 56.º e 57.º do Regime Jurídico da Cibersegurança são adotadas pela autoridade de cibersegurança competente, atendendo aos princípios da prossecução do interesse público, da legalidade, da eficiência, da eficácia e da proporcionalidade, devendo minimizar, sempre que possível, o seu impacto nas atividades públicas, sociais e empresariais das entidades supervisionadas, nos termos do n.º 2 do artigo 53.º do mesmo RJC.

2 — As medidas de bloqueio e redirecionamento previstas no artigo 57.º do RJC são adotadas pela autoridade de cibersegurança competente apenas em circunstâncias manifestamente excecionais, designadamente para fazer face a uma ciberameaça significativa ou durante ou na sequência da ocorrência de um incidente de impacto significativo e quando a adoção de outras medidas menos gravosas não seja adequadamente eficaz.

3 — As medidas de execução adotadas pela autoridade de cibersegurança competente são especialmente fundamentadas pelo CNCS e notificadas às entidades que as devam conhecer e aplicar, pelo meio disponível mais expedito, podendo recorrer-se à área reservada da plataforma eletrónica.

4 — A autoridade de cibersegurança competente tem em consideração, na fundamentação prevista no número anterior, os elementos ou informações fornecidas pelas entidades responsáveis pela implementação das medidas de bloqueio ou redirecionamento, bem como propostas de medidas alternativas.

CAPÍTULO V

Disposições Finais

Artigo 34.º

Entrada em vigor

O presente Regulamento entra em vigor no dia seguinte após a sua publicação.

Artigo 35.º

Produção de efeitos

1 — O presente Regulamento produz efeitos na data da sua entrada em vigor, sem prejuízo do disposto no n.º 2 do artigo 10.º do Decreto-Lei n.º 125/2025, de 4 de dezembro.

2 — As disposições do presente Regulamento que careçam de instruções técnicas ou outros normativos a aprovar pela autoridade de cibersegurança competente, produzem efeitos à data da publicação dos mesmos.

3 — Sem prejuízo do número anterior, as entidades devem enviar à autoridade de cibersegurança competente a informação que seja determinada ou determinável com base nos critérios ou requisitos já existentes na legislação ou regulamentação em vigor.

ANEXO I

QNRCS

Sumário Executivo

O Quadro Nacional de Referência para a Cibersegurança 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.

A segunda versão do Quadro Nacional de Referência para a Cibersegurança, doravante designado QNRCS, encontra-se alinhada com o novo Regime Jurídico da Cibersegurança (RJC) mais concretamente o Decreto-Lei n.º 125/2025, de 4 de dezembro, que transpõe a Diretiva da União Europeia (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 (Diretiva SRI 2) relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. O QNRCS, identificado no RJC como um instrumento estruturante da segurança do ciberespaço, tem como missão providenciar às entidades um referencial que sistematiza e disponibiliza bases para um conjunto de controlos e medidas de cibersegurança.

Este referencial é composto por um conjunto de controlos de cibersegurança que as entidades podem adotar para incrementar a sua ciber-resiliência, com base em normas internacionais comummente utilizadas (NIST Cybersecurity Framework (CSF) 2.0; CyberFundamentals Framework; ISO/IEC 27001:2022; ISO/IEC 27002:2022; CIS Critical Security Controls Version 8.1 e NIST Special Publication 800-53 Rev.5).

O QNRCS é constituído por controlos e medidas de cibersegurança das redes e sistemas de informação, nas suas diversas componentes, que visam cumprir seis objetivos: Gerir, Identificar, Proteger, Detetar, Responder e Recuperar.

A versão atualizada do QNRCS, procura refletir uma nova realidade e ambiente de cibersegurança que está em constante mudança. Nesse sentido, o documento incorpora novos referenciais, cumpre com as orientações e medidas definidas no novo RJC e descreve controlos e medidas de cibersegurança que pretendem refletir uma realidade complexa e heterogénea.

Esta versão do QNRCS incorpora novos controlos de acordo com o RJC e normativos internacionais, sendo também reflexo de uma análise dos incidentes mais relevantes em Portugal nos últimos anos. Esta versão pretende igualmente simplificar as orientações e exemplos para a aplicação das medidas de cibersegurança pelas entidades.

Na sequência da evolução do QNRCS, foi acrescentado um novo objetivo (Gerir) à sua estrutura com o propósito de incluir controlos e medidas que reflitam as condições transversais que as entidades podem implementar para garantir o cumprimento dos restantes objetivos. Assim, este novo objetivo integra categorias relacionadas com o contexto organizacional, a gestão dos riscos da entidade e da sua cadeia de abastecimento, as funções, responsabilidades e autoridades nesta matéria, políticas e atividades de supervisão. Esta alteração decorre dos referenciais nos quais o QNRCS se suporta, e das boas práticas, mais concretamente, de uma evolução por parte da *Cybersecurity Framework do National Institute of Standards and Technology (NIST*).

De notar, que esta versão do QNRCS pretende continuar a ser implementada por toda a comunidade, contribuindo assim para um desenvolvimento económico sustentável.

Finalmente, nos termos do disposto do n.º 2 do artigo 14.º do Decreto-Lei n.º 125/2025 o QNRCS será atualizado, pelo menos, de cinco em cinco anos.

1 — Enquadramento:

1.1 — O QNRCS:

O QNRCS pretende ser um referencial que guia as entidades para uma maior ciberresiliência, perante um ambiente complexo e heterogéneo, que oferece novas possibilidades e oportunidades, enquanto potencia e cria espaço para a ocorrência de incidentes.

As infraestruturas operam baseadas na premissa de que os elementos tecnológicos são robustos e fiáveis e que tecnologias emergentes e complexas (e.g., *Internet of Things* (*IoT*), Tecnologia Quântica, Inteligência Artificial (IA) têm o potencial para oferecer uma elevada flexibilidade e eficiência na comunicação e coordenação de serviços e processos. Porém, o uso de tecnologias de informação também significa que estas se tornam mais vulneráveis a atividades ilícitas e maliciosas e a processos de manutenção operacionais inadequados.

Neste contexto, a implementação exclusiva de controlos de segurança tecnológicos e processuais não é suficiente para reduzir o risco de exploração de vulnerabilidades, uma vez que o fator humano assume um papel central na cibersegurança e deve também ser integrado na estratégia de cibersegurança da entidade.

Deste modo, uma gestão adequada dos riscos de cibersegurança pelas entidades possibilita a melhoria e manutenção da qualidade dos seus serviços prestados, na adoção de novas práticas, no desenvolvimento de novos produtos ou serviços e num menor custo operacional decorrente do impacto dos ciberataques.

A versão atualizada do QNRCS complementa o Decreto-Lei n.º 125/2025, de 4 de dezembro que transpõe a Diretiva SRI2, aprovada pela UE e Estados-Membros. Esta Diretiva tem em consideração a crescente digitalização das entidades e sociedade, e pretende responder ao facto de que "o número, a amplitude, a sofisticação, a frequência e o impacto dos incidentes estão a aumentar e constituem uma grave ameaça ao funcionamento dos sistemas de rede e informação" (Considerando 3, Diretiva 2022/2555, do Parlamento Europeu e Conselho).

Assim, o QNRCS constitui-se como uma ferramenta de referência à disposição da sociedade para apoio sistemático, alinhado com o RJC. O QNRCS consubstancia-se numa visão homogénea e inclusiva da realidade organizacional (pública e privada) portuguesa, guiando as entidades para a implementação de controlos de cibersegurança. As entidades podem aplicar o documento de forma adaptada ao seu contexto, para melhor endereçar necessidades específicas inerentes ao seu setor, dimensão ou qualquer outro aspeto distintivo que caracterize a entidade.

A estrutura central do QNRCS foi definida numa perspetiva de ciclo de vida da gestão da cibersegurança de uma entidade, considerando os aspetos humanos, tecnológicos e processuais, com especial foco nos processos e procedimentos da gestão dos riscos.

Uma característica intrínseca do risco é o facto de este não poder ser totalmente eliminado, tornando-se fundamental a concretização, pelas entidades, de uma estratégia global para garantir a implementação de um processo eficaz de gestão dos riscos. Este é um processo contínuo de identificação, análise, avaliação e tratamento, sendo que, para que seja possível gerir os riscos, as entidades devem compreender a probabilidade de um determinado evento ocorrer, bem como os potenciais impactos adversos e vulnerabilidades existentes. A aplicação do QNRCS poderá ser complementada por guias, ferramentas e orientações que venham a ser emitidas pelo Centro Nacional de Cibersegurança.

1.2 — Âmbito e Aplicabilidade:

O QNRCS é aplicável a todas as entidades públicas e privadas, sejam elas abrangidas pelo Regime Jurídico da Cibersegurança ou não, que utilizem redes e sistemas de informação.

O QNRCS pode ser utilizado em complemento com processos já existentes nas entidades, permitindo a identificação de lacunas na estratégia organizacional de cibersegurança e promovendo a definição de um caminho de melhoria contínua.

A estrutura central do QNRCS sistematiza um universo essencial de controlos de cibersegurança que as entidades podem utilizar para comparar com os controlos de cibersegurança já implementados.

1.3 — Estrutura QNRCS:

As categorias, controlos e medidas de cibersegurança descritos no QNRCS, atendem, mas não exclusivamente, aos seguintes princípios:

1) Considerar todos os aspetos característicos de um ecossistema de cibersegurança nas entidades nacionais, independentemente da sua dimensão, natureza (pública ou privada), criticidade ou orientação tecnológica;

2) Abranger transversalmente todos os setores de atividade;

3) Atender às características do tecido social e económico do país;

4) Permitir e promover que determinadas entidades possam definir o respetivo contexto de aplicação do QNRCS para o seu setor de atividade/regulação.

A estrutura central do QNRCS é constituída por:

1) Objetivos de cibersegurança;

2) Categorias;

3) Controlos de cibersegurança;

Cada um dos seis objetivos subdivide-se em categorias, que agrupam propósitos e atividades particulares. Por sua vez, as categorias dividem-se em um ou mais controlos de cibersegurança, os quais se baseiam em referenciais reconhecidos a nível nacional e internacional, na legislação europeia e nacional.

Cada controlo de cibersegurança contém descrições que pretendem sistematizar o objetivo do controlo, definindo objetivos para a aplicação dos mesmos pelas entidades. Os controlos de cibersegurança visam suportar as entidades no processo de sistematização da sua estratégia de gestão dos riscos de cibersegurança, e fomentam a melhoria contínua, recorrendo a lições aprendidas no âmbito de atividades realizadas.

De notar que a utilização do QNRCS deve ser conduzida numa perspetiva de melhoria contínua e não deve ser efetuada uma utilização estática das práticas identificadas no QNRCS, permitindo uma evolução de acordo com a maturidade da entidade e o seu contexto.

2 — Definições, Abreviaturas e Contexto Referencial:

2.1 — Definições:

Na tabela seguinte, identificam-se os termos utilizados ao longo do documento, cuja definição importa apresentar. Sempre que aplicável, são usados termos definidos em normas ou legislação nacional em vigor. Na coluna "Fonte" é indicada a norma ou legislação onde o termo se encontra definido.

Termo	Definição	Fonte
Aceitação do risco	Decisão informada de assumir determinado risco.	ISO 22300:2025
Ameaça	Potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou entidade.	ISO/IEC 27032:2023
Ativo	Todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.	DL 125/2025
Ativo Crítico	Ativo que suporta pelo menos um serviço considerado crítico.	QNRCS
Ciberameaça	Uma circunstância, um evento ou uma ação potencial suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas.	Regulamento Europeu 2019/881
Cibersegurança	Todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas.	Regulamento Europeu 2019/881
Confidencialidade	A propriedade de a informação não ser acedida por pessoas ou entidades não autorizadas, ou segundo processos não autorizados.	ISO/IEC 27000:2018
Continuidade do negócio	Capacidade da entidade para continuar a fornecer produtos ou serviços a níveis aceitáveis pré-definidos, na sequência de um incidente disruptivo.	ISO 22301:2019

Termo	Definição	Fonte
Disponibilidade	Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada.	ISO/IEC 27000:2018
Entidade	Uma pessoa coletiva criada e reconhecida como tal pelo direito nacional do seu local de estabelecimento, que, atuando em seu próprio nome, pode exercer direitos e estar sujeita a obrigações.	DL 125/2025
Exercício	Processo para formar, avaliar, praticar e melhorar o desempenho de uma entidade.	ISO 22301:2019
Fornecedor	Entidade ou pessoa que fornece um produto/serviço, (sendo o produto, entendido como resultado de um processo).	NP EN ISO 9000:2015
Gestão dos riscos	Atividades coordenadas para gerir uma entidade, no que respeita ao risco.	ISO/IEC 27000:2018
Incidente	Um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por redes e sistemas de informação ou acessíveis por intermédio destas.	DL 125/2025
Integridade	A propriedade de salvaguardar o caráter exato e completo da informação e dos ativos.	ISO/IEC 27000:2018
Internet	Sistema global de redes interconectadas e de domínio público.	ISO/IEC 27032:2023
Medidas de Cibersegurança	Medidas de âmbito técnico, operacional e organizacional, visando gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações ou na prestação dos seus serviços, bem como impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços.	DL 125/2025
Melhoria contínua	Atividade recorrente para aperfeiçoar o desempenho.	ISO 22300:2025
Norma	Uma especificação técnica, aprovada por um organismo de normalização reconhecido para aplicação repetida ou continuada, cuja observância não é obrigatória.	Regulamento 1025/2012
Parte Interessada	Pessoa ou entidade que pode afetar, ser afetada por, ou considerar-se como sendo afetada por uma decisão ou atividade. Pode ser um indivíduo ou um grupo que tem um interesse em qualquer decisão ou atividade de uma entidade.	ISO 22301:2019
Plano de continuidade do negócio	Informação documentada que orienta as entidades a responder, recuperar, retomar e restaurar um nível pré-definido de operacionalização, após disrupção.	ISO 22301:2019
Política	Intenções e orientação de uma entidade, conforme formalmente expressas pelos seus órgãos de gestão, direção e administração.	ISO 22300:2025
Processo	Conjunto de atividades interrelacionadas que transformam entradas em saídas.	ISO 22300:2025
Procedimento	Modo especificado de realizar uma atividade ou um processo.	ISO 22300:2025
Registo	Documento que expressa resultados obtidos ou fornece evidência das atividades realizadas.	ISO 9000:2015
Risco	Medida da possibilidade de uma perda ou perturbação causada por um incidente, resultante da combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente.	DL 125/2025
Risco residual	Medida de risco existente após adoção das medidas cibersegurança mínimas.	DL 125/2025

Termo	Definição	Fonte
Segurança das redes e dos sistemas de informação	A capacidade dos sistemas de rede e informação para resistir, com um dado nível de confiança, a eventos suscetíveis de pôr em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos por esses sistemas de rede e informação, ou acessíveis por intermédio destes.	DL 125/2025
Sistema crítico	Conjunto de ativos críticos que suportam os serviços críticos.	QNRCS
Sistema de gestão	Conjunto de elementos interrelacionados de uma entidade para o estabelecimento de políticas, objetivos e de processos para atingir esses objetivos.	ISO 22301:2019
Tolerância ao risco	Disposição da entidade ou das partes interessadas para assumirem o risco após o seu o tratamento, por forma a poderem alcançar os seus objetivos.	ISO 22300:2025
Tratamento de incidentes	Todas as ações e procedimentos que visam a prevenção, a deteção, a análise, a contenção ou a resposta a um incidente e a recuperação de um incidente.	DL 125/2025
Vulnerabilidade	Uma fragilidade, suscetibilidade ou falha, que afeta redes e sistemas de informação, produtos ou serviços de tecnologias da informação ou comunicação (TIC), passível de ser explorada por uma ciberameaça.	DL 125/2025

4.2 — Abreviaturas:

Abreviatura	Definição
CIS	*Center for Internet Security* — Centro de segurança para a Internet.
CSC	*Critical Security Controls* — Controlos críticos de segurança.
CERT	*Computer Emergency Response Team* — Equipa de Resposta a Emergências Informáticas.
CSIRT	*Computer Security Incident Response Team* — Equipa de Resposta a Incidentes de Segurança Informática.
DNS	*Domain Name System* — Sistema de resolução de nomes de domínio.
HTTP	*Hypertext Transfer Protocol* — Protocolo de Transferência de Hipertexto
IA	Inteligência Artificial.
IoT	*Internet of Things* — Internet das coisas.
IP	*Internet Protocol* — Protocolo de Internet comunicações.
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commission* — Entidade internacional de normalização/Comissão eletrotécnica internacional.
MFA	*Multi factor authentication*- Autenticação Multi-fator.
NIST	*National Institute of Standards and Technology* — Instituto Nacional de Padrões e Tecnologia (Norte-americano).
RGPD	Regulamento Geral de Proteção de Dados.
SGSI	Sistema de Gestão de Segurança da Informação.
SLA	*Service Level Agreement* — Acordo de Nível de Serviço.
SOC	Security Operations Center — Centro de Operações de Segurança.
SRI	Segurança das Redes e da Informação.
VPN	*Virtual Private Network* — Rede privada virtual.

Abreviatura	Definição
TIC	Tecnologias de Informação e Comunicação.
TO	Tecnologia Operacional.

4.3 — Contexto Referencial:

O QNRCS é suportado, quanto às práticas e controlos sugeridos, principalmente por seis referenciais. Estes referenciais abordam o tema da cibersegurança de forma complementar, sendo internacionalmente aceites como base para a implementação e avaliação de controlos de tratamento do risco e de boas práticas de governação, e cibersegurança.

1 — NIST Cybersecurity Framework — CSF 2.0:

Publicado pela NIST, o NIST CSF 2.0 foi desenhado para permitir que entidades, de todas as dimensões e setores possam gerir os seus riscos de cibersegurança. O documento inclui uma estrutura baseado em funções, categorias e subcategorias que incluem resultados a seguir pelas entidades.

2 — Cyber Fundamentals Framework (CyFun) 2025:

O CyFun desenvolvido pelo Centro de Cibersegurança Belga, reúne um conjunto de medidas para proteger informações e dados das entidades, reduzir os riscos mais comuns de ciberataques e aumentar a ciber-resiliência das entidades. O *Framework* divide-se nas categorias Basic,Important and Essential, dispondo de medidas para os diferentes níveis.

3 — ISO/IEC 27001:2022:

A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um sistema de gestão de segurança da informação, bem como os requisitos para os controlos de segurança a serem implementados, de acordo com as necessidades e realidade da entidade.

4 — ISO/IEC 27002:2022:

A norma ISO/IEC 27002 contém um conjunto de referência a controlos de segurança da informação e guias de implementação a ser utilizado pelas entidades no contexto de SGSI baseado no ISO/ESC 27001, para implementação de controlos de segurança de informação basados em boas práticas internacionalmente reconhecidas e para o desenvolvimento de guias de gestão específicos para cada entidade.

5 — CIS Critical Security Controls Version 8.1:

O CSC é publicado pelo CIS. Este catálogo disponibiliza uma lista de ações que é regularmente revista pela comunidade académica, de forma a ser utilizável pelas entidades.

6 — NIST Special Publication 800-53 Rev.5:

Publicado pela NIST93 este é um catálogo de controlos para gestão dos riscos de cibersegurança e riscos de outra natureza, disponibilizando um processo de seleção de controlos para proteção da operação e dos ativos das organizações, gestão de incidentes, desastres naturais, falhas estruturais ou erro humano.

5 — Quadro Resumo de Objetivos e Categorias

De seguida, apresenta-se o quadro resumo que reúne os seis objetivos e respetivas categorias, seguido de capítulos específicos para cada objetivo com a descrição em detalhe dos controlos de cibersegurança correspondentes.

OBJETIVO	CATEGORIA
Gerir	Contexto Organizacional (GR.CO)
	Estratégia de Gestão de Risco (GR.GR)
	Funções, Responsabilidades e Autoridades (GR.FR)
	Políticas e Planos de Cibersegurança (GR.PP)
	Supervisão (GR.SP)
	Gestão do Risco da Cadeia de Abastecimento (GR.CA)
Identificar	Gestão de Ativos (ID.GA)
	Avaliação do Risco (ID.AR)
	Melhoria Contínua (ID.MC)
Proteger	Gestão de Identidades, Autenticação e Controlo de Acessos (PR.GA)
	Formação e Sensibilização (PR.FC)
	Segurança de Dados (PR.SD)
	Segurança de Plataformas (PR.SP)
	Resiliência da Infraestrutura Tecnológica (PR.RI)

OBJETIVO	CATEGORIA
Detetar	Monitorização Contínua (DE.MC)
	Anomalias e Eventos (DE.AE)
Responder	Gestão de Incidentes (RS.GI)
	Análise de Incidentes (RS.AI)
	Notificação e Comunicação de Incidentes (RS.NC)
	Mitigação de Incidentes (RS.MI)
Recuperar	Execução do Plano de Recuperação (RC.PR)
	Comunicação de Recuperação (RC.CO)

4 — Gerir:

O objetivo Gerir integra controlos que refletem as condições transversais que as entidades podem implementar para garantir o cumprimento dos restantes objetivos. Este inclui categorias relacionadas com o contexto organizacional, a gestão dos riscos da entidade e da sua cadeia de abastecimento, as funções, responsabilidades e autoridades nesta matéria, políticas e atividades de supervisão.

4.1 — GR.CO — Contexto Organizacional:

A entidade define, compreende e prioriza a sua missão e objetivos, identifica as suas partes interessadas e respetivas atividades/serviços. Esta informação é utilizada para identificar os papéis e responsabilidades no contexto da cibersegurança e para a tomada de decisões no âmbito da gestão de riscos.

GR.CO-1 — A missão, visão, estratégia de gestão dos riscos e objetivos da entidade são definidos e comunicados.

Descrição

A missão, visão, valores, estratégias de gestão dos riscos e objetivos são os princípios fundamentais de orientação de uma entidade. Estes princípios indicam a forma como a entidade se posiciona no seu setor de atividade e como procura ser reconhecida pelo pessoal, clientes, fornecedores e outras entidades terceiras.

Referências

ISO/IEC 27001:2022 — 5.1,5.2 6.1, 6.2,7.4

ISO/IEC 27002:2022 — 5.1

NIST SP-800-53 Rev.5 — SR -1

NIST CSF 2.0- GV. OC-01

CyFun 2025-GV.OC-01

GR.CO-2 — As necessidades e expectativas das partes interessadas internas e externas são compreendidas e encontram-se refletidas na gestão dos riscos de cibersegurança da entidade.

Descrição

A entidade identifica as partes interessadas internas e externas relevantes e ausculta as suas necessidades e expectativas no contexto de cibersegurança, refletindo-as na sua estratégia de gestão dos riscos de cibersegurança.

