Política para a Segurança da Informação Digital

Este componente responde aos standards ISO 9001 e ISO 27001

Aplica-se a Todos os Colaboradores Internos e Externos

Proposta atualizada em 2018-04-10

pelo Grupo de Trabalho TI

e consultor Vitor Mendes

A aprovar pelo Conselho Intermunicipal

Região de Aveiro	**inserido na iniciativa RAD Governança para as Tecnologias de Informação na Região de Aveiro**	

Convidamos todos os Colaboradores
a contribuir para garantir a
Segurança e Privacidade de toda a Informação
pertencente à Organização e aos Cidadãos.

Obrigado pela sua colaboração
São esperadas do Colaborador as seguintes Boas Práticas:

- Melhorar a atitude e o comportamento responsável;
- Conhecer as Regras de Segurança em detalhe;
- Cumprir as Regras e Boas Práticas;
- Contribuir e propor melhorias;
- Divulgar, Informar e Sensibilizar os Colegas;
- Comunicar qualquer não cumprimento, com vista à sua correção.

«A melhor defesa e segurança
é o seu adequado comportamento em cada dia»

INDEX

Capítulo Termos e Condições

1. Glossário – Termos e Conceitos

Este ponto foi propositadamente colocado em primeiro lugar para o melhor entendimento do sentido em que são utilizados os seguintes termos neste documento.

Política	Conjunto de Regras e Procedimentos que deve ser seguido pelos Colaboradores para garantir os fins de utilização Segura e Responsável dos Sistemas Digitais da Organização.
Colaborador	Utilizador dos Sistemas Digitais da Organização. Inclui Colaboradores Internos, Autarcas e pessoas externas prestadoras de serviços. O termo Colaborador foi escolhido porque ser mais amplo e ter um significado mais atual, sublinhando a importância central do comportamento humano para o sucesso da Organização e o cumprimento de regulamentos, tais como RGPD.
Sistemas Digitais	Qualquer Equipamento digital informático, solução de software, plataforma de serviço, site, rede ou canal de comunicações digitais. Foi escolhida esta designação como genérica. Dependendo da regra representa um ou mais elementos antes listados.
Perfil	Conjunto de características ou competências necessárias ao desempenho de uma atividade, cargo ou função.

1. Âmbito e Descrição

Esta Política define as boas práticas para a utilização segura dos sistemas de informação digitais e assegurar as melhores condições de trabalho aos colaboradores para a prestação de serviços aos Cidadãos.

2. A quem se aplica

Esta política aplica-se a todos os Colaboradores internos e externos da Organização, sempre que utilizem ou tenham acesso a qualquer sistema ou informação digital propriedade da organização.

«Obrigado pela sua colaboração.

A melhor defesa e segurança

é o seu comportamento responsável.»

3. Aceitação e validade

Esta Política é mandatória, deve ser respeitada por todos os Colaboradores e não carece de aceitação ou consentimento explícito.

Esta Política mantem-se em vigor permanentemente. Uma nova versão de Melhoria Contínua será publicada sempre que possível.

4. Autoridade

Esta Política foi aprovada pelo Presidente do Município e é considerada da mais elevada importância.

5. Monitorização da utilização dos Sistemas Digitais

O Colaborador deve ter presente que será monitorizada, registada e rastreada toda a atividade de acesso aos Sistemas Digitais da Organização, à Internet e envio de correio eletrónico. Este registo será utilizado para prevenir e identificar violações de segurança, políticas definidas ou qualquer atividade que possa pôr em risco o serviço da Organização.

6. Contacto para todos os assuntos sobre segurança da informação digital, esclarecimentos e comunicação de incidente de segurança

O Colaborador está obrigado a comunicar de imediato ao Serviço TI qualquer incidente ou suspeita de incidente relacionado com segurança.

Contacto:

Procedimento:

7. Contacto do Responsável pela Melhoria Contínua

Convidamos Todos os Colaboradores a contribuir para a melhoria contínua desta política.

Deve propor melhorias pelos seguintes contactos: …

8. Comunicação, sensibilização e formação

Convidamos Todos os Colaboradores a contribuir para a melhoria contínua desta política.

