

# | POLÍTICA DE TIC – SEAPDR RS

| **DTIC**- DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

| **DA** - DEPARTAMENTO ADMINISTRATIVO

## 1. INTRODUÇÃO

As políticas de TIC mencionadas foram previamente discutidas, analisadas e aprovadas pela DTIC. Tais políticas estão de acordo com as boas práticas de Governança em TIC e, também, seguem os princípios norteadores de TIC adotados pelo Estado do Rio Grande do Sul, conforme o Decreto Nº 48.048, de 20 de maio de 2011 – publicado no DOE nº 098 de 23 de maio de 2011.

As políticas aqui adotadas poderão sofrer revisão, conforme necessidades apresentadas pela SEAPI, funcionários, tecnologias envolvidas ou mercado. Qualquer alteração feita será comunicada internamente, e as alterações inseridas serão divulgadas para o conhecimento de todos.

A segurança das informações é um trabalho de equipe, ou seja, o envolvimento, participação e colaboração de todos os funcionários da SEAPDR são fundamentais para o sucesso e bom andamento das práticas adotadas. É responsabilidade de cada usuário da Rede SEAPDR conhecer esta política e conduzir suas atividades de acordo com a mesma.

A intenção da DTIC com a publicação da Política de TIC tem por missão proteger a SEAPDR de ações ilegais ou danosas praticadas por qualquer indivíduo, de forma proposital ou inadvertidamente.

Sistemas relacionados à Internet/Intranet/Extranet - incluídos, mas não limitados, os equipamentos de computação, softwares, sistemas operacionais, dispositivos de armazenamento, contas de rede que permitem acesso ao correio eletrônico, acesso à rede SEAPDR, consultas WWW e FTP a partir de IP's (endereços de protocolo internet) devem ser utilizados com o exclusivo propósito de servir aos interesses da SEAPDR e de seus clientes no desempenho de suas atividades, ou seja, tarefas pessoais ou particulares não serão apoiadas ou suportadas por essa política.

A segurança efetiva da informação é um trabalho de equipe envolvendo a participação e colaboração de todos os funcionários e afiliados da SEAPDR. Todo funcionário que manipula informações e/ou sistemas de informações possui responsabilidade direta em nossa rede e cada usuário de computador deve conhecer esta política e conduzir suas atividades de acordo com a mesma.

## 2. PROPÓSITO

O propósito desta política é delinear a utilização aceitável dos equipamentos e serviços de TIC. Estas regras foram definidas para proteger os funcionários e a SEAPDR. A utilização inapropriada dos equipamentos e sistemas relacionados no item anterior torna-os vulneráveis à atuação de agentes externos como de hackers, contaminação por “vírus” e danificação, gerando comprometimento dos sistemas e serviços da rede, além de problemas legais. Definir regras de utilização de equipamentos e serviços, visando minimizar os riscos aos quais a SEAPDR poderá estar exposta, monitorar e garantir o cumprimento das regras definidas pela SEAPDR e prover medidas apropriadas para assegurar a confidencialidade, integridade e segurança de dados e agir em conformidade com as leis locais, com os acordos previstos nas licenças de softwares.

### 3. ABRANGÊNCIA

Esta política se aplica aos funcionários, prestadores de serviços, consultores, auditores, fiscais, temporários e demais colaboradores que estejam a serviço da SEAPDR, incluindo toda a mão-de-obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas; e abrange todos os sistemas e equipamentos de propriedade da SEAPDR, bem como aqueles de propriedade de terceiros que lhe sejam confiados a qualquer título, ou cedidos pela mesma a terceiros. A DTIC não presta serviços a equipamentos e dispositivos particulares.

### 4. POLÍTICA SOBRE O USO DE EQUIPAMENTOS DE TI

Este tópico procura sintetizar todas as **Regras de Utilização dos Equipamentos de TIC**. Tem como objetivo dar informações suficientes para que não haja qualquer incidente causado por mau uso dos equipamentos e serviços de TIC dentro e fora da SEAPDR (Link Dedicado, 3G ou ADSL).

São autorizados a utilizar os equipamentos e serviços da SEAPDR, todos os funcionários efetivos, desde que previamente solicitado pelo Chefe de Setor, Chefe de Divisão ou Diretor de Departamento. A referida solicitação deverá ser feita por e-mail ou Mensagem Rápida (MR), pelo requisitante ao Chefe de TIC, o qual deverá analisar e efetuar liberação após avaliação.

