MUNICÍPIO DE VINHAIS

CÂMARA MUNICIPAL

REUNIÃO ORDINÁRIA

DATA: 2023/08/10 ATA N.º 13/2023

Presenças: ----------

- Luís dos Santos Fernandes, que presidiu; ----------
- Martinho Magno Martins; ----------
- Artur Jorge Pereira dos Santos Marques; ----------
- Margarida Garcia dos Santos Patrício em substituição de Carlos Abel Almendra Frias Vieira; ----------
- Luís Miguel Pires Gomes. ----------

Local da reunião: Salão Nobre dos Paços do Município.----------

Hora de abertura: Quinze horas e quinze minutos.----------

Hora de encerramento: Quinze horas e cinquenta minutos.----------

Secretariou: Ana Maria Martins Rodrigues, assistente técnica do Gabinete de Apoio aos Órgãos Municipais. ----------

1 – Período de Antes da Ordem do Dia. ----------

ORDEM DO DIA

2 – Ata da Reunião Anterior. ----------

3 – Execução de Obras Públicas.----------

4 – Assuntos deferidos no uso de competências delegadas. ----------

5 - Resumo Diário de Tesouraria. ----------

6 – Obras Particulares: ----------

6.1 – António Luís Alves de Sá – Ervedosa – Pedido de Prorrogação do Prazo para Conclusão da Obra. ----------

7 – Obras Públicas: ----------

7.1 – Requalificação e Modernização da EBS D. Afonso III de Vinhais – Trabalhos Complementares - Adenda ao Contrato N.º 22/2019. ----------

8 – Apoios:----------

8.1 – Protocolo de Colaboração - Futebol Clube de Vinhais;----------

8.2 – Protocolo de Colaboração - Associação Desportiva e Cultural de Rebordelo; -----

8.3 – Prémios Chegas de Touros de Bovinos Raça Mirandesa 2023; ----------

8.4 – Prémios Concurso Concelhio de Bovinos Raça Mirandesa 2023. ----------

9 – Proposta de Plano de Segurança para o Município de Vinhais (Decreto-Lei N.º 65/2021). ----------

10 – Plano Municipal de Defesa da Floresta Contra Incêndios de Vinhais (2022-2031) – Alterações Após Audiência Pública. ----------

1 – PERÍODO DE ANTES DA ORDEM DO DIA. ----------

Solicitou a palavra o Senhor Presidente da Câmara Municipal para fazer referência ao seguinte: ----------

- Agradeceu a todos os trabalhadores do Município que prestam serviço na colocação de redes sombra, palcos e stands, em várias localidades do Concelho a pedido das Comissões de Festas e Juntas de Freguesia, pois com as temperaturas tão elevadas que se tem registado, por vezes não é um trabalho fácil; ----------
- Referiu ainda que a candidatura do BUPI vai ser renovada e que neste momento tinham já agendado, novamente, visitas às aldeias do Concelho, permitindo assim uma maior ajuda às pessoas. ----------
- De seguida informou todos os presentes que na próxima Reunião do Órgão Executivo iria apresentar uma moção sobre a falta de caixas multibanco no nosso Concelho, para fazer chegar ao Banco de Portugal, isto tendo em atenção o próprio estudo divulgado pelo Banco de Portugal. ----------
- Para finalizar parabenizou a Associação Javalis do Asfalto pelo sucesso que foi o XI Encontro Motard, pelo que teve um enorme número de visitantes. ----------

Solicitou a palavra o Senhor Vereador Artur Jorge Pereira dos Santos Marques para referir que o XI Encontro Motard tinha superado todas as expetativas e pretendia deixar um agradecimento à organização e a todas as entidades que contribuíram para o sucesso do evento. ----------

Concedida a palavra à Senhora Vereadora Margarida Garcia dos Santos Patrício referiu que pretendiam associar-se a todas as felicitações e agradecimentos mencionados. ----------

ORDEM DO DIA

2 – ATA DA REUNIÃO ANTERIOR. ----------

A ata da reunião anterior previamente enviada por email aos Senhores Vereadores, tendo sido dispensada a sua leitura, foi submetida a votação, a qual foi aprovada por unanimidade.

3 – EXECUÇÃO DE OBRAS PÚBLICAS. ----------

Foi tomado conhecimento da situação das obras municipais em curso, quer por empreitada, quer por administração direta, cuja relação foi previamente enviada aos Senhores Vereadores, e que fica arquivada na pasta respetiva. ----------

4 – ASSUNTOS DEFERIDOS NO USO COMPETÊNCIAS DELEGADAS. ----------

Foi presente a relação dos assuntos deferidos no uso de competências delegadas, que a seguir se transcreve: ----------

- Aprovação do projeto de arquitetura para construção de um armazém agrícola, na povoação de Moimenta, em nome de Rui Miguel Barreira Rodrigues; ----------
- Licenciamento e aprovação de todos os projetos para legalização de uma moradia, na povoação de Soeira em nome de Ana Rosa dos Anjos Carneiro – Cabeça de Casal da herança de Armindo António Pereira Carneiro; ----------
- Licenciamento e aprovação de todos os projetos para construção de um armazém agrícola, na povoação de Vilar de Peregrinos, em nome de Eurico dos Santos Afonso; ----------
- Licenciamento e aprovação de todos os projetos para construção de um armazém agrícola, na povoação de Moimenta, em nome de Rui Miguel Barreira Rodrigues;----------
- Licenciamento e aprovação de todos os projetos para construção de uma moradia, na povoação de Edral, em nome de Maria de Fátima Lourenço Barreira;----------
- Licenciamento e aprovação de todos os projetos para legalização de uma moradia, na povoação de Soeira, em nome de Maria Rita Pires; ----------
- Aprovação do projeto de arquitetura para construção de arranjos exteriores, na Zona Industrial de Vinhais – Lote 31, em nome de Jorge Manuel – Sociedade de Granitos e Mármores, Lda..----------

5 - RESUMO DIÁRIO DE TESOURARIA. ----------

Foi tomado conhecimento do resumo diário de tesouraria, datado do dia nove do mês de agosto, do ano de dois mil e vinte e três, que regista os seguintes saldos:----------

Em dotações Orçamentais .....3.173.579,79 €
Em dotações Não Orçamentais .....494.022,69 €

6 – OBRAS PARTICULARES: ----------

6.1 – ANTÓNIO LUÍS ALVES DE SÁ – ERVEDOSA – PEDIDO DE PRORROGAÇÃO DO PRAZO PARA CONCLUSÃO DA OBRA. ----------

Presente ao Órgão Executivo uma informação subscrita pela Técnica Superior de Arquitetura Susana Martins Oliveira, cujo teor é o seguinte: ----------

"A presente apreciação fundamenta-se nas disposições conjugadas da legislação em vigor, nomeadamente DL n.º 555/99, de 16 de dezembro, na sua redação atual.----------

1- O requerente pretende prorrogação do prazo para conclusão das obras (segunda prorrogação);----------
2- A fiscalização informa que até à presente data as obras licenciadas não foram iniciadas;
3- Nos termos do disposto na alínea a) do n.º 3 do artigo 71.º do RJUE, a licença caduca se as obras não forem iniciadas no prazo de 12 meses a contar da data de emissão do alvará de obras de edificação;----------
4- O alvará de licença de obras de edificação foi emitido em 18 de março de 2022, com um prazo de seis meses para conclusão da obra:----------
5- Foi concedida uma primeira prorrogação por mais seis meses até 19 de março de 2023;--
6- E passado um ano, 12 meses, o requerente não início a obra;----------
7- A caducidade prevista neste artigo é declarada pela Câmara Municipal, após audiência prévia do interessado;----------
8- Ora o requerente já vem dizer que pretende realizar a obra e só não a iniciou porque o poste da E-Redes continua a impedir a realização dos trabalhos;----------
9- Face ao exposto proponho que seja encaminhado o presente pedido para a Câmara Municipal a fim de se pronunciar se de facto deve ser determinada a caducidade, ou não e viabilizar a prorrogação por mais seis meses." ----------

Deliberado, por unanimidade e em minuta, concordar com o proposto e conceder a prorrogação de prazo de mais 6 (seis) meses, a contar da data da deliberação. ----------

7 – OBRAS PÚBLICAS: ----------

7.1 – REQUALIFICAÇÃO E MODERNIZAÇÃO DA EBS D. AFONSO III DE VINHAIS – TRABALHOS COMPLEMENTARES - ADENDA AO CONTRATO N.º 22/2019. ----------

Presente ao Órgão Executivo a Adenda ao Contrato n.º 22/2019 relativa à empreitada de "Requalificação e Modernização da EBS D. Afonso III de Vinhais – Trabalhos complementares" celebrada entre o Município de Vinhais e a empresa Manuel Joaquim Caldeira, Ld.ª, no valor de cento e cinquenta e nove mil setecentos e oitenta e um euros e cinquenta e seis cêntimos (159.781,56 €). ----------

Após análise e discussão, foi deliberado, por unanimidade e em minuta, aprovar a referida adenda. ----------

8 – APOIOS:----------

8.1 – PROTOCOLO DE COLABORAÇÃO - FUTEBOL CLUBE DE VINHAIS.-------

No seguimento da deliberação tomada na reunião do Órgão Executivo realizada no dia vinte e cinco de julho de dois mil e vinte e três, foi presente o protocolo de colaboração celebrado entre o Município e o Futebol Clube de Vinhais, cujo teor é o seguinte: ----------

"Nos termos das atribuições que lhe são conferidas no domínio do desporto, pela alínea f), n.º 2, do art.º 23.º, do Anexo I à Lei n.º 75/2013, de 12 de setembro conjugada com a alínea u), do n.º 1 do art.º 33.º da referida Lei, com as alterações introduzidas pela Lei n.º 69/2015, de 16 de julho, entre o Município de Vinhais, adiante designado por Município, aqui representado pelo Presidente da Câmara Municipal, **Luís dos Santos Fernandes**, e o **Futebol Clube de Vinhais**, adiante designado por clube, com o número de identificação de pessoa coletiva 501 632 743, com sede em Vinhais, concelho de Vinhais, aqui representado pelo presidente da Direção, **Manuel José Silva Morais Rodrigues**, é celebrado o presente protocolo de dinamização e desenvolvimento desportivo, dentro das condições aprovadas na reunião ordinária da Câmara Municipal de **vinte e cinco de julho de dois mil e vinte e três**, e que se rege pelas cláusulas seguintes: ----------

1.ª - Objeto

Constitui objeto deste protocolo o apoio ao Futebol Clube de Vinhais, no âmbito do fomento e desenvolvimento da prática desportiva no Concelho. ----------

2.ª - Objetivos

São objetivos deste protocolo, nomeadamente, o fomento do desporto e a representatividade e divulgação do Concelho, em particular no exterior, nas necessárias deslocações a outras localidades, e ainda a ocupação dos tempos livres, numa actividade que entretém e enriquece a formação da população. ----------

3.ª - Compromissos do Município

O Município obriga-se a: ----------

1 - Atribuir um subsídio no valor de **sessenta e cinco mil euros (65.000,00€)** a ser transferido da seguinte forma: ----------

- **40% vinte e seis mil euros (26.000,00€)** para o apoio base ao Plano de Atividades durante o mês de agosto de 2023; ----------
- **60% trinta e nove mil euros (39.000,00€)** até ao mês de abril de 2024. ----------

Sendo que são: ----------

- ✓ 20.000,00€ para despesas com a equipa sénior; ----------
- ✓ 30.000,00€ para despesas com equipas de formação; ----------
- ✓ 5.000,00€ para despesas com as modalidades (natação, atletismo e triatlo); ----------
- ✓ 5.000,00€ para despesas com a equipa de veteranos; ----------
- ✓ 5.000,00€ referentes à presença da Taça de Portugal 2022/2023. ----------

2 - Ceder a utilização do Estádio Municipal para realizar treinos e jogos no calendário e horários a definir. ----------

3 - A utilização do estádio será acompanhada por um funcionário municipal. ----------

4 - Ceder o autocarro para as deslocações das equipas nas várias competições. ----------

5 - Disponibilizar o material didáctico de que dispõe, necessário ao exercício da modalidade a praticar. ----------

4.ª - Compromissos do Clube

O clube obriga-se a: ----------

1- Apresentar ao Município documentação que comprove a participação em provas da federação ou em competições com calendário desportivo, no escalão sénior, escalões de formação e veteranos. ----------
2- Informar o Município, por escrito, do início da atividade. ----------
3- Cumprir as regras e normas de utilização das instalações e equipamentos do estádio municipal. ----------
4- Comunicar com a devida antecedência o calendário e horário dos jogos. ----------
5- Assumir a responsabilidade por qualquer acidente que envolva os atletas, ou outros ligados ao clube, mesmo que aconteça nas instalações municipais. ----------
6- Assegurar a presença dos treinadores durante a utilização das instalações municipais. --
7- Suportar os encargos com os motoristas, nas deslocações. ----------

5.ª - Penalizações

1- O incumprimento da cláusula anterior pode obrigar o clube à reposição das quantias transferidas, tal como for deliberado pela Câmara Municipal. ----------
2- A prática, por parte do clube, de comprovadas ações de anti-desportivismo, confere ao Município o direito de rescisão do presente protocolo para além das reposições financeiras que a Câmara Municipal entender. ----------

6.ª - Vigência

O presente protocolo produz efeitos para a época desportiva 2023/2024. ----------

7.ª - Acompanhamento

1- Apresentar relatório de contas no Núcleo de Contabilidade, Aprovisionamento e Armazéns, no final da época. ----------
2- A Câmara Municipal acompanhará a execução deste protocolo, através do Serviço de Desporto, Juventude e Associativismo. ----------
3- O clube obriga-se a elaborar um relatório informativo no fim da época desportiva, e a apresentá-lo à Câmara Municipal no mês seguinte. ----------

O presente protocolo foi feito em dois (2) exemplares, para que cada outorgante fique com seu.”----------

Após análise e discussão foi deliberado, por unanimidade e em minuta, aprovar o presente protocolo. ----------

8.2 – PROTOCOLO DE COLABORAÇÃO - ASSOCIAÇÃO DESPORTIVA E CULTURAL DE REBORDELO; ----------

No seguimento da deliberação tomada na reunião do Órgão Executivo realizada no dia vinte e cinco de julho de dois mil e vinte e três, foi presente o protocolo de colaboração celebrado entre o Município e a Associação Desportiva e Cultural de Rebordelo, cujo teor é o seguinte:

"Nos termos das atribuições que lhe são conferidas no domínio do desporto, pela alínea f), n.º 2, do art.º 23.º, conjugada com a alínea u), do n.º 1 do art.º 33.º do Anexo I à Lei n.º 75/2013 de 12 de setembro na sua atual redação, entre o Município de Vinhais, adiante designado por Município, aqui representado pelo Presidente da Câmara Municipal, **Luís dos Santos Fernandes** e a **Associação Desportiva e Cultural de Rebordelo**, adiante designada por Associação, com o número de identificação de pessoa coletiva 504 037 340, com sede em Rebordelo, concelho de Vinhais, aqui representada pelo Presidente da Direção, **Alberto Nascimento Dias**, é celebrado o presente protocolo de dinamização e desenvolvimento desportivo, dentro das condições aprovadas na reunião ordinária da Câmara Municipal de **vinte e cinco de julho de dois mil e vinte e três**, e que se rege pelas cláusulas seguintes: --

1.ª - Objeto

Constitui objeto deste protocolo o apoio a Associação Desportiva e Cultural de Rebordelo, no âmbito do fomento e desenvolvimento da prática desportiva no Concelho.----------

2.ª - Objetivos

São objetivos deste protocolo, nomeadamente, o fomento do desporto e a representatividade e divulgação do concelho, em particular no exterior, nas necessárias deslocações a outras localidades, e ainda a ocupação dos tempos livres, numa atividade que entretém e enriquece a formação da população. ----------

3.ª - Compromissos do município

O Município obriga-se a: ----------

1 - Atribuir um subsídio no valor de **trinta e cinco mil euros (35.000,00€)** a ser transferido da seguinte forma: ----------

- **40% catorze mil euros (14.000,00€)** para o apoio base ao Plano de Atividades durante o mês de agosto de 2023; ----------
- **60% vinte e um mil euros (21.000,00€)** até ao mês de abril de 2024. ----------

Sendo que são: ----------

- ✓ 20.000,00€ para as despesas com a equipa sénior;----------
- ✓ 5.000,00€ para as despesas referentes a gás, eletricidade e despesas de manutenção do campo; ----------
- ✓ 5.000,00€ referentes à representação na Taça de Portugal; ----------
- ✓ 5.000,00 € para as despesas da equipa de veteranos.----------

2 - Ceder a utilização do Estádio Municipal para realizar treinos e jogos no calendário e horários a definir, sempre que tal se torne necessário. ----------

3 - A utilização do estádio será acompanhada por um funcionário municipal. ----------

4 - Ceder o autocarro para as deslocações das equipas nas várias competições. ----------

5 -Disponibilizar o material didático de que dispõe, necessário ao exercício da modalidade a praticar. ----------

4.ª - Compromissos da Associação

A Associação obriga-se a: ----------

1 - Apresentar ao Município documentação que comprove a participação em provas da federação ou em competições com calendário desportivo, no escalão sénior e veteranos. ---

2 - Informar o Município, por escrito, do início da atividade. ----------

3 - Cumprir as regras e normas de utilização das instalações e equipamentos do estádio municipal. ----------

4 - Comunicar com a devida antecedência o calendário e horário dos jogos. ----------

5 - Assumir a responsabilidade por qualquer acidente que envolva os atletas, ou outros ligados à Associação, mesmo que aconteça nas instalações municipais. ----------

6 - Assegurar a presença dos treinadores durante a utilização das instalações municipais.----

7 - Suportar os encargos com os motoristas, nas deslocações. ----------

5.ª - Penalizações

1 - O incumprimento da cláusula anterior pode obrigar a associação à reposição das quantias transferidas, tal como for deliberado pela Câmara Municipal. ----------

2 - A prática, por parte da associação, de comprovadas ações de anti-desportivismo, confere ao Município o direito de rescisão do presente protocolo para além das reposições financeiras que a Câmara Municipal entender. ----------

6.ª - Vigência

O presente protocolo produz efeitos para a época desportiva 2023/2024. ----------

7.ª - Acompanhamento

1 - Apresentação relatório de contas no Núcleo de Contabilidade, Aprovisionamento e Armazéns, no final da época. ----------

2 - A Câmara Municipal acompanhará a execução deste protocolo, através do Serviço de Desporto, Juventude e Associativismo. ----------

3 - A associação obriga-se a elaborar um relatório informativo no fim da época desportiva, e a apresentá-lo à Câmara Municipal no mês seguinte. ----------

O presente protocolo foi feito em dois (2) exemplares, para que cada outorgante fique com seu. "----------

Após análise e discussão foi deliberado, por unanimidade e em minuta, aprovar o presente protocolo. ----------

8.3 – PRÉMIOS CHEGAS DE TOUROS DE BOVINOS RAÇA MIRANDESA 2023. -

Presente ao Órgão Executivo uma informação subscrita pelo Técnico Superior Médico Veterinário Ricardo André Ramos Marcos, cujo teor é o seguinte: ----------

"Relativamente ao assunto mencionado em epígrafe, com efeito na demonstração e valorização da Raça Autóctone de Bovinos de Raça Mirandesa, com o intuito de promover a raça autóctone mirandesa irá decorrer no dia 12 de agosto de 2023 às Chegas de Touros de Bovinos da Raça Mirandesa 2023. ----------

No sentido de premiar os animais a concurso e apoiar os criadores que irão participar, e conforme regulamento aprovado, estes têm os prémios de participação conforme o seu desempenho e prestação no decorrer do evento, no valor total de prémios de 2.000€." -------

Após análise e discussão, foi deliberado por unanimidade e em minuta, concordar com o proposto e autorizar a atribuição dos referidos prémios, nos termos da alínea u), do n.º 1, do

art.º 33.º, do Regime Jurídico das Autarquias Locais, aprovado e publicado como Anexo I à Lei n.º 75/2013 de 12 de setembro, na sua atual redação, ficando os mesmos sob a responsabilidade do Técnico Superior Médico Veterinário Ricardo André Ramos Marcos. –

8.4 – PRÉMIOS CONCURSO CONCELHIO DE BOVINOS RAÇA MIRANDESA 2023. ----------

Presente ao Órgão Executivo uma informação subscrita pelo Técnico Superior Médico Veterinário Ricardo André Ramos Marcos, cujo teor é o seguinte: ----------

"Relativamente ao assunto mencionado em epígrafe, com efeito na demonstração e valorização da Raça Autóctone de Bovinos de Raça Mirandesa, com o intuito de promover a raça autóctone mirandesa irá decorrer no dia 12 de agosto de 2023 o Concurso Concelhio de Bovinos da Raça Mirandesa 2023. ----------

No sentido de premiar os animais a concurso e apoiar os criadores que irão participar, e conforme regulamento aprovado, estes têm os prémios de participação conforme a sua secção e classificação pelo júri do concurso, no valor total de prémios de 4.700€." ----------

Após análise e discussão, foi deliberado por unanimidade e em minuta, concordar com o proposto e autorizar a atribuição dos referidos prémios, nos termos da alínea u), do n.º 1, do art.º 33.º, do Regime Jurídico das Autarquias Locais, aprovado e publicado como Anexo I à Lei n.º 75/2013 de 12 de setembro, na sua atual redação, ficando os mesmos sob a responsabilidade do Técnico Superior Médico Veterinário Ricardo André Ramos Marcos. –

9 – PROPOSTA DE PLANO DE SEGURANÇA PARA O MUNICÍPIO DE VINHAIS (DECRETO-LEI N.º 65/2021). ----------

Presente ao Órgão Executivo uma informação subscrita pelo Técnico Superior de Informática, José António Gomes Assis Rodrigues, que vinha acompanhada do Plano de

Segurança para o Município de Vinhais (em conformidade com o Decreto-Lei n.º 65/2021), cujo teor é o seguinte: ----------

"Segue em anexo o Plano de Segurança alinhado com o Decreto-Lei n.º 65/2021, e o enquadramento do mesmo. ----------
O Plano de Segurança tem um sumário executivo e engloba todas as políticas e documentos individuais, em conformidade com o Decreto-Lei n.º 65/2021.----------
O Plano de Segurança deve ser aprovado em reunião de Câmara.----------
O documento é interno à entidade, e por esse motivo não é necessário a sua comunicação ao Centro Nacional de Cibersegurança (CNCS).----------
O documento principal «Plano de Segurança» é composto pelas Políticas e documentos:----

