Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.5. Política de segurança								
A.5.1. Diretrizes da gestão para a segurança da informação	Proporcionar diretrizes e apoio da gestão para a segurança da informação, de acordo com os requisitos de negócio, leis e regulamentações relevantes	**A.5.1.1. Políticas para a segurança da informação**	Um conjunto de políticas para a segurança da informação deve ser definido, aprovado pela gestão, publicado e comunicado aos colaboradores e partes externas relevantes	√		Política do SG, implementada, coerente, consistente e comunicada a todos, tanto a nível interno como externo (publicada no site)	Manual do SG	Implementado
		A.5.1.2. Revisão das políticas para a segurança da informação	As políticas para a segurança da informação devem ser revistas em intervalos planeados ou quando ocorrerem alterações significativas, de modo a assegurar a sua contínua aplicabilidade, adequabilidade e eficácia	√		Está definido. A revisão das políticas é efetuado, pelo menos, uma vez por ano, quando da revisão pela gestão	Planeamento e revisão do SG (PG-01)	Implementado
A.6. Organização de segurança da informação								
A.6.1. Organização interna	Estabelecer um modelo de referência de gestão para iniciar e controlar a implementação e operação de segurança da informação dentro da organização	**A.6.1.1. Papéis e responsabilidades de segurança da Informação**	Todas as responsabilidades de segurança da informação devem ser definidas e alocadas	√		Cada colaborador tem conhecimento das suas funções e responsabilidades, pelo conhecimento das matrizes associadas à função. Funções genéricas estão definidas também no MO	Manual do SG; Matrizes de competências (Aplicação)	Em atualização
		A.6.1.2. Segregação de funções	As funções e áreas de responsabilidades conflituantes devem ser segregadas para reduzir oportunidades para a modificação não autorizada ou não intencional, ou a utilização indevida dos ativos da organização		√	A estrutura organizacional assenta numa definição coerente, clara e objetiva das competências e responsabilidades de cada unidade orgânica, com competências claramente definidas, com linhas de reporte e de autoridade claras, bem como do grau e âmbito de cooperação entre as diversas unidades do organigrama, contemplando uma adequada segregação de funções potencialmente conflituantes. Vai ser desenvolvido, para 2015, um documento "Diagnóstico de Transparência", que terá na sua gênese, o Código de Ética da CMA.		
		A.6.1.3. Contacto com autoridades competentes	Devem ser mantidos contactos apropriados com as autoridades competentes que sejam relevantes	√		No que diz respeito à legislação e normas aplicáveis, por consulta ao DR, assim como a sites normativos/ entidades certificadoras	Manual do SG (Gestão e controlo da informação documentada)	Implementado
		A.6.1.4. Contacto com grupos de interesse especial	Devem ser mantidos contactos apropriados com grupos de interesse especial ou outros fóruns de especialistas de segurança e associações de profissionais		√	Ainda não surgiu a oportunidade de efetuarmos este tipo de contacto. No entanto, existem contactos com fornecedores, especificamente da parte das TI, que têm oferecido a sua ajuda prestável, na resolução/ clarificação de algumas situações que têm surgido a este nível		
		A.6.1.5. Segurança da informação na gestão de projeto	A segurança da informação deve ser endereçada na gestão de projeto, independentemente do tipo de projeto	√		Sempre que seja iniciado/ desenvolvido um novo projeto (ou alteração de um projeto existente), são seguidos os procedimentos estabelecidos ao nível da Segurança da Informação.	Conceção e desenvolvimento de novos serviços (PG-02); Gestão e avaliação do risco (PG-14); Gestão de Alterações (PG-15)	Implementado
A.6.2. Dispositivos móveis e teletrabalho	Assegurar a segurança no teletrabalho e na utilização de dispositivos móveis	**A.6.2.1. Política de dispositivos móveis**	Deve ser adotada uma política e as respetivas medidas de segurança para gerir os riscos introduzidos pela utilização de dispositivos móveis	√		Está a ser implementada uma solução de segurança, com a aquisição de um software KasperSky mobile security, para garantir a segurança da informação acedida através de dispositivos móveis		Em implementação
		A.6.2.2. Teletrabalho	Deve ser implementada uma política e as respetivas medidas de segurança para proteger a informação acedida, processada ou armazenada em locais de teletrabalho	√		Estão definidas políticas de acesso remoto à informação e aplicações da CMA, sob a autorização prévia do Sr. Presidente da CMA.	Políticas Específicas de Segurança da Informação - Acessos - Acesso remoto; Gestão das infraestruturas (PG-06)	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.7. Segurança na gestão de recursos humanos								
A.7.1. Antes da relação contratual	Assegurar que os colaboradores e prestadores de serviço compreendem as suas responsabilidades, e que são adequados para as funções para as quais estão a ser considerados	**A.7.1.1. Verificação de credenciais e referências**	Devem ser realizadas verificações de credenciais e referências de todos os candidatos a uma relação contratual, de acordo com as leis, regulamentações e códigos de ética relevantes, e de forma proporcional aos requisitos de negócio, à classificação da informação que será acedida e aos riscos percecionados		√	A CMA apenas tem em conta os requisitos definidos nos procedimentos concursais, não sendo exigida, salvo casos específicos, qualquer declaração ou credencial comprovativa do não incumprimento de regras relacionadas com a segurança da informação, por outras entidades onde o concursante possa ter trabalhado		
		A.7.1.2. Termos e condições da relação contratual	Os acordos contratuais com os colaboradores e prestadores de serviço devem estabelecer as suas responsabilidades e as da organização relativamente à segurança da informação	√		Os contratos celebrados com colaboradores têm na sua essência a referência à obrigatoriedade de cumprimento das regras, procedimentos e políticas da segurança da informação. Isto também se verifica para os prestadores de serviço, podendo ser efetuado por acordo entre as partes interessadas	Gestão de recursos humanos (PG-03); Contrato de trabalho; Acordo (estágios); Contrato de prestação de serviços	Implementado
A.7.2. Durante a relação contratual	Assegurar que os colaboradores e prestadores de serviço estão conscientes e cumprem as suas responsabilidades de segurança da informação	**A.7.2.1. Responsabilidade da gestão**	A gestão deve requerer a todos os colaboradores e prestadores de serviço que apliquem a segurança da informação, de acordo com os procedimentos e políticas estabelecidos pela organização	√		A liderança está comprometida com a segurança da informação e transmite este comprometimento aos seus colaboradores e prestadores de serviço, disponibilizando a informação relacionada com o tema, pela entrega do Manual de Acolhimento e o Manual do SG. O superior hierárquico tem um papel importante, na fase de acolhimento e integração na CMA	Manual do SG; Políticas específicas de segurança de informação; Gestão de recursos humanos (PG-03); Manual de Acolhimento; Acolhimento e integração de novos colaboradores (IT-03-01)	Implementado, sujeito a melhorias
		A.7.2.2. Consciencialização, escolaridade e formação em segurança da informação	Todos os colaboradores da organização e, quando relevante, os prestadores de serviço devem ser destinatários de ações de consciencialização, educação e formação apropriadas, bem como de atualizações regulares nas políticas e procedimentos da organização que sejam relevantes para o desempenho da sua função	√		Tanto na fase de integração na CMA, como no decorrer da relação contratual, são efetuados momentos de levantamento de necessidades de formação, podendo também acontecer, de forma pontual, pela realização de novas tarefas, que obriguem à realização de sensibilização/ formação para a melhoria ou obtenção de conhecimentos específicos	Gestão de recursos humanos (PG-03); Levantamento de necessidades de formação (aplicação); Plano de formação (Imp-03-02)	Implementado, sujeito a melhorias
		A.7.2.3. Procedimento disciplinar	Deve existir e ser comunicado um procedimento disciplinar formal que seja acionável em relação aos colaboradores que tenham cometido uma violação de segurança da informação	√		Está estabelecida e implementada uma metodologia para a execução de um processo disciplinar formal para os colaboradores que violem a segurança da informação	Gestão de recursos humanos (PG-03); Processo disciplinar (PT-03-01)	Implementado
A.7.3. Cessação e alteração da relação contratual	Proteger os interesses da organização no processo de cessação ou alteração da relação contratual	**A.7.3.1. Responsabilidades na cessação ou alteração da relação contratual**	Devem ser definidas, comunicadas e asseguradas as responsabilidades e deveres de segurança da informação que permaneçam válidas após a cessação ou alteração da relação contratual com os colaboradores ou prestadores de serviço	√		Estão definidas políticas e responsabilidades relacionadas com a saída ou mudança de funções, dos colaboradores da CMA, relativamente à desativação de acessos a sistemas da CMA. Cabe à UT-RH comunicar a sída de um colaborador à DV-AF e à DV-TI (procede à desativação do acesso). De igual modo, quando se verifiquem alterações/ mudança de funções, a chefia comunica à DV-TI, a necessidade de alteração de acesso aos sistemas da CMA. Também, quando se verificar a saída de colaboradores da CMA, as respetivas mailboxes serão desativadas e os e-mails destinados a esses colaboradores reencaminhados para o superior hierárquico ou outro designado.	Gestão de recursos humanos (PG-03); Políticas específicas de segurança de informação - Acessos - Desativação de acessos a sistemas; Alteração de acesso a sistemas; Políticas específicas de segurança de informação - Correio eletrónico, Gestão de e-mail, Utilização da Internet	Implementado, sujeito a melhorias