### 5. DIREITOS DE USO

Os colaboradores da SEAPDR têm os seguintes direitos:

- 5.1. Fazer uso legal dos recursos computacionais colocados à sua disposição, respeitadas as normas de utilização estabelecidas pela DTIC;
- 5.2. Ter conta de acesso à rede corporativa, respeitadas as normas de utilização estabelecidas pela DTIC;
- 5.3. Ter conta de correio eletrônico com a extensão do domínio da SEAPDR (EXPRESSO);
- 5.4. Acessar a Intranet e a Internet, respeitando as políticas de TIC expostas pela DTIC;
- 5.5. Acessar as informações que forem franqueadas, relativas às áreas de armazenamento privado e compartilhado, respeitadas as normas de utilização e confidencialidade estabelecidas pela DTIC;
- 5.6. Solicitar suporte técnico sempre que verificado o mau funcionamento dos equipamentos ou do sistema de rede corporativa;

### 6. DEVERES CORRESPONDENTES

Os colaboradores da SEAPDR têm as seguintes obrigações:

- 6.1. Responder pelo uso exclusivo de sua conta pessoal de acesso à rede corporativa;
- 6.2. Identificar, classificar e enquadrar as informações da rede corporativa relacionadas às atividades por si desempenhadas;
- 6.3. Zelar por toda e qualquer informação armazenada na rede corporativa contra alteração, destruição, divulgação, cópia e acessos não autorizados;
- 6.4. Guardar sigilo das informações confidenciais, mantendo-as em caráter restrito;

- 6.5. Manter, em caráter confidencial e intransferível, a senha de acesso aos recursos computacionais e de informação da organização, informando-a formalmente ao Administrador da Rede quando necessitar;
- 6.6. Informar imediatamente à gerência sobre quaisquer falhas ou desvios das regras estabelecidas neste documento, bem como sobre a ocorrência de qualquer violação às mesmas, praticada em atividades relacionadas ao trabalho, dentro ou fora das dependências da SEAPDR;
- 6.7. Responder cível e criminalmente pelos danos causados em decorrência da não observância das regras de proteção da informação e dos recursos computacionais da rede corporativa;
- 6.8. Fazer uso dos recursos computacionais para trabalhos de interesse exclusivo da SEAPDR, e nunca, de cunho pessoal ou particular;
- 6.9. Solicitar apoio, suporte e esclarecimentos aos softwares que compõem a imagem de dados instalada nos microcomputadores utilizados para desempenho de suas atividades funcionais. Softwares que não compõem a imagem citada não serão suportados pela DTIC;
- 6.10. O armazenamento e cópia dos arquivos de dados sempre deverão ser salvos na pasta do servidor do respectivo setor, ou seja, o usuário da rede SEAPDR não deve salvar seus arquivos no microcomputador utilizado para desempenhar suas atividades funcionais. Assim, a DTIC garante a integridade dos dados através do backup corporativo;
- 6.11. Cada colaborador que acessa a rede SEAPDR deve possuir os conhecimentos mínimos relacionados à tecnologia da informação e comunicação e aos softwares básicos para a utilização correta dos recursos de dados.

## 7. PROIBIÇÕES

É proibido aos colaboradores da SEAPDR:

- 7.1. Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais (copyright), bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista, pedofilia ou que faça apologia ao crime;
- 7.2. Utilizar os recursos computacionais ou quaisquer outros de propriedade da SEAPDR, colocados à disposição do colaborador em razão do exercício de sua função, para constranger, assediar, prejudicar ou ameaçar a mesma ou terceiros, sejam eles indivíduos ou organizações;
- 7.3. Passar-se por outra pessoa ou falsificar, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade da SEAPDR, colocados à disposição do colaborador em razão do exercício de sua função; tão pouco, fornecer seu login de rede ou e-mail e respectiva senha à funcionário com permissão menor ou à terceiro.
- 7.4. Alterar os sistemas que onde possui permissão ou poder de administrador, sem autorização e/ou que lese a SEAPDR;
- 7.5. Divulgar quaisquer informações confidenciais para qualquer pessoa ou organização não ligada às atividades da SEAPDR;
- 7.6. Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à SEAPDR;
- 7.7. Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso e demais mecanismos de segurança e restrição de acesso;
- 7.8. Utilizar acesso discado através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado às redes instaladas nas dependências da SEAPDR acarretando problemas na rede;
- 7.9. Acessar ou tentar acesso a sites não autorizados;