- 01 - Política de segurança da informação----------
- 02 - Política de cibersegurança----------
- 03 - Política de Utilização Aceitável de Ativos e Boas Práticas de Cibersegurança---
- 04 - Política de privacidade----------
- 05 - Análise e gestão de risco----------
- 06 - Notificação e gestão de incidentes----------
- 07 - Responsáveis de segurança----------
- 08 – Contactos permanentes----------

Sumário Executivo

O plano de segurança é um documento que, no âmbito de aplicação do Decreto-Lei n.º 65/2021, pretende descrever como a Câmara Municipal de Vinhais aborda todas as suas necessidades e intenções de segurança de informação e cibersegurança. O documento é enquadrado ao nível estratégico da entidade, de forma a garantir o envolvimento e compromisso da gestão de topo. A Câmara Municipal de Vinhais deve, de forma periódica, adaptar, rever, melhorar e atualizar o documento com o objetivo de acompanhar a evolução da própria entidade. ----------

O plano de segurança é assinado pelo responsável de segurança, formalmente aprovado pela gestão de topo, e disponibilizado em formato digital, de fácil acesso pelas todas partes interessadas. Não é previsto o envio deste documento para o CNCS.----------

O plano de segurança do Município de Vinhais engloba:----------

» Política de segurança da informação----------
A segurança da informação é fundamental e uma das maiores prioridades do Município de Vinhais. Sempre com a preocupação de transparência e imparcialidade, a Política de Segurança da Informação estabelece os princípios gerais que devem ser aplicados pela Câmara Municipal de Vinhais, de modo a garantir confidencialidade, integridade, disponibilidade e legitimidade de toda informação, quer esta se encontre em suporte físico, digital ou intelectual.----------

» Política de cibersegurança----------
A cibersegurança define-se como a preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço e o Município de Vinhais tem a preocupação constante de garantir que os seus ativos e sistemas de informação estão em conformidade com padrões, regulamentos, leis e normas nacionais, europeus e internacionais. O Município de Vinhais estabelece, através a Política de Cibersegurança, os princípios da gestão da cibersegurança, visando atingir um nível de capacidade aceitável nos seguintes macro objetivos: Identificação, Proteção, Deteção, Resposta, Recuperação, Testes, Cooperação e partilha de informação e Melhoria contínua.----------

» Política de Utilização Aceitável de Ativos e Boas Práticas de Cibersegurança----------
Com o objetivo de reforçar e amadurecer a ciber resiliência, melhorar a proteção dos dados e garantir o funcionamento contínuo de todos os serviços prestados, é necessário que todos os colaboradores tenham conhecimento da Política de Utilização Aceitável de ativos de tecnologias de informação e comunicação do Município de Vinhais. Um colaborador que tem uma boa ciber consciência, e que conhece e segue as boas práticas de cibersegurança, passa a fazer parte da primeira linha de defesa na proteção do Município de Vinhais. Este documento define a Política de Utilização Aceitável de Ativos de tecnologias de informação

e comunicação do Município de Vinhais, bem como as responsabilidades dos colaboradores na sua utilização, de forma a garantir a confidencialidade, disponibilidade e integridade da informação. O documento pretende também sensibilizar os colaboradores e servir de guia de boas práticas de cibersegurança.----------

» Política de privacidade----------

O Regulamento Geral Sobre a Proteção de Dados (RGPD) da União Europeia estabelece uma norma importante no que se refere a direitos de privacidade, segurança das informações e conformidade. O Município de Vinhais acredita que a privacidade é um direito fundamental e que o RGPD representa um importante passo em frente no sentido da proteção e do respeito pelos direitos de privacidade das pessoas. O documento pretende descrever como o Município de Vinhais está alinhado, e em conformidade, com o Regulamento Geral sobre a Proteção de Dados.----------

» Análise e gestão de risco----------

A Câmara Municipal de Vinhais deve realizar, pelo menos uma vez por ano, uma análise dos riscos de âmbito global. Deve também realizar uma análise dos riscos, de forma contínua, em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, também aos ativos que garantam a prestação dos serviços essenciais. O documento pretende reportar o estado de segurança atual da entidade, objetivos e planos de melhoria futura, riscos e vulnerabilidades detetados e sugerir, de forma priorizada, medidas técnicas e organizativas de mitigação e, de forma sumária, descrever a metodologia a ser usada na gestão de risco dos ativos.----------

» Notificação e gestão de incidentes----------

A Câmara Municipal de Vinhais deve notificar o CNCS da ocorrência de incidentes detetados, ou a estes comunicados pelos seus clientes, utilizadores ou outras entidades, com impacto relevante ou substancial. O documento pretende descrever o procedimento a seguir relacionado com a notificação de incidentes, em conformidade com o Decreto-Lei n.º 65/2021, e de forma sumária, fornecer recomendações sobre como abordar a gestão de incidentes de cibersegurança.----------

» Responsável de segurança----------

Identificação do responsável de segurança do Município de Vinhais, que é comunicado ao CNCS em conformidade com o Decreto-Lei n.º 65/2021, e permanentemente atualizado.---

» Contacto permanente----------

Identificação do ponto de contacto permanente do Município de Vinhais, que é comunicado ao CNCS em conformidade com o Decreto-Lei n.º 65/2021, e permanentemente atualizado.

» Política de distribuição ----------

O documento visa definir como as políticas e os documentos, que integram este plano de segurança, devem ser distribuídos.----------

Índice ----------

Política de Segurança da Informação ----------

Município de Vinhais ----------

Rua das Freiras, 13----------

5320-326 Vinhais ----------

Introdução----------

A segurança da informação é fundamental e uma das maiores prioridades do Município de Vinhais. Sempre com a preocupação de transparência e imparcialidade, a presente Política

de Segurança da Informação estabelece, através o Sistema de Gestão de Segurança da Informação (SGSI), os princípios gerais que devem ser aplicados pela entidade, de modo a garantir confidencialidade, integridade, disponibilidade e legitimidade de toda informação, quer esta se encontre em suporte físico, digital ou intelectual.----------

Todos nós somos responsáveis pela segurança da informação e todos temos a responsabilidade de proteger os nossos dados e os que nos são confiados.----------

Público-alvo e âmbito----------

A Política de Segurança da Informação do Município de Vinhais destina-se a colaboradores, estagiários, fornecedores, prestadores de serviços, parceiros, bem como terceiros e todas partes interessadas que, de alguma forma, possam interagir com a informação do Município de Vinhais, de forma direta ou indireta.----------

O âmbito de aplicação desta política estende-se a todas as áreas de funcionamento do Município de Vinhais cuja atuação tem impactos na segurança da informação.----------

Sistema de Gestão de Segurança da Informação----------

O modelo do Sistema de Gestão de Segurança da Informação (SGSI) do Município de Vinhais, assenta em quatro pilares: ----------

- **Confidencialidade**: assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é restrito a utilizadores legítimos.-
- **Integridade**: garantir a veracidade e complementaridade da informação, bem como os seus métodos de processamento. O conteúdo da informação não pode ser modificado de forma inesperada. ----------
- **Disponibilidade**: assegurar o acesso à informação e bens associados por quem devidamente autorizado. A informação deve estar acessível sempre que necessário.
- **Conformidade**: garantir que toda a informação é recolhida e tratada em conformidade com os padrões, regulamentos, leis e normas nacionais, europeus e internacionais, relevantes em matéria de segurança da informação.----------

Objetivos globais ----------

O Município de Vinhais mantém um Sistema de Gestão de Segurança de Informação (SGSI) constituído por políticas, processos e procedimentos. O SGSI foi elaborado para manter, rever e continuamente melhorar a segurança de informação no Município de Vinhais, e pretende:----------

- Garantir que todos os colaboradores, e terceiros, têm conhecimento e cumprem esta política, e outras políticas e/ou procedimentos de segurança existentes. ----------
- Definir e comunicar responsabilidades ao nível da Segurança de Informação na entidade.----------
- Promover uma cultura de sensibilização e compromisso contínua para a segurança da informação e realizar ações de formação para garantir que todos os colaboradores compreendem a forma como a segurança de informação faz parte das suas funções e as responsabilidades que têm na proteção da confidencialidade, integridade e disponibilidade da informação.----------
- Incluir a segurança de informação como componente essencial de todos os aspetos de planeamento, atividades e operações da entidade.----------
- Avaliar continuamente as ameaças de segurança de informação, garantindo que estas são identificadas e geridas tendo por base a avaliação de risco e com a aplicação dos controlos adequados.----------
- Assegurar a disponibilidade e fiabilidade dos equipamentos, infraestruturas e sistemas que suportam a atividades da entidade e promover a proteção adequada de sistemas de informação e comunicações. ----------
- Promover a deteção, documentação, notificação e investigação de incidentes de segurança de forma eficaz e eficiente para mitigar os impactos deste tipo de incidentes na entidade.----------
- Assegurar que a entidade tem a capacidade de recuperar e continuar a prestação dos seus serviços, dentro prazos aceitáveis, caso ocorram incidentes de segurança graves.
- Garantir a disponibilização dos recursos necessários a garantir a efetiva manutenção, revisão e melhoria contínua do SGSI. ----------
- Assegurar que os fornecedores externos se enquadram nas necessidades e requisitos de segurança da entidade.----------

- Garantir a proteção de dados pessoais.----------

Responsabilidades----------

Todos os colaboradores do Município de Vinhais, bem como terceiros e demais entidades que, de alguma forma, possam interagir com a informação do Município de Vinhais, de forma direta ou indireta, estão obrigados a cumprir e a fazer cumprir todas as políticas de segurança da informação. Devem contribuir proactivamente para a devida proteção da informação e ativos que lhe são confiados, e devem imediatamente reportar ao Município de Vinhais a ocorrência de qualquer incidente ou anomalia que possa provocar, ou que já provocou, uma quebra de segurança da informação.----------

Princípios da Segurança de Informação----------

Normas de conduta ----------

O Município de Vinhais define normas de conduta relativas à segurança da informação, aplicáveis aos seus colaboradores, fornecedores externos e demais entidades externas, nomeadamente no:----------

- Cumprimento da presente Política e da demais documentação de segurança da informação.----------
- Utilização dos recursos tecnológicos e dos sistemas disponibilizados pelo Município de Vinhais.----------
- Tratamento da informação e dados pessoais sob a responsabilidade do Município de Vinhais.----------
- Tratamento dos incumprimentos ou violações da presente política ou das demais políticas e procedimentos de segurança da informação. ----------

Recursos humanos----------

A segurança da informação é aplicável a todos os colaboradores do Município de Vinhais em todos os departamentos, de forma transversal, devendo ser atribuídas responsabilidades específicas a determinadas funções. Nesse sentido, o Município de Vinhais deve promover a formação e transmitir a informação necessária para que os seus colaboradores, bem como

os colaboradores de fornecedores e outras entidades externas, estejam aptos a assumir as suas responsabilidades no âmbito da segurança da informação.----------

Gestão de Ativos----------

A informação gerida pelo Município de Vinhais, os seus processos e infraestruturas de suporte, colaboradores, terceiras partes, instalações, equipamentos, documentos, sistemas, aplicações e redes são ativos valiosos para a organização. Devem ser, por isso, adequadamente protegidos, em conformidade com os procedimentos de segurança da informação aprovados pelo Município de Vinhais, em todo o seu ciclo de vida, o qual inclui a sua criação, manuseamento, armazenamento, transporte e destruição. A informação gerida pelo Município de Vinhais deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi gerada ou confiada.----------

Sistemas de informação----------

O armazenamento de informação é maioritariamente realizado em arquivos tecnológicos, pelo que deve ser prestada especial atenção aos procedimentos específicos que gerem os sistemas de informação, bem como os ativos que os suportam. Os sistemas de informação do Município de Vinhais devem ser planeados, especificados, desenvolvidos, testados, implantados e geridos tendo em conta as necessidades e os requisitos de segurança da informação; confidencialidade, integridade, disponibilidade e legitimidade.----------

Dados Pessoais----------

O Município de Vinhais assume o compromisso de efetuar todos os esforços para garantir a privacidade e a proteção dos dados pessoais que lhe são confiados, em conformidade com a regulamentação aplicável e, em particular, com o Regulamento Geral sobre Proteção de Dados. O Município de Vinhais classifica os dados pessoais como confidenciais ou sensíveis, adotando as medidas adequadas de segurança físicas, lógicas, técnicas e organizativas, de forma a proteger os dados pessoais contra a sua difusão, alteração, perda, má utilização, tratamento e acesso não autorizado ou roubo, bem como contra qualquer outra forma de tratamento ilícito.----------

Gestão de risco----------

Uma das áreas prioritárias do Município de Vinhais é a gestão (identificação, avaliação e tratamento) contínua dos riscos. A gestão de risco inclui a implementação de controlos e mecanismos de segurança que visam mitigar ou limitar os potenciais danos provocados pela exploração das vulnerabilidades dos ativos, de forma a minimizar a ocorrência de incidentes e garantir um nível de segurança adequado face ao risco que o Município de Vinhais está disposto a assumir. Estas medidas devem ser definidas de acordo com os objetivos e as responsabilidades do Município de Vinhais, tendo em consideração a eficiência, o custo, o esforço e a sua aplicabilidade.----------

Gestão de incidentes e Continuidade da prestação de serviços----------

Todos os eventos que possam pôr em causa a prestação de serviços, ou comprometer a segurança da informação, serão tratados como incidentes de segurança, em conformidade com os procedimentos de gestão de incidentes do Município de Vinhais. A disponibilidade da informação, não descurando a responsabilidade dos restantes compromissos de segurança da informação, será assegurada pela implementação de respostas a incidentes disruptivos e que se integram no âmbito da gestão da continuidade da prestação de serviços do Município de Vinhais.----------

Cibersegurança e resiliência----------

Reconhecendo a importância da cibersegurança como área específica e essencial no âmbito da segurança da informação, o Município de Vinhais deverá, de forma contínua, desenvolver ações dedicadas com o propósito de aumentar o nível de cibersegurança e resiliência da organização. O Município de Vinhais deverá tomar medidas de cibersegurança e estabelecer, sempre que possível, protocolos e processos de cooperação com entidades com funções de autoridade nacional competente em matéria de cibersegurança. ----------

Segurança física e controlo de acesso----------

O Município de Vinhais deve controlar, monitorizar e limitar o acesso e permanência de terceiros, e colaboradores, em áreas seguras (datacenters, arquivos centrais, server rooms etc.) das instalações da entidade.----------

Disposições Finais----------

A presente política deve ser revista sempre que se verifique alguma alteração no âmbito da segurança da informação, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas recomendadas pela indústria, garantindo que continua a ser relevante e adequado. As exceções à presente política deverão ser previamente justificadas através de um processo formal de aceitação de risco e previamente autorizadas e formalmente registadas e monitorizadas. ----------

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.----------

Política de Cibersegurança ----------

Município de Vinhais ----------

Rua das Freiras, 13----------

5320-326 Vinhais----------

Introdução----------

A cibersegurança define-se como a preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço, ou seja, no espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar e interagir por via de software, plataformas ou outros serviços de informação.----------

O Município de Vinhais tem a preocupação constante de garantir que os seus ativos e sistemas de informação estão em conformidade com padrões, regulamentos, leis e normas nacionais, europeus e internacionais, nomeadamente;----------

- Quadro Nacional de Referência para a Cibersegurança, Centro Nacional de Cibersegurança (CNCS) ----------
- O Regime Jurídico da Segurança do Ciberespaço, Decreto-Lei n.º 65/2021----------
- O Regulamento Geral sobre a Proteção de Dados 2016/679 ----------

O Município de Vinhais estabelece, através da presente Política de Cibersegurança, os princípios da gestão da cibersegurança, visando atingir um nível de capacidade aceitável nos seguintes macro objetivos: **Identificação, Proteção, Deteção, Resposta, Recuperação, Testes, Cooperação e partilha de informação e Melhoria contínua**.----------

Público-alvo e âmbito ----------

A Política de cibersegurança do Município de Vinhais destina-se a colaboradores, estagiários, fornecedores, prestadores de serviços, parceiros, bem como terceiros e todas partes interessadas que, de alguma forma, possam interagir com a cibersegurança do Município de Vinhais, de forma direta ou indireta. O âmbito de aplicação desta política estende-se a todas as áreas de funcionamento do Município de Vinhais cuja atuação tem impactos na cibersegurança.----------

Objetivos globais----------

São prosseguidos os seguintes objetivos para assegurar a cibersegurança no Município de Vinhais:----------

» **Identificação**----------

- Assegurar a conformidade com a legislação, regulamentação e demais normas aplicáveis.----------
- Cumprir com os requisitos de confidencialidade, integridade e disponibilidade adequados aos objetivos definidos pelo Município de Vinhais.----------
- Identificar e classificar os ativos de informação em função da sua relevância e criticidade, de forma a que possam ser adequadamente protegidos em todo o seu ciclo de vida.----------
- Assegurar que os fornecedores e prestadores de serviço se enquadram nas necessidades e requisitos de cibersegurança do Município de Vinhais.----------
- Identificar, avaliar e tratar os riscos de cibersegurança inerentes à atividade e serviços prestados do Município de Vinhais e aos quais os seus ativos se encontram expostos.
- Estabelecer uma estratégia de gestão do risco de acordo com a tolerância ao risco da organização.----------
- Implementar controlos e mecanismos de segurança que visam mitigar ou limitar os potenciais danos provocados pela exploração das vulnerabilidades dos ativos, de forma a minimizar a ocorrência de incidentes de segurança da informação e garantir um nível de segurança adequado face ao risco que o Município de Vinhais está disposto a assumir.----------

» **Proteção** ----------

- Estabelecer e implementar controlos para proteger os ativos de informação do Município de Vinhais de roubo, intrusão, abuso ou outras formas de tratamento ilícito.----------
- Assegurar a disponibilidade e fiabilidade dos equipamentos, infraestruturas e sistemas que suportam a atividade e os serviços prestados do Município de Vinhais.
- Promover uma cultura de sensibilização e compromisso para a cibersegurança motivando colaboradores e terceiros a tomarem conhecimento e assumirem a responsabilidade pela sua intervenção, de forma a minimizar o risco de ciber incidentes.----------
- Assegurar a proteção de dados pessoais, nos termos previstos na legislação aplicável.

» **Deteção**

- Monitorizar anomalias e eventos de cibersegurança, em tempo útil, e compreender o impacto potencial desses eventos.----------
- Monitorizar continuamente as redes e sistemas de informação para identificar eventos de cibersegurança e verificar a eficácia das medidas de proteção aplicadas.
- Implementar e manter processos de deteção de eventos de ciber risco.----------

» **Resposta**----------

- Identificar, conter e solucionar incidentes de segurança da informação e, em particular, ciberataques.----------
- Reduzir os danos inerentes à ocorrência de incidentes de segurança da informação, bem como minimizar o seu impacto.----------
- Garantir que os incidentes de segurança da informação são reportados em conformidade com a legislação em vigor e com os procedimentos internos definidos para o efeito.----------

» **Recuperação**----------

- Assegurar que o Município de Vinhais tem a capacidade de continuar a prestação dos seus serviços, nomeadamente serviços críticos, caso ocorram incidentes de segurança

da informação graves ou ciberataques, nas condições definidas na regulamentação, normas e procedimentos específicos aplicáveis.----------

- Assegurar a redundância de equipamentos, infraestruturas e sistemas de informação que suportam os serviços essenciais e críticos, evitando assim pontos únicos de falha.
- Minimizar os impactos negativos que possam advir da ocorrência de incidentes de segurança graves, tanto para a reputação da entidade como para todas as partes interessadas do Município de Vinhais.----------

» **Testes**----------

- Avaliar a eficácia dos controlos implementados no Município de Vinhais para mitigação dos riscos identificados. ----------
- Garantir a manutenção da integridade, disponibilidade e confidencialidade dos sistemas de informação do Município de Vinhais.----------
- Identificar e mitigar as vulnerabilidades existentes na infraestrutura do Município de Vinhais.----------
- Avaliar a eficácia e identificar pontos de falha e potenciais melhorias dos procedimentos e planos de resposta e recuperação a incidentes de segurança da informação. ----------

» **Cooperação e partilha de informação**----------

- Promover a partilha de informação relevante em matéria de cibersegurança, internamente e externamente.----------
- Contribuir para a globalização da consciencialização sobre cibersegurança.----------

» **Melhoria Contínua**----------

- Atualizar os procedimentos, políticas, planos e processos do Município de Vinhais sempre que se verifique alguma alteração no âmbito da cibersegurança, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas de cibersegurança recomendadas pela indústria.----------
- Promover estratégias de implementação de oportunidades de melhoria, nomeadamente as propostas resultantes de auditorias, testes de intrusão ou outros projetos internos ou externos em matéria de Cibersegurança.----------

Responsabilidades ----------

Colaboradores----------

Os colaboradores do Município de Vinhais devem compreender claramente os riscos de cibersegurança a que estão expostos no exercício das suas funções, bem como os seus papéis e responsabilidades no âmbito da mitigação desses riscos e da consequente proteção dos ativos e da informação do Município de Vinhais. Em particular, os colaboradores do Município de Vinhais são responsáveis por:----------

- Cumprir todas as normas, códigos, políticas e procedimentos definidos no âmbito da cibersegurança.----------
- Os ativos de informação que lhe são confiados, devendo contribuir proactivamente para a devida proteção dos mesmos.----------

Fornecedores, prestadores de serviço e outras entidades externas----------

Os fornecedores, prestadores de serviço e demais entidades externas devem adotar condutas e procedimentos consistentes com a presente Política. Em particular, os contratos entre o Município de Vinhais e as empresas prestadoras de serviços com acesso aos sistemas de informação e/ou ambiente tecnológico devem conter cláusulas e requisitos de segurança que garantam a confidencialidade entre as partes e que assegurem que os profissionais sob a sua responsabilidade cumpram a presente política, norma, códigos e demais procedimentos que sejam aplicáveis. Os fornecedores e demais entidades externas são também responsáveis por reportar ao Município de Vinhais a ocorrência de qualquer incidente ou anomalia que possa provocar, ou que já provocou, uma quebra de segurança da informação.----------

Objetivos de Cibersegurança no Município de Vinhais----------

Identificação----------

Gestão de Ativos----------

A informação gerida pelo Município de Vinhais, os seus processos e infraestruturas de suporte, colaboradores, terceiras partes, equipamentos, documentos, sistemas, aplicações e redes são ativos relevantes para a organização. São, por isso, devidamente identificados, inventariados e classificados em função dessa mesma importância e criticidade, de forma a que possam ser adequadamente protegidos em todo o seu ciclo de vida (o qual inclui a sua criação, manuseamento, armazenamento, transporte e destruição). ----------

Gestão de fornecedores e prestadores de serviços ----------

Na contratação de fornecedores e prestadores de serviços, o Município de Vinhais segue um processo standard, o qual inclui uma pesquisa de mercado a várias entidades às quais se reconheça competência e conhecimentos técnicos adequados para a prestação dos serviços ou fornecimento dos produtos. Devido à dimensão reduzida do número de fornecedores e prestadores de serviço com acesso aos sistemas de informação e/ou ambiente tecnológico do Município de Vinhais, o acompanhamento do seu desempenho é feito continuamente. De forma regular e em conformidade com o contratualizado, é ainda efetuada a avaliação do cumprimento dos níveis de serviço e dos requisitos de segurança e cibersegurança acordados.

