



GOVERNO DO ESTADO
RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

Governo do Estado do Rio Grande do Sul

Secretaria de Igualdade Cidadania, Direitos Humanos e Assistência Social

Divisão de Tecnologia da Informação

Política de Segurança da Informação - PSI

Documento de Diretrizes e Normas Administrativas



GOVERNO DO ESTADO
RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

Sumário

ANEXO – Política de Segurança da Informação – PSI	3
1.0 INTRODUÇÃO	3
2.0 TERMOS UTILIZADOS	3
3.0 OBJETIVOS	3
4.0 APLICAÇÕES DA PSI	4
5.0 PRINCÍPIOS DA PSI	4
6.0 REQUISITOS DA PSI	4
7.0 DAS RESPONSABILIDADES ESPECÍFICAS	5
7.1 Dos Usuários em Geral	5
8.0 CORREIO ELETRÔNICO	6
9.0 INTERNET	7



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

ANEXA – Política de Segurança da Informação – PSI

1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Secretaria da Igualdade, Cidadania, Direitos humanos e Assistência Social, para proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários da sua rede de informática, em conformidade aos Decretos Estaduais nº 55.647, de 14 de dezembro de 2020, Decreto Estadual nº 55.986 de 07 de julho de 2021 e Decreto Estadual nº 55.987 de 07 de julho de 2021, que tratam da regulamentação da Lei Federal nº 13.709 de 14 de agosto de 2018, instituindo assim a Política de Segurança de TIC e normatizando a Lei Geral de Proteção a dados Pessoais (LGPD).

Deve, portanto, ser cumprida e aplicada em todas as áreas da Instituição.

2. TERMOS UTILIZADOS

2.1 SICDHAS: Secretaria de Igualdade, Cidadania, Direitos Humanos e Assistência Social

2.2 DTI: Divisão de Informática da SICDHAS

2.3 Recursos de TI: conjunto de recursos de informática em funcionamento na SICDHAS, envolvendo servidores de rede, estações de trabalho, impressoras, storages e outros equipamentos, além de programas, aplicativos e sistemas. Utilizados pela SICDHAS.

2.4 Colaborador: toda e qualquer pessoa física (servidor, CC, estagiário, conselheiro, terceirizado, contratado diretamente ou por intermédio de pessoa jurídica, etc.) que tenha acesso a qualquer recurso da rede da SICDHAS.

2.5 Gestores: Administrador ou responsável por atividade laboral que utilize recursos da rede da SICDHAS, incluindo pessoas, processos e/ou materiais.

2.6 Cidadãos: Indivíduo no gozo dos direitos civis e políticos de um Estado, ou no desempenho de seus deveres para com este.

2.6 Chamados: Relato de incidente e ou qualquer outra solicitação registrada de atendimento para a área de TI que gere um numero de chamado .

2.7 LGPD: Lei Geral de Proteção a Dados Pessoais.

2.8 CAU: Central de Atendimento ao Usuário.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

3.0 OBJETIVOS

3.1 Estabelecer diretrizes que permitam aos usuários da rede da SICDHAS seguir padrões de comportamento relacionados à segurança da informação adequados às necessidades das suas atividades de trabalho e de proteção legal da Instituição e dos dados pessoais dos cidadãos.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da SICDHAS quanto à:

- **Integridade:** garantir que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantir que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Em atendimento do Decreto Estadual 55.647 de 14 de dezembro de 2020 que define e regulamenta procedimentos gerais, prazos e as fases de implementação no âmbito do Poder Executivo Estadual à Lei Federal nº 13.709 de 14 de agosto de 2018 – LGPD.

4.0 APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os usuários, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada usuário de que os ambientes, sistemas, computadores, operações de tratamento de dados pessoais e redes da SICDHAS poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada usuário se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da DTI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

5.0 PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos usuários como resultado da sua atividade profissional pertence à SICDHAS.

Os equipamentos de informática e comunicação, além de sistemas e informações, são utilizados pelos usuários para a realização das suas atividades profissionais.

O uso de dados pessoais dos cidadãos pelos servidores públicos deve atender a finalidades específicas de execução de políticas públicas e atribuição legal da SICDHAS conforme Lei Complementar 15.680/2021 que dispõe sobre Estrutura Administrativa e Diretriz do Poder Executivo do Estado Rio Grande do Sul, respeitando os princípios de proteção de dados pessoais.