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.8. Gestão de ativos								
A.8.1. Responsabilidade pelos ativos	Identificar os ativos da organização e definir responsabilidades de proteção apropriadas	**A.8.1.1. Inventário de ativos**	Devem ser identificados os ativos associados com a informação e os recursos de processamento de informação e deve ser criado e mantido um inventário destes ativos	√		Está definido o procedimento a seguir para gerir, manter e controlar os riscos da segurança de informação, no que diz respeito à identificação dos ativos e respetivos cenários de risco da CMA, assim como os processos associados e respetivos responsáveis	Gestão do risco (PG-14) - Pontos 1 e 2	Implementado
		A.8.1.2. Responsabilidade pelos ativos	Os ativos registados no inventário devem ter um responsável	√		Está definido o procedimento a seguir para gerir, manter e controlar os riscos da segurança de informação, no que diz respeito à identificação dos ativos e respetivos cenários de risco da CMA, assim como os processos associados e respetivos responsáveis	Gestão do risco (PG-14) - Pontos 1 e 2	Implementado
		A.8.1.3. Utilização aceitável dos ativos	Devem ser identificadas, documentadas e implementadas regras para a utilização aceitável da informação, dos ativos associados com a informação e dos recursos de processamento de informação	√		Está definido o procedimento a seguir para gerir, manter e controlar os riscos da segurança de informação, no que diz respeito aos ativos e cenários de risco associados, pela aplicação de controlos para evitar, mitigar ou transferir o risco, de forma a diminuir o nível de risco associado.	Gestão do risco (PG-14)	Implementado
		A.8.1.4. Devolução de ativos	Todos os colaboradores e utilizadores de entidades externas devem devolver os ativos da organização que estejam na sua posse no momento da cessação da relação contratual ou acordo	√		Está definido o procedimento a seguir para gerir, manter e controlar os riscos da segurança de informação, no que diz respeito à identificação dos ativos e respetivos cenários de risco da CMA. são geridos, mantidos e controlados, no que diz respeito à identificação, avaliação, tratamento, gestão, monitorização e revisão	Gestão de recursos humanos (PG-03); Políticas específicas de segurança de informação	Implementado, sujeito a melhorias (colocação da obrigatoriedade de devolução no "acordo"/ "contrato")
A.8.2. Classificação da informação	Assegurar que a informação recebe um nível adequado de proteção, de acordo com a sua importância para a organização	**A.8.2.1. Classificação da informação**	A informação deve ser classificada com base nos requisitos legais, valor, importância e sensibilidade em caso de divulgação ou modificação não autorizada	√		Está definido e documentado um procedimento, onde está definida a forma de classificação dos ativos de informação, tendo em conta os graus de acesso à mesma, com as seguintes categorias: Uso Restrito; Uso Interno e Público	Gestão do risco (PG-14) - pontos 3 e 4	Implementado
		A.8.2.2. Etiquetagem da informação	Deve ser desenvolvido e implementado um conjunto de procedimentos apropriados para a etiquetagem da informação, de acordo com o esquema de classificação da informação adotado pela organização	√		Está definido e documentado um procedimento, onde está definida a forma de classificação dos ativos de informação, tendo em conta os graus de acesso à mesma, com as seguintes categorias: Uso Restrito; Uso Interno e Público	Gestão do risco (PG-14) - pontos 3 e 4	Implementado
		A.8.2.3. Manuseamento de ativos	Devem ser desenvolvidos e implementados procedimentos para o manuseamento de ativos, de acordo com o esquema de classificação da informação adotado pela organização	√		Está definido e documentado um procedimento, onde está definida a forma de movimentação/ utilização dos ativos de informação, tendo em conta os graus de acesso à mesma, com as seguintes categorias: Grupo limitado de utilizadores definidos caso a caso; Toda a CMA; e Todos os stakeholders da CMA	Gestão do risco (PG-14) - pontos 3 e 4	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.8.3. Manuseamento de suporte de dados	Prevenir a divulgação não autorizada, modificação, remoção ou eliminação da informação armazenada em suportes de dados	**A.8.3.1. Gestão de suportes de dados amovíveis**	Devem ser implementados procedimentos para a gestão de suportes de dados amovíveis, de acordo com o esquema de classificação adotado pela organização	√		Está definida uma política para a utilização de suportes de informação amovíveis externos (pen drive, CD, discos externos, …) nos equipamentos incluídos no âmbito de proteção. Excetuam-se aqueles provenientes dos munícipes para descarregar os processos de Licenciamento de Obras Particulares, sendo da responsabilidade dos colaboradores da CMA	Gestão das infraestruturas (PG-06); Políticas específicas de segurança de informação - Utilização de suportes amovíveis	Implementado
		A.8.3.2. Eliminação de suportes de dados	Os suportes de dados devem ser eliminados de forma segura, quando deixarem de ser necessários, através da utilização de procedimentos formais	√		Estão definidas as instruções necessárias para executar as tarefas de limpeza permanente de dados e destruição/ abate de suportes de informação amovíveis (discos rígidos, pens, CD, discos USB, etc.).	Gestão das infraestruturas (PG-06); Abate/ Limpeza de suportes de informação amovíveis (IT-06-10); Políticas específicas de segurança de informação	Implementado
		A.8.3.3. Transporte de suportes de dados	Os suportes de dados devem ser protegidos contra acessos não autorizados, utilização indevida ou corrupção durante o seu transporte	√		Estão estabelecidas regras de movimentação "física" de processos em suporte papel, a partir do arquivo e para o arquivo, sendo efetuada devidamente acondicionada (em caixas, pastas), de forma a garantir que tais suportes são transportados nas devidas condições de segurança.	Acessibilidade e Comunicabilidade - Utilizadores externos (PT-05-04) - Consulta presencial	Implementado
A.9. Controlo de acesso								
A.9.1. Requisitos de negócio para controlo de acesso	Limitar o acesso à informação e aos recursos de processamento de informação	**A.9.1.1. Política de controlo de acesso**	Deve ser estabelecida, documentada e revista uma política de controlo de acesso, tendo como base os requisitos de negócio e de segurança da informação	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo. Estão definidos quais os colaboradores que podem aceder a estas áreas e de que forma o fazem. Também estão definidas as regras para o acesso a pessoas externas à CMA.	Políticas específicas de segurança de informação - Acessos - Acesso a zonas seguras; Ficha de Controlo (Imp-06-94)	Implementado
		A.9.1.2. Acesso a redes e a serviços de rede	Aos utilizadores apenas deve ser atribuído acesso à rede e a serviços de rede para os quais tenham sido especificamente autorizados a utilizar	√		Estão definidas políticas de administração de acessos aos utilizadores, mediante prévia autorização do Sr. Presidente da CMA, nomeadamente no que diz respeito à criação, alteração e desativação de acessos a sistemas. Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes; Ativar o acesso interno e remoto de utilizadores à rede da CMA	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado
		A.9.2.1. Registo e cancelamento de utilizador	Deve ser implementado um processo formal de registo e cancelamento de utilizadores para assegurar a atribuição de direitos de acesso	√		Estão definidas políticas de administração de acessos aos utilizadores, mediante prévia autorização do Sr. Presidente da CMA, nomeadamente no que diz respeito à criação e desativação de acessos a sistemas. Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes; Desativação do acesso interno de utilizadores à rede da CMA	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.9.2. Gestão de acesso de utilizadores	Assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas e serviços	**A.9.2.2. Disponibilização de acesso aos utilizadores**	Deve ser implementado um processo formal de disponibilização de acesso aos utilizadores para atribuir ou revogar os direitos de acesso para todos os tipos de utilizadores em todos os sistemas e serviços	√		Estão definidas políticas de administração de acessos aos utilizadores, mediante prévia autorização do Sr. Presidente da CMA, nomeadamente no que diz respeito à criação e desativação de acessos a sistemas. Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes; Ativar o acesso interno e remoto de utilizadores à rede da CMA	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado
		A.9.2.3. Gestão de direitos de acesso privilegiado	A atribuição e utilização de direitos de acesso privilegiado devem ser restritas e controladas	√		Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes; Ativar o acesso interno e remoto de utilizadores à rede da CMA	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso	Implementado
		A.9.2.4. Gestão da informação secreta para autenticação de utilizadores	A atribuição da informação secreta para autenticação deve ser controlada através de um processo formal de gestão	√		Estão definidas políticas de gestão de usernames e password, controladas, para autenticação dos utilizadores	Políticas específicas de segurança de informação - Logs, Usernames e Passwords - Política de gestão de usernames; Política de gestão de passwords	Implementado