Esta política será alvo de divulgação a todos os Colaboradores ao abrigo das iniciativas de Qualidade Total e RGPD.

Todos os Colaboradores que utilizem um sistema digital da organização têm a obrigação de conhecer, praticar e promover, as boas práticas de segurança.

Um novo Colaborador receberá formação de acolhimento sobre a política de segurança da organização.

Qualquer Colaborador é encorajado e pode pedir formação ou esclarecimento adicional sobre a política de segurança da organização.

9. Outras Políticas e Procedimentos relacionados

- Procedimento Comunicar Incidente de Segurança
- Outras Políticas e Procedimentos a adicionar…

10. Histórico de Revisões

Data da Mudança	**Responsável**	**Sumário de alterações**
2018-04-10	VM	Primeira versão 1.0

Capítulo REGRAS

As REGRAS apresentam-se agrupadas em 10 categorias.

O Colaborador deve ter presente que será monitorizada, registada e rastreada toda a atividade de acesso aos Sistemas Digitais da Organização, à Internet e envio de correio eletrónico. Este registo será utilizado para prevenir e identificar violações de segurança, políticas definidas ou qualquer atividade que possa pôr em risco o serviço da Organização.

Todas as regras e recomendações gerais comunicadas pela organização e Serviço TI aplicam-se a todos os Colaboradores qualquer que seja a atividade exercida.

1. REGRAS sobre Obrigações Legais

O Colaborador poderá incorrer em procedimento interno ou em penalizações legais caso execute ações propositadas ou negligentes no âmbito das regras descritas em seguida.

É expressamente proibido ao Colaborador:

1.1 **Executar ações que prejudiquem** o bom funcionamento dos Sistemas de Informação da Organização;

1.2 **Divulgar informação sensível ou sigilosa**, incluindo informação acerca dos Sistemas de Informação da Organização;

1.3 **Utilizar para qualquer atividade ilícita** os sistemas digitais, equipamentos e redes de comunicação da Organização, nomeadamente, o acesso ilícito a qualquer sistema ou informação, interno ou externo;

1.4 **Tentar introduzir ou difundir propositadamente código malicioso** nos Sistemas de Informação e de Comunicações tal como: vírus, worm, trojan horse (cavalo de troia), e-mail bomb, e-mail spam, spyware(software espião), adware(software de publicidade), keylogger(software registo de teclado) ou outro análogo;

1.5 **Violar os direitos legais de propriedade**, incluindo cópias indevidas de ficheiros e software violando a legislação em vigor ou regulamentos internos.

2. REGRAS sobre Comunicação de Incidentes e Quebras de Segurança

O Colaborador está obrigado a comunicar de imediato ao Serviço de Tecnologias de Informação:

[ver Procedimento Comunicações ao Serviço de Tecnologias de Informação]

2.1 **Qualquer Incidente ou suspeita relacionados com possível Quebra de Segurança**;

2.2 **Sempre que perca a posse ou controlo de qualquer equipamento** digital que contenha informação da Organização ou direitos de acesso aos Sistemas de Informação da Organização. **DEVE comunicar imediatamente** ao Serviço TI a perda ou furto de equipamentos por escrito, incluindo descrição total sobre a ocorrência. O Serviço TI ativará o procedimento de segurança adequado dependendo do relato efetuado pelo Colaborador.

3. REGRAS sobre Segurança da Informação

3.1 **O Colaborador é responsabilizado pelas ações** sobre a informação produzida e/ou modificada com recurso às credenciais de contas de utilizador que lhe foram atribuídas;

3.2 **O Colaborador não pode aceder a informação,** sistemas informáticos ou redes de comunicação, aos **quais não tenha autorização**;

3.3 **O Colaborador deve assegurar a privacidade da informação que utiliza e a que tiver acesso**. Não pode divulgar ou permitir a outra pessoa o acesso físico ou digital à informação da Organização, para qualquer fim que não seja adequado às boas práticas da Organização;

3.4 **Toda a informação em ficheiros é propriedade da Organização**. Os Documentos de trabalho armazenados e alterados pelo Colaborador no disco local devem ser copiados logo que possível para a pasta adequada em servidor.