Gestão do Risco ----------

Uma das áreas prioritárias do Município de Vinhais é a gestão (identificação, avaliação e tratamento) contínua dos riscos. A metodologia de gestão do risco do Município de Vinhais envolve:----------

- Identificação e documentação das ameaças, internas e externas, que possam explorar as vulnerabilidades dos ativos do Município de Vinhais, pondo em causa a integridade, confidencialidade ou disponibilidade dos mesmos.----------
- Avaliação baseada em cenários de risco, para os quais são aferidos a probabilidade e o impacto, que compõem o nível de risco. ----------
- Tratamento dos riscos, priorizados de acordo com o nível de risco determinado, a criticidade do ativo e a tolerância ao risco da organização.----------

No âmbito do tratamento, a gestão do risco inclui a implementação de controlos e mecanismos de segurança que visam mitigar ou limitar os potenciais danos provocados pela exploração das vulnerabilidades dos ativos, de forma a minimizar a ocorrência de incidentes de segurança da informação e garantir um nível de segurança adequado face ao risco que o Município de Vinhais pode assumir. Estas medidas são definidas de acordo com os objetivos e as responsabilidades do Município de Vinhais, tendo em conta a eficiência, o custo, o esforço e a sua aplicabilidade. A gestão do risco do Município de Vinhais incorpora ainda o acompanhamento dos riscos operacionais aos quais o Município de Vinhais se encontra

exposto, através do estabelecimento de procedimentos de avaliação do nível de exposição e do limite de risco considerado aceitável visando os objetivos da entidade.----------

Proteção ----------

Controlo de Acessos----------

As identidades e credenciais de acesso às redes e sistemas de informação do Município de Vinhais são emitidas, geridas, verificadas, revistas, revogadas e auditadas segundo os princípios do menor privilégio, da funcionalidade mínima e da segregação de funções. Estes princípios aplicam-se transversalmente a acessos internos (de colaboradores), externos (de fornecedores, prestadores de serviço ou clientes) e remotos (internos ou externos). Os mecanismos de autenticação nas redes e sistemas de informação do Município de Vinhais são definidos e mantidos de acordo com as suas características e perfis de acessos, por forma a permitir a manutenção da integridade e confidencialidade da informação.----------

Segurança de dados e das comunicações----------

As redes e os sistemas de informação do Município de Vinhais devem proteger a segurança (confidencialidade, integridade e disponibilidade) dos dados armazenados, dos dados em circulação, dos dados em utilização e dos fluxos de transferência da informação. Para tal, o Município de Vinhais tem implementados controlos de: ----------

- Classificação, manuseamento e destruição da informação.----------
- Criptografia.----------
- Prevenção de exfiltração e perda de informação (DLP/Data Loss Protection).--------
- Desenvolvimento seguro e restrição na utilização de software.----------
- Prevenção e deteção de atividade maliciosa.----------

Recursos Humanos----------

O Município de Vinhais promove ações de formação e sensibilização em Segurança da Informação e transmite a informação necessária para que a gestão de topo e os seus colaboradores estejam aptos a assumir as suas responsabilidades no âmbito da cibersegurança. Os colaboradores dos departamentos com acessos privilegiados às redes e aos sistemas de informação do Município de Vinhais têm, adicionalmente e antes de

assumirem funções, formação específica sobre gestão de acessos e demais procedimentos operacionais. Os colaboradores com responsabilidades acrescidas na cibersegurança do Município de Vinhais têm ainda formação especializada na área de Segurança da Informação.----------

Deteção ----------

O Município de Vinhais recorre a serviços externos especializados em cibersegurança para a avaliação periódica de vulnerabilidades sistemas de informação, nomeadamente através de processos automáticos de deteção, identificação, catalogação e monitorização de atividade maliciosa. Os resultados e vulnerabilidades identificadas são posteriormente incorporados no plano interno de ação do Município de Vinhais, de forma a serem alvo de análise no âmbito da gestão do risco.----------

Resposta----------

O processo de resposta a incidentes do Município de Vinhais encontra-se sistematizado em procedimentos de gestão de incidentes e, em particular, de ciberataques, nos quais se encontram definidas as tarefas de identificação, classificação, intervenção técnica, registo e tratamento que devem ser realizadas após a deteção de um incidente. Desta forma, o Município de Vinhais visa garantir uma resposta rápida e eficaz que permita minimizar os danos potenciais ao nível da confidencialidade, integridade e disponibilidade dos sistemas de informação. Estes procedimentos, a par com outros procedimentos de comunicação e reporte transversais a todas as áreas da organização, definem ainda o plano de comunicações para as partes interessadas (internas e externas) do Município de Vinhais, nomeadamente o conteúdo relevante a ser partilhado e os canais adequados, com a finalidade de identificar, conter e solucionar o incidente, bem como de minimizar o seu impacto para essas mesmas partes interessadas.----------

Recuperação----------

Cópias de segurança----------

O Município de Vinhais realiza cópias de segurança da informação crítica armazenada nos seus sistemas de informação, guardando as mesmas numa localização alternativa, quando possível, e garantido a manutenção da confidencialidade da informação. O Município de

Vinhais assegura ainda a integridade e disponibilidade das cópias de segurança, estabelecendo para isso procedimentos de restauro que garantem a reposição eficiente das cópias de segurança em caso de necessidade dentro do objetivo de tempo de recuperação. Estes procedimentos são testados com regularidade, de forma a validar a adequação dos mesmos, bem como, precisamente, a integridade e disponibilidade das cópias realizadas.---

Plano de Recuperação e Continuidade de Prestação de Serviços ----------

A disponibilidade da informação, dos sistemas e da infraestrutura encontram-se asseguradas pela implementação de procedimentos de gestão e planos de recuperação de incidentes de segurança da informação graves ou ciberataques. Deste modo e na ocorrência de tais incidentes, o Município de Vinhais tem a capacidade de continuar a prestação dos seus serviços, nomeadamente serviços essenciais e críticos, em condições adequadas e nos termos definidos na regulamentação, normas e procedimentos específicos aplicáveis, minimizando os impactos negativos. No que diz respeito à redundância da infraestrutura, o datacenter do Município de Vinhais está configurado de forma a minimizar o tempo de disrupção da operação do Município de Vinhais.----------

Testes----------

No âmbito da gestão do risco, o Município de Vinhais realiza testes para avaliar a eficácia dos controlos implementados para mitigação dos riscos identificados. Além disso, sempre que a infraestrutura do Município de Vinhais sofre atualizações, seja por via da integração de um novo sistema de informação ou por alteração significativa de um sistema já existente, é aplicado um plano de testes de segurança para assegurar a manutenção da integridade, disponibilidade e confidencialidade da informação. O Município de Vinhais realiza ainda testes periódicos aos seus procedimentos de gestão de incidentes, de ciberataques, aos planos de continuidade de prestação de serviços e de recuperação de datacenter, baseados em cenários plausíveis, com o objetivo de avaliar a sua eficácia e identificar pontos de falha e potenciais melhorias.----------

Cooperação e partilha de informação ----------

A informação relevante em matéria de cibersegurança é partilhada com as partes interessadas do Município de Vinhais. Adicionalmente, o Município de Vinhais procura colaborar com

outros grupos de interesse, associações ou organizações da indústria, de forma a alcançar uma consciência mais abrangente sobre cibersegurança e informações sobre boas práticas, indicadores de risco, ameaças, vulnerabilidades e ciberataques.----------

Melhoria Contínua----------

O Município de Vinhais está ciente não só da sua realidade dinâmica ao nível dos processos de atividade, ativos e recursos humanos, mas também da constante evolução das ciberameaças e exploração de novas vulnerabilidades. A cibersegurança é transversal a todas as atividades da organização, pelo que a sua melhoria contínua constitui um dos objetivos do Município de Vinhais. Neste sentido, o Município de Vinhais atualiza os seus procedimentos, políticas, planos e processos sempre que se verifique alguma alteração no âmbito da cibersegurança, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas de cibersegurança recomendadas pela indústria. Para além disso, o plano da melhoria contínua incorpora as oportunidades de melhoria propostas por auditorias, testes de intrusão ou outros projetos internos ou externos em matéria de cibersegurança, bem como as lições aprendidas no decorrer da resposta e recuperação de incidentes de segurança da informação.----------

Disposições Finais----------

A presente política deve ser revista sempre que se verifique alguma alteração no âmbito da cibersegurança, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas recomendadas pela indústria, garantindo que continua a ser relevante e adequado. As exceções à presente política deverão ser previamente justificadas através de um processo formal de aceitação de risco e previamente autorizadas e formalmente registadas e monitorizadas.----------

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.----------

Política de Utilização Aceitável de Ativos e Boas Práticas de Cibersegurança----------

Município de Vinhais----------

Rua das Freiras, 13----------

5320-326 Vinhais----------

Introdução ----------

Para reforçar e amadurecer a ciber resiliência, melhorar a proteção dos dados e garantir o funcionamento contínuo de todos os serviços prestados, é necessário que todos os colaboradores tenham conhecimento da Política de Utilização Aceitável de ativos de tecnologias de informação e comunicação do Município de Vinhais. Um colaborador que tem uma boa ciber consciência, e que conhece e segue as boas práticas de cibersegurança, passa a fazer parte da primeira linha de defesa na proteção do Município de Vinhais.--------

Público-alvo ----------

Este documento é destinado a todos os colaboradores do Município de Vinhais, bem como estagiários, fornecedores, prestadores de serviços, parceiros, terceiros e demais entidades externas, que prestem serviços ao Município de Vinhais, e que acedem à informação, e/ou dados pessoais, e/ou têm acesso à rede, e/ou usem equipamentos de informática e/ou de comunicação do Município de Vinhais.----------

Objetivo do presente documento----------

Este documento define a Política de Utilização Aceitável de Ativos de tecnologias de informação e comunicação do Município de Vinhais, bem como as responsabilidades dos colaboradores na sua utilização, de forma a garantir a confidencialidade, disponibilidade e integridade da informação. O documento pretende também sensibilizar os colaboradores e servir de guia de boas práticas de cibersegurança.----------

5 Recomendações essenciais de boas práticas de cibersegurança ----------

» Nunca partilhe passwords e códigos de acesso. ----------

» Não use dispositivos USB desconhecidos no PC de trabalho.----------

» Não deixe o PC desbloqueado, mesmo entre amigos ou colegas, sempre usando a combinação de teclas "(WINDOWS) ⊞ + L".----------

» Não deve clicar em anexos ou links de emails ou mensagens suspeitas.----------

» Mantém sempre todos os dispositivos móveis (portáteis, telemóveis, tablets, etc) atualizados, seguros e protegidos.----------

Zero-trust: nunca confiar, sempre verificar.----------

Utilização de computadores ----------

Política de ecrã limpo----------

Se um colaborador estiver ausente do seu computador de trabalho, deve manualmente ativar o bloqueio do ecrã do seu computador, que obrigará à reintrodução da password para entrar na sessão, usando a combinação das teclas "(WINDOWS) ⊞ + L". Sugere-se o administrador de sistemas usar a Política de Grupo para configurar computadores do domínio para automaticamente ativar o bloqueio do ecrã ao fim de 5 minutos de inatividade. Sempre possível deve ter o cuidado de posicionar o ecrã do seu computador de forma a não permitir a sua leitura por terceiros. Os colaboradores que habitualmente usam o seu computador em aviões ou comboios devem utilizar filtros de proteção do ecrã.----------

Instalação de software----------

De forma a assegurar a proteção da informação do Município de Vinhais, os colaboradores **não** podem:----------

- Instalar jogos de computador.----------
- Instalar software que permita a partilha de arquivos na internet (software P2P).------
- Instalar software pessoal, mesmo que licenciado pelo colaborador.----------
- Instalar software ilegal (sem licenciamento ou sem aprovação prévia).----------
- Instalar outro tipo de software nos computadores sem que exista uma razão legítima e devidamente justificada e autorizada pelo Município de Vinhais.----------

Software de segurança do computador----------

Os colaboradores não podem remover, desabilitar ou alterar as configurações dos sistemas de segurança (ex. firewall, definições de encriptação, software de deteção de vírus e atividade malicioso, instalação de patches, etc), sem que exista uma razão válida, com aprovação expressa para o efeito, e autorizada pelo Município de Vinhais. ----------

Proteção dos equipamentos e da informação no trabalho remoto e durante as viagens

Os colaboradores devem garantir que tomam todas as precauções necessárias para proteger os equipamentos do Município de Vinhais em sua posse e a respetiva informação, independentemente da forma como esta seja guardada, evitando o acesso indevido por terceiros. Atualmente o trabalho remoto é prática comum, resultado da oferta tecnológica,

que permite aos colaboradores realizarem tarefas profissionais a partir de casa, do hotel ou de qualquer outro local, de forma simples e eficaz. É importante ter os seguintes cuidados:

- Transporte apenas os documentos (impressos ou digitais) estritamente necessários para o trabalho a realizar.----------
- Os equipamentos não devem ser deixados nas viaturas. ----------
- Os equipamentos não devem ser deixados desprotegidos, devendo a utilização do equipamento ser restrita ao utilizador ao qual está atribuído. É proibida a utilização dos equipamentos do Município de Vinhais por parte de familiares ou amigos do colaborador.----------
- Proteja sempre os dispositivos com palavra-passe, e na sua ausência bloqueie-os. ---
- Deve utilizar apenas ligações a redes Wi-Fi seguras e de confiança.----------
- Não deve solicitar qualquer apoio técnico ou assistência de entidades ou pessoas não autorizadas.----------

Cópia de segurança ----------

Quando possível, de forma a prevenir a perda de informação, os colaboradores devem sempre utilizar o sistema de backup disponibilizado pelo Município de Vinhais e seguir as respetivas instruções. Deve evitar o armazenamento de dados em pastas locais, todos os documentos de trabalho devem estar armazenados nas pastas da rede. Nas localizações onde a ferramenta não esteja disponível, os colaboradores devem solicitar instruções de como proceder de forma a garantir uma cópia de segurança dos seus dados. Caso seja realizada uma cópia para um disco externo amovível o mesmo deverá ser encriptado, isso caso a política se encontra implementada, e não pode ser transportado em conjunto com o computador. O disco deverá ser guardado noutra localização, de forma a garantir a existência de uma cópia da informação.----------

Política de secretária limpa----------

Os dispositivos, documentos, impressões, agendas e blocos de apontamentos com dados confidenciais devem ser tratados de forma a garantir que terceiros não possam ter conhecimento do seu conteúdo. Quando um colaborador estiver ausente do seu posto de trabalho, todos os documentos em papel e todos os dispositivos amovíveis de

armazenamento de dados que possuam informação do Município de Vinhais, devem ser removidos da secretária e colocados dentro de armários ou gavetas devidamente trancadas.

Dispositivos portáteis de armazenamento----------

A utilização de dispositivos portáteis de armazenamento (ex.: Pens USB, Discos externos, SD Cards, etc.) para armazenar, transferir ou transportar informação do Município de Vinhais só é permitida se os mesmos forem previamente encriptados utilizando a tecnologia disponibilizada pela Câmara Municipal de Vinhais, de acordo com os procedimentos existentes, e caso a política se encontra implementada. Sempre que seja necessário disponibilizar a password para acesso à informação encriptada de um dispositivo portátil de armazenamento, esta deve ser comunicada oralmente ou enviada por mensagem, sem mencionar o objetivo da mesma. Os dispositivos portáteis de armazenamento devem ser guardados em locais protegidos, quando não estejam em utilização, e sempre que um colaborador pretenda destruir um dispositivo amovível o mesmo deve ser entregue ao Município de Vinhais para o efeito.----------

Gestão de passwords----------

É da responsabilidade do utilizador garantir a confidencialidade da password da sua conta individual de acesso aos sistemas de informação do Município de Vinhais, sendo proibido partilhar a mesma. Os colaboradores devem aplicar boas práticas de segurança na proteção da sua password: As passwords não devem ser divulgadas a outras pessoas, incluindo quaisquer colaboradores do Município de Vinhais, incluindo os administradores de sistemas ou colaboradores do Helpdesk. Sempre que haja necessidade de guardar alguma password deverá ser realizado num programa que garanta a proteção das mesmas com criptografia.

Sempre que aplicável, a palavra-passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa.----------

A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres:----

- Letras minúsculas (a…z);----------
- Letras maiúsculas (A…Z);----------
- Números (0…9);----------
- Caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : “ ; ‘ < > ? , . /);-------

Para garantir uma adequada gestão das passwords são estabelecidas as seguintes regras:----

- Não conter o primeiro ou último nome do utilizador, de um familiar, de uma pessoa famosa, datas de nascimento ou outra informação pessoal. ----------
- Não conter qualquer outro nome ou palavras facilmente associadas ao utilizador.----
- Não deve ser uma palavra de um dicionário ou outra que faça parte de um dialeto ou gíria de qualquer idioma, nem qualquer uma dessas palavras escrita ao contrário.---
- As últimas vinte e quatro passwords não podem ser reutilizadas.----------
- É exigido ao utilizador a alteração da password inicial que lhe foi atribuída e enviada, após o primeiro login.----------
- Por defeito o período de validade da password é de 60 dias. Findo este período, a password expira e o utilizador terá de a alterar para continuar a ter acesso aos sistemas de informação.----------
- A password deve ser alterada sempre que hajam suspeitas de que a mesma possa ter sido comprometida.----------
- A password não deve ser visualizada no ecrã enquanto está a ser inserida.----------
- Só é possível alterar a password a cada 24 horas.----------
- Passwords usadas pelos utilizadores em contas para fins particulares (por exemplo de emails pessoais), não devem ser usadas nas contas de acesso aos sistemas de informação do Município de Vinhais.----------
- As passwords não devem ser armazenadas em sistemas de registo automático (por exemplo, lembrar/guardar password no browser) ou nos telemóveis.----------
- O número consecutivo de tentativas erradas de acesso aos sistemas com uma password é limitado a 5. O sistema deve recusar o acesso quando este limite é atingido, bloqueando a conta do utilizador por um período de 30 minutos.----------

Vírus, phishing e malware----------

Todos os computadores com acesso à rede do Município de Vinhais, deverão ter um software de antivírus devidamente legalizado e atualizado. Esta regra aplica-se não só aos computadores dos colaboradores do Município de Vinhais como também a computadores de terceiros que necessitem de ligar os seus dispositivos à rede. Os colaboradores devem tomar todas as medidas razoáveis para garantir que não são responsáveis pela introdução de código

malicioso (vírus, malware, etc.) nos sistemas de informação e comunicação, e devem seguir as seguintes recomendações:----------

- Não clicar em anexos ou links de emails, de mensagens instantâneas ou de SMS suspeitos.----------
- Quando se é contactado, confirmar a veracidade do endereço de email, do perfil ou do número de telefone de origem.----------
- Avaliar sempre a oportunidade dos conteúdos de emails, de mensagens instantâneas, de SMS ou de telefonemas.----------
- Não partilhar dados pessoais ou profissionais ou seguir instruções sem verificar noutras fontes a veracidade do pedido.----------
- Desconfiar de mensagens com erros formais de linguagem, mas também não confiar em todas as mensagens apenas porque não apresentam erros formais de linguagem.
- Não partilhar dados sensíveis nas redes sociais porque essa prática pode fornecer informação a possíveis atacantes que queiram realizar spear phishing (phishing dirigido a uma pessoa específica).----------
- Notificar os responsáveis de segurança informática do Município de Vinhais ou das autoridades competentes sempre que se é alvo ou vítima de um ataque deste tipo;---
- Estar atento e não se deixar persuadir sem reflexão por solicitações autoritárias, promessas ou pedidos urgentes. ----------

Utilização do correio eletrónico----------

O correio eletrónico (e-mail) é uma ferramenta de trabalho que deve ser utilizada de forma profissional e cuidada. A utilização imprudente ou inadequada pode dar origem a ataques aos nossos sistemas e à nossa informação. O Município de Vinhais pode disponibilizar acesso a uma conta de email aos seus colaboradores, para desempenho das suas atividades profissionais. O envio e/ou receção de emails relacionados com atividades do Município de Vinhais só pode ser efetuado por via da utilização de contas de email da própria entidade. Não é permitida a utilização de emails pessoais do colaborador (Hotmail, Gmail, Yahoo, etc) para comunicações relacionadas com a atividade da entidade. De igual forma, não devem ser efetuadas comunicações relacionadas com a atividade da entidade para emails pessoais de colaboradores ou terceiros. Devem seguir as seguintes recomendações: ----------

- Verifique sempre os endereços dos destinatários.----------
- Utilize o e-mail de forma segura, produtiva, profissional e educada.----------
- Não abra e-mails e ficheiros de origem desconhecida, elimine-os imediatamente.----
- Não siga as ligações (links) de e-mails suspeitos.----------
- Nunca envie informação pessoal que lhe seja solicitada por e-mail, tal como: n.º do cartão de crédito, username, password, nomes, etc.----------
- Informações críticas ou dados pessoais só podem ser enviados em formato encriptado.----------
- As passwords das contas de email pessoais não podem ser partilhadas. Sempre que for necessário dar acesso a outro colaborador à sua conta de email (por razões justificáveis tais como às assistentes administrativas), tal deve ser feito através das funcionalidades de delegação de permissões do sistema de email.----------

Dispositivos móveis----------

Os equipamentos móveis são uma potencial fonte de perda de informação crítica. Por este motivo, devem ser tratados com especial atenção e devem estar sempre protegidos. Olhe para os seus dispositivos móveis (telemóvel, portátil, PEN, token, pasta de documentos) e verifique se estão aplicadas algumas das seguintes regras de segurança:----------

- Todos os dispositivos portáteis estão protegidos com password.----------
- Os dispositivos portáteis devem ter os dados encriptados sempre que seja tecnicamente possível.----------
- O software deve estar atualizado.----------
- Quando possível, equipamento deve ter instalado um antivírus e uma firewall.-------
- Devem ser feitas cópias de segurança dos dados.----------
- Em locais públicos e transportes públicos os equipamentos devem estar sob vigilância.----------
- O trabalho com equipamentos móveis em locais públicos deve garantir que os dados do ecrã estão protegidos contra pessoas não autorizadas.----------
- Os equipamentos móveis não devem ser deixados nos veículos automóveis.----------
- É proibido desbloquear equipamentos com recurso a ferramentas ou sistemas operativos não autorizados (ex. Jailbreak ou Root).----------

- Os documentos que são levados para trabalhar em casa ou em viagem devem estar protegidos contra acesso indevido.----------

Utilização da internet----------

O Município de Vinhais disponibiliza um acesso à Internet, para que os seus colaboradores possam executar as suas atividades profissionais diariamente. Só é permitido o seu uso para fins pessoais de uma forma razoável, desde que:----------

- Não se traduza em consumo de recursos da entidade com impacto significativo.-----
- Não interfira com a produtividade do colaborador e/ou colegas.----------
- Não impeça ou tenha impacto na prestação do serviço da entidade.----------
- Não viole as políticas da entidade ou quaisquer requisitos de confidencialidade, disponibilidade ou integridade estabelecidos.----------

Todos os colaboradores do Município de Vinhais devem estar conscientes que o acesso à Internet é monitorizado embora de modo não permanente e não sistemático.----------

Os colaboradores do Município de Vinhais não devem utilizar a internet da entidade para:--

- Atividades pessoais tais como ouvir e/ou fazer download de música.----------
- Ver vídeos e fazer streaming.----------
- Jogar ou aceder a sites de jogos ou apostas online.----------
- Organizar jogos ou administrar fóruns de jogos.----------
- Aceder a redes sociais de forma abusiva.----------

É expressamente proibido utilizar a internet corporativa da firma para:----------

- Fazer o download de software ilegal ou software não licenciado.----------
- Fazer o download de freeware sem que exista uma razão legítima e devidamente aprovada.----------
- Fazer o download ou copiar material protegido por direitos de autor, registo de marca, patente ou segredo comercial sem autorização do proprietário de tais direitos.