Referências

NIST CSF 2.0-GV.OC-02

CyFun 2025-GV.OC-02

GR.CO-3 — Os requisitos legais, regulamentares e contratuais para a cibersegurança, são compreendidos e geridos.

Descrição

A entidade garante que cumpre com a legislação e regulamentação de cibersegurança nacional e europeia em vigor. Para esse efeito, a entidade define quais são os requisitos legais, regulamentares e contratuais nacionais e europeus que necessitam de ser observados e seguidos.

Referências

ISO/IEC 27001:2022 — 4.1, 4.2, 7.2

ISO/IEC 27002:2022 — 5.5,5.31, 5.32, 5.33, 5.34, 5.35

NIST SP-800-53 Rev.5 — SR-1

NIST CSF 2.0- GV.CO-03

CIS CSC v8.1-17

CyFun 2025-GV.OC-03

GR.CO-4 — Os serviços críticos da entidade dos quais as partes interessadas externas dependem são identificados e comunicados.

Descrição

A entidade identifica os seus serviços críticos, dos quais as partes interessadas externas dependem, e utiliza esta informação, integrando-a e gerindo-a no seu processo de gestão dos riscos. Ao integrar a informação na gestão dos riscos, a entidade classifica e prioriza os serviços críticos identificados. A entidade comunica esta identificação às partes interessadas externas.

Referências

ISO/IEC 27001:2022 — 6.1.2,7.1,7.5.2,8.1,8.2

ISO/IEC 27002:2022 — 5.5,7.11,7.12,8.6

NIST CSF 2.0- GV.OC-05

CyFun 2025-GV.OC-04

GR.CO-5 — Os requisitos de resiliência necessários para suportar a prestação de serviços críticos são definidos.

Descrição

A entidade identifica e define quais são os requisitos de resiliência adequados para suportar a prestação dos seus serviços críticos. A entidade define e implementa um Plano de Continuidade de Negócio que contém disposições quanto a redundâncias, planos e tempos de resposta para a recuperação dos serviços críticos e respetivos processos. De maneira a garantir que o Plano de Continuidade de Negócio responde às necessidades a entidade realiza testes ao mesmo.

Referências

ISO/IEC 27001:2022 — 6.2,7.5.2,8.1

ISO/IEC 27002:2022 — 5.5,5.29, 7.5, 7.11, 8.14

NIST CSF 2.0-GV.OC-05

CyFun 2025 — GV.OC-04

GR.CO-6 — Os serviços externos dos quais a entidade depende, são identificados e comunicados.
Descrição

A entidade identifica as dependências externas que, em caso de falha, podem afetar as suas operações e serviços críticos, e partilha esta informação com as partes interessadas. A entidade identifica qual o seu papel na cadeia de abastecimento.

Referências

ISO/IEC 27001:2022 — 7.5.2

ISO/IEC 27002:2022 — 5.19,5.20,5.21

NIST CSF 2.0-GV.OC-05

CyFun 2025 — GV.OC-05

4.2 — GR.GR — Estratégia de Gestão do Risco:

A entidade estabelece as prioridades, restrições e níveis de tolerância ao risco adequados para suportar a tomada de decisão no âmbito da gestão dos riscos de cibersegurança.

GR.GR-1 — O apetite e a tolerância ao risco da entidade são definidos, aprovados, comunicados e revistos regularmente.

Descrição

A entidade define, aprova, comunica e atualiza o nível de risco que está disposta a aceitar por forma a permitir aferir as expectativas sobre o seu nível de risco tolerável. O apetite ao risco considera o contexto organizacional e o setor no qual a entidade se insere.

Referências

ISO/IEC 27001:2022 — 5.1, 6.1.1, 6.1.3, 8.3, 9.3.2, 9.3.3

NIST CSF 2.0 — GV.RM-02

CyFun 2025 — GV.RM-02

GR.GR-2 — Os processos de gestão dos riscos de cibersegurança estão incluídos na estratégia transversal de gestão dos riscos da entidade.

Descrição

A entidade garante que os seus processos da gestão dos riscos se encontram devidamente definidos, aprovados e geridos. É assegurado que os processos de gestão dos riscos de cibersegurança são consistentes e transversais à entidade, e à sua estratégia de gestão do risco. Isto é, os processos de gestão dos riscos de cibersegurança são tidos em conta na gestão dos restantes riscos da entidade, e são devidamente acompanhados pelos órgãos de gestão, administração e direção, tal como os restantes riscos.

Referências

ISO/IEC 27001:2022 — 6.1.1., 7.5.2, 9.3.2

ISO/IEC 27002:2022 — 5.8,8.6

NIST CSF 2.0 — GV.RM-03, GV.RM-07

CyFun 2025-GV.RM-03

GR.GR-3 — A entidade define a sua estratégia de tratamento do risco.

Descrição

A entidade define a resposta de tratamento do risco a aplica-a aos seus ativos, tendo em conta a sua tolerância ao risco.

Referências

NIST CSF 2.0 — GV.RM-04

CyFun 2025 — GV.RM-04

GR.GR-4 — A entidade estabelece um canal de comunicação interno para partilha de riscos de cibersegurança.

Descrição

A entidade determina e usa regularmente um canal interno a utilizar para comunicar os riscos de cibersegurança aos órgãos de gestão, direção e administração e às restantes áreas relevantes da entidade.

Referências

NIST CSF 2.0 — GV.RM-05

CyFun 2025 — GV.RM-05

GR.GR-5 — A entidade define uma Política de Gestão dos Riscos de Cibersegurança a qual prevê uma metodologia para a gestão dos riscos de cibersegurança.

Descrição

A entidade define, comunica, atualiza e revê, uma Política de Gestão dos Riscos de Cibersegurança por forma a refletir alterações nos requisitos legais e regulamentares, nas ameaças, em novas tecnologias, e na missão organizacional. Esta Política inclui a metodologia para calcular, registar, categorizar e dar prioridade aos riscos de cibersegurança da entidade.

Referências

NIST CSF 2.0 — GV.PO-02

4.3 — GR.FR — Funções, Responsabilidades e Autoridades:

São definidas e comunicadas as funções, papéis e responsabilidades em matéria de cibersegurança para promover a responsabilização, a avaliação do desempenho e a melhoria contínua.

GR.FR-1 — Os órgãos de gestão, direção e administração compreendem as suas funções e responsabilidades, e promovem uma cultura de cibersegurança, ética e de melhoria contínua.

Descrição

Os órgãos de gestão, direção e administração demonstram estar comprometidos com a temática da cibersegurança, promovendo uma cultura de cibersegurança. Estes órgãos compreendem qual é o seu papel e responsabilidade na cibersegurança.

Referências

ISO/IEC 27001:2022 — 5.1, 5.3, 7.2, 8.1

ISO/IEC 27002:2022 — 5.2,5.4, 5.12, 6.3

NIST SP-800-53 Rev. 5 — AT-3

NIST CSF 2.0 — GV.RR-01

CIS CSC v8.1 — 14,17

CyFun 2025 — GV.RR-01

GR.FR-2 — São atribuídos recursos adequados e proporcionais à estratégia de gestão do risco de cibersegurança, às funções, responsabilidades e políticas de cibersegurança da entidade.

Descrição

A entidade garante que são atribuídos recursos adequados e proporcionais à estratégia de risco de cibersegurança, às funções, responsabilidades e políticas da mesma.

Referências

NIST CSF 2.0 — GV.RR-03

CyFun 2025 — GV.RR-03

GR.FR-3 — As funções, responsabilidades e autoridades em matéria de cibersegurança são definidas e comunicadas ao pessoal, fornecedores e partes interessadas.

Descrição

As funções, responsabilidades e autoridades de cibersegurança dentro da entidade são documentadas,, aprovadas, alinhadas com as funções internas da entidade e partes interessadas externas e atualizadas. O estabelecido deve ser comunicado ao pessoal, fornecedores e outras partes interessadas.

Referências

ISO/IEC 27001:2022 — 5.3, 5.1, 7.5, 7.5.2, 7.5.3, 9.1, 9.3

ISO/IEC 27002:2022 — 5.2, 5.4, 5.5

NIST CSF 2.0 — GV.RR-02

CIS CSC v8.1 — 14,17

CyFun 2025 — GV.RR-02

GR.FR-4 — A cibersegurança é contemplada nos processos de gestão de recursos humanos.

Descrição

Os processos organizacionais que gerem os recursos humanos, que incluem a seleção de candidatos, contratação, categorização das posições e a cessação de vínculo laboral, são avaliados e revistos com base nos requisitos de cibersegurança estabelecidos pela entidade.

Referências

ISO/IEC 27001:2022 — 4.1, 4.2, 7.1, 7.3

ISO/IEC 27002:2022 — 5.4, 5.5, 5.11, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7

NIST SP-800-53 Rev.5 — PS-1, AT-1, AT-2 e AT-3

NIST CSF 2.0 — GV.RR-04

CyFun 2025 — GV.RR-04

4.4 — GR.PP — Políticas e Planos de Cibersegurança:

As Políticas e Planos de Cibersegurança da entidade são definidos, comunicados e implementados.

GR.PP-1 — As Políticas para a gestão de Cibersegurança, incluindo a Política de Cibersegurança, são definidas com base no contexto organizacional, na estratégia de cibersegurança e nas prioridades da entidade.

Descrição

A entidade define e aprova superiormente a sua Política de Cibersegurança e garante o compromisso dos órgãos de gestão, direção e administração com a Política. A entidade comunica às partes interessadas a existência da Política de Cibersegurança.

A entidade desenvolve, e identifica na Política de Cibersegurança as várias políticas que compõem o seu processo da gestão da cibersegurança, e que poderão ser nomeadamente:

a) Política de Gestão dos Riscos de Cibersegurança;

b) Política de Gestão do Risco da Cadeia de Abastecimento;

c) Política de Gestão do Ciclo de Vida de Ativos;

d) Política de Classificação e Gestão de Dados;

e) Política de Monitorização, Identificação e Documentação das Vulnerabilidades;

f) Política de Palavra-Passe;

g) Política de Gestão de Identidades, Autenticação e Controlo de Acessos;

h) Política de Uso Aceitável;

i) Política de Cópias de Segurança.

Referências

ISO/IEC 27001:2022 — 4,4, 7.2, 7.5.2., 9.1

ISO/IEC 27002:2022 — 5.1, 5.5, 5.8

NIST SP-800-53 Rev.5 — SR-1

NIST CSF 2.0 — GV.PO-1

CIS CSC v8.1 — 14

CyFun 2025 — GV.PO-01

GR.PP-2 — O Plano de Resposta a Incidentes é definido, comunicado, mantido e melhorado.

Descrição

O Plano de Reposta a Incidentes é definido, implementado e atualizado com frequência, com vista à sua melhoria.

A entidade garante que as partes interessadas relevantes, internas e externas, têm o conhecimento apropriado de todas as atualizações efetuadas.

Referências

ISO/IEC 27001:2022 — 4.1, 4.2, 6.2, 7.5.2, 7.5.3, 8.1, 9.3.2, 10.2

ISO/IEC 27002:2022 — 5.5, 5.20, 5.24, 5.29, 8.6

NIST SP-800-53 Rev.5 — IR-8

NIST CSF 2.0 — ID.IM-04

CIS CSC v8.1 — 17

CyFun 2025 — ID.IM-04

GR.PP-3 — O Plano de Recuperação de Desastres é definido, comunicado, mantido e melhorado.

Descrição

O Plano de Recuperação de Desastres é definido, implementado e atualizado com frequência, com vista à sua melhoria.

A entidade garante que as partes interessadas relevantes, internas e externas, têm o conhecimento apropriado de todas as atualizações efetuadas.

Referências

ISO/IEC 27001:2022 — 4.1, 4.2, 6.2, 7.5.2, 7.5.3, 8.1, 9.3.2, 10.2

ISO/IEC 27002:2022 — 5.5, 5.20, 5.29, 8.6

NIST SP-800-53 Rev.5 — CP-2

NIST CSF 2.0 — ID.IM-04

CIS CSC v8.1 — 17

CyFun 2025 — ID.IM-04

4.5 — GR.SP — Supervisão:

Os resultados das atividades e do desempenho da gestão dos riscos de cibersegurança são utilizados para apoiar a tomada de decisões.

GR. SP-1 — Os resultados da estratégia de gestão dos riscos de cibersegurança são analisados para informar os órgãos de gestão, direção e administração e, caso necessário, para adaptar a estratégia da entidade quanto aos riscos.

Descrição

Os responsáveis pela análise de atividades e desempenho da estratégia de gestão dos riscos de cibersegurança informam os órgãos de gestão, direção e administração e, quando necessário, adaptam a estratégia de acordo com os resultados obtidos, considerando possíveis limitações no normal funcionamento operacional da entidade, no orçamento e em processos de inovação, entre outros.

Referências

NIST CSF 2.0 — GV.OV-01

GR. SP-2 — A estratégia de gestão de riscos de cibersegurança é regularmente revista e adaptada para garantir a cobertura dos requisitos e riscos organizacionais.

Descrição

A entidade revê regularmente a estratégia de gestão dos riscos de cibersegurança para incorporar requisitos e riscos organizacionais que sejam identificados através de análises de auditorias, de incidentes e do desempenho das funções de cibersegurança.

Referências

NIST CSF 2.0 — GV.OV-O2

CyFun 2025 — GV.OV-02

GR.SP-3 — O desempenho da gestão dos riscos de cibersegurança da entidade é avaliado e revisto para alterações necessárias.

Descrição

A entidade avalia e revê o seu desempenho da gestão dos riscos de cibersegurança, através da implementação de mecanismos de avaliação e monitorização de desempenho, para garantir que alterações são consideradas e aplicadas quando necessário.

Referências

NIST CSF 2.0 — GR.OV-3

CyFun 2025 — GV.OV-03

4.6 — GR.CA — Gestão do Risco na Cadeia de Abastecimento:

A entidade estabelece as prioridades, restrições e níveis de tolerância ao risco que são utilizadas para suportar a tomada de decisão, no âmbito da gestão do risco operacional da cadeia de abastecimento. A entidade estabelece e implementa processos para identificar, avaliar e gerir os riscos inerentes à cadeia de abastecimento.

GR.CA-1 — As políticas e processos de gestão dos riscos da cadeia de abastecimento são identificados, estabelecidos, avaliados e geridos.

Descrição

A entidade identifica e implementa processos e procedimentos para gerir os riscos de segurança associados à utilização de produtos e serviços fornecidos por terceiros, incluindo serviços de computação em nuvem. Estes procedimentos incluem as obrigações da própria entidade e as obrigações dos fornecedores para o início ou término da utilização dos produtos e serviços fornecidos por terceiros.

Referências

ISO/IEC 27001:2022 — 5.1, 5.3, 6.1.1, 6.1.2, 6.1.3, 6.2, 7.1, 7.5.2., 7.5.3, 8.1, 8.2, 8.3, 9.3.2

ISO/IEC 27002:2022 — 5.19, 5.20, 5.21, 5.22

NIST SP-800-53 Rev. 5 — RA-3

NIST CSF 2.0 — GV.SC-01

CyFun 2025-GV.SC-01

GR.CA-2 — Os papéis e responsabilidades dos parceiros, fornecedores e clientes no âmbito da gestão da cibersegurança são definidos, comunicados e coordenados interna e externamente.

Descrição

A entidade define, coordena e comunica os papéis e responsabilidades no âmbito do sistema de gestão de cibersegurança das partes interessadas externas relevantes para a entidade, sendo este entendimento essencial para aumentar o nível de cibersegurança da entidade.

A entidade comunica e efetua ações de sensibilização para garantir que o entendimento das partes interessadas sobre este tema é o adequado e necessário.

Referências

ISO/IEC 27001:2022 — 5.3, 8.1, 9.2

ISO/IEC 27002:2022 — 5.2, 5.4, 5.12, 5.20, 5.22, 6.3, 8.30

NIST SP-800-53 Rev. 5 — AT-3

NIST CSF 2.0 — GV.SC-02

CIS CSC v8.1-14

CyFun 2025-GV.SC-02

GR.CA-3 — Os processos de gestão dos riscos de cibersegurança da cadeia de abastecimento da entidade estão incluídos nos processos transversais de cibersegurança e na estratégia de gestão dos riscos da entidade.

Descrição

A entidade inclui os riscos associados à sua cadeia de abastecimento, incluindo fornecedores, prestadores de serviços e parceiros tecnológicos e, de forma sistemática, identifica, avalia, gere e monitoriza estes riscos. A entidade garante o alinhamento da gestão de riscos da cadeia de abastecimento com a gestão de riscos de cibersegurança e risco global da entidade. Esta gestão do risco de cibersegurança da cadeia de abastecimento deve garantir a resiliência da entidade face a potenciais incidentes com origem nos seus fornecedores, parceiros, prestadores de serviços e outros.

Referências

NIST CSF 2.0 — GV.SC-03

CyFun 2025-GV.SC-03

GR.CA-4 — Os fornecedores são periodicamente avaliados.

Descrição

A entidade define o processo de gestão de fornecedores na cadeia de abastecimento de acordo com as prestações contratualizadas com os mesmos.

Referências

ISO/IEC 27001:2022 — 8.1, 9.2

ISO/IEC 27002:2022 — 5.20, 5.22

NIST CSF 2.0 — GV.SC-04

GR.CA-5 — A entidade define e integra nos contratos e outros acordos com fornecedores os requisitos para gerir os riscos de cibersegurança da cadeia de abastecimento.

Descrição

A entidade garante que os seus fornecedores cumprem com os requisitos de cibersegurança estabelecidos no quadro contratual.

Os contratos e outros acordos com fornecedores são utilizados para implementar medidas adequadas, de modo a garantir o cumprimento dos objetivos da Política de Cibersegurança da entidade e da Política de Gestão dos Riscos para a Cadeia de Abastecimento.

Referências

ISO/IEC 27001:2022 — 6.1.3, 7.5.2, 8.1, 9.1

ISO/IEC 27002:2022 — 5.20, 5.35

NIST CSF 2.0 — GV.SC-05

CyFun 2025-GV.SC-05

GR.CA-6 — Antes da contratação de fornecedores são realizados processos de devida diligência para reduzir os riscos da entidade.

Descrição

A entidade planeia e conduz processos de devida diligência antes de formalizar uma relação, contratação ou aquisição de serviço com um fornecedor, com o objetivo de minimizar a exposição ao risco.

Referências

NIST CSF 2.0 — GV.SC-06

CyFun 2025-GV.SC-06

GR.CA-7 — A entidade avalia os riscos de cibersegurança da cadeia de abastecimento.

Descrição

Os fornecedores de redes e sistemas de informação, componentes e serviços de cibersegurança são identificados, priorizados e avaliados, recorrendo a um processo de avaliação do risco da cadeia de abastecimento de cibersegurança.

A entidade, após a identificação dos fornecedores, categoriza-os considerando:

1) A exposição da sua informação aos mesmos;

2) O impacto na cadeia de abastecimento;

3) O tipo de bens e serviços fornecidos.

Referências

ISO/IEC 27001:2022 — 5.1, 6.1.2, 7.4, 7.5.2, 7.5.3, 8.1, 8.2

ISO/IEC 27002:2022 — 5.19, 5.21, 5.22

NIST SP-800-53 Rev. 5 — PM-9

NIST CSF 2.0 — GV.SC-07 CyFun 2025-GV.SC-07

GR.CA-8 — O Plano de Resposta a Incidentes e o Plano de Recuperação de Desastres são testados com o acompanhamento dos fornecedores.

Descrição

A entidade identifica os fornecedores e pontos de contacto a participar nas atividades previstas nos Planos de Resposta a Incidentes e Plano de Recuperação de Desastres e garante que os mesmos são envolvidos nos testes e nos exercícios planeados.

Referências

ISO/IEC 27001:2022 — 6.1.3, 7.5.2, 8.1, 8.3

ISO/IEC 27002:2022 — 5.26, 5.29

NIST SP-800-53 Rev. 5 — CP-2

NIST CSF 2.0 — GV.SC-08

CIS CSC v8.1-18

CyFun 2025-GV.SC-08

GR.CA-9 — As práticas de cibersegurança da cadeia de abastecimento são integradas em programas de cibersegurança e de gestão de riscos organizacionais, e o seu desempenho é monitorizado ao longo do ciclo de vida dos produtos e serviços tecnológicos.

Descrição

A entidade garante que todas as práticas de segurança relacionadas com a cadeia de abastecimento são integradas na Política de Cibersegurança, garantindo também uma monitorização contínua de todo o ciclo de vida dos produtos e serviços tecnológicos adquiridos. Esta sinergia permite a manutenção de um ambiente seguro e resiliente, capaz de endereçar os riscos emergentes de forma proativa.

Referências

NIST CSF 2.0 — GV.SC-09

CyFun 2025-GV.SC-09

GR.CA-10 — Aquando da definição de processos de gestão dos riscos da cadeia de abastecimento de cibersegurança a entidade inclui disposições para atividades que possam ocorrer durante ou após a cessação de contratos com fornecedores ou parceiros.

Descrição

A entidade garante que estão instituídos procedimentos internos para o término de parcerias, contratos ou acordos com fornecedores ou parceiros. Esta prática protege a entidade de determinados riscos inerentes às anteriores atividades ou responsabilidades dos fornecedores, como acesso não autorizado a informação ou sistemas, uso indevido de informação interna partilhada, divulgação de vulnerabilidades internas, entre outros aspetos.

Referências

NIST CSF 2.0 — GV.SC-10

CyFun 2025-GV.SC-10

5 — Identificar:

O objetivo Identificar pretende estabelecer uma base comum, transversal à entidade, para a abordagem à gestão de riscos de cibersegurança no contexto da envolvência das suas redes e sistemas de informação, pessoas, ativos, dados e respetivas capacidades. A entidade identifica quais os ativos que suportam os seus processos críticos e os riscos associados relevantes. Esta identificação permite que a entidade consiga definir e priorizar os seus recursos e investimentos, de acordo com os seus objetivos gerais e com a sua estratégia de gestão de riscos. As práticas que se enquadram no objetivo Identificar são basilares para a efetiva utilização do QNRCS. Conhecer, num contexto organizacional, os recursos que suportam as funções importantes e os respetivos riscos associados, permite às entidades priorizar os seus esforços de forma consistente.

5.1 — ID.GA — Gestão de Ativos:

A entidade identifica e gere, de acordo com a sua relevância para o cumprimento dos objetivos organizacionais e a estratégia de gestão do risco da entidade, os dados, equipamentos, sistemas e instalações que permitem cumprir os seus objetivos, no decorrer da sua atividade.