3.5 **A informação considerada propriedade da organização não pode ser armazenada em equipamentos pessoais ou em ambientes não controlados pelo Serviço TI**, incluindo recursos de organismos externos com quem a organização não tenha um contrato para o efeito;

4. REGRAS sobre Utilização responsável dos Recursos Informáticos

O Colaborador deve garantir a utilização responsável dos recursos informáticos (equipamentos digitais, software e comunicações) seguindo as seguintes orientações:

4.1 **DEVE evitar** utilizar os recursos informáticos **para qualquer outra finalidade que não seja ao serviço do interesse da Organização,** e ter sempre presente o bom senso;

4.2 **DEVE garantir a segurança e proteção contra terceiros** dos recursos que lhe estão atribuídos. **NÃO deve abandonar** recursos informáticos portáteis sem vigilância. **Deve** garantir que são guardados em local seguro;

4.3 **DEVE entregar ao Serviço Responsável** todos os recursos informáticos que tenha em sua posse, em caso de extinção do vínculo com a Organização. De igual modo, quando aplicável, em caso de Mobilidade para outro serviço ou localização, ou alteração para funções que não requeiram esses recursos.

5. REGRAS sobre Utilização responsável da Internet e Correio eletrónico

A Internet e o Correio eletrónico são recursos fornecidos pela Organização para facilitar as atividades de trabalho do Colaborador.

Todas as regras e recomendações gerais comunicadas pela organização e Serviço TI aplicam-se a todos os Colaboradores qualquer que seja a atividade exercida.

A Organização reserva o direito de limitar através de regras o acesso à Internet e o conteúdo das mensagens de Correio eletrónico recebidas e enviadas, por perfil funcional do Colaborador.

5.1 **O Colaborador responde pela utilização adequada do acesso à Internet e do Correio eletrónico**, e deve utilizar apenas de acordo com o âmbito e fins da respetiva atividade que lhe é pedida pela Organização.

5.2 **É proibida** a utilização da Internet, Correio eletrónico ou qualquer outro canal de comunicação que viole ou coloque em causa: as Políticas da organização, as Políticas de Segurança dos Sistemas de Informação, a Legislação em vigor, valores Éticos e Morais, a Imagem da Organização.

5.3 **É proibido** o acesso, utilização, download, envio ou reencaminhamento de mensagens e conteúdos impróprios e que não se relacionem com os interesses da Organização, tais como: Chat público; Hacking; Crime e Violência; Racismo e descriminação; Estupefacientes; Pornografia; Jogos; Filmes; qualquer outro conteúdo proibido por lei.

5.4 **O Colaborador é responsável** por garantir a segurança, fidedignidade e adequação dos ficheiros que recebe e obtém através da Internet e Correio eletrónico. Todos os ficheiros que cheguem ao Colaborador a partir de origem externa à Organização devem ser sempre considerados suspeitos à partida, obrigando ao bom senso na confirmação de que proveem de fonte fidedigna e confiável.

5.5 **É proibido** o acesso a *proxies* remotos e a comunicações VPN de rede privada com mecanismos *tunneling* que permitam esconder e anonimizar os acessos ou ludibriar sistemas de auditoria e proteção das redes de comunicação. São exceção a esta regra os acessos a sites da função pública, ou acessos VPN fornecidos pelo Município.

5.6 **É proibida** a instalação de qualquer equipamento ou software na infraestrutura de comunicações ou computadores alterando, contornando ou colocando em risco as comunicações controladas pelo Serviço TI.

5.7 **É proibido** o acesso à Internet através de uma ligação alternativa aos acessos oficiais de comunicação disponibilizados pela Organização, nas instalações da Organização.

5.8 Em **caso de extinção do vínculo** com a Organização, o Colaborador deve eliminar do sistema a informação pessoal que não diga respeito à Organização.

5.9 O endereço de email institucional **não deve** ser utilizado com fins particulares para registo em plataformas de compras online, redes sociais, ou outras plataformas que não estejam relacionadas com as funções desempenhadas pelo colaborador;

6. REGRAS sobre Utilização responsável das Contas de Utilizador e Palavras-passe

O Colaborador:

6.1 **NÃO PODE** autenticar-se nos sistemas com qualquer conta de utilizador que não lhe tenha sido atribuída;

6.2 **NÃO PODE permitir ou facilitar a terceiros o acesso** aos sistemas digitais da organização.