		A.9.2.5. Revisão de direitos de acesso de utilizadores	Os responsáveis pelos ativos devem rever os direitos de acesso dos utilizadores em intervalos regulares	√		Estão definidas as regras de revisão dos acessos pelos utilizadores, que recebem uma mensagem para alteração da sua passwird (60 dias)	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso	Implementado
		A.9.2.6. Remoção ou ajuste de direitos de acesso	Os direitos de acesso à informação e aos recursos de processamento de informação, de todos os colaboradores e utilizadores de entidades externas, devem ser removidos após a cessação de relação contratual ou acordo, ou ajustados em caso de alteração destes	√		Estão definidas políticas de administração de acessos aos utilizadores, nomeadamente no que diz respeito à alteração e desativação de acessos a sistemas. Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes; Desativação do acesso interno de utilizadores à rede da CMA	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado
A.9.3. Responsabilidades dos utilizadores	Tornar os utilizadores responsáveis pela proteção da sua informação de autenticação	**A.9.3.1. Utilização da informação secreta para autenticação**	Deve ser exigido aos utilizadores o cumprimento das práticas da organização na utilização da informação secreta para autenticação	√		Estão definidas políticas de gestão de usernames e password, controladas, para autenticação dos utilizadores	Políticas específicas de segurança de informação - Logs, Usernames e Passwords - Política de gestão de usernames; Política de gestão de passwords	Implementado
A.9.4. Controlo de acesso a sistemas e	Prevenir o acesso não autorizado a sistemas e	**A.9.4.1. Restrição de acesso à informação**	O acesso à informação e funções de sistema das aplicações deve ser limitado de acordo com a política de controlo de acesso	√		Estão definidas políticas de administração de acessos aos utilizadores. Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes; Ativação e desativação do acesso interno de utilizadores à rede da CMA	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado
		A.9.4.2. Procedimentos seguros de início de sessão	O acesso aos sistemas operativos deve ser controlado por um procedimento seguro de autenticação	√		Estão definidas políticas de administração de autenticação dos utilizadores, por password criada com determinadas regras. Estão definidas as regras de configuração e instalação de equipamentos, tendo em conta as práticas de instalação, configuração, autenticação e atribuição de privilégios existentes	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
acesso a sistemas e aplicações	autorizado a sistemas e aplicações	**A.9.4.3. Sistema de gestão de senhas**	Os sistemas para gestão de senhas devem ser interativos e assegurar senhas de qualidade	√		A política de complexidade da palavra-chave dos utilizadores obriga a um mínimo de seis caracteres de tipos diferentes (maiúsculas, minúsculas, números e/ou carateres especiais), sendo válida por 60 dias e não pode ser igual a nenhuma das últimas duas palavras-chave utilizadas	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso; Políticas específicas de segurança de informação - Acessos - Política de administração de acessos	Implementado
		A.9.4.4. Utilização de programas utilitários privilegiados	A utilização de programas utilitários que se possam sobrepor aos controlos dos sistemas e aplicações deve ser restringida e controlada de forma rígida	√		A instalação de outro *software*, não incluído nos diferentes perfis definidos, deve ser solicitada à DV-TI e previamente autorizada pelo Presidente da CMA e pelo responsável do respetivo serviço	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso	Implementado
		A.9.4.5. Controlo de acesso ao código fonte de programas	O acesso ao código fonte de programas deve ser restrito	√		O acesso a esta informação está restrita aos técnicos da DV-TI	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso - 7. Acessos ao código fonte das aplicações MEDIDATA	Implementado
A.10. Criptografia								
A.10.1. Controlos criptográficos	Assegurar a utilização adequada e eficaz de criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação	**A.10.1.1. Política sobre a utilização de controlos criptográficos**	Deve ser desenvolvida e implementada uma política sobre a utilização de controlos criptográficos para proteção da informação	√		Estão definidas as instruções necessárias para encriptar os e-mails, por recurso à assinatura digital com Cartão de Cidadão, de forma a assegurar as medidas necessárias que visem garantir a integridade e confidencialidade da informação, quando se considerar necessário, em mensagens de correio eletrónico, contendo o envio de informação considerada crítica/ importante para a CMA	Encriptação de e-mails (IT-06-11)	
		A.10.1.2. Gestão de chaves	Deve ser desenvolvida e implementada uma política sobre a utilização, proteção e vida útil das chaves criptográficas ao longo de todo o seu ciclo de vida	√		Está instalado um software/ serviço "Entidade Certificadora", que permite a emissão de um certificado por estação de trabalho/ servidores e utilizador, para autenticação na Active Directory	Gestão das infraestruturas (PG-06) - Ponto A1 - Configuração, Instalação e Acesso - 1. Instalar e configurar equipamentos	Implementado
A.11. Segurança física e ambiental								
		A.11.1.1. Perímetro de segurança física	Devem ser definidos e utilizados perímetros de segurança para proteger as áreas que contenham informação sensível ou crítica e recursos de processamento de informação	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo. Estão definidos quais os colaboradores que podem aceder a estas áreas e de que forma o fazem. Também estão definidas as regras para o acesso a pessoas externas à CMA.	Políticas específicas de segurança de informação - Acessos - Acesso a zonas seguras; Ficha de Controlo (Imp-06-94)	Implementado
		A.11.1.2. Controlos de entrada física	As áreas seguras devem ser protegidas através de controlos de entrada apropriados que assegurem que apenas é permitido o acesso a pessoas autorizadas	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo. Estão definidos quais os colaboradores que podem aceder a estas áreas e de que forma o fazem. Também estão definidas as regras para o acesso a pessoas externas à CMA.	Políticas específicas de segurança de informação - Acessos - Acesso a zonas seguras; Ficha de Controlo (Imp-06-94)	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.11.1. Áreas seguras	Prevenir o acesso físico não autorizado, os danos e as interferências na informação e nos recursos de processamento de informação da organização	**A.11.1.3. Segurança em escritórios, salas e instalações**	Devem ser concebidas e aplicadas medidas de segurança física para escritórios, salas e instalações	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo. Estão definidos quais os colaboradores que podem aceder a estas áreas e de que forma o fazem. Também estão definidas as regras para o acesso a pessoas externas à CMA.	Políticas específicas de segurança de informação - Acessos - Acesso a zonas seguras; Ficha de Controlo (Imp-06-94)	Implementado
		A.11.1.4. Proteção contra ameaças externas e ambientais	Devem ser concebidas e aplicadas medidas de proteção física contra desastres naturais, ataques maliciosos ou acidentes	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo, contendo portas e chaves de acesso restrito. Quanto a desastres naturais, não existe quaisquer proteção, assumindo-se a eventualidade de acontecerem. Está definido um plano de continuidade de negócio.	Políticas específicas de segurança de informação; Plano de continuidade de negócio (Imp-05-33); Ficha de controlo (Imp-06-94)	Parcialmente implementado/ aplicado
		A.11.1.5. Trabalhar em áreas seguras	Devem ser concebidos e aplicados procedimentos para trabalhar em áreas seguras	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo. Estão definidos quais os colaboradores que podem aceder a estas áreas e de que forma o fazem. Também estão definidas as regras para o acesso a pessoas externas à CMA.	Políticas específicas de segurança de informação - Acessos - Acesso a zonas seguras; Ficha de Controlo (Imp-06-94)	Implementado
		A.11.1.6. Áreas de carga e descarga	Os pontos de acesso, tais como as áreas de carga e descarga e outros pontos onde pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados dos recursos de processamento de informação para evitar o acesso não autorizado	√		Estão definidas políticas de acesso a zonas seguras da CMA, que contém informação considerada sensível, como é o caso do Datacenter, da Sala dos Técnicos da DV-TI, da Sala de Servidores da BMMA, e o Arquivo. Estão definidos quais os colaboradores que podem aceder a estas áreas e de que forma o fazem. Também estão definidas as regras para o acesso a pessoas externas à CMA.	Políticas específicas de segurança de informação - Acessos - Acesso a zonas seguras; Ficha de Controlo (Imp-06-94)	Implementado
		A.11.2.1. Colocação e proteção de equipamentos	Os equipamentos devem ser colocados e protegidos de forma a reduzir os riscos de ameaças e perigos ambientais, e as oportunidades para acesso não autorizado		√	Estão definidas políticas de acesso apenas a zonas seguras da CMA, que contém informação considerada sensível. Relativamente ao acesso "geral" ao edifício e às salas de trabalho dos colaboradores, não estão definidas quaisquer regras, existindo apenas um porteiro na garagem do edifício, podendo os munícipes circular livremente pelo edifício.		