7.10. Utilizar quaisquer recursos ou equipamentos da SEAPDR para fins diversos daqueles necessários ao desempenho da função;

## **8. COMPROMISSOS**

Os colaboradores da rede SEAPDR comprometem-se a:

- 8.1. Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores;
- 8.2. Não desenvolver, fomentar ou promover ações na rede SEAPDR que incentivem o racismo ou qualquer tipo de discriminação que viole quaisquer outros direitos constitucionais do cidadão;
- 8.3. Não fazer uso da rede para molestar, ameaçar, assediar ou ofender seus usuários ou terceiros, por quaisquer meios, sejam textos, imagens, vídeos ou correios eletrônicos;
- 8.4. Não fazer uso da rede para circulação de propaganda política e/ou partidária;
- 8.5. Não tomar atitude ou ação que possa, direta ou indiretamente, indisponibilizar recursos da rede corporativa da SEAPDR;
- 8.6. Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;
- 8.7. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da SEAPDR;
- 8.8. Zelar por todos os recursos, equipamentos e informações que lhe sejam confiados em razão do desempenho de sua atividade profissional;
- 8.9. Responsabilizar-se perante a SEAPDR e terceiros por quaisquer prejuízos advindos da violação dos compromissos, deveres e proibições estabelecidas neste documento;
- 8.10. Utilizar-se, de forma ética e em conformidade com as normas de conduta e segurança estabelecidas pela empresa.

## **9. REGRAS DE UTILIZAÇÃO DE SERVIÇO DE E-MAIL**

### **9.1 DIREITOS**

Usuários autorizados poderão utilizar o serviço de e-mail nas seguintes situações:

- 9.1.1. Negócios, tarefas e demandas relacionados à SEAPDR;
- 9.1.2. Comunicações e trocas de informações de uso profissional;
- 9.1.3. Demais atividades profissionais, incluindo pesquisa e desenvolvimento em qualquer domínio público relacionado ao negócio da SEAPDR;

### **9.2. RESTRIÇÕES**

Usuários autorizados não poderão utilizar e-mail nas seguintes situações:

- 9.2.1. Acesso sem a devida autorização às senhas e chaves criptografadas de outros funcionários;
- 9.2.2. Atividades ilegais ou antiéticas como: tentar obter um acesso não autorizado a recursos de e-mail e internet de terceiros;
- 9.2.3. Acessar, realizar download, divulgar, criar ou transmitir conteúdos racistas, imagens pornográficas, pedofilia, propagandas, correntes, ação entre amigos, religião, opção e/ou opinião sobre sexualidade ou qualquer outro tipo de mensagem similar ao que foi citado neste tópico;

- 9.2.4. Violar ou tentar violar direitos autorais e acordos de licenças de softwares;
- 9.2.5. Atividades que não estejam ligadas diretamente ao negócio, estas restrições incluem qualquer propósito religioso, político, caridoso, social e pessoal. Spam (mala direta virtual não solicitada pelo destinatário), mensagens pejorativas e remessa de correntes são expressamente proibidos;
- 9.2.6. Usuário terá que ter cuidado com comunicação geral via e-mail para listas públicas;
- 9.2.7. Enviar e-mails internos como: correntes, fotos pessoais, etc, não relacionados ao serviço da SEAPI;
- 9.2.8. Limite de tamanho do e-mail, por norma e configuração da Procergs, referente ao envio e recebimento não podem exceder 3MB, incluindo os anexos;
- 9.2.9. Limite de caixa de e-mail, visando uma melhor autonomia e desempenho do servidor de e-mail, as caixas de e-mails devem ter limite conforme regras:
- 9.2.10. Limite de caixa de e-mail tem tamanho padrão de 200Mb;
- 9.2.11. Solicitação de aumento de caixa de e-mail deverá ser encaminhada para a direção do Departamento Administrativo, pois, as demais caixas (400Mb e 1Gb), geram custos para SEAPDR, e por este motivo, precisam de aval da Diretoria Administrativa;
- 9.2.12. Para evitar o estouro do limite da capacidade da caixa de e-mail, o usuário, deve usar a função exportar do Direto e salvar os e-mails e mensagens desejadas em sua pasta pessoal na rede de dados da SEAPDR ou em dispositivo externo (Pen Drive, HD Externo, CD ou DVD).