6.3 **DEVE manter confidencial qualquer palavras-passe** que utilize para aceder aos Sistemas Digitais da Organização, ou qualquer outra que venha a ter conhecimento;

6.4 **NÃO revelar ou partilhar qualquer palavras-passe**, de nenhuma forma, seja com pessoas externas ou internas à Organização;

6.5 **Manter confidencial qualquer palavras-passe de conta de grupo** de trabalho e não a pode revelar a pessoas que não pertençam a esse grupo de trabalho;

6.6 **NÃO DEVE deixar as suas palavras-passe gravadas num browser** internet de um equipamento que não seja do seu uso exclusivo;

6.7 **DEVE evitar a visualização** por terceiros da digitação **da palavra-passe**. A introdução deve ser efetuada no formato ilegível (ex. ****). Evitar que a introdução seja observada ou copiada.

6.8 **NÃO DEVE escrever as palavras-passe**, seja em papel ou em formato digital.

6.9 **DEVE alterar a palavra-passe** sempre que perceba que esta pode estar comprometida;

6.10 **DEVE alterar as palavras-passe em intervalos regulares no prazo máximo de 180 dias**.
Mesmo quando tal não é exigido pelo sistema.
As palavras-passe de contas privilegiadas devem ser alteradas mais frequentemente;

6.11 **DEVE bloquear ou terminar a sessão** sempre que não esteja junto do equipamento informático;

6.12 **DEVE manter seguros** todos os equipamentos informáticos com o pedido automático de palavra-passe por inatividade, fixada no máximo em 15 minutos.

7. REGRAS sobre Criar Palavras-passe Seguras

O Colaborador está obrigado a criar Palavras-passe Seguras, respeitando as seguintes regras:

7.1 **Escolher palavras-passe fortes** que cumpram as regras de complexidade definidas pela Organização, Serviço TI e que não possam ser facilmente descobertas (De acordo com Resolução do Conselho de Ministros n.º 41/2018):

- Deve ter no mínimo 9 carateres;
- Tem de conter pelo menos um carater de 3 dos 4 conjuntos: letras minúsculas (a…z); letras maiúsculas (A…Z); números (0…9) ; carateres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /).
- NÃO PODE ser igual às 2 últimas anteriores;
- NÃO PODE ser derivada do nome identificador do utilizador;
- NÃO DEVE conter nomes de família;
- NÃO DEVE conter data de nascimento;
- Em alternativa poderá ser constituída por frase ou excerto de texto longo conhecido pelo utilizador, sem caracteres «espaço».

7.2 **NÃO DEVE utilizar a mesma palavras-passe** para vários sistemas, especialmente aqueles mais críticos que podem por em maior risco a Segurança e Privacidade da Informação;

7.3 **NÃO DEVE utilizar as mesmas palavras-passe** para uso pessoal e profissional;

7.4 **Evitar reutilizar palavras-passe** previamente usadas;

8. REGRAS sobre Acessos Remotos

8.1 **O acesso remoto a um computador** de um utilizador por uma pessoa não pertencente ao Serviço TI, só pode ser efetuado após o consentimento do Serviço TI.

9. REGRAS sobre Consulta obrigatória ao Serviço TI

9.1 O Colaborador não está autorizado a instalar no computador qualquer software ou hardware.

9.2 O Colaborador não está autorizado a ligar qualquer equipamento digital externo às redes de comunicação internas da Organização.

9.3 O Serviço TI deve sempre ser Consultado para Avaliar tecnicamente a alteração da atribuição e guarda de um recurso digital.

9.4 O Serviço TI deve ser Consultado para avaliação técnica antes de ocorrer a mobilidade do posto de trabalho do Colaborador e do equipamento que lhe está associado.

10. REGRAS: Procedimentos efetuados pelo Serviço TI

10.1 O Serviço TI pode auditar todos os sistemas digitais e redes de comunicação da Organização para garantir as melhores práticas de segurança e gestão dos sistemas digitais.