		A.11.2.2. Serviços básicos de suporte	Os equipamentos devem ser protegidos contra interrupções de energia elétrica e outras falhas causadas pelos serviços básicos de suporte	√		Os serviços básicos de suporte apenas estão instalados no Datacenter, onde existem UPS para suporte a falhas de energia elétrica, no prazo de 30 minutos. Relativamente aos restantes equipamentos, não existe qualquer medida de proteção a interrupções elétricas, sendo uma opção de aceitação do risco, assumindo-se a eventualidade de acontecerem, estando definido um plano de continuidade de negócio.	Gestão das infraestruturas (PG-06); Políticas específicas de segurança de informação; Plano de continuidade de negócio (Imp-05-33)	Parcialmente implementado/ aplicado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.11.2. Equipamento	Prevenir a perda, dano, furto ou comprometimento de ativos e a interrupção das operações da organização	**A.11.2.3. Segurança da cablagem**	A cablagem elétrica e de telecomunicações que transporta dados ou que suporta os serviços de informação deve ser protegida contra interceção, interferência ou dano	√		A cablagem é distribuída em calhas técnicas, periodicamente verificadas, com pontos de rede numerados com correspondência no painel de ligação que está alojada no Datacenter, que é de acesso restrito aos funcionários autorizados, que estão registados na aplicação de controlo de acessos da Innux	Gestão das infraestruturas (PG-06) - A2 - Segurança Física e de Dados	Implementado
		A.11.2.4. Manutenção dos equipamentos	Os equipamentos devem ser mantidos de forma correta para assegurar a sua contínua disponibilidade e integridade	√		Estão estabelecidos critérios/ requisitos para a realização de ações de manutenção dos equipamentos, com o objetivo de manter a infraestrutura íntegra e disponível	Gestão das infraestruturas (PG-06) - A3 - Manutenção; Gestão da manutenção preventiva na DV-TI (IT-06-02) e Escolas (IT-06-03)	Implementado, sujeito a melhorias
		A.11.2.5. Remoção de ativos	Os equipamentos, informação ou *software* não devem ser retirados das instalações sem autorização prévia	√		Estão definidas as regras para remoção de equipamentos, informação ou software para utilização fora das instalações da CMA, assim como a forma de os requisitar e de assegurar a sua integridade. Os equipamentos são requisitados pela Intranet, sendo a DV-TI a proceder ao controlo de entrega e receção dos mesmos	Gestão das infraestruturas (PG-06) - A2 - Segurança Física e de Dados	Implementado
		A.11.2.6. Segurança de equipamentos e ativos fora das instalações	Devem ser aplicadas medidas de segurança para os equipamentos que operem fora das instalações, tendo em conta os diferentes riscos decorrentes do trabalho fora das instalações da organização	√		Estão definidas as regras de gestão da segurança de equipamentos para utilização fora das instalações da CMA, assim como a forma de os requisitar e de assegurar a sua integridade. Os equipamentos são requisitados pela Intranet, sendo a DV-TI a proceder ao controlo de entrega e receção dos mesmos	Gestão das infraestruturas (PG-06) - A2 - Segurança Física e de Dados	Implementado
		A.11.2.7. Eliminação e reutilização seguras de equipamentos	Todos os itens de equipamentos contendo suporte de dados devem ser verificados, antes da sua eliminação ou reutilização para assegurar que qualquer dado sensível e *software* licenciado é removido ou eliminado através de reescrita segura	√		Estão definidas as instruções necessárias para executar as tarefas de limpeza permanente de dados e destruição/ abate de suportes de informação amovíveis (discos rígidos, pens, CD, discos USB, etc.).	Abate/ Limpeza de suportes de informação amovíveis (IT-06-10)	Implementado
		A.11.2.8. Equipamento de utilizador não vigiado	Os utilizadores devem assegurar que os equipamentos não vigiados têm uma proteção adequada	√		Estão definidas medidas que não permitem que utilizadores não autorizados acedam aos equipamentos (acesso mediante login/password)	Políticas específicas de segurança de informação - Logs, Usernames e Passwords	Implementado
		A.11.2.9. Política de secretária limpa e ecrã limpo	Deve ser adotada uma política de secretária limpa de papéis e suportes de dados removíveis e uma política de ecrã limpo para os recursos de processamento de informação	√		Está definida uma política referente à acessibilidade física a informação restrita, existente nos gabinetes/ postos de trabalho. Também está definida uma regra de bloqueio automático das estações de trabalho, assim como, um procedimento de bloqueio da estação de trabalho pelo utilizador, sempre que o mesmo se ausente deste.	Políticas específicas de segurança de informação - Gestão de privilégios/ acessos à informação - Controlo de acesso à informação	Implementado, sujeito a melhorias
A.12. Segurança de operações								
A.12.1.	Assegurar a operação	**A.12.1.1. Procedimentos de operação documentados**	Os procedimentos de operação devem ser documentados e disponibilizados a todos os utilizadores que deles necessitem	√		Existem circuitos pre-definidos, com especificação relativamente às tarefas, tempos e responsáveis, para cada procedimento de licenciamento de obras particulares.	Circuitos de obras particulares	Implementado
		A.12.1.2. Gestão de alterações	As alterações na organização, processos de negócio, recursos de processamento de informação e nos sistemas que afetem a segurança da informação devem ser controladas	√		Existem procedimentos a efetuar aquando da necessidade de alterações que, consoante a sua importância, podem ou não ser aplicadas.	Gestão de alterações (PG-15)	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
Procedimentos e responsabilidades operacionais	correta e segura dos recursos de processamento de informação	**A.12.1.3. Gestão da capacidade**	A utilização dos recursos deve ser monitorizada e ajustada e devem ser elaboradas projeções para os requisitos de capacidade futura, de modo a assegurar o desempenho dos sistemas	√		O Plano de Capacidade é revisto anualmente, para verificar o nível de capacidade atual, adequando o mesmo à realidade da CMA. Semestralmente, o nível de capacidade é monitorizado, garantindo o cumprimento das necessidades dos serviços.	Gestão da capacidade (PG-16)	Implementado
		A.12.1.4. Separação entre ambientes de desenvolvimento, teste e de produção	Os ambientes de desenvolvimento, teste e de produção devem ser separados para reduzir os riscos de acesso não autorizado ou alterações no ambiente de produção	√		Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
A.12.2. Proteção contra código malicioso	Assegurar que a informação e os recursos de processamento de informação estão protegidos contra código malicioso	**A.12.2.1. Controlos contra código malicioso**	Devem ser implementados controlos de deteção, prevenção e recuperação para proteger contra código malicioso, em conjugação com ações apropriadas de consciencialização dos utilizadores	√		Estão criadas instruções de trabalho, onde está definido o controlo de antivírus e anti-spyware das aplicações informáticas e infraestruturas tecnológicas. Existe uma consola de gestão centralizada, gerida pela DV-TI que é monitorizada mensalmente.	Antivírus e *backups* (IT-05-02)	Implementado
A.12.3. Salvaguarda de dados	Proteger contra a perda de dados	**A.12.3.1. Salvaguarda de informação**	Devem ser efetuadas e testadas, de forma regular, as cópias de salvaguarda de informação, *softwares* e imagens de sistemas, conforme a política de salvaguarda de informação	√		Estão criadas instruções de trabalho, onde está definido o plano de backups, bem como a periodicidade dos testes aos mesmos. Os backups são efetuados numa localização remota.	Antivírus e *backups* (IT-05-02); Gestão das infraestruturas (PG-06) - A2- Segurança Física e de Dados - 4. Gestão de Antivírus e Anti-spyware; 5. Realização de Cópias de Segurança; 6. Reposições de dados desde as cópias de segurança	Implementado
A.12.4 Registos de eventos e monitorização	Registar eventos e gerar evidências	**A.12.4.1 Registos de eventos**	Devem ser produzidos, mantidos e revistos de forma regular os registos de eventos que contenham informação sobre as atividades dos utilizadores, exceções, falhas e eventos de segurança da informação	√		Os eventos são registados com base no sistema de monitorização do Windows, utilizando o software SpiceWorks e o sistema de monitorização (em testes)	Gestão das infraestruturas (PG-06) - A4- Monitorização e Controlo	Implementado
		A.12.4.2 Proteção da informação registada	Os recursos de registo e as informações registadas devem ser protegidas contra a adulteração e acesso não autorizado	√		Os eventos são registados com base no sistema de monitorização do Windows, utilizando o software SpiceWorks	Gestão das infraestruturas (PG-06) - A4- Monitorização e Controlo	Implementado