ID.GA-1 — Os equipamentos e os demais recursos físicos geridos ou detidos pela entidade são inventariados.

Descrição

A entidade inventaria os seus equipamentos e os demais recursos físicos existentes, por forma a garantir que existe um mapeamento estruturado dos mesmos, e realiza um mapeamento das dependências entre ativos. Todos os dispositivos inventariados são classificados de acordo com a sua relevância para a entidade.

Referências

ISO/IEC 27001:2022 — 7.5.2, 7.5.3, 8.1

ISO/IEC 27002:2022 — 5.9, 7.1

NIST SP-800-53 Rev.5- CM — 8

NIST CSF 2.0 — ID.AM-01

CIS CSC v8.1 — 1

CyFun 2025 — ID.AM-01

ID.GA-2 — Os recursos lógicos que suportam os processos dos serviços da entidade são inventariados

Descrição

A entidade inventaria os recursos lógicos que suportam os processos dos serviços da entidade, por forma a garantir que existe um mapeamento estruturado dos mesmos, e realiza um mapeamento das dependências entre ativos. Todos os dispositivos inventariados são classificados de acordo com a sua relevância para a entidade.

Referências

ISO/IEC 27001:2022- 7.5.2, 7.5.3, 8.1

ISO/IEC 27002:2022 — 5.9, 8.30

NIST SP-800-53 Rev.5- CM-8

NIST CSF 2.0 — ID.AM-02

CIS CSC v8.1-2

CyFun 2025-ID.AM-02

ID.GA-3 — As redes e fluxos de comunicação são mapeados.

Descrição

A entidade dispõe de um inventário com todas as suas redes de comunicações e de gestão e o mapeamento dos seus fluxos de comunicação internos e externos. O mapeamento de fluxos de comunicação externos inclui, por exemplo, conexões VPN e acessos à internet.

Esta informação é essencial para que a entidade tenha conhecimento dos ativos que suportam a sua infraestrutura de comunicações e dos respetivos fluxos de comunicação existentes.

Referências

ISO/IEC 27001:2022- 7.5.2, 7.5.3, 8.1, 9.1

ISO/IEC 27002:2022 — 5.5., 5.9, 8.12

NIST SP-800-53 Rev.5 — AC-4

NIST CSF 2.0 — ID.AM-03

CIS CSC v8.1 — 12

CyFun 2025 — ID.AM-03

ID.GA-4 — Os serviços prestados por fornecedores são inventariados.

Descrição A entidade mantém um inventário atualizado de todos os serviços externos prestados por fornecedores os quais utiliza e depende. Este inventário permite que a entidade tenha conhecimento do(s) responsáveis pela gestão destes serviços e das suas dependências.

Referências

ISO/IEC 27001:2022- 7.5.2, 7.5.3, 8.1

ISO/IEC 27002:2022 — 5.9, 5.12, 8.6

NIST SP-800-53 Rev.5 — AC-20

NIST CSF 2.0 — ID.AM-04

CIS CSC v8.1 — 12

CyFun 2025 — ID.AM-04

ID.GA-5 — Os ativos são classificados de acordo com a sua criticidade.

Descrição

A entidade classifica os seus ativos de acordo com a criticidade e valor que estes ativos representem para si.

No processo de inventariação, a entidade:

1 — Identifica um método de classificação de ativos que seja aprovado internamente;

2 — Garante que os responsáveis pelos ativos os classificam de acordo com a importância dos mesmos para a entidade.

Referências

ISO/IEC 27002:2022 — 5.9, 5.12, 8.6

NIST CSF 2.0 — ID.AM-05

CIS CSC v8.1 — 3

CyFun 2025-ID.AM-05

ID.GA-6 — Os dados e respetivos metadados são identificados e registados.

Descrição

A entidade mantém um registo atualizado dos dados e respetivos metadados para cada tipo de dados designados. sendo que se entendem como dados designados os dados que a entidade explicitamente identifica, categoriza e sinaliza como requerendo tratamento, proteção ou gestão especial.

Este inclui o seu tipo, localização, responsável e classificação em termos de criticidade. Esta prática permite à entidade uma melhor gestão dos dados gerados, guardados e que circulam na rede, facilitando a gestão ao nível do cumprimento de requisitos legais e a correta e ponderada aplicação de medidas de cibersegurança que restrinjam e protejam o uso e retenção dos dados com base no risco.

Os metadados são dados sobre dados, isto é, informação que descreve os dados. São exemplos de metadados:

a) Metadados descritivos (título, autor, palavras-chave);

b) Metadados estruturais (formato, esquema);

c) Metadados administrativos (acessos, políticas de armazenamento da informação);

d) Metadados técnicos (arquivo, informações de codificação e local de armazenamento).

Referências

NIST CSF 2.0 — ID.AM-07

CyFun 2025-ID.AM-07

ID.GA-7 — Sistemas, *hardware, software*, serviços e dados são geridos ao longo dos seus ciclos de vida

Descrição

A entidade gere todos os aspetos relacionados com o ciclo de vida dos seus sistemas, *hardware, software*, serviços e dados ao longo dos seus ciclos de vida, desde a sua aquisição/criação até à sua eventual destruição. Este ciclo é monitorizado por forma a assegurar que os ativos da entidade são protegidos e mantidos em todas as suas fases da vida da forma mais eficiente e considerando o seu nível de risco.

No ciclo de vidaé incluída a manutenção do *software* da entidade, que é sujeita a processos de aprovação. A manutenção é registada de forma a impedir a existência de acessos e utilização não autorizados. A entidade executa as tarefas de manutenção dos seus ativos críticos, de forma regular e atempada. A manutenção é registada, efetuada e supervisionada por pessoal da entidade com as autorizações e competências adequadas.

A entidade tem procedimentos de autorização, monitorização, registo e de controlo do *hardware*, sendo este mantido, substituído e removido de acordo com o risco.

Referências

ISO/IEC 27001:2022 — 7.1, 7.5.2, 8.1, 9.1

ISO/IEC 27002:2022 — 5.10, 5.11, 5.19, 5.37, 7.2, 7.9, 7.10, 7.13, 7.14, 8.7, 8.11, 8.12, 8.15, 8.21

NIST CSF 2.0- PR.PS-03, PR.PS-02, ID.AM-08

CIS CSC v8.1-1,4,7

CyFun 2025-ID.AM-08

ID.GA-8 — Os dados são destruídos de acordo com a Política de Classificação e Gestão de Dados definida.

Descrição

As informações digitais e físicas são sujeitas aos métodos apropriados de destruição, de acordo com a classificação de informação.

Referências

ISO/IEC 27001:2022 — 7.5.2, 7.5.3., 8.1

ISO/IEC 27002:2022 — 5.10, 7.10, 7.14, 8.10

NIST SP-800-53 Rev.5 — MP-4

NIST CSF 2.0 — ID.AM-08

ID.GA-9 — A entidade implementa um processo de gestão de alterações.

Descrição

A entidade implementa um processo formal de gestão de alterações, assegurando que todas as alterações nos sistemas de informação, planeadas ou não planeadas, e que possam ter impacto na infraestrutura, sistemas, aplicações, serviços ou processos internos, são geridas de forma controlada e segura.

As alterações incluem, mas não se limitam a:

Atualizações de *software, patches* de segurança e correções de vulnerabilidades;

Alteração de configurações de servidores, redes ou bases de dados;

Implementação de novas políticas de segurança, como regras de *firewall*;

Alteração de permissões de acesso para utilizadores:

Substituição ou atualização de *hardware*;

Introdução de novas aplicações ou descontinuação de sistemas antigos.

Referências

ISO/IEC 27001:2022 — 7.5.3, 8.1

ISO/IEC 27002:2022 — 8.9, 8.19, 8.32, 8.33

NIST SP-800-53 Rev.5 — CM-9

NIST CSF 2.0-ID.RA-07

CIS CSC v8.1-4, 5, 12

5.2 — ID.AR — Avaliação do Risco:

A entidade identifica e determina os riscos de cibersegurança para a sua atividade (incluindo missão, funções, imagem ou reputação), ativos e pessoas. A entidade define ainda o seu tratamento aos riscos identificados.

ID.AR-1 — As vulnerabilidades dos ativos são identificadas e documentadas com base na metodologia definida.

Descrição

Uma das bases da avaliação do risco da entidade é o processo de gestão de vulnerabilidades, nomeadamente, todas as vulnerabilidades conhecidas que não foram mitigadas.

Estas vulnerabilidades são avaliadas em sede de análise do risco da entidade, sendo formalmente definida qual a estratégia a aplicar, respeitando a metodologia de gestão dos riscos da entidade.

Referências

ISO/IEC 27001:2022 — 6.1.2, 6.1.3, 7.5.2, 8.2, 8.3

ISO/IEC 27002:2022 — 5.36,8.8, 8.33

NIST SP-800-53 Rev.5 — RA-5

NIST CSF 2.0- ID.RA-01

CIS CSC v8.1-7

CyFun 2025 — ID.RA-01

ID.AR-2 — A entidade partilha informações sobre ameaças de cibersegurança com partes interessadas.

Descrição

A entidade estabelece contacto com grupos de interesse sobre cibersegurança, para trocar experiências sobre boas práticas e ter acesso a informações relevantes sobre cibersegurança. As informações sobre ameaças podem ser recolhidas junto de fóruns ou em fontes de partilha de informações da especialidade.

Caso as fontes de partilha de informação sejam de formato eletrónico e passíveis de ser consumidas por interfaces aplicacionais, devem ser sistematizados processos automáticos de recolha, tratamento e armazenamento das mesmas, para posterior correlação pelos sistemas de gestão e correlação de eventos de segurança.

Referências

ISO/IEC 27001:2022 — 4.2, 6.1.3, 7.3, 7.4, 8.3

ISO/IEC 27002:2022 — 5.5, 5.6, 5.7, 5.12, 5.13, 5.20, 5.21

NIST CSF 2.0-ID.RA-02

CIS CSC v8.1 — 14

CyFun 2025 — ID.RA-02

ID.AR-3 — As ameaças internas e externas são identificadas e documentadas com base na metodologia definida.

Descrição

No âmbito do processo de gestão dos riscos, a entidade identifica potenciais ameaças que possam explorar vulnerabilidades eventualmente existentes nos seus ativos. As ameaças podem ser internas ou externas à entidade, podendo ser de origem natural ou humana, e acidentais ou intencionais.

Referências

ISO/IEC 27001:2022 — 6.1.2

NIST SP 800-53 Rev. 5-RA-3, NIST CSF 2.0- ID.RA-03

CIS CSC v8.1-7

CyFun 2025-ID.RA-05

ID.AR-4 — São identificados e registados potenciais impactos e as respetivas probabilidades de ameaças.

Descrição

A entidade identifica, na sua metodologia de gestão do risco, os critérios associados à aferição de probabilidade e impacto das ameaças. Os critérios para a definição da probabilidade e do impacto das ameaças devem considerar o contexto organizacional, os objetivos de negócio, bem como os próprios objetivos do processo de gestão dos riscos.

Referências

ISO/IEC 27001:2022 — 6, 8

ISO/IEC 27002:2022 — 5.36, 6.8, 8.8, 8.32

NIST CSF 2.0 — ID.RA-04

CIS CSC v8.1-2, 4, 5, 16, 18

CyFun 2025-ID.RA-06

ID.AR-5 — A entidade avalia os riscos identificados.

Descrição

A entidade avalia os riscos identificados com base na lista das ameaças e vulnerabilidades dos ativos, das medidas implementados e a sua eficácia. O risco é expresso como a combinação do impacto de um evento e a sua probabilidade de acontecer.

Referências

ISO/IEC 27001:2022 — 4.1, 6.1.2, 7.4, 7.5.2, 8.2, 9.3.2

ISO/IEC 27002:2022 — 5.5, 5.27, 6.8, 8.8

NIST SP-800-53 Rev.5 — RA-3

NIST CSF 2.0-ID.RA-05

CIS CSC v8.1 — 7, 10

CyFun 2025 — ID.RA-05

ID.AR-6 — A entidade garante que as respostas aos riscos são identificadas e priorizadas.

Descrição

A entidade define a resposta adequada ao nível do risco encontrado. A prioridade de tratamento dos riscos é definida de acordo com o nível do risco observado e a criticidade do ativo para a entidade.

Referências

ISO/IEC 27001:2022 — 5.1, 6.1.3, 8.3, 10.1

ISO/IEC 27002:2022 — 8.8

NIST SP-800-53 Rev.5 — RA-7

NIST CSF 2.0 — ID.RA-06

CIS CSC v8.1 — 7, 10

CyFun 2025 — ID.RA-06

ID.AR-7 — A entidade define processos para receber informação, analisar e responder a vulnerabilidades provenientes de fontes internas e externas.

Descrição

A entidade define um processo formal para receber a submissão de vulnerabilidades, provenientes de fontes internas ou externas (por exemplo: formulários semi-automatizados, testes internos, relatórios de segurança ou investigadores de segurança).

Cada submissão é analisada, verificada e, no caso de se confirmar que a informação configura uma vulnerabilidade, a entidade segue o processo de resposta a vulnerabilidades conforme definido.

Referências

ISO/IEC 27001:2022 — 4.4, 7.5.2, 8.3, 9.1

ISO/IEC 27002:2022 — 5.7, 5.37,8.8, 8.16, 8.29

NIST CSF 2.0 — ID.RA-08

CIS CSC v8.1 — 17

CyFun 2025 — ID.RA-08

5.3 — ID.MC — Melhoria Contínua:

As melhorias nos processos, procedimentos e atividades de gestão do risco de cibersegurança são identificadas em todos os Objetivos do QNRCS.

ID.MC-1- As melhorias são identificadas através de avaliações e a informação é partilhada com as partes interessadas.

Descrição

A entidade tem um compromisso com a melhoria dos seus processos de gestão do risco de cibersegurança, efetuando sessões de lições aprendidas, analisando os incidentes já ocorridos, entre outros, para reduzir o risco da ocorrência de incidentes futuros. A entidade partilha com as partes relevantes a informação sobre melhorias identificadas.

Referências

ISO/IEC 27001:2022 — 7.4

ISO/IEC 27002:2022 — 5.27

NIST CSF 2.0 — ID.IM-01

ID.MC-2 — São identificadas melhorias a partir de testes e exercícios de cibersegurança.

Descrição

A entidade realiza testes e exercícios de cibersegurança, incluindo com partes interessadas, quando se justificar, para identificar pontos de melhoria. A entidade garante que Planos de Reposta a Incidentes, Planos de Recuperação de Desastres, e Planos de Continuidade de Negócio estabelecidos são testados, para que se possa determinar a eficácia, prontidão de execução dos mesmos e identificar possíveis pontos de falha.

Referências

ISO/IEC 27001:2022 — 6.1.3, 7.5.2, 8.1, 8.3

ISO/IEC 27002:2022- 5.26, 5.29

NIST SP-800-53 Rev.5- CP-4, IR-3, PM-14

NIST CSF 2.0 — ID.IM-02

CIS CSC v8.1 — 18

CyFun 2025-ID.IM-02

ID.MC-3 — As melhorias são identificadas a partir da execução de processos, procedimentos e atividades operacionais.

Descrição

A entidade avalia e atualiza regularmente os seus processos e procedimentos de cibersegurança para que as possíveis fragilidades existentes sejam identificadas e alvo de um plano de correção. A entidade extrai conclusões com os incidentes que ocorrem nas suas redes e sistemas de informação, identificando medidas operacionais e/ou processuais que possam melhorar a capacidade de deteção de novos incidentes.

Referências

ISO/IEC 27001:2022 — 9.1, 9.2.1, 10.1

ISO/IEC 27002:2022 — 5.27

NIST CSF 2.0 — ID.IM-03

CyFun 2025 — ID.IM-03

6 — Proteger:

Pretende-se, como resultado do objetivo Proteger, proporcionar o desenvolvimento e a implementação de controlos de cibersegurança necessários à garantia de prestação de serviços ou bens, reforçando a capacidade da entidade em limitar ou conter o impacto de uma eventual ocorrência de um incidente de cibersegurança. Através da implementação de controlos que protejam os processos organizativos e os ativos da entidade, independentemente da sua natureza tecnológica, a entidade garante a sua proteção em três dimensões: Pessoas, Processos e Tecnologia.

Esta capacidade potencia-se e assegura-se, na gestão da identidade eletrónica e respetivas autorizações, na realização de ações de formação e de sensibilização e na definição e implementação de procedimentos, processos e tecnologias de proteção da informação, entre outras.

6.1 — PR.GA — Gestão de Identidades, Autenticação e Controlo de Acessos:

Os acessos aos ativos físicos, lógicos e às instalações associadas são limitados às pessoas, processos e equipamentos autorizados. Estes são geridos de acordo com a avaliação do risco de acesso não autorizado.

PR.GA-1 — Os ciclos de vida de gestão de identidades são definidos

Descrição

A entidade garante que as identidades e credenciais de acesso às suas redes e sistemas de informação são emitidas, geridas, verificadas, revogadas e auditadas em conformidade com os processos instituídos.

Referências

ISO/IEC 27001:2022 — 6.1.1, 8.1

ISO/IEC 27002:2022 — 5.16, 5.17, 5.18, 8.2, 8.3, 8.5

NIST SP-800-53 Rev. 5 — AC-2

NIST CSF 2.0 — PR.AA-01

CIS CSC v8.1 — 1, 3, 4, 5, 12, 13

CyFun 2025-PR.AA-01

PR.GA-2 — A entidade verifica a identidade dos utilizadores e vincula-a às respetivas credenciais.

Descrição

A identidade dos utilizadores é vinculada, revista e as suas credenciais confirmadas de forma iterativa e quando necessário.

Referências

ISO/IEC 27001:2022 -7.5.2, 8.1

ISO/IEC 27002:2022 — 5.15, 8.2, 8.3, 8.18

NIST SP-800-53 Rev. 5 — AC -17

NIST CSF 2.0-PR.AA-02, PR.AA-04

CIS CSC v8.1-3,4,5,6

CyFun 2025-PR.AA-02

PR.GA-3 — São definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação.

Descrição

Os mecanismos de autenticação são definidos e mantidos de acordo com as características dos sistemas e dos perfis de acesso, por forma a permitir a manutenção da integridade e a confidencialidade da informação.

Referências

ISO/IEC 27001:2022 — 6.1.2, 7.5.2, 8.1,

ISO/IEC 27002:2022 — 5.16, 5.17, 5.34, 8.5, 8.27

NIST SP-800-53 Rev. 5 — AC-17

NIST CSF 2.0-PR. AA-03

CIS CSC v8.1-3,4,5,6,9,12,13 CyFun 2025-PR.AA-03 PR.GA-4- As afirmações de identidade são protegidas, transmitidas e verificadas.

Descrição

A entidade protege as afirmações de identidade utilizadas para transmitir a autenticação e as informações do utilizador, por exemplo, através de sistemas de início de sessão único (SSO — Single Sign-On).

Entendem-se por afirmações de identidade, uma declaração digital utilizada durante a autenticação que confirma a identidade de um utilizador, dispositivo ou processo.

Referências

NIST CSF 2.0-PR. AA-04

CyFun 2025-PR. AA-04

PR.GA-5 — As permissões de acesso, os direitos e as autorizações são definidas numa política, são geridas, aplicadas e atualizadas, e incorporam os princípios do menor privilégio e da separação de funções.

Descrição

As permissões de acesso e as autorizações são geridas de acordo com os princípios de acesso adequados à função, de acordo com os princípios de necessidade de conhecer e de segregação de funções, sendo que estes princípios e medidas de cibersegurança se aplicam a sistemas de TIC e TO, sempre que aplicável.

Entende-se, por menor privilégio o acesso às redes e sistemas de informação da entidade concedido de acordo com o correto desempenho das suas funções. Por segregação de funções, entende-se

a divisão de atribuição de funções e de privilégios entre múltiplos indivíduos, de forma que um processo em particular não possa ser executado ou controlado apenas por um deles.

O principal fundamento, para a aplicação desta prática de segregação de funções, é a prevenção de incidentes com impacto significativo nas atividades operacionais da entidade.

Existindo múltiplas pessoas envolvidas, minimiza-se a oportunidade de transgressões e fomenta-se a probabilidade de estas serem detetadas e reportadas.

O princípio de segregação de funções pode ser aplicado nos seguintes tipos de processos:

1 — Sequenciais: quando as atividades podem ser executadas em tarefas sequenciais e por pessoas diferentes (por exemplo: na atribuição de acessos, uma pessoa solicita, outra aprova e uma terceira atribui os acessos);

2 — Quórum: Quando as atividades requerem um quórum mínimo de aprovações para poderem ser executadas (por exemplo: a recuperação de uma chave de cifra, onde é requerida a presença de dois ou mais administradores de sistemas);

3 — Geoespacial: quando as atividades podem ser divididas em tarefas que são realizadas em locais diferentes (por exemplo: gestão de sistemas de informação, cujas tarefas são efetuadas por pessoal sediado em diferentes zonas geográficas).

Referências

ISO/IEC 27001:2022 — 8.1, 9.1, 9,2

ISO/IEC 27002:2022 — 5.3, 5.15, 8.2, 8.3, 8.4, 8.18

NIST SP-800-53 Rev. 5 — AC -17

NIST CSF 2.0- PR.AA-05

CIS CSC v8.1-3, 4, 6, 7, 12, 13, 16

CyFun 2025-PR.AA-05

PR.GA-6 — Os controlos de acesso físico a ativos da entidade são geridos, monitorizados e aplicados em função do risco.

Descrição

A entidade protege e gere os acessos físicos às suas infraestruturas de rede e de sistemas de informação. A entidade aplica este controlo ao seu pessoal, visitantes, e terceiros que colaboram com a entidade, nas zonas da entidade que sejam de acesso restrito e/ou a áreas sensíveis que alojem informação confidencial, redes e/ou sistemas de informação.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.8, 7.9, 7.11, 7.12, 8.1

NIST SP-800-53 Rev. 5 — PE -2

NIST CSF 2.0 — PR.AA-06

CyFun 2025 — PR.AS-06

PR.GA-7 — A entidade gere os seus acessos remotos.

Descrição

A entidade documenta, gere e controla os acessos remotos às suas redes e sistemas de informação.

São considerados acessos remotos, todos os acessos feitos às redes e sistemas de informação por pessoal que comuniquem através de redes de comunicações externas à entidade. As VPN, quando criadas, devem ser consideradas redes de comunicações internas, observando-se os controlos de segurança apropriados. Cumulativamente, apenas são considerados acessos remotos a redes e sistemas de informação, aqueles que sejam realizados a sistemas que não estejam propositadamente disponíveis publicamente.