10.2 O Serviço TI pedirá ao Colaborador que remova das redes de comunicação internas da Organização, ou a sua presença física, qualquer equipamento digital não autorizado por este.

10.3 A instalação e configuração de Software nos equipamentos digitais da Organização apenas pode ser efetuada pelo Serviço TI ou com o seu conhecimento.

10.4 A extinção do vínculo com a Organização determina o cancelamento e eliminação do conteúdo das contas de correio eletrónico após um período de 30 dias ou outro prazo acordado com o Colaborador.

Documento de Governança acompanha Política para a Segurança da Informação Digital

Este componente responde aos standards ISO 9001 e ISO 27001

Este documento tem como função:

Estabelecer uma comunicação efetiva e bem informada

entre

o nível Governança TI Intermunicipal

e

o nível Governança do Intermunicipal

com o objetivo de

Aprovação e Adoção desta Política

por todos Municípios da Região de Aveiro

Região de Aveiro	inserido na iniciativa RAD **Governança para as Tecnologias de Informação na Região de Aveiro**	

1. Apresentação da iniciativa, contexto e justificação

O Grupo de Trabalho TI da Região, daqui em diante designado GTTI, vem submeter à vossa apreciação, para aprovação e recomendação de aplicação ao nível Regional uma "Política para a Segurança da Informação Digital".

Esta Política será a primeira de um conjunto de políticas e procedimentos que definem orientações de Governança uniformes a aplicar nos Municípios da Região.

Esta Política tem também o valor de evidência em como condições estão a ser criadas para a conformidade da RGPD.

Este documento pretende ser um exemplo de aplicação de Governança TI. Destina-se a garantir a aprovação bem informada pelo Conselho Intermunicipal. Acompanhada a entrega da política para aprovação explicando as orientações que a justificam.

2. Referências que orientam esta Política

- **Regulamento (UE) 2016/679 RGPD**
  - O seguimento desta Política por todos os Colaboradores é essencial para reduzir o risco de quebras de segurança na privacidade da informação dos Cidadãos.
- **Resolução do Conselho de Ministros n.º 41/2018**
  - Esta Política incorpora os requisitos técnicos obrigatórios.
- **Norma ISO 2001 – Sistema de Gestão da Qualidade**
  - Demonstração da capacidade da organização em satisfazer as necessidades dos Cidadãos de acordo com a regulamentação aplicável. Esta Política é uma componente essencial da responsabilidade da área TI.
- **Norma ISO 27001 – Sistema de Gestão da Segurança da Informação**
  - Esta Política é uma componente base essencial para assegurar a Segurança da Informação.

3. Objetivos para a aprovação e aplicação desta Política

- Aproximar o mais possível o desenvolvimento da Iniciativa das Boas Práticas internacionais na área da Segurança dos Sistemas Digitais.
- Contribuir com uma entrega TI essencial como evidência de conformidade RGPD.
- Aplicar os requisitos de segurança obrigatórios da Resolução do Conselho de Ministros n.º 41/2018.
- Tornar a Iniciativa num exemplo de aplicação de Governança TI em contexto intermunicipal.
- Continuar a aprendizagem e melhoria de colaboração TI em contexto intermunicipal.

4. Ganhos de Valor para os Municípios da Região

- Contribuir e suportar ganhos de Imagem para os Municípios e para o Serviço TI na defesa da privacidade da informação dos Cidadãos.
- Primeira Política TI criada em colaboração para a Região.
- Componente requisito essencial a gestão da Qualidade.
- Componente requisito essencial entre as Políticas de Segurança da Informação e básico para o caminho ISO27001.
- Componente importante para demonstração de conformidade RGPD, a incluir no "Dossier para Demonstração de Evidências".
- Aprendizagem e demonstração piloto sobre os conceitos e boas práticas recomendadas para Governança TI.
- Fazer o caminho de aprendizagem em como separar a Governança TI da Gestão TI, e como tirar partido para facilitar o processo de colaboração e tomada de decisão em TI na Região.