		A.12.4.3 Registos de administrador e operador	As atividades dos administradoes e dos operadores de sistema devem ser protegidas contra a adulteração e acesso não autorizado	√		Os eventos são registados com base no sistema de monitorização do Windows, utilizando o software SpiceWorks	Gestão das infraestruturas (PG-06) - A4- Monitorização e Controlo	Implementado
		A.12.4.4 Sincronização de relógio	Os relógios de todos os sistemas relevantes de processamento de informação numa organização ou num dominio de segurança devem ser sincronizados, de acordo com uma única referência horária	√		Estão definidas instruções para a sincronização do relógio de forma automática entre todos os servidores e posteriormente das estações de trabalho através de uma única referência horária.	Gestão das infraestruturas (PG-06) - A1- Configuração, Instalação e Acesso - 2. Sincronizar relógio dos equipamentos	Implementado
A.12.5 Controlo de software em sistemas de produção	Assegurar a integridade dos sistemas de produção	**A.12.5.1 Instalação de software nos sistemas de produção**	Devem ser implementados procedimentos para controlar a instalação de software nos sistemas de produção	√		Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
A.12.6. Gestão de	Prevenir a exploração de	**A.12.6.1. Gestão de vulnerabilidades técnicas**	A informação sobre as vulnerabilidades técnicas dos sistemas de informação em utilização deve ser obtida de forma atempada, a exposição da organização a estas vulnerabilidades deve ser avaliada, e ser tomadas medidas apropriadas para endereçar os riscos associados	√		A DV-TI mantém um registo atualizada as infraestruturas existente que é monitorizada periodicamente. Esta monitorização permite identificar vulnerabilidades para posterior tratamento. Também, na gestão e avaliaçõ de risco, as vulnerabilidades, em relação à segurança da informação, são tidas em conta.	Gestão das infraestruturas (PG-06); Gestão do risco (PG-14)	Implementado, sujeito a melhorias

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
vulnerabilidades técnicas	Prevenir a exploração de vulnerabilidades técnicas	**A.12.6.2. Restrições sobre a instalação de software**	Devem ser estabelecidas e implementadas regras sobre a instalação de software pelos utilizadores	√		Existem regras definidas, onde estão claramente especificados quais os papéis que podem ser atribuidos aos utilizadores. O utilizador comum não tem permissões de instalação. A instalação de outro software, não incluído nos diferentes perfis definidos, deve ser solicitada à DV-TI e previamente autorizada pelo Presidente da CMA e pelo responsável do respetivo serviço	Gestão das infraestruturas (PG-06) - A1-Configuração, Instalação e Acesso - 1. Instalar e configurar equipamentos	Implementado
A.12.7. Considerações para auditorias a sistemas de informação	Minimizar o impacto das atividades de auditoria nos sistemas de produção	**A.12.7.1. Controlos de auditoria nos sistemas de informação**	Os requisitos e atividades de auditoria que envolvam verificações nos sistemas de produção devem ser planeados de forma cuidada e acordados para minimizar as interrupções nos processos de negócio	√		Existem acordos/ contratos com os fornecedores, que incluem informação relativamente a este controlo. Normalmente, estas atividades são realizadas em períodos fora do horário normal de trabalho.	Contratos com fornecedores; Cadernos de Encargos de fornecimento	Implementado
A.13. Segurança de comunicações								
A.13.1. Gestão da segurança da rede	Assegurar a proteção da informação nas redes e nos seus recursos de processamento de informação	**A.13.1.1. Controlos da rede**	As redes devem ser geridas e controladas para proteger a informação nos sistemas e nas aplicações	√		Existem procedimentos/ regras definidos para garantir a confidencialidade, integridade, disponibilidade dos dados e segurança física e dos equipamentos associados.	Gestão das infraestruturas (PG-06) - A2-Segurança Física e de Dados	Implementado
		A.13.1.2. Segurança de serviços de rede	Os mecanismos de segurança, níveis de serviço e requisitos de gestão para todos os serviços de rede devem ser identificados e incluídos nos acordos para serviços de rede, independentemente desses serviços prestados serem internos ou externos	√		Os requisitos relacionados com este controlo encontram-se definidos, garantindo a definição de mecanismos de segurança e gestão de rede.	Gestão das infraestruturas (PG-06) - A1-Configuração, Instalação e Acesso, A2-Segurança Física e de Dados; Políticas específicas de segurança de informação	Implementado
		A.13.1.3. Segregação das redes	Os grupos de serviços de informação, utilizadores e sistemas de informação devem ser segregados em redes	√		Existem politicas de gestão de rede onde estão definidos os diferentes mecanismos de segurança utilizados. Os utilizadores podem ter diferentes perfis definidos superiormente.	Gestão das infraestruturas (PG-06); Políticas específicas de segurança de informação	Implementado
A.13.2. Transferência de informação	Manter a segurança da informação transferida dentro da organização e para qualquer entidade externa	**A.13.2.1. Políticas e procedimentos de transferência de informação**	Devem existir políticas, procedimentos e controlos formais para proteger a transferência da informação através da utilização de qualquer tipo de meio de comunicação	√		Estão definidos e implementodas mecanismos, políticas e regras que mantêm a rede segura contra ataques maliciosos, sejam eles internos ou externos, através de firewall SonicWall, que filtra e protege as comunicações	Gestão das infraestruturas (PG-06) - A1-Configuração, Instalação e Acesso, A2-Segurança Física e de Dados; Políticas específicas de segurança de informação - Acessos	Implementado
		A.13.2.2. Acordos sobre transferência de informação	Os acordos devem endereçar a transferência segura de informação de negócio entre a organização e entidades externas	√		Existem acordos/ contratos com os fornecedores, que incluem informação relativamente a este controlo, de forma a assegurar que a transferência da informação é realizada de forma a mantê-la segura e íntegra	Contratos com fornecedores; Cadernos de Encargos de fornecimento	Implementado
		A.13.2.3. Mensagens eletrónicas	A informação contida nas mensagens eletrónicas deve ser protegida de forma apropriada	√		Estão definidas as instruções necessárias para encriptar os e-mails, por recurso à assinatura digital com Cartão de Cidadão, de forma a assegurar as medidas necessárias que visem garantir a integridade e confidencialidade da informação, quando se considerar necessário, em mensagens de correio eletrónico, contendo o envio de informação considerada crítica/ importante para a CMA	Encriptação de e-mails (IT-06-11)	Implementado
		A.13.2.4. Acordos de confidencialidade ou de não divulgação	Devem ser identificados, revistos regularmente e documentados os requisitos para acordos de confidencialidade ou de não divulgação que reflitam as necessidades da organização para proteção da informação	√		Existem acordos/ contratos com os fornecedores, que incluem informação relativamente a este controlo, de forma a assegurar que a confidencialidade (ou não divulgação) da informação da CMA.	Contratos com fornecedores; Cadernos de Encargos de fornecimento	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.14. Aquisição, desenvolvimento e manutenção de sistemas								
A.14.1. Requisitos de segurança de sistemas de informação	Assegurar que a segurança da informação é uma parte integrante dos sistemas de informações ao longo de todo o seu ciclo de vida. Isto inclui também os requisitos para sistemas de informação que prestam serviços através de redes públicas	**A.14.1.1. Especificação e análise de requisitos de segurança da informação**	Os requisitos relacionados com a segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou para melhorias nos sistemas de informação existentes	√		Quando procedemos à realização de aquisições de equipamentos, temos sempre em conta que as características dos mesmos respondam a requisitos de segurança atuais, mesmo quando se trate de melhorias aos já existentes	Aquisição de bens e serviços/ Armazéns e materiais (PG-04); Caderno de Encargos	Implementado