## **10. REGRAS DE UTILIZAÇÃO DE INTERNET**

As regras para utilizar a internet são:

- 10.1. Para realizar download de softwares (incluindo drivers e ferramentas de busca e programas) é fundamental que seja comunicado à DTIC para que a mesma faça a análise, suporte e viabilidade do download;
- 10.2. Havendo autorização, todos os arquivos “baixados” deverão ser submetidos à verificação da existência de vírus, worms e trojans com o devido acompanhamento técnico da DTIC;
- 10.3. Os usuários devem agir em conformidade com as leis locais, com os acordos previstos nas licenças de softwares e diretrizes da DTIC;
- 10.4. Os usuários não poderão acessar site ou serviço web que não está autorizado;
- 10.5. Para desbloqueio de site, o encarregado do setor interessado terá que enviar, via e-mail ou MR, solicitação à direção do D.A. pedido justificado para desbloqueio cuja necessidade deverá ser fundamentada e que vise às atividades da SEAPDR;
- 10.6. Caso usuário acesse site ou serviço web não autorizado, e, tal site ou serviço web danifique a rede lógica de dados da SEAPDR, o mesmo será responsabilizado proporcionalmente aos danos causados.

## **11. MONITORAMENTOS E RESTRIÇÕES**

### **11.1 MONITORAMENTO**

- 11.1.2. E-mails e endereços acessados na internet são mantidos, monitorados e rastreados pela DTIC;
- 11.1.3. Qualquer solicitação de monitoramento de e-mail ou de endereços de internet, por uso suspeito ou impróprio, deverá ser encaminhada ao Chefe de TIC da SEAPDR, com prévia autorização da Diretoria Administrativa;

11.1.4. A DTIC auditará somente os pontos onde houver suspeita e que tornem o funcionário sujeito às eventuais medidas disciplinares;

11.1.5. Cabe a DTIC relatar ao superior imediato do funcionário problemas de uso indevido.

## **11.2 RESTRIÇÕES**

11.2.1. A DTIC pode utilizar software para identificar e bloquear a utilização e acesso a determinados sites dentro da rede SEAPDR;

11.2.2. É obrigação da DTIC, cancelar a seção de internet ou e-mail que está degradando o desempenho dos serviços de rede - exemplo: download de arquivo internet muito grande (vídeo no youtube), mesmo que seja para uso profissional, em horário de expediente ou de pico;

11.2.3. Qualquer equipamento de TIC ou insumo do mesmo não pode ser transportado de um local ao outro sem a prévia comunicação à DTIC;

11.2.4. Qualquer mudança de layout em setor da SEAPDR estará sujeito à disponibilidade de infraestrutura lógica para rede de dados. A DTIC não garante disponibilidade de ponto de rede para microcomputador e impressora quando ocorrer troca ou mudança de local.

## **12. REGRAS DE UTILIZAÇÃO DE HARDWARE**

As regras para utilização correta do hardware são:

12.1. Usuários não podem modificar, trocar ou alterar a configuração do hardware do seu equipamento, tão pouco instalar um novo periférico, sem a aprovação formal do Chefe de TIC após consultar seus técnicos;

12.2. Equipamentos distribuídos pela DTIC aos funcionários não poderão ser trocados entre si, ou seja, o usuário é responsável pelo equipamento que utiliza e não deve troca o mesmo com outro usuário.

## **13. REGRAS DE UTILIZAÇÃO DE SOFTWARE**

As regras para correta utilização dos softwares são:

13.1. Usuários não poderão executar os itens descritos abaixo sem prévia aprovação do Chefe de TIC, são eles:

13.2. Instalar e/ou realizar download de programas não autorizados, softwares sem licença e softwares particulares (mesmo que sejam softwares livres ou freeware);

13.3. Fazer mudanças ou alterações em qualquer software instalado no seu equipamento;

13.4. A utilização de softwares de qualquer espécie deverá ser solicitada a equipe da DTIC, via e-mail ou MR;

13.5. Os softwares e recursos de TIC não devem ser utilizados de maneira pessoal ou particular, apenas para utilização aos interesses públicos e da SEAPDR.