Referências

ISO/IEC 27001:2022 — 7.52, 8.1

ISO/IEC 27002:2022 — 5.14, 6.7, 7.9, 8.1, 8.5, 8.11, 8.20

NIST SP-800-53 Rev. 5 — AC -17

CIS CSC v8.1 — 5, 6, 13

6.2 — PR.FC — Formação e Sensibilização:

A entidade promove a sensibilização e formação em cibersegurança do pessoal. O pessoal será sensibilizado e formado para cumprir com as suas responsabilidades e os seus deveres relacionados com a cibersegurança, em conformidade com as políticas, processos, procedimentos e acordos relevantes estabelecidos.

PR.FC-1 — Todo o pessoal é sensibilizado e formado em matérias de cibersegurança.

Descrição

A entidade estabelece um plano de ações de sensibilização e formação em cibersegurança e define os processos e procedimentos necessários para garantir a sua correta implementação. A entidade mede o sucesso das suas ações de formação.

As ações de sensibilização visam consciencializar um grupo abrangente de pessoas sobre um determinado tema enquanto as ações de formação têm como objetivo capacitar um determinado grupo de pessoas com conhecimento e competências específicas.

Referências

ISO/IEC 27001:2022 — 7.2, 7.3, 7.4, 9.1

ISO/IEC 27002:2022 — 6.3, 8.7

NIST SP-800-53 Rev. 5 — AT-2

NIST CSF 2.0-PR.AT-01

CIS CSC v8.1-14, 16

CyFun 2025 — PR.AT-01

PR.FC-2 — O pessoal com funções especializadas em cibersegurança e os órgãos de gestão, direção e administração recebem formação adequada para o exercício das suas funções.

Descrição

As pessoas que desempenham funções especializadas em cibersegurança e os órgãos de gestão, direção e administração são sensibilizadas e formadas de modo a possuírem os conhecimentos e as competências necessárias para desempenharem tarefas relevantes, tendo em conta os riscos de cibersegurança.

Referências

ISO/IEC 27001:2022- 5.3, 7.2, 7.3

ISO/IEC 27002:2022- 5.2, 6.3

NIST SP-800-53 Rev. 5-AT-3

NIST CSF 2.0- PR.AT-02

CIS CSC v8.1-4,14,16

CyFun 2025 — PR-AT-02

6.3 — PR.SD — Segurança de Dados:

As informações e os dados da entidade são geridos de acordo com a estratégia de gestão de riscos de maneira a proteger a confidencialidade, integridade e disponibilidade da informação.

PR.SD-1 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados em repouso.

Descrição

As redes e sistemas de informação protegem a confidencialidade, integridade e disponibilidade dos dados armazenados.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 5.10, 8.11, 8.17

NIST CSF 2.0-PR.DS-01

CIS CSC v8.1 — 3

CyFun 2025-PR.DS-01

PR.SD-2 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados em trânsito.

Descrição

A entidade protege adequadamente a integridade e a confidencialidade da informação transmitida. Este controlo é aplicado, quer a redes de comunicações internas, como externas. Para sistemas distribuídos, este controlo aplica-se em toda a linha, por forma a garantir a integridade entre os componentes e serviços que geram a informação e os componentes e serviços que a recebem.

Quando for impraticável ou impossível garantir os controlos de cibersegurança necessários e as garantias de controlo efetivo através dos veículos contratuais apropriados, a entidade implementa os controlos compensatórios necessários ou explicitamente aceita o risco adicional e/ou transfere o risco para o fornecedor contratual.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 5.10, 5.14, 8.11,8.20, 8.26

NIST CSF 2.0- PR.DS-02

CIS CSC v8.1 — 3

CyFun 2025-PR.DS-02

PR.SD-3 — A entidade implementa proteções que evitem exfiltração de dados.

Descrição

A entidade implementa controlos de segurança nas fronteiras das suas instalações ou das suas redes e sistemas de informação, para detetar acessos e atividades não autorizadas e impedir a exfiltração não autorizada de dados.

É definido o âmbito de atuação e frequência da aplicação, com o objetivo de se adequar a mitigação do risco associado. Este risco deve ser calculado tendo por base a classificação de confidencialidade da informação.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 6.6, 7.5, 7.6, 7.8, 8.2, 8.3, 8.4, 8.11, 8.12, 8.18, 8.20, 8.22, 8.24, 8.26

NIST CSF 2.0 — PR.DS-02

CIS CSC v8.1-3

PR.SD-4 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados em uso.

Descrição

As redes e sistemas de informação protegem a confidencialidade, integridade e disponibilidade da informação em utilização.

Referências

NIST CSF 2.0-PR.DS-10

CyFun 2025-PR.DS-10

PR.SD-5 -São realizadas, mantidas e testadas cópias de segurança dos dados da entidade.

Descrição

A entidade garante que as suas cópias de segurança são testadas e validadas regularmente, através da execução de planos de testes de restauro. Estes testes são efetuados no âmbito dos Planos de Continuidade do Negócio da entidade ou através de exercícios periódicos e planeados, para validação da integridade das cópias de segurança efetuadas.

Referências

ISO/IEC 27001:2022 — 6.2, 7.5.1, 8.1

ISO/IEC 27002:2022 — 5.1, 5.20, 5.23, 5.29, 5.32, 5.33, 5.37, 6.7, 8.6, 8.7, 8.9, 8.12, 8.13, 8.17

NIST SP-800-53 Rev.5 — CP-9

NIST CSF 2.0 — PR.DS-11

CIS CSC v8.1 — 11

CyFun 2025-PR.DS-11

6.4 — PR.SP — Segurança de plataformas:

As políticas de segurança, processos e procedimentos são mantidas e utilizadas para permitir gerir a proteção das redes e sistemas de informação.

PR.SP-1 — É criada e mantida uma configuração base de redes e sistemas de informação que incorpora os princípios de segurança.

Descrição

A entidade estabelece uma configuração base para redes e sistemas de informação, para os seus componentes e para as suas comunicações e conectividades.

Por configuração base, entende-se:

1) Programas informáticos instalados em estações de trabalho;

2) Equipamentos pessoais, tais como computadores portáteis, impressoras e outros dispositivos móveis;

3) Servidores e elementos de rede;

4) Versões e atualizações aplicadas a sistemas operativos e aplicações, configurações e parâmetros por omissão, topologia de rede e composição lógica das arquiteturas das redes e sistemas de informação.

Referências

ISO/IEC 27001:2022 — 7.5.2, 7.5.3, 8.1, 9.1

ISO/IEC 27002:2022 — 8.16, 8.19, 8.28, 8.32

NIST SP-800-53 Rev. 5 — CM-2

NIST CSF 2.0 — PR.PS-01

CIS CSC v8.1- 1, 4, 7, 12

CyFun 2025-PR.PS01

PR.SP-2 — Os *logs* de sistemas e o histórico de atividades são documentados, implementados e revistos de acordo com as Políticas da entidade.

Descrição

Os logs de sistemas e o histórico de atividades da entidade são determinados, documentados, implementados e revistos.

Referências

ISO/IEC 27001:2022 — 7.5.2., 7.5.3, 9.1, 9.2

ISO/IEC 27002:2022 — 5.37, 8.15, 8.17, 8.34

NIST CSF 2.0 — PR.PS-04 CIS CSC v8.1 — 1, 3, 4, 8

CyFun 2025-PR.PS-04

PR.SP-3 — A instalação e execução de *software* não autorizado são impedidas.

Descrição

A entidade impede a instalação e execução de *software* não autorizado ou não aprovado nos dispositivos e sistemas corporativos. Estas ações, caso não sejam monitorizadas e corretamente prevenidas, constituem comportamentos de risco, possibilitando a introdução de vulnerabilidades, *malware* ou outro tipo de riscos/ameaças que comprometam a segurança, integridade ou confidencialidade dos sistemas ou informação da entidade.

Referências

ISO/IEC 27002:2022 — 8.7

NIST SP-800-53 Rev. 5 — CM-7, CM-11

NIST CSF 2.0 — PR.PS-06

CIS CSC v8.1-2, 3

CyFun 2025-PR.PS-05

PR.SP-4 — É implementado um ciclo de vida de desenvolvimento seguro de *software*.

Descrição

A entidade aplica princípios de cibersegurança na especificação, desenho, desenvolvimento, implementação e modificação das suas redes e sistemas de informação. Estes princípios devem ser aplicados, quer a novos sistemas, como a sistemas que estejam a passar por alterações significativas. Para sistemas legados, estes princípios devem ser aplicados, na medida do possível, tendo em conta o estado atual do *hardware*, *software* e *firmware* desses sistemas.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 5.8, 8.17, 8.25, 8.27, 8.28, 8.30, 8.33 NIST SP-800-53 Rev. 5 — CM-9

NIST CSF 2.0-PR.PS-06

CIS CSC v8.1-16

CyFun 2025-PR.PS-06

6.5 — PR.RI — Resiliência da Infraestrutura Tecnológica:

As soluções técnicas de segurança são geridas por forma a garantir a segurança e resiliência dos sistemas e ativos, em concordância com as políticas relacionadas, processos, procedimentos e acordos relevantes.

PR.RI-1 — A entidade protege a integridade das redes de comunicações.

Descrição

A integridade das redes de comunicações é protegida através da sua segregação e segmentação. A rede de comunicações é desenhada de forma a não ser possível aceder-se a qualquer sistema, a partir de qualquer ponto da mesma.

São criadas zonas de segurança com propósitos identificados e com barreiras bem definidas e forçadas por equipamentos de rede de comunicações com capacidade para o efeito (*routers, gateways, firewalls*, entre outros).

As segregações da rede de comunicação são documentadas em políticas que definam o seu modelo de governação, nomeadamente, que autorizações são necessárias para a aprovação de novos fluxos e que fluxos entre zonas são pré-aprovados. Os fluxos de informação entre sistemas obrigam a autorizações específicas e conformidade com as políticas definidas para o efeito.

Exemplos do que as restrições de fluxos incluem:

1) Impedimentos de transmissão de informação sensível em claro para a Internet;

2) Bloqueio de tráfego externo que indica ser interno (forjado);

3) Restrição de acessos diretos à Internet que não sejam feitos através de um proxy corporativo;

4) Limitação de transferências de informação, com base em estruturas de dados e conteúdos.

O controlo dos fluxos de comunicação é efetuado com base nas características da informação e no caminho que a mesma efetua ao longo do seu transporte. A aplicação de restrições deve ser efetuada nos equipamentos de fronteira, como *routers*, *firewalls* ou *proxies*. Os fluxos regulam a transferência

de informação e os caminhos que podem ser abertos dentro de cada sistema ou entre sistemas. Estes são controlados operacionalmente e são sempre requeridas as autorizações prévias para que possam ser alterados.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 5.14, 5.37, 8.8, 8.11, 8.16, 8.20, 8.21, 8.22, 8.23, 8.26

NIST CSF 2.0-PR.IR-01

CIS CSC v8.1 — 3, 4, 7, 10, 12, 13

CyFun 2025-PR.IR-01

PR.RI-2 — Os ambientes de desenvolvimento e de teste são separados de ambientes de produção.

Descrição

A entidade efetua a separação dos ambientes das suas redes e dos seus sistemas de informação, de forma física ou lógica, de acordo com as suas funções.

Os ambientes de desenvolvimento e testes estão segregados dos ambientes de produção, quer em termos de acessos, quer em termos de dados.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1

ISO/IEC 27002:2022 — 8.31, 8.30, 8.33

NIST SP-800-53 Rev. 5 — PL-8

NIST CSF 2.0 — PR.IR-01

CIS CSC v8.1-16

CyFun 2025-PR.IR-01

PR.RI-3 — Os ativos tecnológicos da entidade são protegidos de ameaças naturais.

Descrição

A entidade protege as redes e sistemas de informação contra desastres naturais, falhas de energia, incêndios e inundações.

Referências

ISO/IEC 27001:2022 — 4.1, 4.2, 6.1.1, 7.1, 8.1

ISO/IEC 27002:2022 — 5.5, 7.2, 7.5, 7.6, 7.8, 7.11, 7.12, 8.14, 8.32

NIST SP-800-53 Rev.5 — MA-1

NIST CSF 2.0 — PR.IR-02

CyFun 2025-PR.IR-02

PR.RI-4 — São implementados mecanismos para cumprir os requisitos de resiliência em situações adversas.

Descrição

A entidade implementa os controlos necessários para que possa cumprir os requisitos de resiliência básicos em situações fora do comum e que garantam a alocação de recursos e equipamentos

adicionais. Caso seja necessário responder a situações adversas, coloca-se em prática o Plano de Continuidade de Negócio.

Referências

ISO/IEC 27001:2022 — 6.2, 7.5.2, 8.1

ISO/IEC 27002:2022 — 5.29, 7.5, 8.14

NIST SP-800-53 Rev. 5 — CP-2

NIST CSF 2.0-PR.IR-03

CyFun 2025-PR.IR-03

PR.RI-5 — A entidade planeia a capacidade adequada dos recursos para garantir a disponibilidade das suas redes e sistemas de informação.

Descrição

A capacidade das redes e dos sistemas de informação é monitorizada e são efetuadas previsões sobre as necessidades de capacidade futura, para garantir que o desempenho dos sistemas está alinhado com os requisitos de prestação dos serviços críticos.

Referências

ISO/IEC 27001:2022 — 7.1, 8.1., 9.2, 9.3.2

ISO/IEC 27002:2022 — 8.6, 8.14, 8.32

NIST SP-800-53 Rev. 5 — PL-8

NIST CSF 2.0 — PR.IR-04

CIS CSC v8.1-1,2

CyFun 2025-PR.IR-04

7 — Detetar:

No contexto do objetivo Detetar, pretende-se desenvolver práticas adequadas e atempadas à deteção da ocorrência de eventos segurança, ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação por via da monitorização contínua das redes e sistemas de informação e da implementação de processos de deteção.

7.1 — DE.MC-Monitorização Contínua de Segurança:

As redes e sistemas de informação são monitorizadas para identificação de eventos de segurança e verificação da eficácia das medidas de proteção aplicadas.

DE.MC-1 — As redes e sistemas de informação são monitorizados para detetar potenciais incidentes.

Descrição

A entidade efetua a monitorização da sua rede e dos seus sistemas de informação, incluindo nos seus sistemas de IA e outros, incluindo a ligação com sistemas externos dos quais depende, como serviços de computação em nuvem. A monitorização está integrada com o processo de gestão e correlação de eventos de segurança.

A monitorização e avaliação permitem que a entidade verifique a necessidade de correções, melhorias e, quando necessário, as comunique às partes interessadas relevantes.

Referências

ISO/IEC 27001:2022 — 8.1,9.1, 9.2

ISO/IEC 27002:2022 — 5.7, 5.22, 8.8, 8.12, 8.15, 8.16, 8.17, 8.21

NIST SP-800-53 Rev. 5 — SC-7

NIST CSF 2.0-DE.CM-01

CIS CSC v8.1 — 1, 8, 10, 13

CyFun 2025-DE.CM-01

DE.MC-2 — O ambiente físico é monitorizado para possibilitar a deteção de potenciais incidentes de segurança.

Descrição

A entidade garante que os seus perímetros de segurança física são monitorizados. A monitorização dos controlos de proteção física é inserida no processo de gestão e correlação de eventos de segurança, associados a categorização e tipificação específica.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1

ISO/IEC 27002:2022 — 5.7, 5.22, 7.1, 7.2, 7.4, 7.5, 7.10, 7.11, 8.3, 8.4, 8.15, 8.26, 8.31, 8.32

NIST CSF 2.0 — DE.CM-02

CyFun 2025-DE.CM-02

DE.MC-3 — A atividade do pessoal da entidade é monitorizada para se detetar potenciais incidentes.

Descrição

A monitorização das atividades do pessoal da entidade está integrada no âmbito do processo de gestão e correlação de eventos de segurança. Esta atividade tem como objetivo recolher informação que possibilite uma atuação célere da entidade, no caso de existência de algum incidente que possa ter origem na atividade de um colaborador. A entidade garante também que a informação recolhida e o seu respetivo tratamento respeitam o enquadramento jurídico aplicável.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1, Anexo A (27002)

ISO/IEC 27002:2022 — 5.7, 8.1, 8.7, 8.12, 8.15, 8.16, 8.19, 8.20, 8.23

NIST SP-800-53 Rev. 5 — SC-7

NIST CSF 2.0-DE.CM-03

CIS CSC v8.1 — 3, 8, 13, 15

CyFun 2025-DE.CM-03

DE.MC-4 — A entidade identifica e implementa mecanismos para deteção de código malicioso.

Descrição

A entidade implementa mecanismos que permitam a deteção e a prevenção de existência de atividade maliciosa nas suas redes e sistemas de informação.

Referências

ISO/IEC 27001:2022 — 8, 9.1

ISO/IEC 27002:2022 — 8.7, 8.12, 8.16

NIST SP-800-53 Rev. 5 — SC-7

CIS CSC v8.1 — 8, 10, 13

DE.MC-5 — A utilização de aplicações não autorizadas em dispositivos móveis é detetada.

Descrição

A entidade é capaz de detetar instalações indevidas de aplicações nas suas redes e sistemas de informação. A deteção deste tipo de atividades está integrada no processo de gestão e correlação de eventos de segurança da entidade.

Referências

ISO/IEC 27001:2022 — 8,1, 9.1

ISO/IEC 27002:2022 — 5.7, 5.21, 8.1, 8.16, 8.19

CIS CSC v8.1 — 8, 10

DE.MC-6 — As atividades dos prestadores de serviços externos são monitorizadas para deteção de incidentes.

Descrição

As atividades dos prestadores de serviços externos são monitorizadas pela entidade, para detetar se as suas redes e sistemas de informação são acedidos sem autorização.

Referências

ISO/IEC 27001:2022 — 8,1, 9.1

ISO/IEC 27002:2022 — 5.7, 5.22, 8.12, 8.15, 8.16, 8.30

NIST CSF 2.0 — DE.CM-06

CyFun 2025 — DE.CM-06

DE.MC-7 — O *hardware, software*, os ambientes em produção e os seus dados são monitorizados para detetar eventos potencialmente adversos.

Descrição

A entidade utiliza mecanismos de verificação que garantam a integridade de *hardware, software, firmware* e respetivos dados. Estes controlos têm como objetivo detetar manipulações não autorizadas ou erros inesperados devido a má utilização.

Referências

ISO/IEC 27001:2022 — 8.1

ISO/IEC 27002:2022 — 8.7, 8.19, 8.24, 8.26, 8.27, 8.32

NIST SP-800-53 Rev. 5 — PL-8

NIST CSF 2.0 — DE.CM-09

CIS CSC v8.1-2, 7

CyFun 2025-DE.CM-09

7.2 — DE.AE — Anomalias e Eventos:

As atividades anómalas são detetadas em tempo útil, sendo assegurada a compreensão do impacto potencial dos eventos.

DE.AE-1 — Os eventos detetados são analisados.

Descrição

A entidade implementa um processo de gestão e de correlação de eventos de segurança que:

1) Suporta o seu processo de análise e tratamento de eventos;

2) Suporta o processo de identificação de possíveis incidentes.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1, 10.2

ISO/IEC 27002:2022 — 5.7, 5.24, 5.25, 8.15

NIST SP-800-53 Rev. 5 — SI-4(2)

NIST CSF 2.0 — DE.AE-02

CIS CSC v8.1 — 1, 8, 13, 15

CyFun 2025 — DE.AE-02

DE.AE-2 — Os eventos são recolhidos e correlacionados a partir de várias fontes e sensores.

Descrição

A entidade implementa os mecanismos tecnológicos e processuais necessários, que permitam a recolha e correlação dos eventos gerados nas suas redes e sistemas de informação e nos dispositivos de segurança.

Estes eventos devem ser correlacionados entre si e, se possível, enriquecidos com fontes de conhecimento externas sobre ameaças.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1, 10.2

ISO/IEC 27002:2022 — 5.7, 5.24, 5.25, 5.28, 8.12, 8.15, 8.16, 8.17

NIST SP-800-53 Rev. 5 — AU-12(2)

NIST CSF 2.0 — DE.AE-03

CIS CSC v8.1 — 1, 3, 8, 10, 13, 15

CyFun 2025-DE.AE-03

DE.AE-3 — O impacto estimado e o âmbito dos eventos adversos detetados são compreendidos e identificados.

Descrição

A entidade efetua uma categorização e tipificação dos eventos, por forma a aferir qual o impacto dos mesmos sobre as suas redes e sistemas de informação.

A categorização dos eventos irá suportar a entidade no processo de decisão sobre que ações desencadear para cada tipo de evento. Os eventos poderão dar origem a incidentes.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1, 10.2

ISO/IEC 27002:2022 — 5.7, 5.25, 8.12

NIST CSF 2.0 — DE.AE-04

CIS CSC v8.1 — 8, 13

CyFun 2025-DE.AE-04

DE.AE-4 — As informações sobre deteções de eventos são comunicadas.

Descrição

A entidade define uma estratégia de comunicação, que mantenha informadas as partes interessadas relevantes sobre a ocorrência de eventos.

A estratégia é suportada num Plano de Comunicação que poderá ser consolidado com os outros planos de comunicação que a entidade disponha.

Referências

ISO/IEC 27001:2022 — 7.4

ISO/IEC 27002:2022 — 6.8

NIST CSF 2.0 — DE.AE-06

CyFun 2025 — DE.AE- 06

DE.AE-5 — As informações sobre ciberameaças e outras informações contextuais são integradas na análise de eventos.

Descrição

A entidade incorpora a informação sobre ameaças provenientes de fontes de conhecimento legítimas e relevantes ao contexto do evento para a sua análise. Estes dados permitem uma maior clareza relativamente a potenciais táticas, técnicas e procedimentos utilizados por potenciais atacantes possibilitando uma análise mais aprofundada e fundamentada do contexto do(s) evento(s) para a determinação duma resposta mais direcionada e eficaz.

Esta análise capacita a entidade em termos de resposta, priorização e mitigação de eventos de segurança potencialmente disruptivos às suas operações.

Referências

NIST CSF 2.0 — DE.AE-07

DE.AE-6 — Os critérios para a declaração de incidentes são definidos

Descrição

Tendo como base a tipificação e categorização dos eventos do seu sistema de gestão e correlação de eventos de segurança, a entidade define quais são os critérios que devem justificar a necessidade de abertura de incidentes.