		A.14.1.2. Proteger serviços aplicacionais nas redes públicas	A informação envolvida em serviços aplicacionais transmitida nas redes públicas deve ser protegida contra atividades fraudulentas, disputas contratuais e divulgação e modificação não autorizadas	√		Estão implementados mecanismos de SSL, ou seja, o acesso aos serviços é efetuado mediante um protocolo de segurança que garante a proteção de toda a informação que neles circula, evitando assim atividades fraudulentas, etc.. Este mecanismo está implementado internamente para o acesso às aplicações MEDIDATA via web (SagaWeb e SigmaDocWeb), serviços online e site municipal.	Gestão das infraestruturas (PG-06) - A2 - Segurança Física e de Dados - 10. Mecanismo/ Protocolo de segurança na publicação de sites da CMA	Implementado
		A.14.1.3. Proteger transações de serviços aplicacionais	A informação envolvida nas transações de serviços aplicacionais deve ser protegida para prevenir a transmissão incompleta, encaminhamento incorreto, alteração não autorizada, divulgação não autorizada, duplicação ou repetição não autorizada da mensagem	√		Estão implementados mecanismos de SSL, ou seja, o acesso aos serviços é efetuado mediante um protocolo de segurança que garante a proteção de toda a informação que neles circula, evitando assim atividades fraudulentas, etc.. Este mecanismo está implementado internamente para o acesso às aplicações MEDIDATA via web (SagaWeb e SigmaDocWeb), serviços online e site municipal.	Gestão das infraestruturas (PG-06) - A2 - Segurança Física e de Dados - 10. Mecanismo/ Protocolo de segurança na publicação de sites da CMA	Implementado
		A.14.2.1. Política de desenvolvimento seguro	Devem ser estabelecidas regras para o desenvolvimento de software e de sistemas e aplicadas ao desenvolvimento realizado na organização	√		Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
		A.14.2.2. Procedimentos de controlo de alterações aos sistemas	As alterações aos sistemas no ciclo de vida do desenvolvimento devem ser controladas através da utilização de procedimentos formais de controlo de alterações	√		Está definido o procedimento a seguir para gerir todas as alterações, através de um processo global de controlo e aprovação, de forma a assegurar que os ambientes de TI permanecem alinhados com os requisitos do serviço, minimizando o impacto dos incidentes relacionados com alterações não autorizadas ou coordenadas sobre a qualidade do serviço e, consequentemente, melhorar as operações diárias da CMA.	Gestão de alterações (PG-15)	Implementado, sujeito a melhorias
		A.14.2.3. Revisão técnica das aplicações após alterações na plataforma de produção	Quando as plataformas de produção são alteradas, as aplicações críticas de negócios devem ser revistas e testadas para assegurar que não há nenhum impacto adverso sobre as operações ou segurança da organização	√		Está definido o procedimento a seguir para gerir todas as alterações, através de um processo global de controlo e aprovação, de forma a assegurar que os ambientes de TI permanecem alinhados com os requisitos do serviço, minimizando o impacto dos incidentes relacionados com alterações não autorizadas ou coordenadas sobre a qualidade do serviço e, consequentemente, melhorar as operações diárias da CMA.	Gestão de alterações (PG-15)	Implementado, sujeito a melhorias

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.14.2. Segurança no desenvolvimento e nos processos de suporte	Assegurar que a segurança da informação é concebida e implementada no âmbito do ciclo de vida do desenvolvimento de sistemas de informação	**A.14.2.4. Restrições sobre alterações em pacotes de *software***	As alterações nos pacotes de *software* devem ser desencorajadas, limitadas às mudanças necessárias e todas as alterações devem ser estritamente controladas	√		Está definido o procedimento a seguir para gerir todas as alterações, através de um processo global de controlo e aprovação, de forma a assegurar que os ambientes de TI permanecem alinhados com os requisitos do serviço, minimizando o impacto dos incidentes relacionados com alterações não autorizadas ou coordenadas sobre a qualidade do serviço e, consequentemente, melhorar as operações diárias da CMA.	Gestão de alterações (PG-15)	Implementado, sujeito a melhorias
		A.14.2.5. Princípios de engenharia de sistemas seguros	Devem ser estabelecidos, documentados, mantidos e aplicados princípios de engenharia de sistemas seguros para todas as iniciativas de implementação de sistemas de informação	√		Está definido o procedimento a seguir para gerir todas as alterações, através de um processo global de controlo e aprovação, de forma a assegurar que os ambientes de TI permanecem alinhados com os requisitos do serviço, minimizando o impacto dos incidentes relacionados com alterações não autorizadas ou coordenadas sobre a qualidade do serviço e, consequentemente, melhorar as operações diárias da CMA. Estas alterações/ atualizações são registadas na aplicação de suporte à DV-TI.	Gestão de alterações (PG-15)	Implementado, sujeito a melhorias
		A.14.2.6. Ambiente de desenvolvimento seguro	As organizações devem estabelecer e proteger, de forma apropriada, ambientes de desenvolvimento seguro para as iniciativas de desenvolvimento e integração de sistemas, que abranjam todo o ciclo de vida do desenvolvimento de sistemas	√		Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
		A.14.2.7. Desenvolvimento subcontratado	A organização deve supervisionar e monitorizar a atividade subcontratada de desenvolvimento de sistemas	√		Todos os fornecedores têm um contrato com a CMA, que determina os requisitos a seguir/ cumprir, neste caso, para o desenvolvimento de sistemas. Este desenvolvimento é acompanhado pela DV-TI, pelo acompanhamento do cumprimento do contrato e caderno de encargos específico para o serviço subcontratado.	Contratos com fornecedores; Cadernos de Encargos de fornecimento	Implementado
		A.14.2.8. Testes de segurança de sistemas	Devem ser realizados testes das funcionalidades de segurança durante o desenvolvimento	√		Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
		A.14.2.9. Testes de aceitação de sistemas	Devem ser estabelecidos programas de testes de aceitação e respetivos critérios de aceitação para novos sistemas de informação, atualizações e novas versões	√		Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
A.14.3. Dados de teste	Assegurar a proteção dos dados usados para testes	**A.14.3.1. Proteção de dados de teste**	Os dados de teste devem ser selecionados cuidadosamente, protegidos e controlados	√		Existem instruções que definem o manuseamento dos dados de teste, por forma a manter a sua integridade bem com a integridade dos dados originais. Os testes efetuados aos dados ficam registados na aplicação de suporte à DV-TI. Foi criado um ambiente de testes configurado, sendo que, neste momento, encontra-se em fase de testes/ implementação.		Em fase de testes/ implementação
A.15. Relações com fornecedores								

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.15.1. Segurança da informação nas relações com os fornecedores	Assegurar a proteção dos ativos da organização que estão acessíveis aos fornecedores	**A.15.1.1. Política de segurança da informação para as relações com fornecedores**	Os requisitos de segurança da informação para a mitigação dos riscos associados ao acesso de fornecedores aos ativos da organização devem ser acordados com os fornecedores e documentados	√		Existem acordos/ contratos e cadernos de encargo com os fornecedores, que incluem informação relativamente aos requisitos de segurança da informação. Também existem políticas no que diz respeito ao acesso à informação e a locais seguros.	Aquisição de bens e serviços/ Armazéns e materiais (PG-04); Contratos; Caderno de Encargos; Políticas específicas de segurança de informação - Acessos	Implementado
		A.15.1.2. Endereçar a segurança nos acordos com os fornecedores	Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa aceder, processar, armazenar, comunicar ou fornecer componentes de infraestrutura de TI para a informação da organização	√		Existem acordos/ contratos e cadernos de encargo com os fornecedores, que incluem informação relativamente aos requisitos de segurança da informação. Também existem políticas no que diz respeito ao acesso à informação e a locais seguros.	Aquisição de bens e serviços/ Armazéns e materiais (PG-04); Contratos; Caderno de Encargos; Políticas específicas de segurança de informação - Acessos	Implementado
		A.15.1.3. Cadeia de fornecimento de tecnologias de informação e comunicação	Os acordos com os fornecedores devem incluir requisitos para endereçar os riscos de segurança da informação associados aos serviços de tecnologias da informação e comunicação e à cadeia de fornecimento de produtos	√		Existem acordos/ contratos e cadernos de encargo com os fornecedores, que incluem informação relativamente aos requisitos de segurança da informação. Também existem políticas no que diz respeito ao acesso à informação e a locais seguros.	Aquisição de bens e serviços/ Armazéns e materiais (PG-04); Contratos; Caderno de Encargos; Políticas específicas de segurança de informação - Acessos	Implementado