- Aceder a conteúdos considerados ilegais, imorais, não éticos, pornográficos, ofensivos, fraudulentos, entre outros.----------

O Município de Vinhais pode bloquear o acesso a páginas da Internet para utilizadores, grupos de utilizadores ou todos os colaboradores da entidade, de forma a dar cumprimento às políticas de segurança e utilização aceitável em vigor. ----------

Ligação segura à internet----------

O tráfego de acesso à internet através da rede interna do Município de Vinhais deverá ser filtrado e autorizado através de firewall existentes. Sempre que um colaborador necessitar de aceder à internet, através do seu computador portátil, fora da rede do Município de Vinhais, não pode alterar ou desabilitar as configurações da firewall do computador portátil. O acesso à rede internet deverá ser realizado através de redes de confiança, devidamente identificadas e seguidas as boas práticas de segurança:----------

- Caso se trate de uma rede Wi-Fi, esta deverá usar um protocolo de encriptação, de preferência WPA2 ou quando possível WPA3.----------
- Não usar redes Wi-Fi publicas que não usem nenhum protocolo de segurança.-------
- Sempre que possível, deverão ser evitadas a utilização de quaisquer redes Wi-Fi públicas, de hotéis ou aeroportos.----------
- Se não existir um serviço Wi-Fi em que possa confiar, considere a possibilidade de utilizar o seu smartphone como Access Point.----------
- Se precisar de aceder a uma rede Wi-Fi pública, limpe primeiro o histórico do browser e os cookies dos seus dispositivos.----------
- Quando possível deve sempre usar a VPN disponibilizada pela entidade.----------
- Certifique-se que o site é seguro fazendo duplo clique sobre o cadeado ou aceda pelo endereço (URL) que deve começar por “https://” e não por http://.----------

Serviços de Cloud----------

É proibido o envio de informação da Câmara Municipal de Vinhais para serviços de Cloud, sem que os respetivos fornecedores desses serviços ou soluções estejam aprovados e autorizados pelo Município de Vinhais. O uso de serviços de Cloud pessoais (Google Drive, Onedrive, Dropbox, etc) é proibido.----------

Comunicação----------

É fundamental garantirmos que comunicamos de forma adequada, nos meios adequados e apenas transmitimos a informação necessária. Os colaboradores devem seguir as seguintes regras e códigos de conduta com o objetivo de melhorar a segurança da informação: -------

- Quando fala ao telefone tenha cuidado para não divulgar informação confidencial.--
- Evite falar de assuntos de trabalho em locais e transportes públicos, proteja-se contra os ouvintes.----------
- Evite ler informações críticas ou confidenciais em locais e transportes públicos.-----
- Evite abrir envelopes com dados confidenciais em espaços públicos.----------
- Não utilize redes sociais ou aplicações para comunicar (por exemplo WhatsApp ou Telegram), estas podem não ser seguras.----------
- Não divulgue a extensão telefónica, e-mail ou telemóvel de um colega sem que este o permita.----------
- Não coloque informações da entidade em sites públicos. ----------
- Não registe o seu endereço de e-mail de trabalho em redes sociais ou outros sites de uso pessoal (de compras, fóruns, viagens, etc).----------
- Pense nas consequências antes de publicar qualquer informação.----------

Impressões e documentos----------

Os colaboradores devem garantir que tomam todas as precauções necessárias com a informação impressa em sua posse, sempre evitando o acesso indevido por terceiros. Para evitar a exposição da informação devem seguir as seguintes recomendações:----------

- Imprimir preferencialmente em modo de impressão protegida.----------
- As impressões devem ser recolhidas da impressora o mais rápido possível.----------
- Quando imprime documentos confidenciais deve acompanhar presencialmente a saídas das folhas e garantir que foram todas recolhidas da impressora.----------
- Não devem utilizar o verso de fotocópias ou impressões como folhas de rascunho.--
- Os documentos impressos e não utilizados, ou encontrados nas impressoras devem ser destruídos de forma segura, de acordo com o procedimento de manuseamento de ativos em vigor. ----------

Transferência de informação----------

A informação do Município de Vinhais deve ser adequadamente protegida quando transferida entre colaboradores ou entidades externas autorizadas. Todos os canais de transferência de informação em formato digital ou físico com terceiros autorizados devem assegurar, sempre que possível, a existência de mecanismos de controlo que protejam a informação contra interceção, cópia ou modificação não autorizada, alterações de percurso ou destruição acidental ou propositada.----------

Destruição de dados e impressões----------

A informação do Município de Vinhais pode existir sob várias formas, como por exemplo: em suportes de papel (impressões, posters, notas, rascunhos, etc.) ou suportes eletrónicos designados por media (CDs, disquetes, tapes, microfilme, discos rígidos, Pen USB, cartões de memória, etc.). A destruição de informação deve ser realizada de acordo com as seguintes regras de segurança e procedimentos:----------

- Apenas empresas certificadas podem fazer a destruição de grandes volumes da informação do Município de Vinhais.----------
- No processo de destruição a empresa produz um relatório detalhado com a descrição dos dispositivos, quantidade e código de barras.----------
- A documentação e certificados de destruição ficarão à guarda do Município de Vinhais.----------
- A destruição de pequenos volumes (documentos de trabalho, impressões, notas, rascunhos) é realizada pelo próprio colaborador nos destruidores de papel disponibilizados pela entidade e a eliminação deve ocorrer no escritório.----------
- Os equipamentos de informática e dispositivos de armazenamento digitais só podem ser destruídos, ou ter os dados apagados, pelo Município de Vinhais.----------

Monitorização e auditoria----------

O Município de Vinhais reserva-se no direito de monitorizar e auditar, sem aviso prévio, de modo aleatório e sempre que tal seja justificável por razões legítimas, e de acordo com a legislação aplicável em vigor:----------

- A informação e o software instalado nos computadores portáteis e dispositivos portáteis de armazenamento. ----------
- As atividades realizadas, pelos seus colaboradores, nos sistemas de informação de suporte ao negócio disponibilizados pela Câmara Municipal de Vinhais.----------
- As atividades realizadas na internet----------
- A origem, destino e assunto de emails enviados.----------

Disposições Finais----------

A presente política deve ser revista sempre que se verifique alguma alteração no âmbito das boas práticas de cibersegurança, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas recomendadas pela indústria, garantindo que continua a ser relevante e adequado. As exceções à presente política deverão ser previamente justificadas através de um processo formal de aceitação de risco e previamente autorizadas e formalmente registadas e monitorizadas.----------

O presente documento, bem como a sua partilha e distribuição, deve ser formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.----------

Política de Privacidade----------

Município de Vinhais----------

Rua das Freiras, 13 ----------

5320-326 Vinhais ----------

Introdução ----------

O Regulamento Geral Sobre a Proteção de Dados (RGPD) da União Europeia estabelece uma norma importante no que se refere a direitos de privacidade, segurança das informações e conformidade. O Município de Vinhais acredita que a privacidade é um direito fundamental e que o RGPD representa um importante passo em frente no sentido da proteção e do respeito pelos direitos de privacidade das pessoas. Sabemos que, quando recolhemos informações, está a confiar-nos os seus dados pessoais e trabalhamos e investimos continuamente para proteger os seus dados, e de dar-lhe o controlo sobre eles. ----------

A presente Política de Privacidade integra Termos e Condições de utilização do website e a Política de Cookies. ----------

Público-alvo----------

Todas partes interessadas.----------

Objetivo do presente documento ----------

O documento pretende descrever como o Município de Vinhais está alinhado, e em conformidade, com o Regulamento Geral sobre a Proteção de Dados (RGPD). Todas políticas (Política de Privacidade, Termos e Condições de utilização do website e a Política de Cookies) devem estar disponíveis no website do Município de Vinhais.----------

» A Política de Privacidade do Município de Vinhais----------

A proteção dos dados pessoais----------

Para o Município de Vinhais a proteção da privacidade e dos dados pessoais de todas os cidadãos e pessoas que de alguma forma se relacionam com o Município de Vinhais é fundamental e criticamente importante. Sabemos que, quando recolhemos informações, está a confiar-nos os seus dados pessoais e compreendemos que é uma grande responsabilidade para o nosso município. Trabalhamos e investimos tempo e recursos continuamente para proteger os seus dados e de dar-lhe o controlo sobre eles, sempre com a preocupação constante de transparência e imparcialidade. Tratamos os seus dados pessoais respeitando a legislação e em conformidade com políticas, normas e orientações nacionais e europeus aplicáveis, nomeadamente o Regulamento Geral sobre a Proteção de Dados (adiante "RGPD").----------

Princípios de proteção de dados----------

O Município de Vinhais, como responsável pelo tratamento dos seus dados pessoais, compromete-se a cumprir com os princípios de proteção de dados pessoais definidos pelo RGPD, seguindo as seguintes recomendações:----------

- Licitude, lealdade e transparência: significa que devemos ter uma razão legítima por força da qual tratamos dados pessoais, por exemplo, consentimento do titular dos dados, cumprimento de uma obrigação legal a que estamos sujeitos. Também

significa que devemos informar, de forma clara, o titular dos dados sobre o tratamento.----------

- Limitação das finalidades: devemos apenas solicitar dados pessoais para finalidades determinadas, explícitas e legítimas e não os tratar para além da finalidade para a qual foram solicitados.----------
- Minimização dos dados: os dados pessoais objeto de tratamento devem ser adequados, pertinentes e limitados ao necessário.----------
- Exatidão: temos a obrigação de garantir que os dados pessoais são exatos e atualizá-los sempre que necessário.----------
- Limitação da conservação: não devemos reter dados pessoais por um período superior ao necessário para as finalidades para as quais são tratados, embora possamos reter alguns para fins históricos e estatísticos.----------
- Integridade e confidencialidade: devemos ter em vigor controlos de segurança adequados para proteção dos dados contra o tratamento não autorizado e ilegal, perda, destruição ou danificação, incluindo medidas técnicas e organizacionais, tais como processos definidos, formação e consciencialização.----------
- Transferência legal fora do Espaço Económico Europeu: apenas transferimos dados pessoais para fora do Espaço Económico Europeu desde que existam salvaguardas adequadas, tal como uma base contratual. ----------
- Direitos do titular de dados: os titulares dos dados têm vários direitos que devemos respeitar (por exemplo, o direito a aceder a uma cópia dos dados que arquivamos e o direito de retirar o consentimento dado para a subscrição de um Newsletter).---------

Quem é o responsável pelo tratamento dos seus dados pessoais----------

O responsável pelo tratamento dos Dados Pessoais é o Município de Vinhais, pessoa coletiva de direito público, titular do número de identificação de pessoa coletiva 501156003, com sede na Rua das Freiras 13, 5320-326 Vinhais.----------

O que são dados pessoais----------

Dados pessoais são qualquer informação, seja de que natureza for ou em que suporte estiver, relativa a uma pessoa singular identificada ou identificável. É considerada identificável qualquer pessoa que possa ser identificada, direta ou indiretamente, em especial por

referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. ----------

O RGPD protege os dados pessoais independentemente da tecnologia utilizada para o tratamento desses dados e é neutra em termos tecnológicos e aplica-se tanto ao tratamento automatizado como ao tratamento manual. Também é irrelevante o modo como os dados são armazenados, como por exemplo, num sistema informático, através de videovigilância, ou em papel. Em todos estes casos, entre outros, os dados pessoais estão sujeitos aos requisitos de proteção previstos no RGPD.----------

Que dados recolhemos----------

O Município de Vinhais recolhe diversos tipos e categorias de dados pessoais em função das diferentes finalidades, como por exemplo:----------

- **Identificação:** Nome, Idade, Data de Nascimento, NIF, Nº de Cartão de Cidadão/Nº do Bilhete de Identidade, Nº da Segurança Social, Nº de Passaporte----------
- **Contactos:** Morada, Endereço de e-mail, Número de telefone/telemóvel----------
- **Dados familiares:** Agregado familiar, Filiação, Estado civil----------
- **Dados de Saúde:** Estado clínico, Baixas médicas, Deficiência----------
- **Dados financeiros/pagamento**: Número de identificação bancária, Rendimentos---
- **Dados de localização:** Localização geográfica----------
- **Dados institucionais:** Email institucional----------
- **Vídeo/Imagem:** Se visitar instalações municipais o visitante pode ser filmado pelo sistema de videovigilância----------
- **Vídeo/Imagem/Som:** Dados recolhidos durante eventos e ações organizados pelo município----------
- **Website:** Dados relacionados com o uso do nosso website, aplicações e cookies (consulte por favor Termos de Utilização e Política de Cookies)----------

Quando recolhemos e tratamos dados pessoais seguimos sempre o princípio da minimização dos dados. Isso significa que o Município de Vinhais recolhe apenas os dados pessoais mínimos necessários para realizar uma tarefa específica.----------

Como recolhemos os dados----------

Recolhemos os dados pessoais quando navegue e use formulários, aplicações e serviços disponíveis no nosso website, quando recebemos dados pessoais no decurso das nossas atividades e iniciativas, ou de outras atividades relacionadas. Os dados podem ser recebidos diretamente de um titular de dados (por exemplo, pessoalmente, por correio, e-mail, telefone, mensagens ou de outras fontes) ou via parceiros, subcontratados, responsáveis conjuntos pelo tratamento, prestadores de serviços entre outros.----------

Recolhemos também as suas informações quando nos envia, por exemplo, o seu curriculum vitae ou um contrato de prestação de serviços ou quando nos contacte em assuntos relacionados com informações, sugestões, reclamações, entre outros. ----------

A comunicação dos seus dados pessoais não constitui uma obrigação legal, mas poderá ser necessária para a celebração de um contrato de prestação de serviços, de estágio ou de qualquer outro tipo caso em que fornecimento dos dados pessoais será obrigatório. Nestes casos o seu não fornecimento resulta, por exemplo, na impossibilidade de celebração de contrato ou no cumprimento de um serviço solicitado.----------

Finalidades do tratamento dos dados ----------

As finalidades do tratamento dos dados pessoais, sempre determinadas, explícitas e legítimas, são as seguintes: ----------

- Para fins de cumprimento de obrigações legais a que o Município de Vinhais está sujeito (como por exemplo, resposta a pedidos e solicitações dos cidadãos, instrução de procedimentos administrativos, emissão de autorizações, licenças, etc.)----------
- Realização de diligências pré-contratuais ou contratuais.----------
- Prossecução de interesses legítimos prosseguidos pelo Município de Vinhais.-------
- Para o exercício de funções de interesse público ou ao exercício da autoridade pública que está investido o Município de Vinhais.----------
- Defesa de interesses do titular dos dados ou de outra pessoa singular.----------
- Divulgação de interesse público, nomeadamente, avisos à população.----------

- Comunicação de informações sobre atividades a decorrer no Município de Vinhais nos termos definidos pelo titular dos dados através do seu consentimento expresso, livre e informado. ----------

Caso decida disponibilizar os seus dados pessoais para outras finalidades poderemos tratar esses dados para os efeitos relevantes, desde legalmente admissíveis.----------

Entidades públicas podem tratar dados pessoais para finalidades diferentes que permite, a título excecional:----------

- O tratamento de dados pessoais por entidades públicas para finalidades diferentes das determinadas pela recolha. O fundamento para o tratamento deve residir na prossecução do interesse público que de outra forma não possa ser acautelado. ------
- A transmissão de dados pessoais entre entidades públicas para finalidades diferentes das determinadas pela recolha. O tratamento deve ser objeto de protocolo que estabeleça as responsabilidades de cada entidade interveniente, quer no ato de transmissão, quer em outros tratamentos a efetuar.----------

Fundamento do tratamento de dados ----------

Sempre que se recolha dados pessoais é necessário ter uma base legal para o inerente tratamento. De acordo com o RGPD, devemos identificar pelo menos um dos seguintes motivos para tratamento de dados pessoais:----------

- Consentimento: o titular dos dados deu o consentimento para que os mesmos sejam tratados para uma ou mais finalidades específicas.----------
- Contratual: o tratamento é necessário para a execução de um contrato do qual o titular dos dados faz parte ou para diligências pré-contratuais. ----------
- Legal: o tratamento é necessário para cumprir com uma obrigação legal, à qual o responsável pelo tratamento está sujeito.----------
- Interesses vitais: o tratamento é necessário para proteger os interesses vitais do titular dos dados.----------
- Interesse público: o tratamento é necessário para o desempenho de uma tarefa realizada no interesse público.----------

- Interesses legítimos: o tratamento é necessário para os interesses legítimos do Responsável pelo tratamento, exceto quando se prevalecerem interesses ou direitos e liberdades fundamentais do titular dos dados. ----------

O RGPD exige que se forneça aos titulares dos dados informações sobre o tratamento a fim de garantir um tratamento equitativo e transparente. Sempre que recolhermos dados pessoais devemos garantir que explicamos apropriadamente a razão pela qual precisamos das informações e como vamos tratá-las.----------

Quem são os destinatários dos seus dados----------

Os dados recolhidos pelo Município de Vinhais são exclusivamente para tratamento interno. O Município de Vinhais, em situação alguma, levará a cabo transferências internacionais dos seus dados para país ou organização que se encontre fora da União Europeia.----------

O Município de Vinhais poderá comunicar os seus dados pessoais, com a finalidade do cumprimento de obrigações legais, a entidades policiais, judiciais, fiscais e reguladoras entre outras.----------

Subcontratação----------

Nos casos em que os subcontratados têm acesso a dados pessoais para realizar os tratamentos de dados por conta do Município de Vinhais, adotámos medidas para assegurar o cumprimento dos requisitos impostos pelo Regulamento Geral de Proteção de Dados (RGPD).----------

Qualquer entidade subcontratada pelo Município de Vinhais tratará os dados pessoais em nome e por conta desta, sendo adotadas as medidas técnicas e organizacionais necessárias para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado e contra qualquer outra forma de tratamento ilícito.----------

Sempre que seja exigido por lei, os dados pessoais poderão ser disponibilizados a agências de supervisão, autoridades tributárias ou autoridades de investigação.----------

Onde armazenamos os seus dados----------

A localização do armazenamento dos seus dados pessoais é geograficamente limitada e garantimos que os dados existem exclusivamente dentro o da União Europeia. ----------

Os seus dados pessoais encontram-se guardados em servidores e dispositivos, físicos, virtuais e no cloud, em ambientes seguros, protegidos de acessos não autorizados. ----------

Como protegemos os seus dados----------

O Município de Vinhais tem implementadas as medidas lógicas, físicas, organizativas e de segurança adequadas, necessárias e suficientes para proteger os seus dados pessoais contra qualquer acesso não autorizado e modificação, divulgação, perda ou destruição. Exigimos contratualmente, caso existem subcontratados com acesso a dados pessoais, que os prestadores de serviço garantem um nível de segurança adequado. ----------

Por quanto tempo armazenamos os seus dados----------

O período de tempo durante o qual os dados são armazenados e conservados varia de acordo com a finalidade para a qual a informação é tratada.----------

Existem requisitos legais que obrigam a conservar os dados por um determinado período de tempo como por exemplo: auditoria, obrigações contabilísticas e fiscais, resolução de disputas judiciais e/ou exercício dos seus direitos legais.----------

Sempre que não exista uma exigência legal específica, os dados serão armazenados e conservados apenas pelo período mínimo necessário para a prossecução das finalidades que motivaram a sua recolha. No caso de uma retenção de dados mais longa por outros motivos, informá-lo-emos sobre esses motivos e sobre o período de retenção aplicável ao recolher os seus dados pessoais.----------

Para determinar o período de retenção dos seus dados pessoais, usamos, por exemplo, os seguintes critérios:----------