Referências

ISO/IEC 27001:2022 — 8.1, 9.1, 10.2

ISO/IEC 27002:2022 — 5.25, 8.5, 8.12, 8.14, 8.16, 8.17

NIST CSF 2.0 — DE.AE-08

CIS CSC v8.1-8, 13

CyFun 2025-DE.AE-08

8 — Responder:

Pretende-se, com o objetivo Responder, desenvolver e implementar práticas de resposta a um incidente de cibersegurança. Estas práticas devem capacitar a entidade para a contenção dos impactos de um potencial incidente, e para mitigar o impacto do incidente, isto é, reduzir e eventualmente reverter os seus potenciais efeitos adversos, através do planeamento da resposta a incidentes, da comunicação com as partes interessadas relevantes, da análise e mitigação de incidentes e da melhoria por intermédio das lições aprendidas.

8.1 — RS.GI — Gestão de Incidentes:

Os processos de resposta e respetivos procedimentos são executados e mantidos para garantir resposta aos incidentes detetados.

RS.GI-1 — O Plano de Resposta a Incidentes é executado, em coordenação com as partes interessadas, durante ou após a ocorrência de um incidente.

Descrição

A entidade sistematiza o seu Plano de Resposta a Incidentes, em coordenação com as partes interessadas, por forma a garantir uma correta alocação de recursos (humanos, tecnológicos e processuais) na resolução do mesmo.

A resolução dos incidentes segue um processo sistematizado, no âmbito do qual é identificado um responsável pelo seu tratamento.

No processo de análise de evidências de um incidente, é relevante garantir-se a integridade das evidências analisadas e recolhidas.

Referências

ISO/IEC 27001:2022 — 8.1, 8.3, 10.2

ISO/IEC 27002:2022 — 5.26, 8.8, 8.13, 8.32

NIST SP-800-53 Rev. 5-CP -2, 2 (2)

NIST CSF 2.0 — RS.MA-01

CIS CSC v8.1 — 17

CyFun 2025-RS.MA-01

RS.GI-2 — As notificações dos sistemas de deteção são triadas e validadas.

Descrição

A entidade garante que as notificações de incidentes originados nos sistemas de deteção (internos ou externos) ou fora da entidade são analisados, categorizados e tratados de forma sistematizada.

Referências

ISO/IEC 27001:2022 — 9.1

ISO/IEC 27002:2022 — Anexo A 5.26, 8.8, 8.16

NIST CSF 2.0-RS.MA-02

CIS CSC v8.1-17

CyFun 2025 — RS.MA-02

RS.GI-3 — Os incidentes são categorizados de acordo com o Plano de Resposta a Incidentes definido.

Descrição

A entidade garante que a categorização dos incidentes é efetuada de acordo com as regras definidas no seu Plano de Resposta a Incidentes.

Referências

ISO/IEC 27001:2022 — 8.3

ISO/IEC 27002:2022 — 5.25

NIST CSF 2.0-RS.MA-03

CIS CSC v8.1-17

CyFun 2025 — RS.MA-03

RS.GI-4 — Os incidentes são escalados ou elevados conforme necessário.

Descrição

A entidade implementa um processo de coordenação e de escalonamento de incidentes, alinhado com a categorização e criticidade dos mesmos.

Referências

ISO/IEC 27001:2022 — 7.3, 7.4, 8.1, 8.3

ISO/IEC 27002:2022 — 5.6, 5.26

NIST SP-800-53 Rev.5 — IR-6

NIST CSF 2.0-RS.MA-04

CIS CSC v8.1-17

RS.GI-5 — São aplicados os critérios para iniciar a recuperação de incidentes.

Descrição

A entidade aplica os critérios definidos para dar início aos procedimentos de recuperação de incidentes, às caraterísticas conhecidas e presumíveis do incidente.

Referências

NIST CSF 2.0 — RS.MA-05

CyFun 2025-RS.MA-05

8.2 — RS.AI — Análise de Incidentes

As entidades realizam investigações para garantir uma resposta eficaz aos incidentes e para apoiar as atividades de análise forense e os procedimentos de recuperação.

RS.AI-1 — É realizada uma análise forense para determinar o que ocorreu durante um incidente e a sua causa raiz.

Descrição

A entidade cria as condições necessárias para que lhe seja possível efetuar análises forenses, no âmbito do processo de resposta a incidentes.

Referências

ISO/IEC 27001:2022 — 9.1, 9.2, 10.2

ISO/IEC 27002:2022 — 5.26, 5.28

NIST CSF 2.0 — RS.AN-03

CyFun 2025 — RS.AN-03

RS.AI-2 — As ações realizadas durante uma investigação são registadas e a integridade e proveniência dos registos são preservadas.

Descrição

A entidade garante que todas as ações realizadas durante a investigação de um incidente são documentadas e que estes registos são protegidos de forma a garantir a sua integridade. Esta preservação é essencial para a realização de análises forenses e para demonstrar que foram tomadas as diligências necessárias para uma resposta eficaz ao incidente.

Referências

NIST CSF 2.0 — RS.AN-06

CyFun 2025 — RS.AN-06

RS.AI-3 — Os dados e metadados do incidente são recolhidos, e a sua integridade e proveniência são preservadas.

Descrição

A entidade recolhe dados e metadados das investigações realizadas dos incidentes, e dos dados analisados. A entidade preserva os dados e garante a sua integridade.

Referências

NIST CSF 2.0 — RS.AN-07

CyFun 2025 — RS.AN-07

RS.AI-4 — O impacto do incidente é estimado e validado.

Descrição

No processo de categorização dos incidentes, a entidade avalia o impacto que os incidentes causam aos seus ativos e, consequentemente, à sua operação, utilizando essa avaliação para definir qual a severidade a atribuir ao incidente.

Referências

ISO/IEC 27001:2022 — 4.1, 9.1

ISO/IEC 27002:2022 — 5.7, 5.25, 5.27, 5.29, 5.30

NIST CSF 2.0- RS.AN-08

CyFun 2025 — RS.AN-08

8.3 — RS.NC-Notificação e Comunicação de Incidentes:

As atividades de resposta a incidentes são coordenadas com as partes interessadas.

RS.NC-1 — As partes interessadas internas e externas são notificadas dos incidentes.

Descrição

A entidade define canais adequados para que os incidentes sejam reportados às partes interessadas relevantes, e identifica quais as partes interessadas que devem ser informadas dos incidentes.

No processo de resposta a um incidente, a entidade identifica qual a informação que tem de ser partilhada com as partes interessadas externas.

Referências

ISO/IEC 27001:2022 — 5.3, 7.4, 10.1

ISO/IEC 27002:2022 — 5.5, 5.24, 5.36, 5.37, 6.3, 6.7, 6.8

NIST SP-800-53 Rev.5 — IR -6

NIST CSF 2.0-RS.CO-02

CIS CSC v8.1 — 17

CyFun 2025 — RS.CO-02

RS.NC-2 — Existe partilha voluntária de informação com partes interessadas externas.

Descrição

A entidade partilha, de forma voluntária, informações sobre os incidentes a grupos de interesse, para que estes possam beneficiar da partilha e melhorar tempos de resposta para identificar, detetar, conter e erradicar essas ameaças na sua circunscrição e no seu círculo de influência.

Referências

ISO/IEC 27001:2022 — 7.3, 7.4

ISO/IEC 27002:2022 — 5.5, 5.6, 5.26

NIST CSF 2.0-RS.CO-03

CIS CSC v8.1-17

8.4 — RS.MI — Mitigação:

São realizadas atividades para conter, mitigar ou resolver um incidente ocorrido.

RS.MI-1 — Os incidentes são contidos.

Descrição

A entidade define processos e procedimentos sistematizados para resolução e tratamento de incidentes que lhe permitam conter, efetivamente, os incidentes ocorridos.

Referências

ISO/IEC 27001:2022 — 6.1.3, 7.5.2, 8.3, 10.2

ISO/IEC 27002:2022 — Anexo A 5.26, 5.37, 8.7, 8.16

NIST SP-800-53 Rev.5 — IR-4

NIST CSF 2.0- RS.M1-01

CIS CSC v8.1-17

CyFun 2025 — RS.M1-01

RS.MI-2 — Os incidentes são resolvidos.

Descrição

A entidade possui processos e procedimentos sistematizados para resolução e tratamento de incidentes que lhe permitam indicar que os incidentes são, efetivamente, resolvidos.

Referências

ISO/IEC 27001:2022 — 6.1.3, 7.5.2, 8.3, 10.2

ISO/IEC 27002:2022 — 5.26, 8.7, 8.8

NIST SP-800-53 Rev.5 — IR-4

NIST CSF 2.0 — RS.MI-02

CIS CSC v8.1 — 17

9 — Recuperar:

No âmbito do objetivo Recuperar, pretende-se desenvolver e implementar práticas e manter planos de resiliência para restaurar qualquer capacidade e/ou serviço que tenha sido comprometido na sequência de um evento de cibersegurança. Estas práticas promovem a recuperação adequada das operações da entidade, para reduzir os impactos do incidente ocorrido. Entre outras, promove-se a execução de planos de continuidade de negócio, de recuperação, da execução de exercícios de simulação de situações de crise e de atualizações dos planos com vista à melhoria dos mesmos. Os controlos pertencentes a este objetivo visam assegurar a resiliência da entidade nas suas dimensões: Pessoas, Processos e Tecnologia. Os controlos tencionam que, no caso de existência de um incidente, a entidade consiga utilizar os controlos para suporte à recuperação em tempo útil da sua atividade.

9.1 — RC.PR — Plano de Recuperação:

Os processos e procedimentos de recuperação são cumpridos e mantidos para garantir a recuperação das redes e sistemas de informação afetados pelos incidentes.

RC.PR-1 — A entidade segue um plano de recuperação durante ou após um incidente.

Descrição

A entidade sistematiza o seu processo de recuperação de incidentes, por forma a garantir uma correta alocação de recursos (humanos/tecnológicos e processuais) à resolução dos mesmos. No processo de recuperação de um incidente é relevante garantir a integridade e disponibilidade dos sistemas.

Referências

ISO/IEC 27001:2022 — 8.3, 10.2ISO/IEC 27002:2022 — 5.19, 5.24, 5.26, 5.29, 8.13

NIST SP-800-53 Rev.5 — CP-2

NIST CSF 2.0- RC.PR-01

CIS CSC v8.1 — 11

CyFun 2025 — RC.RP-01

RC.PR-2 — As ações de recuperação são definidas, priorizadas e executadas.

Descrição

A entidade garante que todas as ações de recuperação de incidentes são ponderadas, planeadas e selecionadas com base no seu âmbito, prioridade e impacto para a entidade. É realizada uma abordagem estruturada e atempada para a recuperação dos sistemas, serviços e operações afetadas.

Referências

NIST CSF 2.0-RC.RP-02

CyFun 2025-RC.PR-02

RC.PR-3 — A integridade das cópias de segurança e de outros ativos de restauro é verificada antes da sua utilização.

Descrição

A entidade verifica a integridade e autenticidade das cópias de segurança e de outros ativos usados no âmbito da recuperação pós-incidentes, antes destes serem colocados novamente em operação. Esta verificação assegura que os elementos para recuperação não estão comprometidos ou corrompidos, reduzindo o risco de prolongar o tempo de recuperação ou situações de reincidência de incidentes.

Referências

NIST CSF 2.0-RC.PR-03

RC.PR-4 — A entidade considera os seus serviços críticos e a gestão dos riscos de cibersegurança para estabelecer normas operacionais pós-incidente.

Descrição

A entidade considera as conclusões retiradas de situações pós-incidente para redefinir, caso aplicável, as suas funções de missão crítica (e respetivas práticas operacionais) e postura de risco (incluindo novas vulnerabilidades identificadas pós-incidente). A entidade reflete quais as suas funções e operações mais críticas e prioritárias e pondera aumentar a sua ciberresiliência.

Referências

NIST CSF 2.0-RC.RP-04

RC.PR-5 — A integridade dos ativos restaurados é verificada, os sistemas e serviços são restaurados e o estado de normal funcionamento é confirmado.

Definição

Após um incidente a entidade verifica a integridade dos ativos que foram restaurados antes dos mesmos serem colocados em funcionamento. A entidade restaura os sistemas e serviços e confirma o estado operacional normal dos mesmos.

Referências

NIST CSF 2.0-RC.RP-05

CyFun 2025-RC.PR-05

RC.PR-6 — O fim da recuperação do incidente é documentado e declarado com base em critérios predefinidos.

Descrição

Tendo por base procedimentos e processos de gestão de incidentes, a entidade declara o fim da recuperação do incidente, baseando-se em critérios específicos. Para dar como terminada a recuperação do incidente, a entidade garante que toda a documentação relacionada com o incidente é concluída.

Referências

NIST CSF 2.0-RC.RP-06

CyFun 2025-RC.PR-06

9.2 — RC.CO — Comunicações

As atividades de recuperação são coordenadas com as partes interessadas envolvidas ou afetadas pelo incidente.

RC.CO-1 — As atividades de recuperação são comunicadas às partes interessadas, bem como aos órgãos de gestão, direção e administração.

Descrição

A entidade garante que as partes interessadas, internas e externas, são informadas quanto às atividades de recuperação e progressos no restauro para garantir o normal funcionamento dos sistemas e aplicações da entidade, após a ocorrência de incidentes.

A entidade define uma estratégia de comunicação baseada num plano de comunicação produzido para o efeito. Este poderá ser consolidado com outros planos de comunicação existentes na entidade.

Referências

ISO/IEC 27001:2022 — 5.1, 7.4, 10.1

ISO/IEC 27002:2022 — 5.6

NIST SP-800-53 Rev.5 — CP-2

NIST CSF 2.0 — RC.CO-03

CyFun 2025 — RC.CO-03

RC.CO-2 — As atualizações sobre a recuperação de incidentes são partilhadas utilizando métodos aprovados pela entidade.

Descrição

A entidade comunica o que é relevante no contexto de cibersegurança. O fluxo de comunicação deve ser controlado pela entidade para minimizar potenciais impactos na sua credibilidade e reputação.

A entidade define uma estratégia de comunicação, que se poderá basear noutras estratégias/panos de comunicação existentes na entidade.

Referências

ISO/IEC 27001:2022 — 4.2, 5.1, 5.3, 7.4

ISO/IEC 27002:2022 — 5.5, 5.6

NIST SP-800-53 Rev.5 — CP-2

NIST CSF 2.0 — RC.CO-4

CyFun 2025-RC.CO-04

ANEXO II

Matriz de risco

O CNCS elabora Matrizes de Risco que se definem, nos termos da alínea m) do artigo 2.º do Regime Jurídico da Cibersegurança, que consubstanciam o quadro referencial que estabelece os valores de risco para o conjunto de cenários de risco que recai sobre um setor e subsetor de atividade, considerando os ativos comuns, as principais ameaças e vulnerabilidades.

Como disposto no n.º 5 do artigo 26.º do Regime Jurídico da Cibersegurança, considerando o setor e subsetor de atividade e a dimensão da entidade, e a respetiva Matriz de Risco, são determinados os níveis de conformidade e as correspondentes medidas de cibersegurança mínimas e específicas a adotar pelas entidades essenciais e importantes, em três níveis, Básico, Substancial e Elevado.

Cada uma das matrizes de risco associadas a um setor ou subsetor, dos elencados nos Anexo I e II do Regime Jurídico da Cibersegurança, produz um valor numérico a utilizar pelas entidades na identificação do seu nível de conformidade. Este valor é estabelecido com base no nível de risco associado ao setor ou subsetor a que a entidade pertence, juntamente com a sua dimensão e com a importância do setor ou subsetor, dependendo da sua criticidade, como definido pelo Regime Jurídico da Cibersegurança.

1 — Matrizes de Risco:

As matrizes procuram descrever o nível de risco num determinado setor com base na correlação entre cenários de risco e tipos de atores tendo em conta vários fatores como o histórico de incidentes conhecidos no setor a nível nacional e internacional.

2 — Cenários e Cálculos:

Para cada um dos cenários dominantes (cenários de risco e atores dominantes) determinou-se o valor de risco. Estes valores são em parte resultado do produto da probabilidade e do impacto em cada um destes cenários de risco dominantes. De modo a garantir a proporcionalidade na aplicação dos níveis de conformidade, os valores de risco associados aos cenários de risco dominantes são ponderados pela dimensão da entidade, se a entidade é Grande (G), Média (M) ou Pequena (P) — e pela importância do setor em que se insere. A determinação do valor de risco segue a seguinte fórmula:

$$\text{valor de risco}_{\text{cenário de risco, ator}} = Probabilidade \times Impacto \times \left(\frac{Dimensão}{3}\right) \times \text{Tipo de setor}$$

A probabilidade e o impacto seguem uma escala que vai de 1 (Muito baixo/a) a 5 (Muito alto/a).

Dimensão	**Critério**	**Valor da ponderação**
Grande (**G**)	Entidade emprega mais de 250 pessoas; **OU** cujo volume de negócios anual excede 50 milhões de euros; **OU** cujo balanço total excede 43 milhões de euros	**3**, *i.e.* $\frac{3}{3}$
Média (**M**)	Valores entre as categorias Grande (G) e Pequena (P)	**2**, *i.e.* $\frac{2}{3}$
Pequena (**P**)	Quando se trate de **entidade pública** que empregue menos de 50 pessoas; **OU**, nos **restantes casos** quando a entidade empregue menos de 50 pessoas, **E** cujo volume de negócios anual não excede 10 milhões de euros, **E** cujo balanço total anual não excede 10 milhões de euros	**1**, *i.e.* $\frac{1}{3}$

O tipo de setor é definido com base no setor da entidade definido pelo Regime Jurídico da Cibersegurança, em concreto:

Tipo de setor	Critério	Valor da ponderação
Setores de Importância Crítica	Setores Anexo I Regime Jurídico da Cibersegurança	1.5
Outros Setores Críticos	Setores Anexo II Regime Jurídico da Cibersegurança	1

Para aferir o nível de conformidade, o valor de risco é calculado para cada cenário de risco e ator, e os valores são somados (*total*). O nível de conformidade será selecionado com base no valor desta soma.

Nível de conformidade	Critério
Básico	$0 \leq total \leq 99$
Substancial	$100 \leq total \leq 199$
Elevado	$200 \leq total \leq 1200$

O CNCS utilizou os níveis de impacto definidos em baixo para os cálculos da Matriz de Risco.

Nível	Impacto
5	Evento que gera impacto sobre toda a entidade ou representa perda de disponibilidade, confidencialidade e/ou integridade causando prejuízos de forma generalizada, inviabilizando todas as funções primárias ou proporcionando perceção negativa e/ou causa efeitos adversos muito graves ou catastróficos a indivíduos terceiros, outras empresas ou o País.
4	Evento que gera impacto sobre vários grupos ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções
	primárias de trabalho de múltiplas áreas da organização e/ou causa efeitos adversos graves a indivíduos terceiros, outras empresas ou o País.
3	Evento que gera impacto sobre um grupo relevante dentro da entidade ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho e/ou causa efeitos adversos a indivíduos terceiros, outras empresas ou o País.
2	Evento que gera impacto sobre um pequeno grupo dentro da entidade ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções secundárias de trabalho, não sendo bastante para intervir nas funções principais, e/ou causar efeitos adversos limitados a indivíduos terceiros, outras empresas ou o País.
1	Evento que gera impacto sobre apenas uma pessoa ou representa perda de disponibilidade, confidencialidade e/ou integridade que não necessita de intervenção ou paralisação imediata.

A definição de probabilidade utilizada pela matriz de risco incorporou componentes quantitativas, qualitativas e informação referente ao histórico do setor. Em particular, a probabilidade de um determinado incidente é calculada com base na seguinte média ponderada:

$$\text{Pr[Cenário,Ator]} = Pr_{a\ priori}\ 0.5 \ + \ Pr_{CERT.PT}0.25 \ + \ Pr_{peritos}0.25$$

A probabilidade *a priori* ($Pr_{apriori_i}$) refere-se a uma avaliação da probabilidade baseada no histórico de incidentes com impacto relevante nacionais ou internacionais associados ao cenário de risco, dependendo sobretudo da proximidade temporal e geográfica dos incidentes identificados.

Nos casos em que não foram identificados quaisquer incidentes de impacto relevante no setor, utilizou-se a seguinte média ponderada:

$$\text{Pr[Cenário,Ator]} = Pr_{CERT.PT}0.4 \ + \ Pr_{peritos}0.6$$

A probabilidade CERT.PT ($Pr_{CERT.PT}$) refere-se à soma da proporção dos tipos de incidentes, seguindo a Taxonomia Comum da Rede Nacional de CSIRTs (pode ser consultado no sítio da internet do CNCS — Classificação de Incidentes — Taxonomia), associados ao cenário de risco em questão, segundo o levantamento de casos relevantes, em Portugal no ano transato.

Para a integração da probabilidade segundo os peritos ($Pr_{peritos}$), consultaram-se várias entidades representativas de cada um dos setores e parceiros, sendo que o valor final representa uma agregação destas contribuições.