A.15.2. Gestão da entrega de serviços pelos fornecedores	Manter o nível acordado de segurança da informação e de disponibilização de serviços, alinhado com os acordos com fornecedores	**A.15.2.1. Monitorizar e rever serviços de fornecedores**	As organizações devem, de forma regular, monitorizar, rever e auditar a disponibilização de serviços pelos fornecedores	√		Existem a prática de verificação/ monitorização dos serviços prestados pelos nossos fornecedores, quer seja no momento da entrega, como no decurso do serviço. É também efetuada uma avaliação dos fornecedores, tendo em conta o cumprimento dos requisitos estabelecidos inicialmente.	Aquisição de bens e serviços/ Armazéns e materiais (PG-04)	Implementado
		A.15.2.2. Gerir alterações aos serviços de fornecedores	As alterações ao fornecimento dos serviços pelos fornecedores, incluindo a manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controlos existentes, devem ser geridas, tendo em consideração a criticidade da informação, dos sistemas e dos processos de negócio envolvidos e a reavaliação dos riscos	√		Existe um procedimento documentado para gerir todas as alterações, através de um processo global de controlo e aprovação, de forma a assegurar que os ambientes de TI permanecem alinhados com os requisitos do serviço, minimizando o impacto dos incidentes relacionados com alterações não autorizadas ou coordenadas sobre a qualidade do serviço e, consequentemente, melhorar as operações diárias da CMA.	Gestão de alterações (PG-15)	Implementado, sujeito a melhorias
A.16. Gestão de incidentes de segurança da informação								
		A.16.1.1. Responsabilidades e procedimentos	Devem ser estabelecidos procedimentos e responsabilidades de gestão para assegurar uma resposta célere, eficaz e ordenada aos incidentes de segurança da informação	√		Está definido um procedimento para assegurar a gestão (registo e tratamento) dos incidentes de segurança da informação, e respetivas responsabilidades.	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Gestão de problemas (PG-18)	Implementado
		A.16.1.2. Reportar eventos de segurança da informação	Os eventos de segurança da informação devem ser reportados através dos canais de gestão apropriados, o mais rapidamente possível	√		Existe uma aplicação GLPI, onde ficam registados todos os eventos e incidentes de segurança da informação. A forma como os utilizadores podem reportá-los é por mail (para suporte.informático), ou pelo preenchimento do Registo de Incidente, existente para o efeito	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Registo de Incidente (Imp-08-02); Gestão de problemas (PG-18)	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.16.1. Gestão de incidentes de segurança da informação e melhorias	Assegurar uma abordagem consistente e eficaz à gestão de incidentes de segurança da informação, incluindo a comunicação de eventos e pontos fracos de segurança	**A.16.1.3. Reportar pontos fracos de segurança da informação**	Os colaboradores e os prestadores de serviço que utilizam os serviços e os sistemas de informação da organização devem ser instruídos a detetar e reportar qualquer ponto fraco de segurança da informação, observado ou suspeito, nos sistemas ou serviços	√		Existe uma aplicação GLPI, onde ficam registados todos os eventos e incidentes de segurança da informação. A forma como os utilizadores podem reportá-los é por mail (para suporte.informático), ou pelo preenchimento do Registo de Incidente, existente para o efeito. Todos os colaboradores têm conhecimento sobre este sprocedimentos, tendo sido informados da sua criação, assim como, a respetiva divulgação/ acessibilidade através da Intranet da CMA.	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Registo de Incidente (Imp-08-02); Intranet; Gestão de problemas (PG-18)	Implementado
		A.16.1.4. Avaliação e decisão sobre eventos de segurança da informação	Os eventos de segurança da informação devem ser avaliados e deve ser decidido se os mesmos serão classificados como incidentes de segurança da informação	√		Está definido um procedimento para assegurar a gestão (registo e tratamento) dos incidentes de segurança da informação, e respetivas responsabilidades, onde está definida a forma de classificação dos eventos como incidentes efetivos.	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Gestão de problemas (PG-18)	Implementado
		A.16.1.5. Resposta a incidentes de segurança da informação	Os incidentes de segurança da informação devem ser respondidos de acordo com os procedimentos documentados	√		Está definido um procedimento para assegurar a gestão (registo e tratamento) dos incidentes de segurança da informação, e respetivas responsabilidades, incluindo a resposta aos incidentes detetados/ registados.	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Registo de Incidente (Imp-08-02); Gestão de problemas (PG-18)	Implementado
		A.16.1.6. Aprender com os incidentes de segurança da informação	O conhecimento obtido através da análise e resolução de incidentes de segurança da informação deve ser empregue de forma a reduzir a probabilidade ou o impacto de futuros incidentes	√		Os incidentes de segurança que se verificaram, servem de conhecimento para situações futuras, porque, quando se verificarem novos incidentes de segurança, proceder-se-á à consulta dos registos de incidentes de segurança anteriores, de forma a perceber de imediato qual a solução que foi tomada anteriormente.	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Registo de Incidente (Imp-08-02); Gestão de problemas (PG-18)	Implementado
		A.16.1.7. Recolha de evidências	A organização deve definir e aplicar procedimentos para identificação, recolha e preservação da informação, que possa servir como evidência	√		Está definido um procedimento para assegurar a gestão (registo e tratamento) dos incidentes de segurança da informação, e respetivas responsabilidades, incluindo a resposta aos incidentes detetados/ registados.	Manual do SG (3.4. NC/ Evento/ Incidentes e melhoria contínua); Registo de Incidente (Imp-08-02); Gestão de problemas (PG-18)	Implementado
A.17. Aspetos de segurança da informação na gestão da continuidade do negócio								
		A.17.1.1. Planeamento da continuidade de negócio de segurança da informação	A organização deve determinar os seus requisitos de segurança da informação e a continuidade da gestão de segurança da informação em situações adversas, por exemplo durante uma crise ou um desastre	√		Está definido um procedimento para garantir que a infraestrutura de Tecnologias de Informação e os serviços da CMA são recuperados dentro dos períodos de tempo acordados, quando se verificar a perda/ interrupção de serviço, onde são planeadas/ definidas as fases do plano de continuidade de negócio. A análise dos cenários de risco, na avaliação do risco, permitem definir controlos para os mesmos, ao mesmo tempo que pode identificar cenários que poderão representar um potencial desastre.	Gestão da continuidade (PG-19) - Ponto 1; Plano de Continuidade de Negócio (Imp-05-33); Plano de Recuperação de Desastres (DRP) (Imp-05-33); Gestão e avaliação do risco (PG-14)	Implementado, sujeito a melhorias

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.17.1. Continuidade de segurança da informação	A continuidade de segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização	**A.17.1.2. Implementação da continuidade de segurança da informação**	A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa	√		Está definido um Plano de Continuidade e respetivo Plano de Recuperação (testado). Está definido um procedimento para garantir que a infraestrutura de Tecnologias de Informação e os serviços da CMA são recuperados dentro dos períodos de tempo acordados, quando se verificar a perda/ interrupção de serviço, onde são planeadas/ definidas as fases do plano de continuidade de negócio. A análise dos cenários de risco, na avaliação do risco, permitem definir controlos para os mesmos, ao mesmo tempo que pode identificar cenários que poderão representar um potencial desastre.	Gestão da continuidade (PG-19) - Ponto 1; Plano de Continuidade de Negócio (Imp-05-33); Plano de Recuperação de Desastres (DRP) (Imp-05-33); Gestão e avaliação do risco (PG-14)	Implementado, sujeito a melhorias