- Ao solicitar um serviço, mantemos os seus dados pessoais enquanto durar a nossa relação e de acordo com o prazo necessário para a prestação do serviço.----------

- Quando nos contacta para uma consulta, mantemos os seus dados pessoais pelo tempo necessário para o processamento da sua consulta.----------
- Quando deu o seu consentimento em ações de comunicação de informações (como envio de newsletters), mantemos os seus dados pessoais até que cancele a subscrição ou solicite que o excluamos ou após um período de inatividade definido de acordo com os regulamentos existentes.----------
- Quando os cookies são colocados no seu computador mantemo-los pelo tempo que for necessário para alcançar a sua finalidade e por um período definido de acordo com os regulamentos existentes.----------
- Para os candidatos de emprego mantemos os seus dados pessoais de acordo com a legislação aplicável.----------

Quando divulgamos e partilhamos os seus dados----------
Os seus dados são partilhados internamente dentro o Município de Vinhais. A partilha é baseada na política de "necessidade de saber e aceder" para lhe prestar o serviço solicitado, com o seu consentimento.----------

O Município de Vinhais poderá necessitar de partilhar os seus dados pessoais com terceiros que agem em seu nome ou lhes prestem serviços. Os seus dados pessoais serão mantidos em segurança em todos os momentos e só serão partilhados com tais terceiros quando estritamente necessário.----------

Os terceiros estarão contratualmente obrigados a garantir a segurança e confidencialidade das suas informações sempre em conformidade com as leis e regulamentos de proteção de dados pessoais existentes.----------

Além disso, o Município de Vinhais poderá partilhar os seus dados pessoais com outros terceiros:----------

- Para proteger os direitos, propriedade ou segurança do Município de Vinhais, dos nossos utilizadores, dos nossos colaboradores ou dos outros.----------
- Para cumprir uma obrigação legal ou responder a processos judiciais de qualquer natureza, ordens judiciais, qualquer ação legal ou medidas de execução exigidas

pelas autoridades competentes com poderes legais para o fazer, de acordo com a legislação em vigor.----------

- Para outros fins exigidos pela legislação aplicável ou com o seu consentimento prévio.----------

Quais são os seus direitos quando nos faculta os seus dados----------

De acordo com a legislação aplicável, o Município de Vinhais compromete-se a respeitar a confidencialidade da sua informação de caráter pessoal e garantir o exercício dos seus direitos de:----------

- Direito a ser informado: todos titulares dos dados têm direito a obter informação clara, transparente e compreensível sobre a forma como o Município de Vinhais usa os seus dados pessoais. ----------
- Direito de acesso: em complemento ao direito de informação, poderá consultar aos seus dados pessoais que tratamos e conservamos. Nestes casos, o Município de Vinhais facultar-lhe-á uma cópia dos dados pessoais que são objeto de tratamento. Além disso, quando o solicite através de meios eletrónicos, a informação será facultada num formato eletrónico de utilização comum e disponibilizado gratuitamente.----------
- Direito de retificação: tem direito de retificar os seus dados pessoais se os mesmos estiverem incorretos, desatualizados ou se pretender completá-los. ----------
- Direito de apagamento/direito a ser esquecido: pode solicitar-nos que eliminemos os seus dados, no entanto, por favor tenha em consideração que este não é um direito universal, uma vez que podemos ter fundamentos legais ou outros interesses legítimos para a retenção dos seus dados pessoais.----------
- Direito de, a qualquer momento, retirar o seu consentimento para o tratamento de dados: pode retirar o seu consentimento ao tratamento de dados quando o referido tratamento for baseado no seu consentimento. A retirada de consentimento não compromete a licitude do tratamento com base no consentimento previamente dado.
- Direito à portabilidade dos dados: tem o direito de mover, copiar ou transferir os dados da nossa base de dados para outra. ----------
- Direito à limitação do tratamento: tem direito a solicitar a restrição do tratamento dos seus dados nas seguintes situações: se contestar a exatidão dos dados, se o tratamento

for ilícito e não quiser apagar os seus dados, mas apenas limitá-los, se os dados já não forem necessários ao Município de Vinhais, mas necessários ao visitante/ utilizador ou se tiver exercido o direito de oposição acima referido, durante o período de tempo em que o Município de Vinhais analisa se os seus interesses legítimos para o tratamento prevalecem ou não sobre aquele direito.----------

- Direito de apresentar queixa junto da Autoridade de Controlo Nacional: O titular dos dados tem direito de apresentar reclamação junto da:----------
  CNPD - Comissão Nacional de Proteção de Dados----------
  Av. D. Carlos I, 134, 1º----------
  1200-651 Lisboa----------
  Call: (+351) 213 928 400----------
  Email: geral@cnpd.pt----------

Como pode o titular dos dados pessoais exercer os seus direitos----------
O direito de acesso, de retificação, de apagamento e de portabilidade, bem como o direito à oposição e direito de reclamação podem ser exercidos pelo titular dos dados mediante contacto com o Município de Vinhais através do seguinte endereço eletrónico: dpo@cm-vinhais.pt.----------

Em caso de dúvida sobre a presente Política de Privacidade, poderá obter informação adicional ou esclarecer qualquer dúvida, remetendo as suas questões para o endereço de correio eletrónico: dpo@cm-vinhais.pt.----------
O Município de Vinhais dará resposta ao pedido do titular no prazo máximo de um mês a contar da receção do pedido, salvo em casos de especial complexidade, em que esse prazo pode ser prorrogado até dois meses.----------

Se os pedidos apresentados pelo titular forem manifestamente infundados ou excessivos, nomeadamente devido ao seu carácter repetitivo, o Município de Vinhais reserva-se o direito de cobrar custos administrativos ou recusar-se a dar seguimento ao pedido.----------

Por favor, note que poderemos exigir prova da sua identidade e todos os detalhes do seu pedido antes de processá-lo. O titular tem o direito de obter os seus dados num formato

estruturado de utilização comum e disponibilizado gratuitamente. Este direito só é aplicável quando o tratamento dos dados é realizado por meios informatizados e o tratamento se baseou no consentimento do titular ou na execução de um contrato. Nas situações em que o tratamento é efetuado em papel este direito não se aplica.----------

Também pode exercer os seus direitos através dos seguintes canais:----------
Por carta, dirigida ao Município de Vinhais, Rua das Freiras 13, 5320-326 Vinhais.----------
Por telefone, (+351) 273 770 300.----------

Encarregado de Proteção de Dados----------
As entidades públicas estão obrigadas, em conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD), a designar um Encarregado de Proteção de Dados (EPD/DPO).

O Encarregado de Proteção de Dados garante a conformidade do tratamento de dados com a legislação em vigor e deve, por exemplo: ----------

- Informar o Município de Vinhais sobre as obrigações do RGPD.----------
- Monitorizar, avaliar e regular o alinhamento e a conformidade com o RGPD, de forma contínua.----------
- Sensibilizar todos colaboradores que tratem dados pessoais e promover ações, iniciativas e formações de boas práticas para a proteção de dados.----------
- Ser o ponto de contacto com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados.----------
- Ser o ponto de contacto com a autoridade de controlo (a Comissão Nacional de Proteção de Dados).----------

Os titulares de dados pessoais podem sempre contactar o Encarregado de Proteção de Dados do Município de Vinhais para esclarecerem todas as dúvidas e questões relacionadas com o tratamento dos seus Dados Pessoais e exercício dos seus direitos.----------

Contacto: dpo@cm-vinhais.pt----------

Legislação e regulamentação----------

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD).----------
- Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.----------
- O regime jurídico de segurança do ciberespaço: Lei n.º 46/2018, de 13 de agosto, Decreto-Lei n.º 65/2021, de 30 de junho, Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa à segurança das redes e da informação em toda a União Europeu.----------

Em caso de violação de dados pessoais, o Município de Vinhais notifica a Comissão Nacional de Proteção de Dados (CNPD), sempre que possível num prazo até 72 horas após ter tido conhecimento da mesma.----------

Qualquer subcontratante do Município de Vinhais deve notificar o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.----------

Recomendamos também a consulta regular do website do Centro Nacional de Cibersegurança (CNCS) em Portugal que promove a utilização do ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional.----------
https://www.cncs.gov.pt ----------

Alterações a esta Política de Privacidade----------
Podemos realizar alterações a esta política de privacidade, para estar em conformidade com requisitos legislativos ou regulamentares, ou com o objetivo de a adaptar às instruções emitidas pela Comissão Nacional de Proteção de Dados, pelo que os utilizadores são aconselhados a consultar a periodicamente. Quaisquer alterações serão imediatamente aplicáveis a si e aos seus dados. Se tais alterações afetaram a forma como os seus dados são processados, tomaremos todos os passos razoáveis para o manter informado.----------

Última atualização: 27 de julho de 2023----------

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.----------

» Termos e Condições de utilização do website do Município de Vinhais----------

Informações Gerais----------

Os presentes Termos e Condições definem a utilização do website www.cm-vinhais.pt, adiante referido por "website", propriedade do Município de Vinhais.----------

Aceitação dos Termos de Utilização----------

O utilizador do website (adiante "Utilizador") reconhece que ao usar este website está a aceitar estes Termos de Utilização.----------

Alteração dos Termos de Utilização----------

O Município de Vinhais reserva-se o direito de, a qualquer momento, sem necessidade de aviso prévio e com efeitos imediatos, alterar, adicionar, atualizar ou eliminar, parcial ou totalmente, os presentes Termos de Utilização.----------

O Utilizador deve consultar periodicamente estes Termos de Utilização para confirmar se foram efetuadas quaisquer atualizações ou alterações. Caso não concorde com alguma das regras de utilização, não deverá utilizar o website.----------

Acesso ao Website----------

O acesso ao website não está sujeito a registo. O Município de Vinhais tem o direito exclusivo de, a todo o tempo, suspender, parcial ou totalmente, o acesso ao website, em especial (mas não exclusivamente) aquando de operações de gestão, manutenção, reparação, alteração ou modernização. O Município de Vinhais poderá ainda optar por encerrar, definitiva ou temporariamente, parcial ou totalmente, a qualquer momento, o website ou qualquer um dos serviços, sem aviso prévio.----------

Utilização do Website----------

A utilização do website está sujeita ao cumprimento das seguintes regras:----------

- Não utilize o website para enviar ou disponibilizar qualquer conteúdo ilegal, falso, enganoso, ameaçador, maldoso, abusivo, difamatório, injurioso, invasivo da privacidade, racial, ética ou moralmente condenável, prejudicial ou atentatório da dignidade das pessoas ou prejudicial para menores, ou ainda que possa afetar negativamente a imagem do Município de Vinhais.----------
- Não utilize o website para enviar ou disponibilizar informação ou conteúdos que pertencem a terceiros e que não tem o direito de utilizar, como, por exemplo, conteúdos protegidos por direito de autor de terceiros ou conteúdos que contenham dados pessoais de terceiros.----------
- Não utilize o website para disponibilizar ou transmitir qualquer tipo de material que contenha ou possa conter vírus, worms, defeitos, trojan horses ou outro item ou códigos informáticos, ficheiros ou programas que sejam suscetíveis de interromper, destruir ou limitar a funcionalidade de qualquer equipamento ou sistema informático (hardware ou software) ou equipamento de comunicações.----------
- Não utilize nem explore, para fins comerciais ou que sejam por qualquer forma pagos, o website, incluindo os seus conteúdos, materiais, funcionalidades ou recursos (quaisquer conteúdos disponibilizados poderão ser acedidos apenas para uso pessoal).----------
- Não remova qualquer aviso de direitos de autor, marca comercial ou avisos de direitos de propriedade. ----------
- Não personifique alguém ou alguma entidade, incluindo, mas não limitado a um responsável do Município de Vinhais, não guie nem receba alguém como se tratasse de um anfitrião, nem testemunhe falsamente parentescos ou ligações com alguém.
- Não disponibilize ou transmita qualquer conteúdo não solicitado ou não autorizado como Spam.----------
- Não recolha, armazene, disponibilize, transmita, explore ou reproduza informações sobre outros utilizadores (incluindo nomes de utilizadores e/ou endereços de e-mail) para fins não autorizados.----------

Em geral, o Utilizador deve utilizar o website de forma responsável, prudente e cuidadosa, não devendo perturbar ou degradar a continuidade, integridade e qualidade dos recursos e funcionalidades do mesmo. O Utilizador reconhece que a utilização que faça do website é por sua conta e risco, sendo o único responsável por qualquer dano causado ao seu sistema

e/ou equipamento informático ou por outros danos ou prejuízos, incluindo perda ou danificação de dados, que resultem da utilização dos materiais, conteúdos ou informações obtidas, por qualquer forma, através do website.----------

Adicionalmente o Utilizador reconhece que o Município de Vinhais não é responsável pela informação, comentários, opiniões, sugestões, dados pessoais ou qualquer outro conteúdo inserido por si ou outro utilizador, são da sua exclusiva responsabilidade.----------

Se tiver menos de 13 anos, peça ajuda aos pais para lhe explicarem estas condições de utilização. Caso sinta que é necessário, deve apenas utilizar o nosso website com a supervisão dos seus pais ou encarregados de educação.----------

Direitos de Propriedade Intelectual ----------

O Utilizador reconhece que o website, a sua estrutura e disposição, a seleção, organização e apresentação do seu conteúdo, incluindo as suas funcionalidades e o software utilizado no mesmo, bem como as marcas, logótipos e símbolos apresentados no website, são da titularidade do Município de Vinhais ou foram devidamente licenciados a favor desta.-----

O Utilizador mais reconhece que os conteúdos deste website (textos, imagens, gráficos, marcas, som e animação e todas as outras informações e elementos constantes do website) estão protegidos por direitos de propriedade intelectual e a sua utilização está limitada aos termos permitidos por lei e com identificação da sua origem.----------

Cabe ao Município de Vinhais gerir o design, layout e disposição de toda a informação, conteúdos e materiais no website, pelo que o Município de Vinhais pode, a qualquer altura, atualizar, modificar ou eliminar quaisquer conteúdos, serviços, opções ou funcionalidades, bem como modificar a sua apresentação e configuração e alterar os respetivos URLs.-------

O Utilizador não está autorizado a transmitir, comunicar ao público, publicar, colocar à disposição do público, modificar, transformar, copiar, vender, utilizar ou distribuir, por qualquer forma, os textos, imagens ou outras informações contidas neste website ou parte do website sem autorização prévia, por escrito, do Município de Vinhais.----------

A utilização de conteúdos em violação do disposto nestes Termos de Utilização e demais legislação aplicável determina a responsabilização individual do utilizador, nos termos gerais, não acarretando quaisquer consequências não imputáveis ao Município de Vinhais. O utilizador defenderá, indemnizará e isentará o Município de Vinhais de todas as reclamações, ações, despesas (incluindo honorários de advogados), danos, perdas e responsabilidades resultantes ou relacionadas com qualquer violação dos presentes termos e condições. ----------

Dados Pessoais----------

A utilização deste website não implica necessariamente o fornecimento de dados pessoais. No entanto, caso pretenda solicitar pedidos de contacto e esclarecimento, apresentar uma reclamação, comentários ou sugestões, ou caso preste o seu consentimento para o tratamento de dados para finalidades de comunicação de informações (incluindo subscrição de newsletters) deverá indicar-nos alguns dados pessoais. Estes dados serão tratados nos termos definidos na Política de Privacidade e Cookies, disponível neste website.----------

Informações----------

A informação disponibilizada no website do Município de Vinhais tem como principal objetivo oferecer aos seus utilizadores conteúdos, notícias, serviços, informação institucional, entre outros. ----------

Responsabilidade e garantias----------

O website foi desenvolvido a pensar nos interesses dos nossos diferentes tipos de Utilizadores. No entanto, não podemos garantir que o website ou qualquer funcionalidade disponível no mesmo vá de encontro a quaisquer necessidades e expectativas que tenha ou que sirva os seus fins específicos.----------

O Município de Vinhais também não garante que:----------

- Os resultados obtidos através da utilização do website sejam corretos, verdadeiros, próprios ou confiáveis.----------
- Qualquer informação ou sugestão, de qualquer tipo, da responsabilidade do Município de Vinhais, apresentados ou disponibilizados no website, ou obtidos

através da sua utilização, sejam atuais, rigorosos, completos ou estejam isentos de erros. O Município de Vinhais não assume qualquer dever jurídico nesta matéria;---

- Qualquer material ou outro tipo de conteúdo disponibilizado por terceiros através do website seja seguro, legal ou adequado.----------
- As qualidades, funcionalidades ou características dos serviços, informações ou outros materiais ou conteúdos divulgados no website preencham qualquer expectativa dos utilizadores.----------

O Município de Vinhais não será responsável por erros que possam ocorrer devido a irregularidades do sistema, falha (temporária ou permanente) do website, das aplicações ou de outras ferramentas. O Município de Vinhais não se responsabilizará por quaisquer danos resultantes da utilização indevida ou da impossibilidade de utilização do website.----------

Links para websites de terceiros----------

O Município de Vinhais poderá disponibilizar links para páginas de outras entidades. Estes websites não pertencem nem são operados ou controlados pelo Município de Vinhais, pelo que o Município de Vinhais não se responsabiliza, aprova ou por qualquer forma apoia ou subscreve o conteúdo desses websites, nem dos websites com ele ligados ou neles referidos. O estabelecimento de links não implica, em caso algum, a existência de relações entre o Município de Vinhais e o proprietário ou gestor da página web para a qual o link remeta. --
Pelo exposto, o Município de Vinhais não se responsabiliza pela legalidade, fidedignidade ou qualidade de qualquer conteúdo aí disponibilizado, nem pelo cumprimento das regras legais aplicáveis em relação aos conteúdos ali disponíveis, sendo a utilização destes links da inteira responsabilidade dos Utilizadores.----------

Segurança----------

O Município de Vinhais não garante que o website funcione de forma ininterrupta, seja isento de erros ou falhas ou que esteja disponível de forma contínua.----------

O Município de Vinhais investe, naturalmente, os seus melhores esforços para que o website não tenha qualquer tipo de vírus ou outros elementos do género perigosos para o seu computador ou outro dispositivo a partir do qual aceda ao website. No entanto, uma vez que o Município de Vinhais não consegue controlar integralmente a circulação de informação

através da Internet, não é possível garantir que os mesmos não contêm qualquer tipo de vírus, malware ou outros elementos que possam danificar o seu computador.----------

Para garantir a segurança do website, o Município de Vinhais poderá, a qualquer momento e sem necessidade de aviso prévio, tomar as providências necessárias para garantir a integridade, segurança, continuidade ou qualidade do website, incluindo restrições ou limitações de acesso.----------

Validade dos Termos e Condições de Utilização----------
Se alguma parte ou disposição dos presentes Termos de Utilização não for executável ou estiver em conflito com a lei aplicável, a validade das restantes partes ou disposições não será afetada.----------

Questões----------
Se tiver alguma questão sobre os presentes Termos de Utilização, por favor envie-nos o seu pedido de esclarecimento através do email geral@cm-vinhais.pt, ou por carta, dirigida ao Por carta, dirigida ao Município de Vinhais, Rua das Freiras 13, 5320-326 Vinhais, ou por telefone, (+351) 273 770 300.----------

Lei aplicável----------
À gestão, administração, utilização e aplicação dos Termos de Utilização do website é aplicável a lei portuguesa.----------

Foro competente----------
Os conflitos e disputas de qualquer natureza relativos à formação, execução ou interpretação do presente contrato, serão regidos pela lei portuguesa e submetidos à jurisdição dos Tribunais Judiciais da Comarca de Lisboa, com expressa renúncia a quaisquer outros.------

» Política de Cookies----------
Esta Política de Cookies é aplicável a todos os websites e aplicações móveis do Município de Vinhais e faz parte da nossa Política de Privacidade. Para mais informações consulte a nossa Política de Privacidade e os Termos de Utilização disponíveis no nosso website. A

navegação neste website permite a recolha de informação com recurso a cookies e demais tecnologias. Ao usar este site aceita o uso de cookies demais tecnologias tal como descrito nesta Política de Cookies.----------

O que são cookies----------
"Cookies" são pequenas etiquetas de software que são armazenadas no seu computador através do navegador (browser), retendo apenas informação relacionada com as suas preferências, não incluindo, como tal, os seus dados pessoais.----------

Para mais informações consulte: www.allaboutcookies.org----------

Para que servem os cookies----------
Os cookies servem para ajudar a determinar a utilidade, interesse e o número de utilizações dos seus websites, permitindo uma navegação mais rápida e eficiente, eliminando a necessidade de introduzir repetidamente as mesmas informações.----------

Que tipo de cookies existem----------
Existem dois grupos cookies que podem ser utilizados:----------

- Cookies permanentes: são cookies que ficam armazenados ao nível do browser nos seus equipamentos de acesso (PC, mobile e tablet) e que são utilizados sempre que faz uma nova visita a um dos nossos websites. São utilizados, geralmente, para direcionar a navegação aos interesses do utilizador, permitindo-nos prestar um serviço mais personalizado.----------
- Cookies de sessão: são cookies temporários que permanecem no arquivo de cookies do seu browser até sair do website. A informação obtida por estes cookies serve para analisar padrões de tráfego na web, permitindo-nos identificar problemas e fornecer uma melhor experiência de navegação.----------

Para que fins utilizamos cookies ----------

- Cookies estritamente necessários: permitem que navegue no website e utilize as suas aplicações, bem como aceder a áreas seguras do website. Sem estes cookies, os serviços que tenha requerido não podem ser prestados.----------

- Cookies analíticos: são utilizados anonimamente para efeitos de criação e análise de estatísticas, no sentido de melhorar o funcionamento do website.----------
- Cookies de funcionalidade: guardam as preferências do utilizador relativamente à utilização do site, para que não seja necessário voltar a configurar o site cada vez que o visita.----------

Este website não recorre à utilização de Targeting cookies para promover publicidade direcionada aos nossos visitantes e não responde aos pedidos "do not track". ----------

Como pode gerir os cookies----------
Todos os browsers permitem ao utilizador aceitar, recusar ou apagar cookies, nomeadamente através da seleção das definições apropriadas no respetivo navegador. Pode configurar os cookies no menu "opções" ou "preferências" do seu browser.----------

Note-se, no entanto, que, ao desativar cookies, pode impedir que alguns serviços da web funcionem corretamente, afetando, parcialmente ou totalmente, a navegação no website. ---