ANEXO III

Medidas de Cibersegurança Mínimas para Entidades Essenciais e Importantes

Básico

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
GR.CO-3 — Os requisitos legais, regulamentares e contratuais para a cibersegurança são compreendidos e geridos.	Os requisitos legais e regulamentares relativos à cibersegurança devem ser identificados e aplicados.	Evidência da gestão quotidiana da entidade que demonstre o cumprimento dos requisitos e obrigações legais de cibersegurança aplicáveis à entidade.
GR.CO-4 — Os serviços críticos da entidade dos quais as partes interessadas externas dependem são identificados e comunicados.	Devem ser identificados e documentados os serviços críticos, dos quais as partes interessadas externas dependem.	Registo documentado da identificação dos serviços críticos dos quais as partes interessadas externas dependem.
GR.CO-5 — Os requisitos de resiliência necessários para suportar a prestação de serviços críticos são definidos.	Os requisitos necessários para garantir o suporte de serviços críticos devem ser identificados e registados.	Registo documentando da identificação dos requisitos de resiliência necessários para garantir o suporte dos serviços críticos.
GR.CO-6 — Os serviços críticos externos, dos quais a entidade depende, são identificados e comunicados.	Devem ser identificados, documentados, classificados e priorizados os serviços críticos externos dos quais a entidade depende, numa lógica de compreensão do seu papel na cadeia de abastecimento. A entidade deve comunicar às partes interessadas esta identificação, respeitando sempre o princípio da necessidade de saber. A entidade deve incluir no processo de gestão dos riscos esta identificação.	Registo da identificação, e da comunicação dos serviços críticos externos dos quais a entidade depende. Registo do processo de gestão dos riscos que contempla os serviços críticos externos dos quais a entidade depende, incluindo a definição de critérios para a classificação e priorização destes serviços.
GR.GR-2 — Os processos de gestão dos riscos de cibersegurança estão incluídos na estratégia transversal da gestão de riscos da entidade.	A entidade deve identificar, aprovar, gerir e manter atualizados os processos de gestão dos riscos de cibersegurança.	Evidência da gestão quotidiana que demonstre a implementação das várias fases de gestão de riscos da cibersegurança.
GR.FR-1 — Os órgãos de gestão, direção e administração compreendem as suas funções e responsabilidades, e promovem uma cultura de cibersegurança, ética e de melhoria contínua.	Os órgãos de gestão, direção e administração devem disponibilizar os recursos necessários para a melhoria contínua da cibersegurança.	Plano de Melhoria Contínua de Cibersegurança com medidas, prazos e recursos a afetar, aprovado pelos órgãos de gestão, direção e administração.
GR.FR-4 — A cibersegurança é contemplada nos processos de gestão de recursos humanos.	A entidade deve definir uma Política de Uso Aceitável, que seja abrangente para toda a entidade e que defina as regras para a utilização segura e responsável dos seus ativos. A entidade deve disponibilizar a Política de Uso Aceitável ao pessoal aquando da sua entrada, sensibilizando-os para garantir o cumprimento da mesma.	Política de Uso Aceitável aprovada e implementada e registo da tomada de conhecimento pelo pessoal aquando da sua entrada.
GR.PP-1 — As Políticas para a gestão de Cibersegurança, incluindo a Política de Cibersegurança, são definidas com base no contexto organizacional, na estratégia de cibersegurança e nas prioridades da entidade.	A entidade deve definir, documentar e atualizar a Política de Cibersegurança aprovada pelos órgãos de gestão, direção e administração, que inclua a identificação e atribuição de funções e responsabilidades em cibersegurança. A entidade deve divulgar a política internamente.	Política de Cibersegurança, aprovada pelos órgãos de gestão, direção e administração. Registos da comunicação interna da Política de Cibersegurança.
GR.PP-2 — O Plano de Resposta a Incidentes é definido, comunicado, mantido e melhorado.	A entidade deve definir, aprovar, implementar e atualizar o Plano de Resposta a Incidentes com a devida atribuição e identificação de funções e responsabilidades.	Plano de Resposta a Incidentes aprovado e implementado e devidamente atualizado.
GR.CA-7 — A entidade avalia os riscos de cibersegurança da cadeia de abastecimento.	A entidade deve efetuar avaliações do risco da cadeia de abastecimento pelo menos uma vez por ano ou sempre que relevante.	Registo documentado das avaliações do risco da cadeia de abastecimento.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
ID.GA-1 — Os equipamentos e os demais recursos físicos geridos ou detidos pela entidade são inventariados.	Os equipamentos e os demais recursos físicos geridos ou detidos pela entidade são inventariados. O inventário deve ser documentado e atualizado.	Inventário atualizado de equipamentos e recursos físicos.
ID.GA-2 — Os recursos lógicos que suportam os processos dos serviços da entidade são inventariados.	O inventário de recursos lógicos deve refletir as plataformas de *software* e aplicações que são geridos ou detidos pela entidade. O inventário deve ser documentado e atualizado.	Inventário atualizado de recursos lógicos.
ID.GA-4 — Os serviços prestados por fornecedores são inventariados.	A entidade deve incluir no seu inventário de ativos os serviços prestados por fornecedores que utiliza e dos quais depende.	Inventário de ativos que inclua os serviços prestados por fornecedores que a entidade utiliza e depende.
ID.GA-5 — Os ativos são classificados de acordo com a sua criticidade.	Os ativos devem ser classificados de acordo com a sua criticidade e valor dos mesmos.	Registo da classificação dos ativos de acordo com a sua criticidade e valor.
ID.GA-7 — Sistemas, *hardware*, *software*, serviços e dados são geridos ao longo dos seus ciclos de vida.	A entidade deve realizar atualizações de segurança dos seus sistemas regularmente e deve aplicar *patches* adequados nas suas aplicações e sistemas, sempre que possível. Na eventual impossibilidade da aplicação de atualizações de segurança, a entidade deve aplicar controlos compensatórios em função do risco A entidade deve garantir a manutenção periódica dos equipamentos e demais recursos físicos existentes. A entidade aprova as ações de manutenção de *software* e *hardware*.	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 manutenção de *software* e *hardware*.
ID.AR-1 — As vulnerabilidades dos ativos são identificadas e documentadas com base na metodologia definida.	A entidade deve identificar vulnerabilidades dos seus ativos.	Registo documentado das vulnerabilidades identificadas
ID.AR-4 — São identificados e registados potenciais impactos e as respetivas probabilidades de ameaças.	A entidade deve determinar e registar, no processo de gestão dos riscos, a probabilidade de concretização de ameaças e avaliar os respetivos potenciais impactos.	Critérios para determinar a probabilidade das ameaças e para a avaliar os potenciais impactos das mesmas.
ID.AR-5 — A entidade avalia os riscos identificados.	A entidade deve realizar 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 utilizam, incluindo os ativos que garantam a prestação dos serviços críticos.	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
ID.AR-6 — A entidade garante que as respostas aos riscos são identificadas e priorizadas.	A entidade implementa controlos de segurança para os riscos identificados.	Evidência técnica da implementação de controlos de segurança para os riscos identificados.
ID.AR-7 — A entidade define processos para receber informação, analisar e responder a vulnerabilidades provenientes de fontes internas e externas.	A entidade deve tratar as vulnerabilidades que tenha conhecimento.	Registo da identificação e de tratamento das vulnerabilidades.
ID.MC-3 — As melhorias são identificadas a partir da execução de processos, procedimentos e atividades operacionais.	A entidade deve efetuar avaliações pós-incidentes para identificar as lições aprendidas e, consequentemente, melhorar os processos/procedimentos/tecn ologias para reforçar a sua ciber-resiliência.	Registo documentado das avaliações pósincidentes, com identificação de lições aprendidas, definição e implementação de melhorias.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.GA-1 — Os ciclos de vida de gestão de identidades são definidos.	As identidades e credenciais de dispositivos, serviços e utilizadores devem ser geridas. A entidade deverá implementar uma Política de Palavra-passe e uma Política de Gestão de Identidades, Autenticação e Controlo de Acessos.	Evidência técnica da gestão de identidades e respetivas credenciais de dispositivos, serviços e utilizadores. Política de Gestão de Identidades, Autenticação e Controlo de Acessos aprovada e implementada. Política de Palavra-passe aprovada e implementada.
PR.GA-3 — São definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação.	A entidade deve implementar autenticação multifator (MFA) nos acessos remotos e contas privilegiadas.	Evidência técnica da implementação de autenticação multifator (MFA) nos acessos remotos e contas privilegiadas.
PR.GA-5 — A entidade aplica na sua gestão de acessos, os princípios do menor privilégio e da segregação de funções.	As permissões de acesso dos utilizadores aos sistemas da entidade devem ser definidas e geridas, em conformidade com a Política de Gestão de Identidades, Autenticação e Controlo de Acessos existente, sendo que as permissões de acesso devem ser revistas periodicamente. Os acessos aos dados, informações e tecnologias críticas, devem ser identificados de acordo com o princípio do menor privilégio. A entidade deve garantir que não são atribuídos privilégios de administração por defeito.	Registo documentado da definição e evidência técnica da gestão de acessos dos utilizadores aos sistemas da entidade em conformidade com a 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.
PR.GA-6 — Os controlos de acesso físico a ativos da entidade são geridos, monitorizados e aplicados em função do risco.	A entidade deve definir quais são as zonas de acesso restrito que alojam informação confidencial, e/ou redes e/ou sistemas de informação e deve protegê-las.	Evidência da definição das zonas de acesso restrito. Evidência da aplicação de medidas para proteção das zonas de acesso restrito.
PR.GA-7 — A entidade gere os seus acessos remotos.	A entidade deve definir e documentar a lista de utilizadores e dispositivos com permissão para aceder remotamente às suas redes e sistemas. A entidade deve implementar controlos de segurança adequados para proteger as suas redes e sistemas quando acedidos remotamente.	Registo documentado dos utilizadores e dispositivos autorizados a aceder remotamente a redes e sistemas da entidade. Evidência técnica da implementação de controlos de segurança para proteção adequada de ligações remotas aos sistemas da entidade.
PR.FC-1 — Todo o pessoal é sensibilizado e formado em matérias de cibersegurança.	A entidade deve garantir que o pessoal é sensibilizado em matéria de cibersegurança e que os mesmos participam em ações de sensibilização periodicamente.	Registo documentado da participação do pessoal em ações de sensibilização em matéria de cibersegurança.
PR.FC-2 — O pessoal com funções especializadas em cibersegurança e os órgãos de gestão, direção e administração recebem formação adequada para o exercício das suas funções.	A entidade deve assegurar que os membros dos órgãos de gestão, direção e administração completam formações periódicas em matéria de cibersegurança.	Registo documentado da participação periódica dos membros dos órgãos de gestão, direção e administração em ações de formação em matéria de cibersegurança.
PR.SD-2 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados em trânsito.	A entidade deve implementar mecanismos criptográficos para o acesso aos dados e informação considerada crítica/ sensível.	Evidência técnica da implementação de mecanismos criptográficos para os dados em trânsito.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.SD-5 — São realizadas, mantidas e testadas cópias de segurança dos dados da entidade.	Devem ser realizadas regularmente cópias de segurança de dados críticos para garantir a continuidade de negócio. A entidade deve armazenar as cópias de segurança num sistema distinto do dispositivo no qual os dados originais estão alojados.	Evidência técnica da execução regular de cópias de segurança, e armazenamento num sistema distinto do dispositivo no qual os dados originais estão alojados.
PR.SP-1 — É criada e mantida uma configuração base de redes e sistemas de informação que incorpora os princípios de segurança.	A entidade deve manter uma configuração base de redes e sistemas de informação que incorpora os princípios de segurança.	Registo da configuração base aplicada nos diferentes sistemas e componentes de rede da entidade.
PR.SP-2 — Os *logs* de sistemas e o histórico de atividades são documentados, implementados e revistos.	Os *logs* dos ativos devem ser recolhidos, guardados, protegidos e revistos regularmente. A definição da duração do armazenamento dos *logs* deve ter em conta a análise do risco dos sistemas e das atividades e o princípio da proporcionalidade.	Evidência técnica da recolha, armazenamento e análise regular dos *logs* dos sistemas da entidade.
PR.SP-3 — A instalação e execução de *software* não autorizado são impedidas.	A entidade deve impedir a instalação e execução de *software* não autorizado. A entidade deve implementar tecnologias de filtro de rede, *e-mail* e *web*.	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*.
PR.RI-1 — A entidade protege a integridade das redes de comunicações.	As *firewalls* devem ser instaladas, configuradas e as suas regras permanentemente atualizadas em todas as redes da entidade. A entidade deve proteger a integridade da rede dos seus sistemas críticos através da incorporação da segmentação e segregação da rede. Todos os pontos de acesso a redes sem fio da entidade devem ser configurados de forma segura, geridos e monitorizados de forma a prevenir acessos não autorizados e assegurar a integridade da rede.	Evidência técnica da instalação e ativação de *firewalls* em todas as redes da entidade. Evidência técnica da segmentação e segregação das redes. Evidência técnica da configuração segura dos pontos de acesso a redes sem fio da entidade, da sua gestão e monitorização.
DE.MC-1 — As redes e sistemas de informação são monitorizados para detetar potenciais incidentes.	Devem ser corretamente configuradas, instaladas e atualizadas soluções de monitorização de tráfego da rede, nomeadamente, através de *firewalls* e proteção contra atividade não autorizada e potencialmente maliciosa.	Evidência técnica de instalação, configuração e atualização de soluções de monitorização de tráfego da rede e proteção contra atividade não autorizada e potencialmente maliciosa.
DE.MC-4 — A entidade identifica e implementa mecanismos para deteção de atividade maliciosa.	A entidade deve instalar e atualizar ferramentas de monitorização de postos cliente (*endpoints*) por forma a detetar atividade maliciosa	Evidência técnica da instalação de ferramentas de monitorização de postos cliente, e da sua atualização.
DE.MC-5 — A utilização de aplicações não autorizadas em dispositivos móveis é detetada.	A entidade deve definir uma lista de aplicações aprovadas para uso em ativos corporativos. Todas as exceções devem ser aprovadas e documentadas. Em caso de utilização de dispositivos pessoais para fins profissionais, a entidade deve definir, na sua Política de Uso Aceitável, critérios a utilização de dispositivos pessoais no trabalho (BYOD).	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.
DE.AE-2 — Os eventos são recolhidos e correlacionados a partir de várias fontes e sensores	A funcionalidade de recolha de eventos de segurança dos sistemas e aplicações deve estar ativa, e esta informação deve ser analisada e preservada através de cópias de segurança, durante um período previamente definido pela entidade.	Evidência técnica da recolha sistemática de eventos. Evidência técnica da preservação da informação da análise de eventos através de cópias de segurança.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
DE.AE-6 — Os critérios para a declaração de incidentes são definidos.	A entidade deve definir os limites a considerar quando um evento, conjunto de eventos ou correlação de múltiplos eventos, configura um incidente.	Registo da definição dos limites que determinam quando um evento ou correlação de múltiplos eventos configura um incidente.
RS.GI-1 — O Plano de Resposta a Incidentes é executado, em coordenação com as partes interessadas, durante ou após a ocorrência de um incidente.	O Plano de Resposta a Incidentes deve incluir as funções, as responsabilidades e as competências dos envolvidos e deve ser executado durante ou logo após um incidente.	Registo da inclusão das funções, responsabilidades e competências dos envolvidos no Plano de Resposta a Incidentes.
RS.NC-1 — As partes interessadas são informadas dos incidentes.	A entidade deve comunicar ao seu pessoal, de forma clara e simples, a ocorrência de incidentes. Os incidentes com impacto significativo devem ser notificados à autoridade competente nos termos do Regime Jurídico da Cibersegurança.	Evidência da partilha de informações quanto à ocorrência de incidentes.
RC.PR-1 — A entidade segue um plano de recuperação durante ou após um incidente.	Devem ser desenvolvidos e executados procedimentos de recuperação de incidentes, de acordo com o Plano de Resposta a Incidentes.	Registo das ações tomadas em resposta a incidentes.
RC.PR-3 — A integridade das cópias de segurança e de outros ativos de restauro é verificada antes da sua utilização.	A integridade das cópias de segurança deve ser verificada antes da sua utilização no âmbito da recuperação pós incidente.	Registo das ações tomadas em resposta a incidentes, que inclua a verificação da integridade das cópias de segurança.