5. Objetivos para o Sucesso

- Já conseguida a criação e aprovação final desta política pelo presente Comité de Orientação TI (IT Steering Committee). Criada e aprovada pelos Responsáveis das tecnologias de Informação dos 11 Municípios e Comunidade Intermunicipal.
- Conseguir a aprovação final desta política pelo Conselho Intermunicipal.
- Conseguir a aplicação efetiva da Política em todos os Municípios.

6. Envolvimento necessário de outras Competências da Organização

Para o sucesso desta iniciativa será necessário mobilizar e envolver todas as Competências, Serviços e Colaboradores intervenientes na Sensibilização, Envolvimento e Formação:

- Gestão da Qualidade
- Recursos Humanos
- Formação
- Chefes de Divisão

7. Melhoria Contínua

O Grupo de Trabalho TI intermunicipal é o gestor desta Política e o responsável por garantir a sua melhoria contínua.

Todos os Serviços e Colaboradores podem propor melhorias, mas apenas o Grupo de Trabalho TI é autoridade na aprovação das melhorias.

8. Princípios que orientaram a criação desta política

- Uma Política só tem um gestor, única Autoridade e Responsável pela sua Melhoria Contínua.
- Uma Política não pode ser simplesmente adotada do exterior da Organização. Para ser efetiva, necessita de ser adaptada e reescrita dentro da Organização. Isto está escrito em todos os quadros de Boas Práticas e referido em todas as abordagens pelos profissionais. Isto ficou bem percebido pelos participantes no Grupo de Trabalho TI.
- Uma Regra aqui incluída deve ser possível de ser verificada em larga percentagem.
- Uma Regra deve estar escrita de forma a ser facilmente percebida por qualquer colaborador.
- A escrita deve ser o mais simples, direta e ligeira possível. Mesmo que algumas regras de escrita na língua não sejam exatamente seguida com o objetivo de obter a leitura e perceção visual mais eficaz.
- O Colaborador deve ser envolvido como responsável em garantir a Segurança pelo cumprimento das Regras.
- O Colaborador deve ser envolvido como recurso essencial na divulgação e sensibilização.
- A auditoria da execução da Política deve privilegiar, sempre que possível, a correção de comportamentos e não a sua punição.

9. Regras de Aplicação para cada Município

A Política Regional será atualizada em Melhoria Contínua.

O Município poderá atualizar a integração desta política no seu Regulamento Interno.

Recomenda-se que o Regulamento Interno remeta para a consulta desta Política atualizada num documento autónomo, em vez de transpor o texto desta política para o Regulamento.

Cada Município é livre de fazer um mínimo de adaptação à sua realidade, respeitando as regras ordenadas seguintes:

- Primeiro deve contribuir para a Melhoria Contínua desta Política ao nível Regional.
- Se necessário pode acrescentar adendas específicas para o Município que não possam ser aceites ao nível Regional.

10. Definir o procedimento para esta Iniciativa.

- Já aprovada a Política ao nível deste Grupo no papel de "Comité de Orientação TI (IT Steering Committee)".
- Garantir a Melhoria Contínua pelo grupo de trabalho TI.
  - Atribuir um Curador responsável por manter a Política
  - Antecipar tópicos a melhorar na próxima revisão da política.
- Aprovar pelo Conselho Intermunicipal.
- Cada Município deve garantir a aplicação efetiva para a entrada em vigor, garantindo o adequado apoio de autoridade.
- Cada Município deve garantir a Comunicação, Sensibilização, Envolvimento e Formação de todos os Colaboradores.
- Iniciar o levantamento das Métricas.

11. Definir Métricas intermunicipais para Segurança TI relacionadas com esta Iniciativa

Proponho que sejam poucas, simples e passíveis de fácil registo. A lista que se segue é ainda sugestão a ser trabalhada em grupo.

- Número de Incidentes de Segurança.
    - comunicados pelos Colaboradores
    - detetados pelo Serviço TI
    - com origem no correio eletrónico
    - com origem em fishing
- Número de Incidentes de Segurança Graves.
- Número de Quebras de Segurança reportadas à autoridade.
- Número de Testes de Segurança.
- Número de Falhas identificados durante Testes de Segurança.
- Tempo de sistemas em baixo devido a Incidentes de Segurança.
- Número de Melhorias relacionadas com Segurança.

Aprovado na reunião de 13/06/2018