Social buttons----------
Nós recorremos ao uso de social buttons relativos a redes sociais as quais poderão obter informações sobre as atividades dos nossos visitantes na Internet, incluindo sobre o nosso website. O entendimento do modo como a informação é utilizada e como podem ser excluídos da sua recolha deve ser obtido através da consulta dos respetivos Termos e Condições e Políticas de Privacidade desses websites. ----------

Web services externos ----------
Por vezes, recorremos ao uso de serviços externos no nosso website para exibir conteúdo nas nossas páginas web para, por exemplo, disponibilizar imagens, vídeos e realizar sondagens. Nestes casos, tal como com os Social buttons, não podemos impedir a recolha de informação sobre a utilização dos nossos visitantes aquando do seu acesso aos estes conteúdos incorporados no nosso website.----------

Esta Política de Cookies pode ser revista a qualquer momento, de acordo com o nosso critério. Recomendamos os utilizadores do nosso website que revejam as Políticas de Cookies periodicamente, com o propósito de ficarem informados sobre a nossa gestão das cookies.----------

Análise e Gestão de Risco----------

Município de Vinhais----------

Rua das Freiras, 13----------

5320-326 Vinhais----------

Introdução----------

Em conformidade com o Decreto-Lei n.º 65/2021, a Câmara Municipal de Vinhais deve realizar, pelo menos uma vez por ano, uma análise dos riscos de âmbito global. Devem também realizar uma análise dos riscos, de forma contínua, em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, também aos ativos que garantam a prestação dos serviços essenciais. Na sequência de cada análise dos riscos, a Câmara Municipal de Vinhais deve adotar as medidas técnicas e organizativas adequadas para gerir os riscos identificados.----------

» O que é um risco?----------

Um risco é uma circunstância ou um evento identificável com um efeito adverso potencial na segurança das redes e dos sistemas de informação de uma entidade. ----------

» O que é a gestão de risco?----------

É a gestão da incerteza e determinação das ações necessárias, para que essa incerteza possa ser minimizada para níveis considerados aceitáveis por parte da entidade.----------

» O que é uma análise do risco?----------

Trata-se de um exercício sistematizado, no âmbito do qual são identificadas possíveis ameaças que possam explorar sobre as vulnerabilidades dos ativos, bem como quais os níveis do risco associado, avaliando-se a probabilidade de ocorrência e possíveis impactos. Quando efetuada de forma sistematizada e numa lógica de melhoria, é uma prática que permite identificar, quantificar e estabelecer as prioridades face a critérios de aceitação do risco e objetivos relevantes para a entidade.----------

» **A Análise dos riscos de âmbito global, deve ser realizada com a seguinte periodicidade:** ----------

- pelo menos uma vez por ano.----------

» **A Análise dos riscos de âmbito parcial, deve ser realizada com a seguinte periodicidade:**----------

- durante o planeamento e preparação da introdução de uma alteração ao ativo ou ativos, em relação ao ativo ou ativos envolvidos----------
- após a ocorrência de um incidente com impacto relevante ou outra situação extraordinária, em relação aos ativos afetados.----------

» **Deve ser sempre realizada uma Análise dos riscos de âmbito global ou parcial:**-------

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

Público-alvo----------

O Município de Vinhais ----------

Objetivo do presente documento----------

O documento pretende reportar riscos e vulnerabilidades detetados no Município de Vinhais e sugerir, de forma priorizada, medidas técnicas e organizativas de mitigação e, de forma sumária, descrever a metodologia a ser usada na gestão de risco dos ativos.----------

Análise de risco global----------

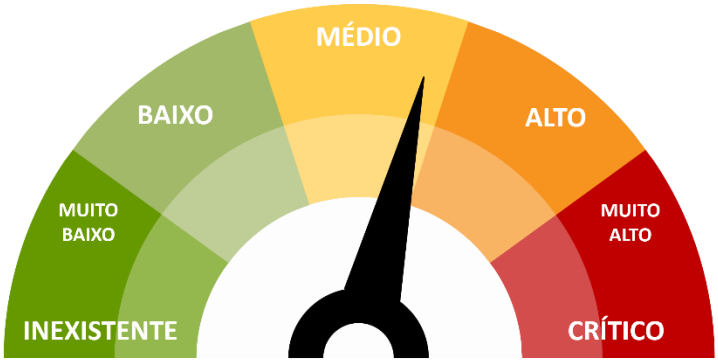
Dada a natureza complexa e dinâmica das ameaças de ciberataques é importante avaliar, gerir e quantificar o risco de cibersegurança periodicamente, independentemente do nível atual de cibersegurança e resiliência atual da organização.----------

É essencial medir os riscos de cibersegurança, sinalizar falhas e vulnerabilidades de segurança e estimar o impacto de novas medidas de mitigação dentro do cenário de ameaças relevantes, criando resultados e recomendações acionáveis, priorizadas e personalizadas, para mitigar riscos e reforçar e amadurecer a ciber resiliência da organização.----------

Principais categorias de ativos vulneráveis ----------
Identificamos, de acordo com a atividade em que o Município de Vinhais se enquadra, as principais categorias de ativos que podem sofrer danos na sequência de um ciber ataque, além da perda financeira envolvida.----------

Informação confidencial da Câmara Municipal de Vinhais; Informação pessoal dos cidadãos; Contratos e procedimentos; Dados de fornecedores; Prestação de serviços aos cidadãos online e/ou offline; Sistemas e processos essenciais; Propriedade intelectual; Reputação e imagem; Dados dos funcionários; Dados sobre a organização.----------

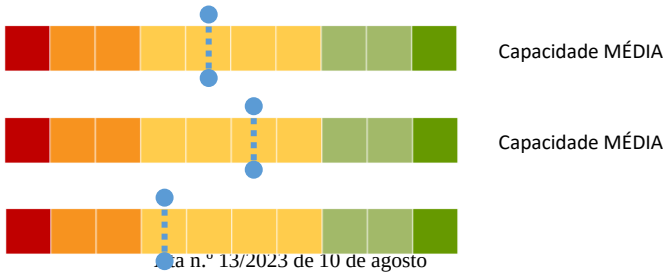
Risk score global do Município de Vinhais



(Escala 0 – 5. Um valor mais alto tem um risco mais alto)

O Município de Vinhais tem um nível de ciber risco MÉDIO ----------
O risk score é de 2.84 e é considerado um risco médio. Sugere-se elaborar e seguir um plano de ação de mitigação de risco (com recomendações de curto e longo prazo).----------

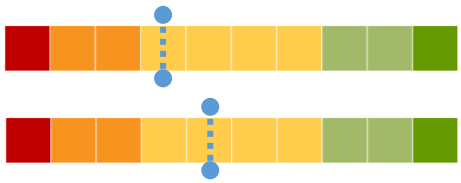
Níveis de capacidades de cibersegurança do Município de Vinhais----------
Resultado da avaliação de capacidades de cibersegurança, para cada um dos cinco controlos de cibersegurança:----------



» Detetar — Capacidade MÉDIA/BAIXA

» Responder — Capacidade MÉDIA/BAIXA

» Recuperar — Capacidade MÉDIA



(Níveis: ●Muito baixa; ●Baixa, ●Média/baixa, ● Média, ● Média/alta, ● Alta, ● Muito alta)

» Identificar
Sub-controlos: Gestão de Ativos, Ambiente da Organização, Governação, Avaliação do Risco, estratégia de Gestão do Risco, Gestão do Risco da Cadeia Logística
» Proteger
Sub-controlos: Gestão de Identidades, Autenticação e Controlo de Acessos, Formação e Sensibilização, Segurança de Dados, Procedimentos e Processos de Proteção da Informação, Manutenção, Tecnologia de Proteção
» Detetar
Sub-controlos: Anomalias e Eventos, Monitorização Contínua de Segurança, Processos de Deteção
» Responder
Sub-controlos: Planeamento da Resposta, Comunicações, Análise, Mitigação, Melhorias
» Recuperar
Sub-controlos: Plano de Recuperação, Melhorias, Comunicações

Threat landscape----------

Analisando o ambiente geopolítico e operacional, as atividades desenvolvidas e os serviços prestados pelo Município de Vinhais, foram identificadas três ameaças principais:----------

» Financial cyber hacker — Ameaça com risco muito alto
» Political cyber warrior — Ameaça com risco muito alto
» Cyber terrorist — Ameaça com risco alto

(Escala 1 – 5. Um valor mais alto tem um risco mais alto)

» Financial cyber hacker
Hackers motivados exclusivamente pelo lucro financeiro, resultante do pagamento de resgates pelas vítimas, do roubo digital de contas, burla digital, apropriação ilegítima de wallets de criptomoedas, venda de credenciais roubados, etc.
» Political cyber warrior
Hackers suportados, patrocinados ou incorporados por estados, com capacidade de provocar disrupções de serviços ao nível nacional, e/ou com o objetivo de obter informações confidenciais sobre diferentes áreas de outros países, informações militares, financeiras, industriais e outros tipos de dados como vulnerabilidades de infraestruturas críticas.
» Cyber terrorist
Hackers motivados pela ideologia, tipicamente com o objetivo de provocar danos permanentes como, data-wiping (eliminação de dados sem possibilidade de recuperação), destruição física de sistemas e infraestruturas lateralmente atacando OT através de IT, e provocando disrupções de grande escala de serviços, como por exemplo, nas áreas de saúde, financeira, transporte, energia, militar, imprensa, e outras infraestruturas críticas.

Método de ataque ----------

Avaliando, de forma holística, a postura de segurança e as capacidades de cibersegurança do Município de Vinhais identificamos os cinco métodos de ataque com mais probabilidade de acontecer: ----------

» Engenharia Social (phishing, spam)
» Ransomware (sequestro e extorsão)
» Código Malicioso (vírus, malware)
» Ataques a ativos e serviços expostos
» Uso de dispositivos USB não autorizados

(Escala 1 – 5. Um valor mais alto tem uma probabilidade mais alta de acontecer)

» Engenharia Social (email, spam, web, pessoal)
Os ataques de engenharia social dependem do erro humano, em vez de vulnerabilidades em software e sistemas operacionais, para conseguir obter informações que permitem iniciar um ciberataque. Os métodos de ataques são, por exemplo, Phishing, Spear-phishing, Smishing, Spam, Scams.
» Ransomware
O ransomware é um tipo de software malicioso (ou malware) que ameaça uma vítima ao destruir ou bloquear o acesso a dados ou sistemas críticos até que o resgate seja pago. A maioria do ransomware é operado por humanos, tem como alvo organizações e é a maior ameaça, e a mais difícil de impedir e inverter. Normalmente, o ransomware tem origem em credenciais de conta roubadas. Assim que os atacantes tiverem obtido acesso à rede de uma organização, utilizam a conta roubada para determinar as credenciais de contas com um maior âmbito de acesso e procuram dados e sistemas críticos para a empresa com o potencial de um alto suborno financeiro. Em seguida, instalam ransomware nestes dados confidenciais ou sistemas críticos para a empresa, por exemplo, ao encriptar ficheiros confidenciais para impedir o acesso da organização até que esta pague o resgate. Os cibercriminosos tendem a pedir o pagamento em criptomoeda para manter o anonimato.
» Código Malicioso
O Malware é o termo utilizado para descrever código malicioso. Estes códigos maliciosos podem dividir-se em diferentes tipos como o vírus, spyware, adware, nagware, trojans, worms, entre outros. Trata-se de um software destinado a infiltrar-se em dispositivos de forma ilícita, com o intuito de causar danos, alterações e/ou furto de informação. Visitar sites infetados ou clicar em links ou anexos de e-mail maliciosos são as principais portas de entrada para que o código malicioso infeta um sistema.
» Ataques a ativos e serviços expostos
O atacante procura explorar vulnerabilidades existentes na superfície de ataque da organização. A superfície de ataque é composta por todo o hardware, software e componentes da rede de uma organização, como por exemplo; Aplicativos expostas, Código visível, APIs, Portas abertas, Servidores e VMs expostos, Sites, Certificados, Serviços mal configurados. O objetivo final dos atacantes pode ser qualquer coisa, desde instalar ransomware, roubar dados, recrutar máquinas para uma botnet, instalar trojans bancários ou outro malware.
» Uso de dispositivos USB não autorizados
O uso de dispositivos USB não autorizados (Pen USB, Discos externos, outros dispositivos USB), acidentais ou intencionais, podem causar incidentes de segurança que provocam danos significantes a qualquer organização. É essencial bloquear, controlar e monitorizar portas USB para proteger dispositivos e informação contra todos malware USB.

Plano de ação ----------

Controlos prioritários para remediação (curto prazo 3-12 meses)----------

Analisando os resultados, e de modo a mitigar riscos de forma priorizada, sugere-se que o Município de Vinhais deve concentrar os seus recursos e focar os seus esforços de cibersegurança nos seguintes três controlos (num total de 51 existentes): ----------

1

» Formação e sensibilização de cibersegurança----------

A sensibilização para a ciber-higiene dos colaboradores é essencial para a resiliência de uma organização relativamente às ameaças no ciberespaço. É fundamental criar um programa de sensibilização junto dos colaboradores, de modo a reforçar a capacitação do fator humano na proteção contra incidentes de cibersegurança. O programa, embora com uma maturidade inicial, deve ser contínuo e periodicamente atualizado com base nas ameaças e cenários de riscos emergentes. Sugere-se a simulação de phishing/smishing pelo menos uma vez por ano.----------

» Teste de intrusão e análise de vulnerabilidades----------

O teste de intrusão, e a análise de vulnerabilidade, tem como objetivo avaliar o estado atual da segurança dos sistemas, ativos, redes, e aplicações, pela simulação de ataques externos e internos, e identificar vulnerabilidades que podem ser exploradas. O resultado permite, de forma sistemática e priorizada, imediatamente corrigir riscos críticos, e elaborar estratégias de mitigação.----------

» Hardening de sistemas----------

Hardening tem como objetivo mitigar o risco de segurança, eliminando o máximo possível potenciais vetores de ataque e reduzindo a superfície de ataque do sistema através de tecnologias, configurações e procedimentos de acordo com as melhores práticas recomendadas pela indústria. O hardening deve ser efetuado em todos sistemas e infraestruturas de TIC (servidores, workstations, aplicações, redes, base de dados, e mais). Exemplos de medidas básicas são; remover programas desnecessários ou inseguros, desativar contas de utilizadores sem uso, desativar serviços, portas, protocolos e funcionalidades, limitar acessos e permissões, implementar políticas de segurança robustas seguindo o princípio de minimização (fornecer apenas recursos essenciais para a execução de tarefas necessárias). O objetivo futuro é a implementação de um programa de hardening com uma abordagem metódica, periódica e eficaz.----------

Recomendações e observações----------

Algumas recomendações para o Município de Vinhais (além das prioritárias identificadas):

» Avaliar o sistema de backup e garantir que existe sempre um backup offline e offsite, com dados disponíveis de acordo com a tolerância aceitável de perda de dados. Procurar seguir a regra de 3-2-1 (ter pelo menos 3 cópias dos dados; armazenar as cópias em pelo menos 2 tipos de suporte diferentes; manter pelo menos 1 das cópias num sítio fora do datacenter principal). Em caso nenhum pode existir um único ativo capaz de comunicar com todas unidades de backup em simultâneo (Storage, Servidores, NAS, Cloud, Tape). É de extrema importância periodicamente testar todas soluções de backup existentes. Os testes devem ser efetuados em hardware e sistemas diferentes para garantir uma alta disponibilidade de dados e uma rápida recuperação dos serviços prestados, caso o hardware que suporta o serviço sofre de uma falha crítica. Redundância é essencial.----------

» Fazer uma auditoria ao software instalado nos equipamentos e validar que só existem software genuíno, com licenças válidas e em conformidade com a política de uso do fabricante, ou de open source. Situações de não conformidade devem ser remediadas imediatamente. É essencial periodicamente analisar os equipamentos de todos os colaboradores, incluindo a gestão de topo. ----------

» Procurar software de open source. Existem várias aplicações de produtividade, de auditoria, utilitários, segurança, entre outras, disponíveis sem qualquer custo, que podem, por exemplo, substituir software não genuíno ou ser ferramentas úteis para o departamento de TI e administradores de sistema.----------

» Estabelecer e formalizar procedimentos relacionados com a entrada, saída e transferência de colaboradores, nomeadamente em articulação com os recursos humanos e os dirigentes, para o departamento de TI poder, imediatamente, criar, atualizar ou cancelar contas, privilégios, permissões e acessos.----------

» Procurar a formalização, a aprovação e a distribuição das políticas relacionadas com a cibersegurança, pela gestão de topo.----------

» Procurar a melhor forma de partilhar as políticas de cibersegurança, nomeadamente em articulação com os recursos humanos, com colaboradores novos, e existentes.----------

» Estudar como estabelecer um programa micro ISAC (Centro de Análise e Partilha de Informação), com outros municípios e entidades, de forma organizada e periódica, com o objetivo de partilhar informação, promover confiança e desenvolver competências, relacionadas com a cibersegurança. Recomenda-se, por exemplo, elaborar e enviar mensalmente um newsletter com CTI (Cyber Threat Intelligence) que permite, em 15 minutos, melhor entender o ambiente de ameaças de modo a melhorar a consciencialização das equipas de TI.----------

» O Departamento de TI deve dedicar pelo menos 5% do tempo aos assuntos relacionados com a cibersegurança e resiliência. Uma pesquisa permite entender quais são as ciber

ameaças atuais e emergentes e quais são as medidas de mitigação recomendadas. Por cada ameaça existem várias medidas, ações e iniciativas que podem ajudar aumentar a capacidade preventiva e defensiva da entidade, sem grande esforço ou custo.----------

» Formalizar um plano de comunicação (de reporting) entre a equipa de TI e a gestão de topo. Recomenda-se, por exemplo trimestralmente, que a equipa de TI apresenta um relatório, embora sumário, incluindo por exemplo; estado global da infraestrutura e os serviços prestados, problemas e riscos detetados (indicando criticidade e sugerindo tratamento), atividades planeadas (curto prazo 120 dias), últimas ocorrências e situações imprevistas, observações relevantes, assuntos por tratar, etc. "Um ponto de situação" trimestral.----------

» Revisão e verificação do cumprimento das responsabilidades do Encarregado de Proteção de Dados (DPO/EPD). O DPO deve garantir a conformidade do tratamento de dados com a legislação em vigor e, por exemplo: Informar o Município de Vinhais sobre as obrigações do RGPD; Monitorizar, avaliar e regular o alinhamento e a conformidade com o RGPD, de forma contínua; Sensibilizar todos colaboradores que tratem dados pessoais e promover ações, iniciativas e formações de boas práticas para a proteção de dados; Ser o ponto de contacto com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados; Ser o ponto de contacto com a autoridade de controlo (a Comissão Nacional de Proteção de Dados). Devem também validar se o website está em conformidade com o RGPD (aviso de cookies, política de privacidade, condições e termos).----------

» É essencial apostar na resiliência e prevenção.----------

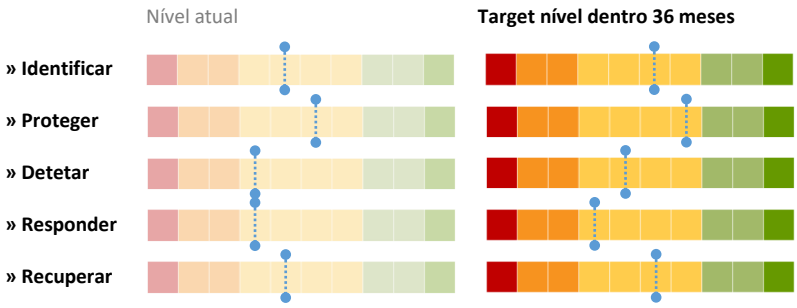
Observações

É importante ter em consideração que a dimensão reduzida da equipa de TI, e os recursos limitados dedicados à cibersegurança, têm um impacto negativo na avaliação da ciber resiliência da Câmara Municipal de Vinhais. Atualmente, a curto prazo, o plano de melhoria deve estar focado nas pessoas e nos procedimentos necessários para identificar e minimizar riscos e ameaças. Caso existem gaps no design dos backups é prioritário e urgente investir em unidades ou soluções adicionais de backups, como

muitas vezes um backup offline ou devidamente protegido é a única maneira de recuperar de um ataque de ransomware ou datawiping. É importante procurar recursos humanos adicionais, para poder delegar a execução de tarefas menos exigentes ou qualificadas, de modo a permitir uma maior dedicação por parte da equipa de TI sénior à implementação das medidas de melhoria sugeridas.