		A.17.1.3. Verificar, rever e avaliar a continuidade de segurança da informação	A organização deve verificar os controlos de continuidade de segurança da informação estabelecidos e implementados em intervalos regulares, para assegurar que estes são válidos e eficazes em situações adversas	√		Estão definidaa as regras para a realização da revisão da continuidade, sendo que o plano de continuidade é revisto quando não estiver alinhado com os objetivos da CMA, pelo menos, uma vez por ano, de forma a garantir que todos os requisitos cumprem o acordado em todas as circunstâncias, inclusive numa grande perda de serviço. O plano é testado, com uma periodicidade específica (pelo menos, anual), seguindo um cronograma de ações, definido no próprio plano, tendo em conta as ações a realizar para cada situação potencial.	Gestão da continuidade (PG-19)	Implementado, sujeito a melhorias
A.17.2. Redundâncias	Assegurar a disponibilidade dos recursos de processamento da informação	**A.17.2.1. Disponibilidade dos recursos de processamento da informação**	Os recursos de processamento da informação devem ser implementados com a redundância necessária para cumprir os requisitos de disponibilidade	√		Existe redundância a nível dos servidores (tanto a nível do equipamento, como a nível dos serviços existentes nos servidores), de forma a garantir a disponibilidade do serviço	Gestão da disponibilidade (PG-17)	Implementado
A.18. Conformidade								
		A.18.1.1. Identificação da legislação aplicável e de requisitos contratuais	Todos os requisitos legais, estatutários, regulamentares, contratuais relevantes, bem como a abordagem da organização para cumprir esses requisitos devem ser identificados explicitamente, documentados e mantidos atualizados, para cada sistema de informação e para a organização	√		A CMA assegura o controlo da legislação, regulamentos e normas aplicáveis à sua atividade. Em relação à legislação e, tendo em conta os sumários do Diário da República eletrónico, o DV-AF informa os colaboradores, por e-mail, das novas/ alterações legislações aplicáveis aos serviços. Cada colaborador poderá também informar quando da entrada em vigor/revogação de legislação aplicável, sendo o GSG a atualizar a lista de legislação. Toda a documentação externa, relacionada com legislação, normas e regulamentos ou outros documentos aplicáveis aos serviços, é arquivada pelo DV-AF/ serviço respetivo.	Manual do SG - 3.2.Gestão e controlo da informação documentada - Pontos 11 e 12; Lista de legislação, regulamentação e normas aplicáveis (Imp-05-16)	Implementado

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.18.1. Conformidade com requisitos legais e contratuais	Evitar violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a segurança da informação e de quaisquer requisitos de segurança	**A.18.1.2. Direitos de propriedade intelectual**	Devem ser implementados procedimentos apropriados para assegurar a conformidade com os requisitos legais, regulamentares e contratuais relativos aos direitos de propriedade intelectual e à utilização de produtos de *software* proprietário	√		Ao efetuar o controlo da legislação, regulamentos e normas aplicáveis à sua atividade, a CMA está a garantir que é do conhecimento de todos, a informação relacionada com a legislação nova/ alterações aplicáveis aos serviços, em qualquer nível. Cada colaborador poderá também informar quando da entrada em vigor/revogação de legislação aplicável, sendo o GSG a atualizar a lista de legislação. Toda a documentação externa, relacionada com legislação, normas e regulamentos ou outros documentos aplicáveis aos serviços, é arquivada pelo DV-AF/ serviço respetivo.	Manual do SG - 3.2.Gestão e controlo da informação documentada - Pontos 11 e 12; Lista de legislação, regulamentação e normas aplicáveis (Imp-05-16)	Implementado
		A.18.1.3. Proteção de registos	Os registos devem ser protegidos contra a perda, eliminação, falsificação, acesso não autorizado e divulgação não autorizada, de acordo com os requisitos legais, regulamentares, contratuais e de negócio	√		A CMA assegura a proteção dos registos produzidos, existindo um procedimento de controlo dos mesmos. Compete aos responsáveis pela emissão dos registos do SG, mantê-los em adequado estado de identificação, indexação e conservação, sendo da responsabilidade do Arquivo o controlo dos registos após o prazo de conservação administrativa. Os registos sujeitos a controlo, prazo de conservação administrativa, prazo e método de eliminação, estão definidos na legislação do regulamento arquivístico para as Autarquias. Os registos que existem apenas em suporte digital, mantêm-se em arquivo digital (informação residente no SI) e sujeitos a backups. Os restantes estão resumidos no Mapa de Registos.	Manual do SG - 3.2.Gestão e controlo da informação documentada - Pontos 8 e 9; Mapa de registos (Imp-05-05); Controlo de Anti-Virus e Backup's (T-05-02); Avaliação, seleção e eliminação de documentos (IT-05-04); Remessa de documentos para o Arquivo Municipal (IT-05-05)	Implementado
		A.18.1.4. Privacidade e proteção de dados pessoais	A privacidade e a proteção de dados pessoais devem ser asseguradas conforme estabelecido pela legislação e regulamentação relevante, onde aplicável	√		A CMA assegura a proteção e privacidade dos dados pessoas, conforme estabelecido na legislação e regulamentação aplicável, seguindo o definido no procedimento implementado de controlo da legislação aplicável/ alterações. Os processos individuais dos colaboradores são mantidos seguros, com controlo de acessos, por se considerarem confidenciais, à luz da legislação em vigor.	Manual do SG - 3.2.Gestão e controlo da informação documentada - Pontos 11 e 12; Lista de legislação, regulamentação e normas aplicáveis (Imp-05-16)	Implementado
		A.18.1.5. Regulamentação de controlos criptográficos	Os controlos criptográficos devem ser utilizados em conformidade com todos os acordos, leis e regulamentos relevantes	√		Estão definidas as instruções necessárias para encriptar os e-mails, por recurso à assinatura digital com Cartão de Cidadão, de forma a assegurar as medidas necessárias que visem garantir a integridade e confidencialidade da informação, quando se considerar necessário, em mensagens de correio eletrónico, contendo o envio de informação considerada crítica/ importante para a CMA	Encriptação de e-mails (IT-06-11)	Parcialmente implementado/ aplicado apenas alguns colaboradores ainda aplicaram este controlo)

Objetivos de Controlo		Identificação do Controlo		Aplicabilidade			Operacionalização do Controlo/ Evidência	Estado
				Sim	Não	Justificação		
A.18.2. Revisões de segurança da informação	Assegurar que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos organizacionais	**A.18.2.1. Revisão independente de segurança da informação**	A abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, objetivos de controlo, controlos, políticas, processos e procedimentos de segurança da informação) devem ser revistos de forma independente, em intervalos planeados ou quando ocorrerem alterações significativas	√		Está definido um procedimento de revisão do SG, de forma a assegurar que a legislação aplicável às atividades da CMA, bem como as orientações dos órgãos municipais, são analisadas garantindo a satisfação das disposições legais aplicáveis e as necessidades e expectativas dos munícipes. De igual modo, está identificada uma revisão da análise e gestão de riscos, com uma periodicidade anual, assim como os planos do SGSI (Disponibilidade, Capacidade, Continuidade)	Planeamento e revisão do SG (PG-01); Gestão e avaliação do risco (PG-14); Gestão da capacidade (PG-16); Gestão da disponibilidade (PG-17); Gestão da continuidade (PG-19)	Implementado
		A.18.2.2. Conformidade com as políticas e normas de segurança	Os gestores devem rever regularmente a conformidade do processamento da informação e dos procedimentos dentro da sua área de responsabilidade com as políticas de segurança, normas e quaisquer outros requisitos de segurança apropriados	√		Está definido um procedimento que descreve o modo de efetuar o planeamento e realização de auditorias internas ao SG, assim como a tomada de decisão face aos resultados, de modo a verificar a sua adequabilidade, grau de implementação e eficácia, identificar e planear as ações necessárias e, posteriormente, verificar a realização e eficácia das mesmas	Manual do SG - 3.3.Auditoria Interna	Implementado, sujeito a melhorias
		A.18.2.3. Revisão da conformidade técnica	Os sistemas de informação devem ser revistos regularmente quanto à sua conformidade com as políticas e normas de segurança da informação da organização	√		Está definido um procedimento que descreve o modo de efetuar o planeamento e realização de auditorias internas ao SG, assim como a tomada de decisão face aos resultados, de modo a verificar a sua adequabilidade, grau de implementação e eficácia, identificar e planear as ações necessárias e, posteriormente, verificar a realização e eficácia das mesmas	Manual do SG - 3.3.Auditoria Interna	Implementado, sujeito a melhorias