Substancial

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
GR.CO-1 — A missão, visão, estratégia de gestão dos riscos e objetivos da entidade são definidos e comunicados.	A missão, visão, estratégia de gestão dos riscos e objetivos da entidade devem ser definidas, comunicadas e priorizadas. A entidade deve, inclusive, definir as prioridades em matéria de cibersegurança.	Registo documentado da missão, visão, estratégia de gestão do risco e objetivos no âmbito da cibersegurança e respetivas prioridades.
GR.CO-4 — Os serviços críticos da entidade dos quais as partes interessadas dependem são geridos e comunicados.	Os serviços críticos da entidade, dos quais as partes interessadas dependem, devem ser classificados, priorizados e integrados no processo de gestão dos riscos.	Registo do processo de gestão dos riscos que contempla os serviços críticos das quais as partes interessadas externas dependem, incluindo a definição de critérios para a classificação e priorização dos serviços críticos.
GR.CO-5 — Os requisitos de resiliência necessários para suportar a prestação de serviços críticos são definidos.	A entidade deve implementar mecanismos de redundância para garantir a disponibilidade dos serviços críticos. A entidade deve definir, aprovar e implementar um Plano de Continuidade de Negócio contendo planos e tempos de resposta para a recuperação dos serviços críticos e respetivos processos.	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.
GR.GR-1 — O apetite e a tolerância ao risco da entidade são definidos, aprovados, comunicados e revistos regularmente.	A entidade deve definir, registar, aprovar, rever regularmente e comunicar internamente, o seu apetite e tolerância ao risco.	Registo documentado e aprovado da definição do apetite e tolerância ao risco. Registo da sua comunicação às partes interessadas internas.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
GR.GR-2 — Os processos de gestão dos riscos de cibersegurança estão incluídos na estratégia transversal de gestão dos riscos da entidade.	A entidade deve garantir que os seus processos de gestão dos riscos de cibersegurança estão incluídos na estratégia transversal da gestão dos riscos da entidade.	Evidência de gestão quotidiana que demonstre a implementação das várias fases de gestão de risco da cibersegurança nos processos transversais de gestão dos riscos da entidade.
GR.GR-3 — A entidade define a sua estratégia de tratamento do risco.	A entidade deve definir e comunicar às partes interessadas a sua estratégia de tratamento do risco, respeitando sempre o princípio da necessidade de saber.	Registo documentado da estratégia de tratamento do risco e da sua comunicação às partes interessadas.
GR.GR-4 — A entidade estabelece um canal de comunicação interno para partilha de riscos de cibersegurança.	A entidade deve estabelecer 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.	Canal interno de comunicação usado para a partilha de riscos de cibersegurança.
GR.GR-5 — A entidade define uma Política de Gestão dos Riscos de Cibersegurança a qual prevê uma metodologia para a gestão dos riscos de cibersegurança.	A entidade define uma metodologia para a gestão dos riscos de cibersegurança que permita identificar, registar, calcular, categorizar e priorizar os riscos de cibersegurança.	Registo da metodologia de gestão dos riscos de cibersegurança.
GR.FR-2 — São atribuídos recursos adequados e proporcionais à estratégia de gestão do risco de cibersegurança, às funções, responsabilidades e políticas de cibersegurança da entidade.	A entidade deve alocar recursos suficientes e proporcionais à gestão do risco de cibersegurança, às funções, responsabilidades e políticas da entidade.	Registo do planeamento das atividades em matéria de cibersegurança a curto ou médio prazo, e evidência da gestão quotidiana que demonstre a alocação dos recursos para a gestão do risco de cibersegurança.
GR.FR-3 — As funções, responsabilidades e autoridades em matéria de cibersegurança são definidas e comunicadas ao pessoal, fornecedores e partes interessadas.	As funções, responsabilidades e autoridades de cibersegurança dentro da entidade devem ser documentadas, aprovadas, comunicadas, alinhadas com as funções internas e entidades externas, e atualizadas.	Registo documentado e aprovado das funções, responsabilidades e autoridades e da sua comunicação às partes interessadas.
GR.FR-4 — A cibersegurança é contemplada nos processos de gestão de recursos humanos.	A entidade deve desenvolver e manter medidas de cibersegurança associadas à gestão dos recursos humanos, aplicável no recrutamento, durante o contrato e após o seu término.	Registo das medidas de cibersegurança para a gestão de recursos humanos, desde a entrada até à saída do pessoal.
GR.PP-1 — As Políticas para a gestão de Cibersegurança, incluindo a Política de Cibersegurança, são definidas com base no contexto organizacional, na estratégia de cibersegurança e nas prioridades da entidade.	A entidade deve definir, aprovar e implementar uma Política de Classificação e Gestão de Dados.	Política de Classificação e Gestão de Dados aprovada e implementada.
GR.PP-3 — O Plano de Recuperação de Desastres é definido, comunicado, mantido e melhorado.	A entidade deve definir, aprovar, implementar e atualizar o Plano de Recuperação de Desastres com a devida atribuição e identificação de funções e responsabilidades.	Plano de Recuperação de Desastres aprovado implementado, e devidamente atualizado.
GR.CA-3 — Os processos de gestão dos riscos de cibersegurança da cadeia de abastecimento estão incluídos nos processos transversais de cibersegurança e de gestão dos riscos da entidade.	A entidade deve identificar, aprovar, gerir e manter atualizados, sempre que ocorram alterações, os riscos de cibersegurança associados à cadeia de abastecimento. A entidade deve incluir os processos de gestão dos riscos de cibersegurança da cadeia de abastecimento nos seus processos transversais de cibersegurança e de gestão dos riscos da entidade.	Registo documentado da identificação, aprovação, gestão e atualização dos riscos de cibersegurança associados à cadeia de abastecimento.
GR.CA-5 — A entidade define e integra nos contratos e outros acordos com fornecedores os requisitos para gerir os riscos de cibersegurança da cadeia de abastecimento.	A entidade deve definir e integrar requisitos de cibersegurança e os meios de partilha de informação sensível nos contratos e outros acordos a definir com fornecedores.	Modelos de contratos/acordos contendo cláusulas específicas de requisitos de cibersegurança.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
GR.CA-7 — A entidade avalia os riscos de cibersegurança da cadeia de abastecimento.	A entidade deve mitigar os riscos identificados durante o processo de avaliação 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.
GR.CA-8 — O Plano de Resposta a Incidentes e o Plano de Recuperação de Desastres são testados com o acompanhamento dos fornecedores.	A entidade deve identificar o pessoal-chave dos fornecedores a incluir nas atividades previstas nos Plano de Resposta a Incidentes e Plano de Recuperação de Desastres.	Registo da inclusão do pessoal-chave dos fornecedores nas atividades previstas nos Plano de Resposta a Incidentes e no Plano de Recuperação de Desastres.
ID.GA-3 — As redes e fluxos de comunicação são mapeados.	A entidade deve criar diagramas de rede e sistemas que demonstrem a topologia da sua rede. A entidade deve mapear os fluxos de comunicação entre os seus sistemas internos.	Diagramas de rede e sistemas e de fluxos de comunicação internos
ID.GA-7 — Sistemas, *hardware, software*, serviços e dados são geridos ao longo dos seus ciclos de vida.	A entidade deve definir, aprovar e implementar uma Política de Gestão do Ciclo de Vida de Ativos para garantir que são implementadas medidas necessárias para gerir a perda, má utilização, dano ou roubo de ativos. A entidade deve planear, executar e documentar a manutenção preventiva e as reparações dos componentes críticos do seu sistema, de acordo com a Política de Gestão do Ciclo de Vida de Ativos.	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.
ID.GA-8 — Os dados são destruídos de acordo com a Política de Classificação e Gestão de Dados definida.	A entidade deve garantir que os dados dos seus sistemas críticos e as informações sensíveis são destruídos de acordo com a Política de Classificação e Gestão de Dados definida e aprovada.	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.
ID.AR-1 — As vulnerabilidades dos ativos são identificadas e documentadas com base na metodologia definida.	A entidade deve aprovar e implementar uma Política de Monitorização, Identificação e Documentação das Vulnerabilidades dos seus sistemas críticos e implementar a mesma através da definição de um processo, que esteja incluído na Política.	Política de Monitorização, Identificação e Documentação das Vulnerabilidades aprovada e implementada.
ID.AR-5 — A entidade avalia os riscos identificados.	As avaliações do risco devem ser conduzidas, documentadas e atualizadas de forma contínua, com base nos critérios definidos na sua metodologia de gestão do risco.	Registo documentado da avaliação do risco e respetiva atualização, tendo por base os critérios definidos na metodologia.
ID.AR-6 — A entidade garante que as respostas aos riscos são identificadas e priorizadas.	As respostas aos riscos devem ser identificadas, priorizadas, planeadas, acompanhadas e comunicadas.	Registo da identificação, priorização, planeamento, acompanhamento e comunicação das respostas aos riscos.
ID.AR-7 — A entidade define processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas.	A entidade deve implementar processos de gestão de vulnerabilidades que incluam processamento, análise e correção de vulnerabilidades de fontes internas e externas. O processo de gestão de vulnerabilidades da entidade deve estar alinhado com a Instrução Técnica de Divulgação Coordenada de 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.
ID.MC-3 — As melhorias são identificadas a partir da avaliação e monitorização de processos, procedimentos e atividades operacionais.	A entidade deve incluir nos seus planos e processos de gestão de cibersegurança, as melhorias derivadas da monitorização e avaliação periódicas, das medidas, controlos e processos de cibersegurança.	Registo das melhorias derivadas da monitorização e avaliação periódicas nos seus planos e processos de gestão de cibersegurança.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.GA-1 — Os ciclos de vida de gestão de identidades são definidos.	As credenciais dos sistemas devem ser 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. Os sistemas críticos da entidade devem ser monitorizados quanto à utilização atípica de credenciais dos sistemas.	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.
PR.GA-2 — A entidade verifica a identidade dos utilizadores, vinculando-a às respetivas credenciais.	A entidade deve implementar 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 entidade.	Registo da implementação de procedimentos de verificação da identidade dos utilizadores, antes da emissão de credenciais.
PR.GA-3 — São definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação.	A entidade deve realizar uma avaliação do risco das comunicações entre sistemas críticos. Como resultado da avaliação, a entidade deve aplicar mecanismos de autenticação aos utilizadores, dispositivos e outros ativos, adequados e proporcionais ao risco identificado. A entidade deve implementar autenticação multifator (MFA) nos seus sistemas críticos.	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.
PR.GA-5 — A entidade aplica na sua gestão de acessos, os princípios do menor privilégio e da segregação de funções	A entidade deve implementar mecanismos para apoiar a gestão de acessos aos seus sistemas críticos, incluindo a desativação, a monitorização, a comunicação e a eliminação de contas de utilizadores. A entidade deve aplicar o princípio de segregação de funções na gestão de permissões de acesso. A entidade deve gerir, documentar e rever regularmente as atribuições de privilégios elevados a utilizadores.	Evidência técnica da implementação de mecanismos para apoiar a gestão do ciclo de vida dos acessos aos sistemas críticos. 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.
PR.GA-6 — Os controlos de acesso físico a ativos da entidade são geridos, monitorizados e aplicados em função do risco.	O acesso físico a zonas de acesso restrito da entidade deve ser monitorizado. O acesso físico a zonas de acesso restrito deve incluir medidas para situações de emergência.	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.
PR.GA-7 — A entidade gere os seus acessos remotos.	A entidade deve definir e implementar de acordo com a Política de Gestão de Identidades, Autenticação e Controlo de Acessos, as restrições de utilização, os requisitos de ligação e as autorizações de acesso remoto ao ambiente dos sistemas críticos da entidade. As ações realizadas no âmbito de manutenções remotas devem ser monitorizadas para análise de potenciais eventos que coloquem em causa a segurança dos sistemas. Os acessos atribuídos para manutenções remotas devem ser revogados assim que deixarem de ser necessários.	Evidencia técnica da implementação de medidas de segurança para garantir que os acessos remotos ao ambiente dos sistemas críticos da entidade cumprem as restrições de utilização, os requisitos de ligação e as autorizações definidas. Evidencia técnica da monitorização das manutenções remotas, e dos acessos autorizados, atribuídos, e revogados após a conclusão da manutenção.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.FC-1 — Todo o pessoal é sensibilizado e formado em matérias de cibersegurança.	A entidade deve realizar ações de formação periódicas para que o pessoal compreenda as suas funções, responsabilidades e prioridades específicas durante um incidente de cibersegurança, incluindo quais as ações que devem seguir para responder de forma eficaz. A entidade deve incluir a sensibilização e a comunicação de ameaças internas na sua formação em cibersegurança, de forma a ajudar o pessoal a reconhecer e responder a potenciais ameaças internas.	Registo documentado da participação periódica do pessoal em ações de formação em matérias de cibersegurança.
PR.FC-2 — O pessoal com funções especializadas em cibersegurança e os órgãos de gestão, direção e administração recebem formação adequada para o exercício das suas funções.	A entidade deve definir, implementar e atualizar periodicamente um plano estruturado de ações de formação em matéria de cibersegurança para o pessoal com funções especializadas em cibersegurança.	Registo documentado da definição do Plano de sensibilização e formação para pessoal com funções especializadas em cibersegurança, e da respetiva execução do mesmo.
PR.SD-1 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados armazenados.	A entidade deve implementar controlos de verificação da integridade da informação, do *software* e *firmware* para detetar alterações não autorizadas aos dados por si armazenados. A restrição da utilização de suportes de armazenamento amovíveis deve ser assegurada em conformidade com a Política de Uso Aceitável.	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.
PR.SD-5 — São realizadas, mantidas e testadas cópias de segurança dos dados da entidade.	Deve ser definida, aprovada e implementada uma Política de Cópias de Segurança que inclua regras internas formais para a realização das cópias de segurança. A entidade deve verificar e testar regularmente a disponibilidade e integridade das cópias de segurança, de forma independente ao ambiente protegido. Deve ser definido e implementado um esquema de redundância aplicado às cópias de segurança da entidade. As cópias de segurança devem ser mantidas em locais distintos e protegidas segundo os mesmos mecanismos de segurança.	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.
PR.SP-1 — É criada e mantida uma configuração base de redes e sistemas de informação que incorpora os princípios de segurança.	A entidade deve desenvolver, documentar e manter atualizada uma configuração base de segurança das suas redes e sistemas de informação.	Evidencia técnica das configurações base de segurança das redes e sistemas de informação.
PR.SP-2 — Os *logs* de sistemas e o histórico de atividades são documentados, implementados e revistos.	Os *logs* dos ativos devem ser sincronizados utilizando uma fonte interna de relógio sincronizada com uma fonte de relógio oficial.	Evidencia técnica da sincronização temporal dos *logs* dos ativos.
PR.SP-4 — É implementado um ciclo de vida de desenvolvimento seguro de *software*.	O ciclo de vida de desenvolvimento de sistemas e aplicações deve incorporar o princípio de segurança por defeito e princípio de segurança desde a conceção. Em caso de alterações e exceções durante o desenvolvimento de *software* a entidade deve efetuar uma análise do impacto na segurança, num ambiente de teste separado, antes da implementação em produção.	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*.
PR.RI-1 — A entidade protege a integridade das redes de comunicações.	A integridade da rede dos sistemas críticos deve ser protegida através da identificação, documentação e controlo das ligações entre os componentes do sistema e da limitação das ligações externas aos sistemas críticos da entidade. A entidade deve monitorizar e controlar as ligações e comunicações nos limites externos e nos principais limites internos dos seus sistemas críticos, implementando dispositivos e tecnologias de proteção.	Diagrama de redes da entidade 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.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.RI-2 — Os ambientes de desenvolvimento e de teste são separados de ambientes de produção.	O(s) ambiente(s) de desenvolvimento e teste deve(m) ser isolado(s) do ambiente de produção.	Evidência técnica da separação de ambientes de teste e de produção.
PR.RI-4 — São implementados controlos de segurança para cumprir os requisitos de resiliência em situações adversas.	A entidade deve garantir a implementação de controlos adequados para responder em tempo útil a eventuais disrupções às normais operações, em conformidade com o Plano de Continuidade de Negócios estabelecido. A entidade deve garantir a existência de mecanismos que garantam a disponibilidade dos seus sistemas críticos, através de soluções de balanceamento de carga e redundâncias dos sistemas.	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.
PR.RI-5 — A entidade planeia a capacidade adequada dos recursos para garantir a disponibilidade das suas redes e sistemas de informação.	A entidade deve planear e disponibilizar a capacidade adequada dos recursos que processam o volume normal, atual e futuro, de informação dos sistemas críticos da entidade, redes, telecomunicações e armazenamento de dados.	Registo do planeamento da capacidade dos recursos para o processamento de informações dos sistemas críticos, redes, telecomunicações e armazenamento de dados.
DE.MC-1 — As redes e sistemas de informação são monitorizados para detetar potenciais incidentes.	A entidade deve monitorizar, identificar e bloquear comunicações, locais e remotas, não autorizadas às suas redes e sistemas críticos e remover conteúdo malicioso.	Evidência da monitorização, identificação e bloqueio de comunicações não autorizadas e conteúdo/ações malicioso/maliciosas.
DE.MC-2 — O ambiente físico é monitorizado para possibilitar a deteção de potenciais incidentes de segurança.	A entidade deve monitorizar o ambiente físico para identificar eventos potencialmente adversos.	Evidência técnica da monitorização do ambiente físico.
DE.MC-5 — A utilização de aplicações não autorizadas em dispositivos móveis é detetada.	A entidade deve incluir requisitos para a utilização de dispositivos móveis corporativos na sua Política de Uso Aceitável e monitorizar o cumprimento dos mesmos, nomeadamente no processo de gestão de eventos.	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.
DE.MC-6 — As atividades dos prestadores de serviços externos são monitorizadas para deteção de incidentes.	Todas as ligações aos sistemas, aplicações ou infraestrutura da entidade, efetuadas por fornecedores ou qualquer entidade externa, devem ser monitorizadas e protegidas por forma a detetar eventos potencialmente adversos. A entidade deve garantir a contínua conformidade dos prestadores de serviços com as suas políticas e procedimentos e com os requisitos de segurança previamente definidos em contratos ou acordos.	Registo da monitorização de todas as ligações aos sistemas, aplicações ou infraestrutura da entidade, efetuadas por fornecedores ou qualquer entidade externa. Registo da avaliação periódica dos prestadores de serviços com acesso às redes e sistemas da entidade por forma a garantir o cumprimento dos requisitos de segurança previamente definidos.
DE.MC-7 — O *hardware* e o *software*, os ambientes em produção e os seus dados são monitorizados para detetar eventos potencialmente adversos.	O *hardware*, *software*, ambientes em produção e respetivos dados devem ser monitorizados para detetar eventos potencialmente adversos.	Evidência técnica da recolha de eventos potencialmente adversos.
DE.AE-1 — Os eventos detetados são analisados.	A entidade deve analisar a informação recolhida sobre os eventos detetados para filtrar eventos com impacto potencialmente relevante e identificar respetivas origens, alvos e métodos de ataque.	Evidência técnica da análise da informação sobre os eventos detetados.
DE.AE-4 — As informações sobre deteções de eventos são comunicadas.	As informações sobre eventos adversos devem ser disponibilizadas ao pessoal autorizado e configuradas nos sistemas relevantes para a devida deteção, investigação e resposta.	Registo da disponibilização da informação sobre eventos adversos ao pessoal autorizado.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
RS.GI-1 — O Plano de Resposta a Incidentes é executado, em coordenação com as partes interessadas, durante ou após a ocorrência de um incidente.	As ações de resposta a incidentes devem ser coordenadas com as partes interessadas definidas no Plano de Resposta a Incidentes.	Registo documentado do planeamento e atualização dos processos de resposta a incidentes que incluam requisitos para escalonamento.
RS.GI-2 — As notificações de incidentes são triadas e validadas.	As notificações de incidentes devem ser triadas e validadas de acordo com o Plano de Resposta a Incidentes da entidade.	Registo da triagem e validação das notificações de incidentes.
RS.GI-3 — Os incidentes são categorizados e priorizados de acordo com o Plano de Resposta a Incidentes definido.	A entidade deve garantir que os incidentes de cibersegurança são categorizados de acordo com o nível de gravidade e impacto, e com os critérios de avaliação incluídos no Plano de Resposta a Incidentes. A entidade deve utilizar uma taxonomia de categorização de incidentes.	Registo da categorização de incidentes e a sua classificação, de acordo com a taxonomia de categorização de incidentes.
RS.GI-5 — São aplicados os critérios para iniciar a recuperação de incidentes.	Os critérios para iniciar a recuperação de incidentes devem estar definidos e ser aplicados.	Registo de critérios e evidência da sua aplicação na fase inicial da recuperação de incidentes.
RS.NC-1 — As partes interessadas internas e externas são informadas dos incidentes.	A entidade deve partilhar informação sobre incidentes com as partes interessadas externas relevantes dentro do prazo estabelecido no seu Plano de Resposta a Incidentes.	Registo da partilha de informações sobre incidentes com as partes interessadas externas relevantes.
RS.MI-1 — Os incidentes são contidos.	A entidade deve conter e resolver os incidentes. As decisões de não contenção e não resolução de incidentes devem ser documentadas.	Evidência dos processos de contenção de incidentes. Registo de decisões tomadas durante o processo de resposta.
RC.PR-5 — A integridade dos ativos restaurados é verificada, os sistemas e serviços são recuperados e o seu estado de normal funcionamento é confirmado.	A integridade dos ativos restaurados deve ser verificada, os sistemas e serviços devem ser recuperados e o seu estado de normal funcionamento deve ser confirmado.	Registo do processo de verificação da integridade dos ativos, recuperação de sistemas e serviços e confirmação do normal estado de funcionamento.
RC.PR-6 — O fim da recuperação do incidente é documentado e declarado com base em critérios prédefinidos.	O fim da recuperação do incidente deve ser documentado e declarado com base em critérios prédefinidos.	Registo da definição de critérios para a declaração do fim da recuperação do incidente e evidência da sua implementação.
RC.CO-1 — As atividades de recuperação são comunicadas às partes interessadas bem como aos órgãos de gestão, direção e administração.	As atividades de recuperação e os progressos no restauro do normal funcionamento dos sistemas e aplicações da entidade, devem ser comunicados às partes interessadas internas e externas.	Registo da comunicação das atividades de recuperação e progresso do restauro, às partes interessadas, internas e externas.
RC.CO-2 — As atualizações sobre a recuperação de incidentes são partilhadas utilizando métodos aprovados pela entidade.	As atualizações públicas sobre a recuperação do incidente devem ser partilhadas utilizando métodos de comunicação definidos e aprovados pela entidade.	Registo dos procedimentos para a comunicação de atualizações públicas sobre a recuperação de incidentes.