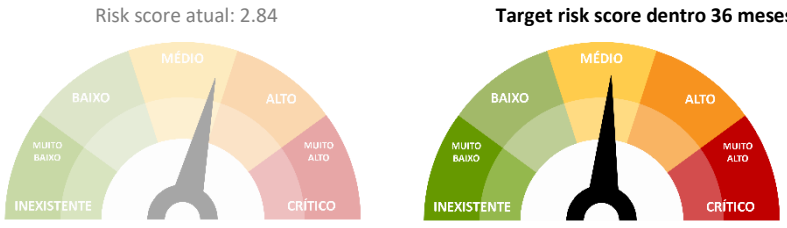
Objetivos (longo prazo 12-36 meses) ----------

Tendo em consideração o ambiente e os recursos disponíveis do Município de Vinhais sugere-se, ao longo prazo, procurar atingir os seguintes níveis de capacidades para cada um dos cinco controlos de cibersegurança:



(Níveis: ●Muito baixa; ●Baixa, ●Média/baixa, ● Média, ● Média/alta, ● Alta, ● Muito alta)

Objetivo 36 meses: Risk score global 2.45-2.65 (médio) ----------

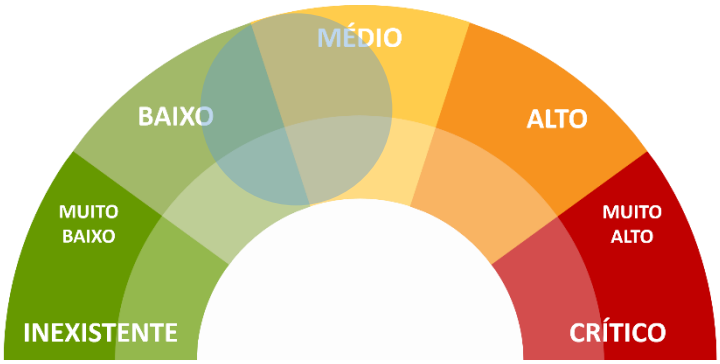


(Escala 0 – 5. Um valor mais alto tem um risco mais alto)

Objetivo futuro: Risk score global 1.90-2.30 (médio/baixo)----------

Considerando o ambiente geopolítico e operacional, as atividades desenvolvidas e os serviços prestados pelo Município de Vinhais, sugere-se continuamente investir esforços e recursos até conseguir um nível de risco médio/baixo, de modo a estar alinhada com padrões

e normas de cibersegurança. A manutenção do nível será garantida através de processos de melhoria contínua em conformidade com a política de cibersegurança. ----------



(Nível de risco)

Análise de risco parcial ----------

Atualmente o Município de Vinhais tem um nível de capacidade inexistente ou inicial do controlo da análise de risco de ativos. Tendo isso em consideração, e sempre procurando uma abordagem adaptada à realidade da entidade, foi efetuada uma análise básica dos ativos que suportem serviços essenciais, no sentido de ter um ponto de partida, e melhor entender a metodologia sugerida. Também, de modo a facilitar essa análise de risco inicial, foram só incluídos ativos e situações onde foram identificados riscos não ordinários. ----------

(Por exemplo, todos ativos de IP e armazenamento digital estão sempre sujeitos a ciberataques (riscos ordinários). Se existe um ativo, por exemplo um servidor de dados, que foi atacado 3 vezes no último ano (por causa de, por exemplo, falta de proteção Endpoint, configurações erradas ou serviços expostos com vulnerabilidades), passa a ser um ativo com um risco não ordinário e será incluído na análise de risco.) ----------

No entanto é essencial reconhecer a alta importância do controlo e o Município de Vinhais deve dedicar esforços com o objetivo de melhorar a capacidade de detetar, analisar e gerir riscos, para no futuro, conseguir implementar um programa eficaz e funcional de Gestão de Risco. ----------

Ativos com riscos identificados----------

Foram identificados os seguintes ativos com riscos.----------

Ativo	Criticidade do ativo	Identificação do risco	Eventual impacto	Prioridade	Tratamento

N/A					

Situações com riscos identificados----------

Foram identificadas as seguintes situações com riscos. Texto livre.----------

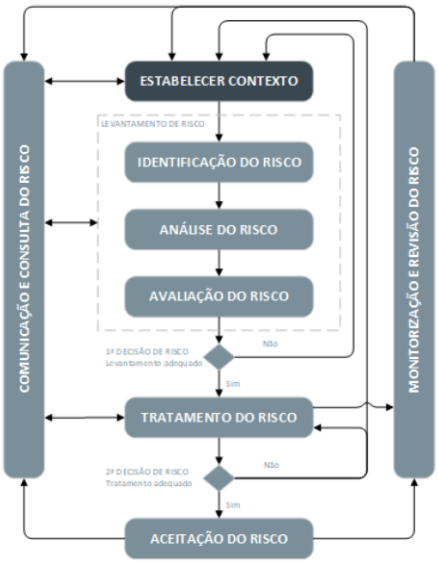
N/A

Metodologia de Gestão do Risco ----------

Uma introdução sumária a metodologia sugerida para gerir riscos. ----------

Estabelecer contexto----------

Conjunto de critérios base necessários à gestão de risco, contemplando a definição do âmbito de aplicabilidade do processo de gestão de risco e os critérios de risco e de avaliação de risco, incluindo o apetite ao risco.----------



» **Organização na gestão do risco:** identificar os recursos humanos e materiais necessários para poder garantir a correta execução de todo o processo de gestão do risco. Nota: sugere-se que todas estas decisões sejam analisadas e aprovadas pela gestão de topo da entidade----------

» **Abordagem à gestão do risco:** definir e implementar as políticas, processos e procedimentos no âmbito da gestão e tratamento do risco.----------

» **Critérios de avaliação do risco:** identificar para se avaliar a relevância do risco, considerando-se o valor estratégico, a criticidade dos ativos e a importância operacional e comercial.----------

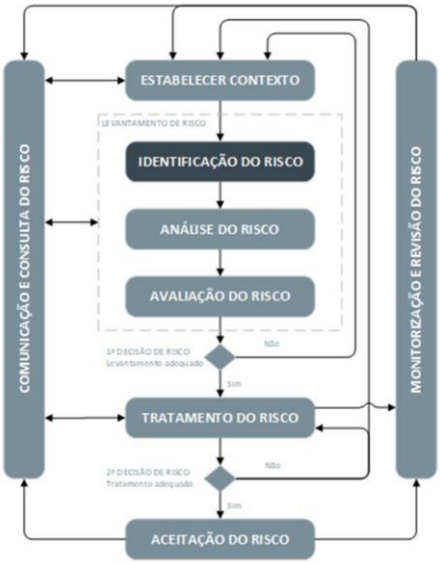
» **Critérios de impacto:** determinar em termos de grau de danos ou custos que um evento de segurança da informação tem para a entidade.----------

» **Critérios de aceitação do risco:** identificar a partir de que nível do risco terá de ser necessária a aprovação da gestão de topo para que o mesmo possa ser aceite.----------

» **Definição de âmbito e fronteiras:** definir o âmbito e as fronteiras do sistema de gestão do risco de segurança e organização da informação.----------

Identificação do risco----------

Identificar, reconhecer e descrever os riscos que possam criar constrangimentos ou impedir a Câmara Municipal de Vinhais de atingir os seus objetivos. O propósito da identificação é determinar as ocorrências que poderão causar uma potencial perda à entidade.----------



» **Identificação dos ativos:** ativos que suportam o âmbito definido na gestão do risco de segurança da informação.----------

» **Identificação de ameaças:** uma ameaça tem o potencial de poder criar impactos e consequências negativas nos ativos da entidade, podendo, esta ser de origem natural ou humana e ser acidental ou deliberada. A informação sobre ameaças pode ser obtida das seguintes formas:----------

- Revisão de incidentes ocorridos.----------
- Responsáveis pelo ativo.----------
- Utilizadores----------
- Especialistas de segurança da informação e segurança física.----------
- Departamentos legais.----------
  - Catálogo de ameaças. ----------

» **São exemplos de ameaças** ----------

- Incêndio.----------
- Destruição de equipamento ou media.----------
- Fenómeno sísmico.----------
- Doenças emergentes (e.g. infeções, pandemias).----------
- Falha de fornecimento de energia.----------
- Falha de equipamento de telecomunicações.----------
- Espionagem remota.----------
- Roubo de equipamento.----------
- Código malicioso (e.g. vírus, malware, ransomware).----------
- Erro humano, entre outros.----------

» **Identificação de controlos:** sistematizar planos de gestão do risco anteriormente efetuados com a identificação dos respetivos controlos implementados, descrevendo o estado de implementação e de utilização dos mesmos.----------

» **Identificação de vulnerabilidades:** lista de potenciais vulnerabilidades, com base na lista de ameaças e dos ativos, que poderão ser associadas aos ativos.----------

» **As vulnerabilidades podem ser identificadas nas seguintes áreas**:----------

- Entidade.----------
- Processos, procedimentos e rotinas de gestão.----------
- Colaboradores.----------
- Ambientes físicos.----------
- Configuração dos sistemas de informação.----------
- Hardware, software e equipamento de rede.----------
- Dependência com partes externas interessadas.----------

» **São exemplos de vulnerabilidades:**----------

- Uso inadequado ou negligente do controlo de acesso físico a edifícios e salas.-------
- Suscetibilidade de variações de corrente elétrica.----------
- Ponto único de falha.----------
- Transferência de palavras-passe em claro.----------
- Falta de controlos para a gestão de ativos fora das instalações.----------
- Utilização incorreta de software e hardware.----------
- Falta de registos nos logs de administrador e operador.----------
- Manutenção insuficiente e/ou instalação defeituosa de suportes de armazenamento de dados, entre outros.----------

» **Identificação de impacto:** consequências dos riscos e aferir qual o impacto que a possível exploração de uma vulnerabilidade por parte de uma ameaça, poderá ter em termos de confidencialidade, integridade e/ou disponibilidade dos ativos. Na aferição de impacto, poderá ser identificado potenciais consequências operacionais em termos de, mas não se limitando a:----------

- Tempo de investigação e de reparação.----------
- Tempo (de trabalho) perdido.----------
- Oportunidades perdidas.----------
- Segurança e saúde.----------

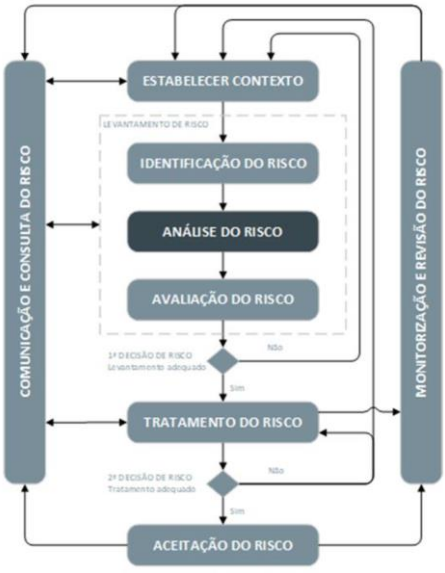
- Custos financeiros com reparação. ----------
- Danos de reputação.----------

Exemplos da fase de Identificação do risco:

Descrição	Ativo	Ameaça	Controlos Atuais	Vulnerabilidade	Impacto genérico
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *(Distributed Denial of Service)*.	Plataforma de Serviços para o Cliente.	Agente malicioso ou *botnet*	Níveis de proteção assegurados pelo prestador de serviços (Controlos Anti-DDoS)	- Conexões de rede pública não protegidas. - Resposta inadequada do serviço de manutenção.	Crítico para a entidade, em especial para os clientes que utilizam a plataforma.
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Plataforma de Serviços para o Cliente.	Mau funcionamento de software	Processo de pedidos realizado e Atidos formalizado em memorando para alterações de maior complexidade.	Especificações para *developers* pouco claras ou incompletas	Crítico para a entidade, em especial para os clientes que utilizam a plataforma.
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Plataforma de Serviços para o Cliente.	Utilização não autorizada de equipamentos/sistemas	Não existem controlos	Falta de procedimentos de reporte de vulnerabilidades de Segurança da Informação	Alta probabilidade tendo em conta o número de vulnerabilidades detetadas diariamente, e o facto da plataforma estar acessível na Internet.

Análise do risco----------

A análise do risco envolve a consideração das incertezas, fontes do risco, consequências, eventos, cenários, controlos e a sua eficácia.----------



Nos critérios de aferição do impacto do risco recomendam-se ser igualmente observadas as seguintes dimensões:----------

» **Reputação:** a ocorrência de determinado risco pode colocar em causa a reputação da entidade (por exemplo: perda de confiança por parte de partes interessadas).----------

» **Legal ou Regulatório:** a ocorrência de determinado risco poderá colocar em causa responsabilidades legais e/ou regulatórias da entidade (por exemplo: responsabilidades regulatórias sectoriais.----------

» **Prestação de Serviço:** a ocorrência de determinado risco poderá colocar em causa o serviço prestado pela entidade (por exemplo: incumprimento de um nível de serviço).----------

» **Financeiro:** a ocorrência de determinado evento pode levar a que a entidade possa incorrer em custos financeiros não previstos (por exemplo: coimas, recursos adicionais).

» **Metodologia de análise do risco:** pode ser consubstanciada por uma abordagem analítica de caráter qualitativo, quantitativo ou por uma combinação de ambas. O método de análise

recomenda-se ser consistente com os critérios de avaliação do risco, definidos em contexto do risco.----------

- Análise qualitativa: utiliza uma escala de atributos de qualificação para identificar a severidade dos potenciais impactos (por exemplo: Baixo, Médio e Alto) e a probabilidade de tais ocorrências. ----------
- Análise quantitativa: utiliza uma escala de valores numéricos (em oposição às escalas descritivas usadas na análise do risco qualitativa) para aferição dos impactos e probabilidades, sendo suportada em diversas fontes.----------

» **Levantamento dos impactos:** avaliado o impacto nos serviços prestados pela entidade que possam resultar na ocorrência de incidentes de segurança. O levantamento do impacto recomenda-se ser igualmente avaliado no contexto da perda de confidencialidade, integridade e/ou disponibilidade dos ativos em análise.----------

» **Análise de probabilidade**: com base nas ameaças, vulnerabilidades e listas de incidentes (incluindo lições aprendidas) existentes, sugere-se que a entidade avalie a probabilidade de ocorrência do risco.----------

» **Determinação do nível do risco: na** análise do risco, é assignado a cada cenário identificado um valor ao impacto e probabilidade.----------

Exemplos da fase de Análise do risco:

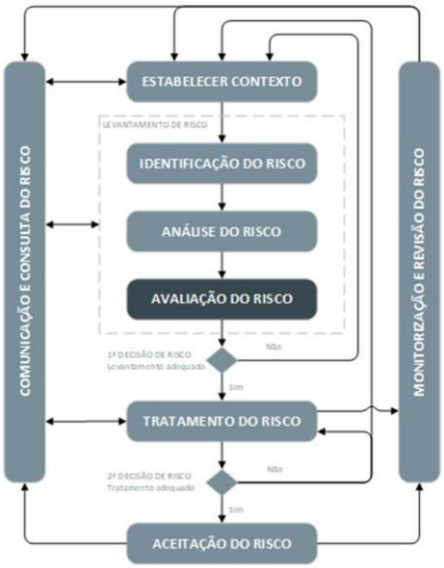
Descrição	Impacto produtividade	Impacto resposta	Impacto requisitos legais	# Impacto	Probabilidade	# Prob.	Classificação do risco
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *(Distributed Denial of Service)*.	Muito elevado	Moderado	Reduzido	Moderado	Improvável tendo em conta os controlos aplicados.	Improvável	Médio
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Elevado	Moderado	Moderado	Moderado	Muito improvável tendo em conta os controlos aplicados.	Muito improvável	Baixo
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Elevado	Moderado	Moderado	Moderado	Provável tendo em conta a ausência de controlos.	Provável	Alto

Exemplos de matriz de Gestão de risco:

		Impacto				
		Insignificante	Redúzio	Moderado	Elevado	Muito elevado
Probabilidade	Muito Improvável	Muito baixo	Muito baixo	Baixo	Baixo	Médio
	Improvável	Muito baixo	Baixo	Médio	Médio	Médio
	Possível	Baixo	Médio	Médio	Alto	Alto
	Provável	Baixo	Médio	Alto	Alto	Muito alto
	Muito provável	Médio	Médio	Alto	Muito alto	Muito alto

Avaliação do risco ----------

A natureza das decisões relativas à avaliação e aos critérios de avaliação dos riscos utilizados são estabelecidos no momento de definição do contexto. Estas decisões, bem como o contexto, recomendam-se ser revisitadas com maior detalhe nesta fase, tendo em conta que existe mais informação sobre os riscos específicos identificados.----------



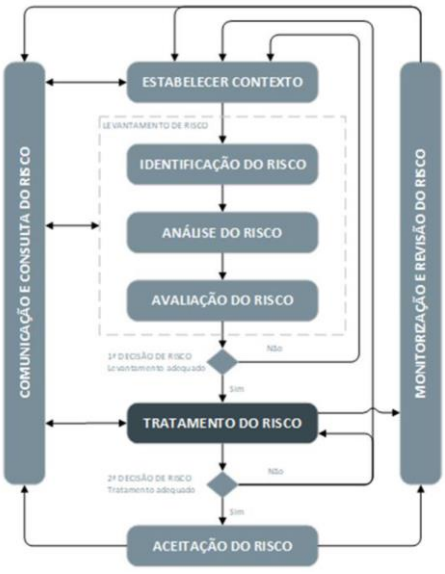
- Sugere-se que os critérios de avaliação do risco sejam utilizados para suportar as tomadas de decisões.
- Recomendam-se que sejam consistentes com o contexto externo e interno da gestão dos riscos de segurança da informação e serem considerados. -------
- As decisões tomadas na avaliação do risco baseiam-se principalmente no nível aceitável do risco.
- Sugere-se que os riscos sejam priorizados de acordo com os critérios de avaliação e em relação aos cenários de incidentes que originaram os riscos identificados.----------

Exemplos da fase de Avaliação do risco:

Descrição	Classificação do risco	Priorização
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *(Distributed Denial of Service)*.	Médio	2º
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Baixo	3º
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Alto	1º

Tratamento do risco ----------

Sugere-se a definição da opção de tratamento adequada, procedendo à identificação dos controlos que podem ser implementados para mitigar, evitar ou transferir o risco, bem como definir um plano de tratamento do mesmo.----------



As opções de tratamento de risco a serem consideradas, são:

» **Evitar o risco:** colocar a probabilidade ou impacto tendencialmente próximo de zero, tornando mais difícil a sua ocorrência e/ou eliminar totalmente o seu impacto. ----------

» **Aceitar o risco:** decisão de aceitação do risco. Sugere-se que a assunção de responsabilidade por essa decisão seja formalmente registada pela entidade.----------

» **Mitigar o risco:** reduzir a probabilidade e/ou impacto de um evento adverso para limites aceitáveis, através da implementação de controlos ou contramedidas.----------

» **Transferir o risco:** transferir, total ou parcialmente, para terceiras partes, o impacto em relação a uma ameaça (por exemplo: efetuar a contratualização de um seguro).----------

Assim que o plano de tratamento do risco seja definido, os riscos residuais necessitam de ser determinados. ----------

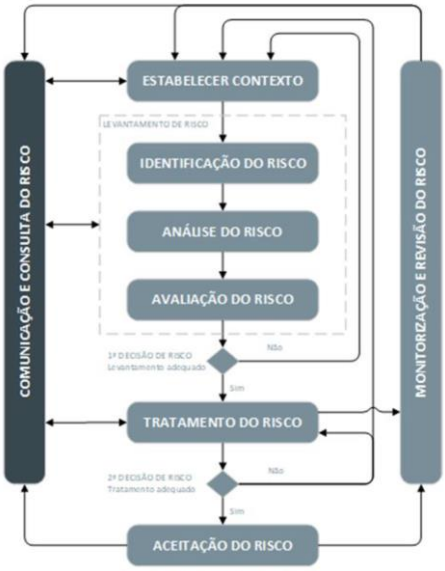
- Este processo envolve uma atualização ou uma nova iteração com a fase de avaliação, tendo como base os efeitos esperados pelo tratamento do risco proposto.----------
- Caso o risco residual ainda não cumpra com os critérios de aceitação do risco da entidade, poderá ser necessária uma iteração adicional do tratamento do risco antes de se proceder à aceitação do mesmo.----------

Exemplo da fase de Tratamento do risco:

Descrição	Classificação do risco	Opção de Tratamento	Justificação para Opção de Tratamento
Indisponibilidade da plataforma devido a um ataque do tipo DDoS *(Distributed Denial of Service)*.	Médio	TRANSFERIR	O prestador de serviços gere toda a infraestrutura e garante capacidades adicionais de monitorização de segurança.
Mau funcionamento da plataforma devido a especificações pouco claras ou incompletas.	Baixo	ACEITAR	Controlos aplicados em conformidade com as boas práticas nacionais e internacionais.
Indisponibilidade da plataforma devido a falhas no processo de gestão de vulnerabilidades.	Alto	MITIGAR	Incluir procedimentos de gestão e reporte de vulnerabilidades de Segurança de Informação à plataforma no contrato de prestação de serviços

Comunicação e consulta do risco ----------

Sugere-se que a informação e as decisões referentes aos riscos sejam partilhadas com todas as partes interessadas relevantes. Recomenda-se que a comunicação do risco seja realizada, de modo a: ----------

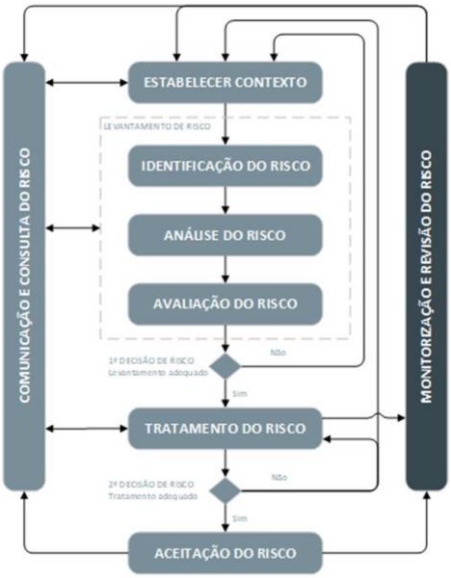


- Providenciar a garantia do resultado da gestão dos riscos da entidade.
- Partilhar os resultados da avaliação dos riscos, apresentar o plano de tratamento dos riscos e melhorar a consciencialização sobre a importância do processo de gestão dos riscos. ----------
- Suportar as tomadas de decisão, e disponibilizar, a quem toma as decisões e às partes interessadas da entidade, uma demonstração de responsabilidade sobre os riscos. ----------
- Coordenar com outras partes interessadas e planear respostas para reduzir o impacto dos incidentes. ----------

Nota: Sugere-se o desenvolvimento de planos de comunicação de suporte aos processos de gestão do risco, comuns e de emergência. ----------

Monitorização e revisão do risco ----------

Sugere-se que os riscos e os seus fatores sejam monitorizados e revistos com regularidade, de modo a que se identifique atempadamente qualquer alteração que se possa traduzir numa alteração à perceção do risco da entidade.----------



Sugere-se a monitorização de forma continua:

- Novos ativos ou alterações na criticidade dos ativos para a entidade. ----------
- Novas ameaças ativas, tanto dentro como fora entidade, e que ainda não foram avaliadas.----------
- Novas vulnerabilidades serem exploradas por novas ameaças.----------
- Possível aumento do impacto, consequências das ameaças, vulnerabilidades ou dos riscos agrupados que resultem num nível inaceitável do risco.----------
- Incidentes de segurança da informação que possam ocorrer.----------

Disposições Finais----------

A presente política deve ser revista sempre que se verifique alguma alteração no âmbito da análise de risco, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas recomendadas pela indústria, garantindo que continua a ser relevante e adequado. ----------

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas. ----------

Política de Notificação e Gestão de Incidentes----------

Município de Vinhais----------
Rua das Freiras, 13----------
5320-326 Vinhais----------