## **14. SOFTWARES E LICENÇAS**

14.1. Todo software executado nos equipamentos da rede na SEAPDR é licenciado, sendo vetada a utilização de qualquer software sem licença;

14.2. A utilização de softwares livres ou temporários deverá ser solicitada ao responsável pela DTIC, via e-mail ou MR;

14.3. A utilização de softwares não licenciados é considerada uma Não-Conformidade Gravíssima e acarretará punições ao funcionário ou colaborador, em qualquer nível, da SEAPDR.

## **15. ADIÇÃO E REMOÇÃO DE RECURSOS**

15.1. É vetada aos usuários da rede de computadores da organização a adição e remoção de quaisquer recursos, sejam eles microcomputadores, impressoras ou outros equipamentos e dispositivos. A adição e remoção desses deverão ser solicitadas a DTIC, para aprovação e, em caso positivo, tais procedimentos deverão ser realizados pelo mesmo.

## **16. ADMINISTRADOR DA REDE**

16.1. O uso das senhas e informações dos usuários, pelo Administrador da Rede, deverá ser realizado com fins operacionais e preventivos, cabendo ao Administrador manter a confidencialidade das informações adquiridas, sobre pena de punição;

16.2. O controle das senhas dos usuários da SEAPDR deve ser feito pelo Administrador da Rede e reportado formalmente para a Alta Direção da SEAPDR com as devidas atualizações, quando solicitadas.

## **17. USO DE SENHA**

17.1. A responsabilidade pela manutenção do sigilo das senhas é exclusiva do colaborador, ao qual é proibido divulgar as senhas pessoais de acesso à rede corporativa a terceiros ou outro funcionário que possua permissão de rede diferente;

17.2. Solicitação de senha tanto de e-mail e login de rede, terá que ser feita pelo responsável do setor solicitante via e-mail ou MR;

17.3. O tempo de criação de e-mail e acesso à rede SEAPDR é de até 24hs após o recebimento da solicitação.

## **18. MANUTENÇÃO PREVENTIVA**

18.1. Será realizada manutenção preventiva nos computadores para corrigir eventuais erros no sistema operacional, troca de imagem quando necessário, limpeza de software e hardware;

18.2. Os setores e departamentos da SEAPDR deverão informar as datas possíveis para realização das visitas técnicas que visem à manutenção preventiva.



## 19. SOLICITAÇÕES QUE NECESSITAM DE PRÉVIA AUTORIZAÇÃO DO GERENTE DE ÁREA

19.1. Para acesso total ou parcial à internet, somente perante autorização da Diretoria Administrativa feita por e-mail ou MR;

19.2. Para acesso a compartilhamentos e pastas na rede, pastas reservadas somente perante solicitação e autorização do encarregado do setor, solicitação deverá ser realizada pelo próprio responsável via e-mail ou MR;

19.3. Acesso à VPN SEAPDR, somente com solicitação justificada via e-mail ou MR;

19.4. Acesso externo a qualquer tipo de ferramenta não ligada diretamente a função exercida pelo solicitante, terá que ser solicitada a DTIC para avaliação; solicitações que visem uso ou interesse pessoal/particular não serão realizadas pela DTIC.

## 20. COMO EFETUAR CORRETAMENTE A SOLICITAÇÃO À DTIC

O procedimento correto para efetuar uma solicitação de serviço junto à DTIC é:

20.1. Usuário deverá informar os dados necessários para efetuar a solicitação de serviço corretamente, tais informações são:

-> Localidade, tipo de conexão (link dedicado ou ADSL), nome do usuário, nome do microcomputador (saa-xxx-xxxx);

-> Descrição do problema e demais informações que o técnico solicitar;

-> A solicitação gerada entrará na fila de demandas e será respeitada a ordem das mesmas; somente em casos especiais ou de extrema urgência a DTIC tratará de maneira diferente uma solicitação.

---

**Pedro José Kercher**

ID 3040151 – DTIC/DA/SEAPDR RS

Chefe da Divisão de Tecnologia da Informação e Comunicação