Elevado

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
GR.CO-5 — Os requisitos de resiliência necessários para suportar a prestação de serviços críticos são definidos.	O Plano de Continuidade de Negócios deve ser testado.	Evidência da execução de testes ao Plano de Continuidade de Negócio.
GR.GR-5 — A entidade define uma Política de Gestão dos Riscos de Cibersegurança a qual prevê uma metodologia para a gestão dos riscos de cibersegurança.	A entidade define, aprova e implementa uma Política de Gestão dos Riscos de Cibersegurança.	Política de Gestão dos Riscos de Cibersegurança aprovada e implementada.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
GR.SP-2 — A estratégia de gestão dos riscos de cibersegurança é regularmente revista e adaptada para garantir a cobertura dos requisitos e riscos organizacionais.	A estratégia de gestão dos riscos de cibersegurança deve ser revista regularmente e adaptada para garantir a cobertura dos requisitos e riscos organizacionais.	Evidência de que a entidade tem atualizado o quadro de ameaças e que revê e adapta a estratégia de gestão dos riscos em conformidade.
GR.SP-3 — O desempenho da gestão dos riscos de cibersegurança da entidade é avaliado e revisto para alterações necessárias.	Devem ser definidos e implementados mecanismos de avaliação do desempenho da gestão dos riscos de cibersegurança.	Registo da definição de mecanismos para avaliar o desempenho da gestão dos riscos de cibersegurança.
GR.CA-1 — As políticas e processos de gestão dos riscos da cadeia de abastecimento são identificados, estabelecidos, avaliados e geridos.	A entidade deve definir, aprovar, implementar, rever e atualizar a Política de Gestão de Riscos da Cadeia de Abastecimento e o respetivo procedimento.	Política e procedimento de Gestão de Riscos da Cadeia de Abastecimento aprovados, implementados e atualizados.
GR.CA-5 — A entidade define e integra nos contratos e outros acordos com fornecedores os requisitos para gerir os riscos de cibersegurança da cadeia de abastecimento.	Os contratos e outros acordos com fornecedores devem integrar disposições legais que permitam a avaliação contínua da cibersegurança dos fornecedores e a correção de eventuais falhas identificadas.	Modelos de contratos/acordos contendo cláusulas específicas que permitam a avaliação contínua da cibersegurança dos fornecedores e a correção de eventuais falhas identificadas.
GR.CA-6 — Antes da contratação de fornecedores são realizados processos de devida diligência para reduzir os riscos.	A entidade deve, antes de estabelecer relações contratuais com fornecedores, conduzir, sempre que possível, processos de devida diligência, com o objetivo de minimizar a sua exposição ao risco.	Registo dos processos de devida diligência realizados antes da contratação.
GR.CA-7 — A entidade avalia os riscos de cibersegurança da cadeia de abastecimento.	A entidade deve realizar avaliações da cibersegurança dos seus fornecedores em conformidade com o nível de exigência requerido.	Registo da avaliação de cibersegurança dos fornecedores em conformidade com o nível de exigência requerido, nomeadamente: Certificados válidos no âmbito do Selo de Maturidade Digital; Relatórios de auditorias realizadas; Resultados de testes realizados no âmbito da cibersegurança.
GR.CA-8 — O Plano de Resposta a Incidentes e o Plano de Recuperação de Desastres são testados com o acompanhamento dos fornecedores.	A entidade deve incluir o pessoal-chave dos fornecedores nos seus exercícios e testes dos Plano de Resposta a Incidentes e Plano de Recuperação de Desastres.	Registo de testes e exercícios ao Plano de Resposta a Incidentes e Plano de Recuperação de Desastres com a inclusão do pessoalchave dos fornecedores.
ID.GA-1 — Os equipamentos e os demais recursos físicos geridos ou detidos pela entidade são inventariados.	A entidade deve utilizar ferramentas de suporte à gestão de equipamentos e os demais recursos físicos.	Evidência técnica da ferramenta de inventariação e de suporte à gestão de equipamentos e os demais recursos físicos.
ID.GA-2 — Os recursos lógicos que suportam os processos dos serviços da entidade são inventariados	A entidade deve utilizar ferramentas ou aplicações de suporte à gestão de recursos lógicos.	Evidência técnica da ferramenta de inventariação e de suporte à gestão de recursos lógicos.
ID.GA-3 — As redes e fluxos de comunicação são mapeados.	A entidade deve mapear os fluxos de comunicação externos, e os mesmos devem ser documentados, devidamente aprovados e atualizados.	Diagramas de rede e sistemas e de fluxos de comunicação externos aprovados e atualizados.
ID.GA-6 — Os dados e respetivos metadados são identificados e registados.	Os dados e respetivos metadados que a entidade trata devem ser identificados e classificados de acordo com a Política de Classificação e Gestão de Dados.	Registo da identificação e classificação dos dados e respetivos metadados, de acordo com a Política de Classificação e Gestão de Dados.
ID.GA-8 — Os dados são destruídos de acordo com a Política de Classificação e Gestão de Dados definida.	Os processos de sanitização, físicos e digitais, devem ser documentados e testados, para garantir a eficácia da destruição da informação.	Registo do processo de sanitização e dos testes realizados.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
ID.GA-9 — A entidade implementa um processo de gestão de alterações.	A entidade deve estabelecer regras internas para a gestão de alterações, incluindo processos de avaliação e aprovação prévia de alterações. As alterações devem ser testadas e validadas antes da sua implementação nos sistemas operacionais. A entidade deve garantir a atualização dos seus procedimentos de forma a acompanhar as alterações efetuadas.	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-1 — As vulnerabilidades dos ativos são identificadas e documentadas com base na metodologia definida.	A entidade deve utilizar ferramentas de identificação e monitorização contínua das vulnerabilidades dos seus ativos. A entidade deve realizar testes de intrusão regulares.	Evidência técnica de ferramentas de identificação e monitorização contínua das vulnerabilidades. Registo do resultado da realização regular de testes de intrusão.
ID.AR-6 — A entidade garante que as respostas aos riscos são identificadas e priorizadas.	A entidade deve incluir na sua estratégia de tratamento dos riscos um plano de monitorização, revisão e melhoria contínua das respostas aos riscos.	Registo da inclusão de um plano de monitorização, revisão e melhoria contínua, na estratégia de tratamento dos riscos.
ID.AR-7 — A entidade define processos para receber informação, analisar e responder a vulnerabilidades provenientes de fontes internas e externas.	As vulnerabilidades registadas devem ser analisadas e avaliadas sistematicamente. A entidade deve implementar mecanismos automatizados, para divulgar e acompanhar os esforços de correção de vulnerabilidades, recolhidas de fontes internas e externas, para as principais partes interessadas.	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-2 — São identificadas melhorias a partir de testes e exercícios de cibersegurança.	Os testes e exercícios de cibersegurança devem ser utilizados para identificar pontos de melhoria dos processos da entidade. A entidade deve realizar testes com partes interessadas.	Registo da realização de testes e exercícios de cibersegurança, incluindo os efetuados com partes interessadas.
PR.GA-1 — Os ciclos de vida de gestão de identidades são definidos.	As identidades e credenciais dos dispositivos, serviços e utilizadores devem ser geridas através de mecanismos automatizados. A entidade deve aplicar autenticação segura nas suas transações entre sistemas críticos, nomeadamente, a autenticação multifator (MFA), certificados criptográficos, *tokens* e chaves criptográficas.	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 — A entidade verifica a identidade dos utilizadores, vinculando-a às respetivas credenciais.	A entidade deve garantir a utilização de credenciais únicas associadas a cada utilizador, dispositivo e processo que interaja com os sistemas críticos da entidade. A entidade deve garantir que todas as exceções estão documentadas e devidamente aprovadas.	Evidência técnica da atribuição de credenciais únicas para cada utilizador, dispositivo ou processo que interaja com sistemas críticos da entidade. Registo documentado das exceções à Política de Gestão de Identidades, Autenticação e Controlo de Acessos e a sua respetiva aprovação.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.GA-3 — São definidos mecanismos de autenticação de utilizadores, dispositivos e outros ativos de sistemas de informação.	A comunicação entre os sistemas da entidade e os sistemas externos (como os de parceiros, fornecedores ou prestadores de serviços, incluindo, serviços de computação em nuvem) deve ser enquadrada num acordo entre as entidades participantes. A entidade deve implementar autenticação multifator (MFA) em todos os seus dispositivos e outros ativos de sistemas de informação, quando estes o permitam.	Modelos de acordos entre a entidade 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 — As afirmações de identidade são protegidas, transmitidas e verificadas.	As afirmações de identidade devem ser protegidas, transmitidas e verificadas.	Evidência técnica da proteção, transmissão e verificação das afirmações de identidade.
PR.GA-5 — As permissões de acesso, os direitos e as autorizações são definidas numa política, geridas, aplicadas e atualizadas, e incorporam os princípios do menor privilégio e da separação de funções.	A entidade deve monitorizar o contexto em que ocorre a autenticação de utilizadores, e identificar os acessos realizados através de dispositivos, localizações e horários não habituais. A entidade deve monitorizar as atividades realizadas por utilizadores com privilégios elevados.	Evidência técnica da aplicação de restrições e monitorização ativa do contexto em que ocorre a autenticação de utilizadores. Evidência técnica da monitorização das atividades realizadas por utilizadores com privilégios elevados.
PR.GA-6 — Os controlos de acesso físico a ativos da entidade são geridos, monitorizados e aplicados em função do risco.	Os ativos alojados nas zonas de acesso restrito devem ser fisicamente protegidos.	Evidência técnica da implementação de proteções físicas aos ativos alojados nas zonas críticas.
PR.GA-7 — A entidade gere os seus acessos remotos.	O acesso remoto aos sistemas críticos da entidade deve ser monitorizado. O acesso remoto deve ser realizado através de canais seguros, utilizando mecanismos de encriptação forte e protocolos seguros aprovados internamente, sendo que o mesmo se aplica a ações de manutenção remota.	Evidencia técnica da implementação de canais seguros para acesso remoto (incluindo ações de manutenção). Evidência técnica da recolha e análise dos registos de atividades dos utilizadores em formato remoto aquando do seu acesso aos sistemas críticos da entidade.
PR.FC-1 — Todo o pessoal é sensibilizado e formado em matérias de cibersegurança.	A entidade deve definir e implementar indicadores para avaliar a eficácia das ações de sensibilização e formação. A entidade deve aplicar os resultados dos indicadores recolhidos, nos seus processos de melhoria contínua.	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.
PR.SD-1 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados armazenados.	A entidade protege as informações dos seus sistemas críticos, consideradas críticas/sensíveis, enquanto estiverem armazenadas, utilizando mecanismos criptográficos.	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 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados em trânsito.	A entidade deve implementar controlos de segurança que garantam a confidencialidade e integridade da informação em trânsito, consoante a sua 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 deve ser devidamente registada.	Evidência técnica da implementação dos controlos de segurança para proteção dos dados em trânsito, de acordo com a classificação, e em conformidade com a Política de Classificação e Gestão de Dados, inclusive nos fluxos de dados e interfaces de comunicação para o exterior.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.SD-3 — A entidade implementa proteções que evitem exfiltração de dados.	A entidade deve adotar controlos de segurança adequados para monitorizar os seus sistemas críticos nas fronteiras externas e nos pontos críticos internos, para evitar acessos e atividades não autorizadas, incluindo exfiltração de dados.	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 — A entidade protege a confidencialidade, integridade e disponibilidade dos dados em uso.	A entidade deve implementar controlos de segurança para proteger os seus sistemas críticos ou limitar o impacto de ataques de negação de serviço.	Evidência técnica da implementação de controlos de segurança para proteger os sistemas críticos ou limitar o impacto de ataques de negação de serviço.
PR.SD-5 — São realizadas, mantidas e testadas cópias de segurança dos dados da entidade.	O processo de verificação das cópias de segurança deve ser implementado em conformidade com os restantes processos, políticas e planos em matéria de cibersegurança da entidade (nomeadamente, o Plano de Continuidade de Negócio e o Plano de Resposta a Incidentes). As cópias de segurança dos sistemas críticos, nomeadamente, de sistemas operativos, configurações e aplicações, devem ser separadas das cópias de segurança de informações críticas.	Registo de um processo de verificação das cópias de segurança em conformidade com os restantes procedimentos, planos e políticas da entidade. Evidência técnica do armazenamento em locais separados, das cópias de segurança dos sistemas críticos e das informações críticas.
PR.SP-1 — É criada e mantida uma configuração base de redes e sistemas de informação que incorpora os princípios de segurança.	A entidade deve configurar os seus sistemas críticos com base no princípio de funcionalidades mínimas e desativar todos os protocolos, portos e serviços desnecessários. A entidade deve implementar controlos de segurança que prevejam os princípios de "*deny-all*" e "*permit by exception*".	Evidência técnica da aplicação do princípio da funcionalidade mínima e desativação de todos os protocolos, portos e serviços desnecessários, aquando da configuração das redes e sistemas da entidade. Evidência técnica da implementação de controlos alinhados com os princípios de segurança de "*denyall*" e "*permit by exception*".
PR.SP-2 — Os *logs* de sistemas e o histórico de atividades são documentados, implementados e revistos.	A entidade deve assegurar que as falhas no processamento de *logs* nos seus sistemas geram alertas. A capacidade de retenção e registo de *logs* deve ser revista periodicamente e ampliada sempre que necessário. Os *logs* gerados por sistemas críticos devem ser armazenados em sistema autónomo.	Evidência técnica de alarmística para situações de falha de processamento de *logs*. Evidência técnica do armazenamento de *logs* gerados por sistemas críticos em sistema autónomo.
PR.SP-4 — É implementado um ciclo de vida de desenvolvimento seguro de *software*.	Ao longo do ciclo de vida do desenvolvimento de *software* as práticas de desenvolvimento seguro devem ser integradas e o seu desempenho monitorizado.	Registo dos testes de qualidade de *software*, respetivas conclusões e acompanhamento da devida integração dos critérios de segurança definidos.
PR.RI-1 — A entidade protege a integridade das redes de comunicações.	A entidade deve implementar servidores *proxy* autenticados para o tráfego de comunicações definido entre os sistemas críticos da entidade e as redes externas. A entidade deve implementar controlos de segurança e de tolerância a falhas em dispositivos e tecnologias de proteção. A entidade deve controlar os fluxos de dados dos seus 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.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
PR.RI-3 — Os ativos tecnológicos da entidade são protegidos de ameaças naturais.	A entidade deve implementar dispositivos de deteção de incêndios que se ativam e notificam automaticamente o pessoal indicado em caso de incêndio. A entidade deve testar periodicamente a eficácia dos controlos de segurança aplicados aos ambientes físicos.	Evidência técnica da implementação de dispositivos de deteção contra ameaças naturais e registo da realização periódica de testes.
DE.MC-1 — As redes e sistemas de informação são monitorizados para detetar potenciais incidentes.	A entidade deve monitorizar os seus sistemas críticos de forma contínua para detetar eventos e indicadores de potenciais incidentes e automaticamente acionar mecanismos de resposta.	Registo de monitorização contínua dos sistemas críticos quanto a potenciais incidentes.
DE.MC-2 — O ambiente físico é monitorizado para possibilitar a deteção de potenciais incidentes de segurança.	Para além da monitorização do acesso físico às instalações, a entidade deve monitorizar o acesso físico aos seus sistemas e dispositivos críticos, com alarmes de intrusão física, equipamento de vigilância e equipas de monitorização independentes.	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-5 — A utilização de aplicações não autorizadas em dispositivos móveis é detetada.	A entidade deve gerir a instalação e suporte de *software* numa ferramenta centralizada. A entidade deve criar alarmística relativamente à instalação de *software* indevido e integrar o processo de alarmística na gestão de incidentes.	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-7 — O *hardware* e o *software*, os ambientes em produção e os seus dados são monitorizados para detetar eventos potencialmente adversos.	A entidade deve efetuar verificações da integridade do *hardware* dos seus sistemas críticos para detetar eventuais adulterações. A deteção de adulterações do *hardware* dos sistemas críticos deve ser incluída no Plano de Resposta a Incidentes. A entidade deve implementar um sistema de deteção e alerta de eventos de segurança, que permita identificar falsos positivos, com vista a uma melhor deteção e bloqueio de código ou atividades maliciosas.	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.
DE.AE-1 — Os eventos detetados são analisados.	A entidade deve implementar um sistema automatizado para agregação, correlação e análise dos eventos de segurança detetados.	Evidência técnica da implementação de sistemas automatizados para agregação, correlação e análise dos eventos de segurança detetados.
DE.AE-2 — Os eventos são recolhidos e correlacionados a partir de várias fontes e sensores.	O sistema automatizado para agregação, correlação e análise de eventos de segurança da entidade deve considerar, para os eventos dos ativos críticos, as diversas fontes e sensores existentes. O sistema automatizado para agregação, correlação e análise de eventos de segurança da entidade deve integrar informação relativa a rastreamentos de vulnerabilidades e estatísticas de performance dos sistemas e aplicações.	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 entidade.
DE.AE-3 — O impacto estimado e o âmbito dos eventos adversos detetados são compreendidos e identificados.	Os potenciais impactos dos eventos de segurança detetados no normal funcionamento da entidade, nas operações, nos ativos ou nas pessoas devem ser tidos em conta durante o processo de gestão dos riscos.	Registo documentado da revisão do processo de gestão dos riscos tendo em o impacto dos eventos de segurança detetados.

Controlo de Cibersegurança	Medida de Cibersegurança	Critério de Verificação
RS.GI-3 — Os incidentes são categorizados e priorizados de acordo com o Plano de Resposta a Incidentes definido.	O Plano de Resposta a Incidentes deve descrever os procedimentos de resposta para os diferentes tipos de incidente definidos na taxonomia de categorização de incidentes. Devem ser utilizadas ferramentas automatizadas para apoiar na investigação e a avaliação do impacto de incidentes previamente validados.	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 avaliação do impacto de incidentes.
RS.AI-1 — É realizada uma análise forense para determinar o que ocorreu durante um incidente e a sua causa raiz.	A entidade deve realizar análises forenses dos artefactos recolhidos para determinar a causa raiz do incidente. A entidade deve garantir a existência de mecanismos *ondemand*, internos ou externos para a realização de análises forenses.	Registo documentado da realização de análises forenses.
RS.AI-2 — As ações realizadas durante uma investigação são registadas e a integridade e proveniência dos registos são preservadas.	As ações realizadas durante uma investigação devem ser registadas e a integridade e a proveniência dos registos devem ser preservadas.	Registo documentado das ações realizadas durante a investigação dos incidentes.
RS.AI-3 — Os dados e metadados do incidente são recolhidos, e a sua integridade e proveniência são preservadas.	Os dados e metadados dos incidentes devem ser recolhidos e armazenados e a sua autenticidade, exatidão e rastreabilidade são protegidas.	Evidência do armazenamento dos dados e metadados dos incidentes e da implementação de mecanismos que garantam a preservação da integridade e proveniência dos mesmos.
RS.AI-4 — O impacto do incidente é estimado e validado.	O resultado da análise de incidentes deve ser considerado na avaliação de impacto do incidente em causa.	Registo da inclusão dos resultados da análise das investigações realizadas, na avaliação de impacto do incidente.
RS.MI-2 — Os incidentes são resolvidos.	O Plano de Resposta a Incidentes deve conter critérios que permitam declarar a conclusão da resolução do incidente.	Registo da inclusão de critérios para declarar a conclusão da resolução do incidente no Plano de Resposta a Incidentes.
RC.CO-2 — As atualizações sobre a recuperação de incidentes são partilhadas utilizando métodos aprovados pela entidade.	A entidade deve implementar uma estratégia de comunicação de crise para mitigar os impactos negativos durante uma crise.	Registo documentado da estratégia de comunicação para situações de crise.

ANEXO IV

Medidas de Cibersegurança Mínimas para Entidades Públicas Relevantes

Abreviaturas

Abreviatura	Definição
MFA	*Multi-factor authentication*- Autenticação Multi-fator
TIC	Tecnologias de Informação e Comunicação.
VDI	*Virtual Desktop Infrastructure*-Infraestrutura de Desktop Virtual
VPN	*Virtual Private Network* — Rede privada virtual.

Grupo B

Área	Medidas de Cibersegurança	Critérios de Verificação
O.CRI — Identificação de ponto de contacto para resposta a incidentes.	A entidade deve identificar um ponto de contacto para a resposta a incidentes. A pessoa identificada deve ser capaz de responder a eventuais solicitações externas, e, caso seja necessário, ter disponibilidade para contactos de emergência fora do horário de expediente.	Evidência documental sobre o ponto de contacto.
O.IAC — Inventariação dos ativos críticos.	A entidade deve inventariar os seus ativos críticos para a execução da sua atividade principal, deve ainda identificar as dependências entre os ativos críticos. A entidade deve atualizar o inventário de ativos críticos regularmente.	Inventário atualizado dos ativos críticos.
O.GAP — Gestão de acessos e permissões.	A entidade deve assegurar que os novos acessos, alteração e revogação dos mesmos são acompanhados por um pedido/aprovação.	Evidência da gestão dos pedidos e respetivas aprovações.
O.GEC — Gestão de equipamentos computacionais.	A entidade deve documentar e atualizar a atribuição e recolha dos equipamentos computacionais.	Registo documentado da atribuição e recolha de equipamentos computacionais.
O.PSF — Política de Segurança de fornecedores.	A entidade deve inventariar os fornecedores com acesso a sistemas de informação e obter contactos para notificação de incidentes de cibersegurança.	Evidência documental da lista de fornecedores.
T.GPT — Gestão de Sistemas, Aplicações e Postos de Trabalho.	A entidade deve garantir que são aplicados controlos de segurança nos sistemas, aplicações e postos de trabalho.	Evidência técnica da implementação de controlos de segurança nos sistemas, aplicações e postos de trabalho.
T.PPT — Proteção de postos de trabalho	A entidade deve garantir que se encontra instalado um antivírus nos seus postos de trabalho e servidores.	Evidência técnica da implementação de antivírus nos postos de trabalho e servidores.
T.AR — Acesso remoto à entidade	A entidade deve garantir que o acesso remoto é efetuado via mecanismo de acesso seguro (e.g. VPN, VDI) e autorizado através de um segundo fator de autenticação (MFA).	Evidência técnica da implementação de mecanismo de acesso seguro para acessos remotos e que requeira segundo fator de autenticação.
T. PAS — Perfil de Administração Segregado.	A entidade deve garantir a disponibilização de diferentes utilizadores dependendo da necessidade de acesso aplicacional ou de administração.	Evidência documentada da segregação das contas de utilizadores das contas de perfil de administração.
T.AS — Atualizações de segurança	A entidade deve garantir atempadamente a aplicação de todas atualizações de segurança de acordo com as recomendações dos fabricantes nos sistemas operativos e componentes de *software* nos seus postos de trabalho e servidores de suporte.	Registo documentado de atualização dos sistemas operativos e componentes de *software*.
T.PEW — Proteção Correio Eletrónico e Serviços Web.	A entidade deve garantir que aplica as melhores práticas a nível de segurança de correio eletrónico e páginas de Internet.	Evidência técnica da implementação de mecanismos de segurança para autenticação do correio eletrónico e utilização de protocolos seguros e certificados digitais nas páginas de Internet.
T.CS — Cópias de segurança	A entidade deve efetuar cópias de segurança e garantir que estas podem ser utilizadas, caso seja necessário.	Evidência técnica da execução de cópias de segurança.
T.RAR — Recolha e armazenamento de registos.	A entidade deve garantir a ativação dos registos definidos por defeito em sistemas operativos, aplicações e outros dispositivos.	Evidência técnica da ativação dos registos por defeito em sistemas operativos, aplicações e outros dispositivos.

Área	Medidas de Cibersegurança	Critérios de Verificação
T.PPL — Proteção perimetral da infraestrutura lógica.	A entidade deve garantir a proteção perimetral de infraestrutura.	Evidência técnica da implementação das medidas de segurança lógica ao nível dos equipamentos.
T.PPF — Proteção perimetral da infraestrutura física.	A entidade deve garantir a proteção física dos componentes da infraestrutura que alojam infraestrutura crítica (e.g. Centro de Processamento de Dados).	Evidência técnica da implementação das medidas de segurança física ao nível dos espaços afetos à infraestrutura crítica.
T.MA — Mecanismos de autenticação	A entidade deve implementar uma Política para garantir uma robustez adequada em relação à complexidade das suas palavras passe.	Evidência da implementação operacional da Política de complexidade de palavras passe nas plataformas tecnológicas.
H-PF — Sensibilização e Formação	A entidade deve estabelecer ações de sensibilização e/ou formação em cibersegurança.	Registo documentado das ações de sensibilização e/ou formação.
H.FIC — Fontes de informação e canais de comunicação.	A entidade deve garantir que existe consulta regular de fontes de informação e o acesso a canais de comunicação fidedignos quanto a ameaças de cibersegurança.	Evidências dos canais de pesquisa e disseminação de informação sobre ameaças de cibersegurança.

Grupo A

Área	Medida de Cibersegurança	Critérios de Verificação
O.PSI — Política de Cibersegurança	A entidade deve definir uma Política de Cibersegurança que determine o compromisso da entidade para com a cibersegurança.	Política de Cibersegurança aprovada e implementada.
O.IAC — Inventariação dos ativos	A entidade deve inventariar todos os seus ativos e identificar as dependências entre os mesmos. A entidade deve atualizar o inventário regularmente.	Inventário completo e atualizado dos ativos.
O.PAP — Política de acessos e permissões.	A entidade deve definir e implementar uma Política de Gestão de Acessos e Permissões.	Política de Gestão de Acessos e Permissões aprovada e implementada.
O.GEC — Gestão de equipamentos computacionais.	A entidade deve garantir a segregação de dispositivos móveis/eletrónicos pessoais dos dispositivos corporativos.	Evidência técnica da segregação de redes.
O.PUA — Política(s) de utilização aceitável.	A entidade deve definir e disponibilizar junto de todos o pessoal a Política de Utilização Aceitável, que seja abrangente para toda a entidade e que defina as regras para a utilização segura e responsável dos seus ativos. Esta Política deve incluir requisitos de segurança para a proteção da confidencialidade e integridade dos ficheiros em circulação entre entidades.	Política de Utilização Aceitável aprovada e implementada.
O.PP — Política de palavra-passe	A entidade deve definir uma Política para Gestão das suas palavras-passe.	Política de Palavra-passe aprovada e implementada.
O.PCF — Processo de Classificação da Informação.	A entidade deve definir um processo de classificação da informação, que permita identificar os critérios/ níveis de sensibilidade relativamente aos seus dados.	Registo documentado da classificação da informação.
O.GMO — Gestão da mudança organizacional.	A entidade deve definir e implementar procedimentos de atualização ao nível das TIC, aquando da entrada, alteração e saída de pessoal, e sincronizá-las com a área de recursos humanos.	Registo documentado dos procedimentos quanto a ações a executar quando existe a saída ou mudança de funções de pessoal.

Área	Medida de Cibersegurança	Critérios de Verificação
O.ID — Identificação de funções ou atividades críticas.	A entidade deve identificar as funções ou atividades críticas e as dependências existentes das TIC.	Registo documentado da identificação de funções ou atividades críticas, dos ativos que as suportam e da relação e/ou dependência que entre eles se estabelece.
O.PSF — Política de Segurança de fornecedores.	A entidade deve definir e implementar uma Política de Segurança de Fornecedores que determine os mecanismos de avaliação de risco da cadeia de abastecimento e os critérios de aceitação.	Política de Segurança de Fornecedores aprovada e implementada.
T.PPT — Proteção de postos de trabalho	A entidade deve implementar mecanismos de controlo de acesso dos postos de trabalho, assim como cópias de segurança da respetiva informação.	Evidência técnica da implementação de controlo de acesso dos postos de trabalho. Evidência técnica da execução de cópias de segurança.
T.PPT — Perfil de trabalho nos dispositivos móveis.	A entidade deve garantir que a informação corporativa apenas é acedida através de um perfil de trabalho nos dispositivos móveis.	Evidência técnica da configuração do perfil de trabalho para acesso a aplicações corporativas.
T.GP — Gestão de palavras-passe	A entidade deve garantir que as palavras-passe para acessos privilegiados se encontram armazenadas através de uma solução para a gestão de palavras-passe.	Evidência técnica da implementação de uma solução para a gestão das palavras-passe para acessos privilegiados.
T.PAD — Privilégios de acesso diferenciados.	A entidade deve garantir que os acessos e permissões são concedidos de acordo com o princípio da necessidade de conhecer e com o princípio do menor privilégio, e em conformidade com a Política de Gestão de Acessos e Permissões.	Registo documentado da identificação de acessos a sistemas e aplicações por perfil funcional, em conformidade com a Política de Gestão de Acessos e Permissões.
T.AS — Atualizações de segurança	A entidade deve garantir a aplicação atempada de todas atualizações de segurança de acordo com as recomendações dos fabricantes nos seus dispositivos de *hardware*.	Registo documentado da atualização dos equipamentos *hardware*.
T.AM — Autenticação multifator	A entidade deve ativar a autenticação multifator nas suas aplicações críticas.	Evidência técnica da implementação de autenticação multifator em aplicações críticas.
T.PEW — Proteção Correio Eletrónico e Serviços Web.	A entidade deve garantir que são aplicadas as melhores práticas a nível de segurança de correio eletrónico e páginas de Internet.	Evidência técnica da implementação de mecanismos de segurança para autenticação e validação do correio eletrónico e utilização de protocolos seguros, certificados digitais e configuração dos cabeçalhos de segurança nas páginas de Internet.
T.CS — Cópias de segurança	A entidade deve segregar o armazenamento das cópias de segurança do ambiente protegido.	Evidência técnica da segregação do armazenamento das cópias de segurança.
T.RAR — Recolha e armazenamento de registos.	A entidade deve garantir a salvaguarda dos *logs* dos sistemas operativos, aplicações e outros dispositivos.	Evidência técnica da recolha de *logs*.
T.SC — Securização (*hardening*) de configurações.	A entidade deve garantir que são implementadas práticas de segurança ao nível do posto de trabalho, das configurações do sistema operativo e principais aplicações utilizadas.	Evidência técnica da implementação das melhores práticas de segurança.

Área	Medida de Cibersegurança	Critérios de Verificação
H.EC — Realização de exercícios de *phishing*.	A entidade deve garantir a realização periódica de exercícios de *phishing*, que permitam avaliar o grau de preparação do seu pessoal.	Registo documentado dos resultados dos exercícios realizados, assim como as conclusões e iniciativas com base nesses resultados.
H-PF — Plano de formação	A entidade deve estabelecer um plano de ações de formação em cibersegurança, bem como definir os processos e procedimentos necessários para garantir a sua correta implementação.	Registos documentado da definição dos planos e ações de formação.

320013455