Introdução----------

Em conformidade com o Decreto-Lei n.º 65/2021, a Câmara Municipal de Vinhais deve notificar o CNCS da ocorrência de incidentes detetados, ou a estes comunicados pelos seus clientes, utilizadores ou outras entidades, com impacto relevante ou substancial. As

entidades devem implementar todos os meios e procedimentos necessários à deteção, avaliação do impacto e notificação de incidentes. Um incidente de cibersegurança é um evento com um efeito adverso real na segurança das redes e dos sistemas de informação. São exemplos de incidentes de cibersegurança:----------

- Todos tipos de ciberataques.----------
- Perda ou roubo de equipamento, informação ou bens, propriedade da entidade.------
- Tentativas de identificação e acesso não autorizado a sistemas ou dados.----------
- Tentativas de identificar e explorar vulnerabilidades em sistemas ou dados.----------
- Ataques de negação de serviço.----------
- Alterações a um sistema, sem o conhecimento, instruções ou consentimento prévio da pessoa responsável pelo mesmo.----------
- Não cumprimento das políticas de segurança.----------

Público-alvo ----------

O Município de Vinhais----------

Objetivo do presente documento----------

O documento pretende descrever o procedimento a seguir relacionado com a notificação de incidentes, em conformidade com o Decreto-Lei n.º 65/2021, e de forma sumária, fornecer recomendações sobre como abordar a gestão de incidentes de cibersegurança.----------

Procedimento por cada incidente objeto de notificação----------

» **Notificação inicial**----------

Deve ser enviada logo que a Câmara Municipal de Vinhais possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até **duas horas** após essa verificação. Deve incluir a seguinte informação:----------

- Nome, número de telefone e endereço de correio eletrónico de um representante da entidade.----------
- Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção do incidente.----------

- Breve descrição do incidente.----------
- Estimativa possível do impacto, considerando número de utilizadores afetados pela perturbação do serviço, duração do incidente e distribuição geográfica.----------

» **Notificação de fim de impacto**----------

Deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de **duas horas** após a perda de impacto relevante ou substancial. Deve incluir a seguinte informação: -----

- Atualização da informação transmitida na notificação inicial, caso exista.----------
- Breve descrição das medidas adotadas para a resolução do incidente.----------
- Descrição da situação do impacto existente no momento da perda de impacto relevante ou substancial, nomeadamente número de utilizadores afetados pela perturbação do serviço, duração do incidente e distribuição geográfica, no que se refere à zona afetada pelo incidente.----------
- Tempo estimado para a recuperação total dos serviços.----------

» **Notificação final**----------

Deve ser enviada no prazo de **30 dias úteis** a contar do momento em que o incidente deixou de se verificar. Deve incluir a seguinte informação:----------

- Data e hora em que o incidente assumiu o impacto relevante ou substancial.---------
- Data e hora em que o incidente perdeu o impacto relevante ou substancial.----------
- Impacto do incidente, considerando número de utilizadores afetados pela perturbação do serviço, duração do incidente e distribuição geográfica.----------
- Descrição do incidente, com indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida.----------
- Indicação das medidas adotadas para mitigar o incidente.----------
- Descrição da situação residual do impacto existente à data da notificação final.------
- Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente Ministério Público, Polícia Judiciária, ANEPC, ANACOM, CNPD e a outras autoridades setoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis.----------

» **Incidentes resolvidas dentro duas horas após deteção**----------

Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final.----------

Instrução técnica ----------

O envio das Notificações de incidentes e de informação adicional, deve ser realizado através da página web do CNCS existente para o efeito, mediante o preenchimento do modelo de reporte estabelecido: ----------

https://www.cncs.gov.pt/pt/notificacao-incidentes/----------

E selecionar a opção: Pretende reportar um incidente ao abrigo do Artigo 13.º do Regime Jurídico da Segurança do Ciberespaço----------

Nos casos em que a Câmara Municipal de Vinhais não tem temporariamente capacidade operacional para assegurar a notificação no website do CNCS, ou nos casos em que o mesmo esteja indisponível, a notificação poderá ser efetuada, a título excecional, através:----------

- De correio eletrónico remetido para o seguinte endereço: cert@cert.pt----------
- Por telefone através do número (+351) 210 497 399.----------
- Por telefone através do número (+351) 910 599 284, em disponibilidade contínua (24/7).----------

Taxonomia de incidentes e de efeitos----------

Causas raiz
Falha de sistema
Fenómeno natural
Erro humano
Ataque malicioso
Falha no fornecimento de bens ou serviços por terceiro

Efeitos produzidos	Tipo do Incidente
Código Malicioso	Sistema Infetado Distribuição de Malware Servidor C2 Configuração de Malware
Disponibilidade	Negação de Serviço Negação de Serviço Distribuída Configuração incorreta Sabotagem Interrupção
Recolha de Informação	Scanning Sniffing Engenharia Social
Intrusão	Compromisso de Conta Privilegiada Compromisso de Conta Não Privilegiada Compromisso de Aplicação Arrombamento
Tentativa de Intrusão	Exploração de Vulnerabilidade Tentativa de Login Nova assinatura de ataque
Segurança da Informação	Acesso não autorizado Modificação não autorizada Perda de dados
Fraude	Utilização indevida ou não autorizada de recursos Direitos de autor Utilização ilegítima de nome de terceiros Phishing
Conteúdo Abusivo	Spam Discurso Nocivo Exploração sexual de menores, racismo e apologia da violência
Vulnerabilidade	Criptografia fraca Amplificador DDoS Serviços acessíveis potencialmente indesejados Revelação de informação Sistema vulnerável
Outro	Sem tipo Indeterminado

Gestão de incidentes de cibersegurança ----------

É necessário procurar estabelecer uma estrutura consistente, eficaz e básica de gestão de incidentes de cibersegurança. Algumas recomendações a ter em conta:----------

- Estabelecer normas, processos e procedimentos para a gestão de incidentes e definir papéis e responsabilidades para a formalização de equipa de resposta a incidentes, interna ou externalizada.----------
- Assegurar que colaboradores e partes interessadas estejam conscientes das suas responsabilidades no que diz respeito à comunicação de eventos, incidentes e vulnerabilidades.----------

- Sensibilizar e informar fornecedores, parceiros e terceiros sobre os requisitos e melhores práticas associadas à gestão de incidentes de cibersegurança, incluindo a sua prevenção, deteção e comunicação.----------
- Melhorar continuamente o processo global de gestão de incidentes de cibersegurança, com base nas lições aprendidas e promovendo a partilha de conhecimento entre as partes interessadas.----------
- Salvaguardar e rever contratos e acordos de serviços, requisitos de comunicação e procedimentos para uma resposta adequada a incidentes de cibersegurança, bem como as obrigações legais e regulamentares aplicáveis e penalidades por incumprimento.----------
- Assegurar a resposta a pedidos do Supervisor e/ou Regulador de cibersegurança ou outros órgãos competentes em relação a possíveis investigações de incidentes de segurança. ----------
- Documentar, classificar, indexar e arquivar cada incidente para consulta futura.-----

Disposições Finais----------

A presente política deve ser revista sempre que se verifique alguma alteração no enquadramento legal e regulatória relacionada com Notificações de incidentes do Decreto-Lei n.º 65/2021.----------

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.----------

Responsável de segurança----------

Município de Vinhais----------

Rua das Freiras, 13----------

5320-326 Vinhais----------

Introdução----------

A Câmara Municipal de Vinhais deve designar um responsável de segurança para a gestão das medidas adotadas em matéria de requisitos de segurança e notificação de incidentes. O responsável de segurança é comunicado ao CNCS em conformidade com o Decreto-Lei n.º 65/2021.----------

Público-alvo----------

O Município de Vinhais e outras partes interessadas.----------

Objetivo do presente documento----------

O documento pretende identificar o responsável de segurança e descrever as principais funções e responsabilidades do mesmo. ----------

Responsáveis de Segurança do Município de Vinhais----------

Nome da entidade:	Município de Vinhais
Nome do responsável de segurança:	Artur Jorge Pereira dos Santos Marques
Cargo do responsável de segurança:	Vereador
Endereço de correio eletrónico:	Artur.marques@cm-vinhais.pt
Endereço de correio eletrónico secundário:	geral@cm-vinhais.pt
Número de telefone fixo, se aplicável:	273770300
Número de telefone móvel:	936190725

Nome da entidade:	Município de Vinhais
Nome do responsável de segurança:	José António Gomes Assis Rodrigues
Cargo do responsável de segurança:	Especialista de informática
Endereço de correio eletrónico:	assis.rodrigues@cm-vinhais.pt
Endereço de correio eletrónico secundário:	geral@cm-vinhais.pt
Número de telefone fixo, se aplicável:	273770300
Número de telefone móvel:	934639281

A substituição do responsável de segurança deve ser comunicada de imediato para o endereço de correio eletrónico: sri@cncs.gov.pt----------

Principal função:----------

- Garantir a Segurança de Informação na Câmara Municipal de Vinhais.----------
- Organicamente recomenda-se reportar à gestão de topo.----------
- Dado que o impacto da sua responsabilidade é potencialmente transversal recomenda-se ter conhecimento pleno dos processos chave da entidade, quer do ponto de vista técnico quer do ponto de vista de negócio.----------
- Recomenda-se ter a capacidade de reencaminhar internamente as solicitações das Autoridades.----------
- Tem um papel fulcral na análise e identificação das medidas de Segurança da Informação adequadas para implementação na entidade.----------

- Recomenda-se acompanhar todo o processo de implementação, definição de prioridades e atividades de melhoria contínua, os quais garantam que a entidade está preparada em termos de Segurança da Informação/Cibersegurança.----------
- Recomenda-se ter a capacidade de traduzir os objetivos da entidade em requisitos de Segurança de Informação.
- Recomenda-se promover processos e procedimentos necessários para a ativação do ponto de contacto permanente.

Principais responsabilidades:

- Assegurar a definição, implementação e manutenção da estratégia de Segurança da Informação e Cibersegurança de forma holística e estruturada.
- Garantir a conformidade com a legislação e regulamentação aplicável como o Regime Jurídico de Segurança do Ciberespaço e Regulamento Geral de Proteção de Dados.
- Ter conhecimento e garantir implementação de boas práticas de Segurança da Informação e Cibersegurança, como o "Quadro Nacional de Referência para a Cibersegurança" e "ISO/IEC 27001".
- Definir e identificar requisitos e medidas de Segurança da Informação e Cibersegurança.
- Assegurar o desenvolvimento e implementação de políticas, processos e procedimentos de Segurança da Informação e Cibersegurança.
- Ter conhecimento sobre a legislação e regulamentação específica do setor de atividade da organização, bem como das localizações onde opera.
- Definir e implementar estratégias de avaliação e de resposta aos riscos.
- Acompanhar e avaliar a execução nomeadamente dos processos de Gestão de Alterações e de Gestão de Incidentes.
- Acompanhar auditorias de Segurança da Informação e Cibersegurança e garantir a implementação de ações de melhoria para mitigação do risco.
- Suportar a entidade na estratégia, desempenho e monitorização dos sistemas aplicacionais e infraestrutura.
- Promover ações de sensibilização/consciencialização em Cibersegurança junto dos colaboradores da entidade.

Disposições Finais

A presente política deve ser revista sempre que se verifique alguma alteração no enquadramento legal e regulatória relacionada com o responsável de segurança do Decreto-Lei n.º 65/2021.

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.

Ponto de contacto permanente

Município de Vinhais
Rua das Freiras, 13
5320-326 Vinhais

Introdução

Devido à importância e o impacto dos sistemas de Informação nas entidades e as necessidades que têm surgido, bem como as ameaças e incidentes associados, torna-se fundamental que as entidades assegurem esta função de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS. Em conformidade com o Decreto-Lei n.º 65/2021, o contacto permanente deve ser comunicado ao CNCS.

Público-alvo

O Município de Vinhais e outras partes interessadas.

Objetivo do presente documento

O documento pretende identificar o ponto de contacto permanente e descrever as principais funções e responsabilidades do mesmo.

Ponto de contacto permanente do Município de Vinhais

Nome ou ponto ou pontos de contacto permanente / serviço disponível ou equipa operacional	Endereço de correio eletrónico principal	Endereço de correio eletrónico alternativo	Número de telefone fixo principal (se aplicável)	Número de telefone móvel principal	Número de telefone fixo secondário (se aplicável)
Artur Jorge Pereira dos	artur.marques@cm-vinhais.pt	geral@cm-vinhais.pt	273770300	936190725	N/A

Santos Marques					
José António Gomes Assis Rodrigues	assis.rodrigues@cm-vinhais.pt	geral@cm-vinhais.pt	273770300	934639281	N/A
Edmundo Alexandre Anta Afonso	edmundo.afonso@cm-vinhais.pt	geral@cm-vinhais.pt	273770300	938032144	N/A

A alteração do ponto de contacto permanente deve ser comunicada de imediato para o endereço de correio eletrónico: sri@cncs.gov.pt

Principal função:

- Função exercida na Câmara Municipal de Vinhais para garantir os fluxos de informação de nível operacional e técnico com o CNCS.
- Deve ser assegurado por uma pessoa ou um departamento, interno ou externo, garantindo uma disponibilidade contínua de 24/7, limitada a períodos de ativação, iniciados e terminados mediante comunicação do CNCS.
- Deve ter conhecimento dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;
- Recomenda-se a capacidade de reencaminhar internamente as solicitações das Autoridades.

Principais responsabilidades:

- Articulação intersectorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores.
- Obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial.
- Obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial.
- Partilha de informação quando estejam ativados planos de emergência de proteção civil com impacto ao nível da segurança do ciberespaço, ou planos de segurança das infraestruturas críticas nacionais ou europeias.

- Operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil ou planeamento civil de emergência do ciberespaço ou planos de segurança internos da organização.
- Receção de instruções técnicas emitidas pelo Centro Nacional de Cibersegurança no âmbito do Regime Jurídico da Segurança do Ciberespaço.

Disposições Finais

A presente política deve ser revista sempre que se verifique alguma alteração no enquadramento legal e regulatória relacionada com o ponto de contacto permanente do Decreto-Lei n.º 65/2021.

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas.

Política de distribuição

Município de Vinhais

Rua das Freiras, 13

5320-326 Vinhais

Introdução

É importante definir e formalizar uma política de distribuição de todos documentos para garantir a partilha da informação relevante com todas as partes interessadas.

Público-alvo

O Município de Vinhais

Objetivo do presente documento

O documento visa definir como as políticas e os documentos, que integram este plano de segurança, devem ser distribuídos.

Distribuição

NOME	PÚBLICO ALVO	PARTILHA
Plano de Segurança	O Município de Vinhais, nomeadamente a gestão de topo, o departamento de TI e outras partes interessadas.	Em formato digital PDF partilhada por email ou via link permanente. Em papel caso necessário. A publicação no website não é recomendada.

Política de Segurança da informação	A Política de Segurança da Informação do Município de Vinhais destina-se a colaboradores, estagiários, fornecedores, prestadores de serviços, parceiros, bem como terceiros e todas partes interessadas que, de alguma forma, possam interagir com a informação do Município de Vinhais, de forma direta ou indireta.	Para colaboradores sugere-se partilhar a política em articulação com os Recursos Humanos. Em formato digital PDF partilhada por email ou via link permanente. Em papel caso necessário. A publicação no website não é necessária.
Política de Cibersegurança	A Política de cibersegurança do Município de Vinhais destina-se a colaboradores, estagiários, fornecedores, prestadores de serviços, parceiros, bem como terceiros e todas partes interessadas que, de alguma forma, possam interagir com a cibersegurança do Município de Vinhais, de forma direta ou indireta.	Para colaboradores sugere-se partilhar a política em articulação com os Recursos Humanos. Em formato digital PDF partilhada por email ou via link permanente. Em papel caso necessário. A publicação no website não é necessária.
Política de Utilização Aceitável de Ativos e Boas Práticas de Cibersegurança	Este documento é destinado a todos os colaboradores do Município de Vinhais, bem como estagiários, fornecedores, prestadores de serviços, parceiros, terceiros e demais entidades externas, que prestem serviços ao Município de Vinhais, e que acedem à informação, e/ou dados pessoais, e/ou têm acesso à rede, e/ou usem equipamentos de informática e/ou de comunicação do Município de Vinhais.	Para colaboradores sugere-se partilhar a política em articulação com os Recursos Humanos. Em formato digital PDF partilhada por email ou via link permanente. Em papel caso necessário. A publicação no website não é necessária.
Política de Privacidade	Todas partes interessadas, nomeadamente colaboradores da entidade, e utilizadores dos serviços prestados pela entidade que podem envolver o tratamento de dados pessoais.	A política é publicada no website, como texto ou via link permanente para o documento em formato digital PDF. Sugere-se partilhar a política em articulação com o Encarregado de Proteção de Dados (EPD/DPO) e os Recursos Humanos, para garantir compliance, fácil acesso e tomada de conhecimento por parte de todos colaboradores.
Análise e Gestão de Risco	O Município de Vinhais, nomeadamente a gestão de topo, o departamento de TI e outras partes interessadas.	Em formato digital PDF partilhada por email, link permanente ou partilha interna. Em papel caso necessário. A publicação no website não é recomendada.
Política de Notificação e Gestão de Incidentes	O Município de Vinhais, nomeadamente o departamento de TI e outras partes interessadas.	Em formato digital PDF partilhada por email, link permanente ou partilha interna. Em papel caso necessário. A publicação no website não é necessária.
Responsável de segurança	O Município de Vinhais, nomeadamente a gestão de topo, o departamento de TI e outras partes interessadas como por exemplo o CNCS.	Em formato digital PDF partilhada por email, link permanente ou partilha interna. A informação deve ser comunicada ao CNCS por email. Em papel caso necessário. A publicação no website não é necessária.
Ponto de contacto permanente	O Município de Vinhais, nomeadamente a gestão de topo, o departamento de TI e outras partes interessadas como por exemplo o CNCS.	Em formato digital PDF partilhada por email, link permanente ou partilha interna. A informação deve ser comunicada ao CNCS por email. Em papel caso necessário. A publicação no website não é necessária.

Disposições Finais

A presente política deve ser revista sempre que se verifique alguma alteração no âmbito da partilha e distribuição dos documentos, na organização interna do Município de Vinhais, no enquadramento legal e regulatório ou nas melhores práticas recomendadas pela indústria, garantindo que continua a ser relevante e adequado.

O presente documento, bem como a sua partilha e distribuição, é formalmente aprovado pela gestão de topo e formalizado junto das partes interessadas." ----------

Após análise e discussão foi deliberado, por unanimidade e em minuta, aprovar o documento transcrito. ----------

10 – PLANO MUNICIPAL DE DEFESA DA FLORESTA CONTRA INCÊNDIOS DE VINHAIS (2022-2031) – ALTERAÇÕES APÓS AUDIÊNCIA PÚBLICA. ----------

No seguimento da deliberação tomada na reunião do Órgão Executivo realizada no dia quinze maio do corrente ano, e após terminada audiência pública do Projeto do "Plano Municipal de Defesa da Floresta Contra Incêndio de Vinhais (2022-2031), a Técnica Superior de Engenharia Florestal subscreveu uma informação que vinha acompanhada de um relatório da consulta pública, cujo teor é o seguinte: ----------

"Compete-me informar V. Ex.ª que o período de consulta pública do Plano Municipal de Defesa da Floresta Contra Incêndios (PMDFCI) de Vinhais terminou no passado dia 30 de junho, tendo-se registado algumas sugestões que resultaram num relatório que reflete a análise e ponderação dessas sugestões que por não contrariarem o parecer vinculativo do ICNF, I.P. foram incorporadas no PMDFCI que foi submetido à Comissão Municipal de Gestão Integrada de Fogos Rurais na reunião extraordinária, realizada a 14 de julho de 2023, para a sua consolidação, conforme o n.º 9 do artigo 4.º do Despacho n.º 443-A/2018, de 9 de janeiro. ----------

Assim, cabe-me dar-lhe conhecimento do relatório da consulta pública e da proposta de **Plano Municipal de Defesa da Floresta Contra Incêndios** do Município de Vinhais, já com as alterações resultantes do período de consulta pública, para as mesmas serem enviadas a Reunião de Câmara para eventual aprovação.----------

Após aprovação em Reunião de Câmara e dando cumprimento ao Despacho n.º 443-A/2018, de 9 de janeiro, alterado pelo Despacho n.º 1222-B/2018, de 2 de fevereiro, este Plano, terá de ser levado a Assembleia Municipal para eventual aprovação e posteriormente ser publicado em Diário da República. ----------

ANÁLISE E PONDERAÇÃO DAS SUGESTÕES, COMENTÁRIOS E OBSERVAÇÕES ----------

Durante o período de Consulta Pública do PMDFCI 2022-2031, registaram-se as observações e contributos que estão inscritos na tabela seguinte, onde também se mostra o resultado da análise dos mesmos.----------

Sugestões, comentários e observações	**Resultado da análise das observações e contributos**	
No Caderno II, na página 6, na lista de acrónimos, o "CDOS" passou a designar-se CSREPC, este acrónimo também deve ser alterado no quadro 30 da página 86.	Acolhido	Foi efetuada a alteração dos acrónimos proposta.
No Caderno II, na página 6, na lista de acrónimos, o "CNOS" passou a designar-se CNEPC, este acrónimo também deve ser alterado no quadro 30 da página 86.	Acolhido	Foi efetuada a alteração dos acrónimos proposta.
No Caderno II, na página 37, no quadro 13, lê-se "013 - Rede elétrica de média tensão", mas deveria ler-se "013 - Rede elétrica de alta tensão".	Acolhido	Foi efetuada a alteração proposta.
No Caderno II, na página 83, no quadro 28, atualizar dados.	Acolhido	Foi efetuada a atualização proposta.

Sugestões, comentários e observações	Resultado da análise das observações e contributos	
No Caderno II, os quadros 9, 12 , 13 e 32 assim como os mapas II.11 a II.18, devem ser atualizados de acordo com os novos dados disponibilizados pela E-REDES.	Acolhido	Foi efetuada a alteração proposta.

Após análise e discussão foi deliberado, e em minuta, aprovar as alterações apresentadas e submeter à apreciação e aprovação da Assembleia Municipal, em cumprimento da alínea ccc), do n.º 1, do art.º 33.º, conjugada com a alínea g), do n.º 1, do art.º 25.º, ambos do Anexo I à Lei n.º 75/2013, de 12 de setembro, na sua atual redação.----------

E eu, Ana Maria Martins Rodrigues, assistente técnica do Gabinete de Apoio aos Órgãos Municipais, a redigi e assino. ----------