A SICDHAS, por meio da DTI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

6.0 REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os usuários da SICDHAS a fim de que a política seja cumprida dentro e fora da Instituição (situações de utilização de equipamentos móveis).

A PSI deverá ser revista e atualizada anualmente ou sempre que algum fato relevante ou evento motive sua revisão.

Todo incidente que possa afetar a segurança da informação deverá ser comunicado à DTI.

O plano de contingência e continuidade do serviço de TI será implantado e testado no mínimo anualmente, visando garantir a segurança da informação.

Conforme a necessidade poderão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas administrativos e financeiros desenvolvidos pela SICDHAS ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

A SICDHAS exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento do disposto nesta PSI acarretará violação às regras internas da Instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

7.0 DAS RESPONSABILIDADES ESPECÍFICAS

7.1 Dos Usuários em Geral

Será de inteira responsabilidade de cada usuário, todo prejuízo ou dano que vier a sofrer ou causar à SICDHAS e/ou a terceiros, em decorrência do não cumprimento às diretrizes e normas aqui referidas.

Deverão comunicar à Gestão e a DTI, por meio de chamado **CAU**, todo e qualquer incidente, evento ou fragilidade de processo que gere vazamento ou possibilidade de vazamento de dados pessoais do cidadão por qualquer meio.

7.2 Dos Usuários em Regime de Exceção (Temporários e visitantes)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no termo de aceite concedido pela SICDHAS.

A concessão poderá ser revogada a qualquer tempo se for verificada que a justificativa de motivo da atividade não mais compensa o risco relacionado ao regime de exceção ou se o usuário que o recebeu não estiver cumprindo as condições definidas no aceite.

Deverão comunicar à Gestão e a DTI, por meio de chamado, todo e qualquer incidente, evento ou fragilidade de processo que gere vazamento ou possibilidade de vazamento de dados pessoais do cidadão por qualquer meio.

7.3 Dos Gestores de Pessoas e/ou Processos

Deverão ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os usuários sob a sua gestão.

Compete aos gestores:

Atribuir aos usuários sob a sua gestão a responsabilidade pelo cumprimento da PSI da SICDHAS.

Solicitar por chamado (CAU), cadastrar ou descadastrar os operadores nos sistemas sob sua responsabilidade e comunicar o seu desligamento e/ou troca de lotação a Divisão de Pessoas da SICDHAS.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

Os dados de identificação de eventuais acessos de terceiros à rede da SICDHAS serão de responsabilidade do gestor do local onde estiver se dando o acesso ou do responsável pelo trabalho que necessitar deste tipo de acesso.

Manter uma lista atualizada compartilhada com a DTI de todos os processos e atividades que lidam com o tratamento de dados pessoais.

Deverão sempre que solicitados, para fins de atendimento à LGPD, nos casos de tratamento de dados pessoais do cidadão, fornecer informações detalhadas sobre as atividades realizadas com uso dos dados dos cidadãos.

Garantir que ao tratar dados pessoais, os processos e atividades utilizem somente as informações estritamente necessárias, e que os dados pessoais não necessários às atividades sejam eliminados.

Deverão comunicar à DTI, por meio de chamado (CAU), todo e qualquer incidente, evento ou fragilidade de processo que gere vazamento ou possibilidade de vazamento de dados pessoais do cidadão por qualquer meio.

7.4 Da Área de Tecnologia da Informação

Compete à Divisão de Informática:

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Gerenciar, junto à PROCERGS, segurança para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Administrar, proteger e testar as cópias de segurança dos programas e dados presentes na rede da SICDHAS.

Planejar, implantar, fornecer e monitorar as capacidades de armazenamento, processamento e comunicação.

Proteger continuamente todos os ativos de informação da Instituição contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da SICDHAS.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Disponibilizar meio para os departamentos, divisões e áreas da SICDHAS mapear atividades que tratem dados pessoais.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

Realizar auditorias internas e estabelecer estratégias de compliance e prevenção de riscos envolvendo dados pessoais

Garantir, da forma mais rápida possível, o bloqueio de acesso de usuários por motivo de desligamento, incidente, investigação vazamento de dados pessoais dos cidadãos ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da SICDHAS.

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Empreender medidas de resposta a incidentes, comunicados por chamado, com vazamento ou furto de dados pessoais.

Elaborar projeto para assegurar a manutenção de registros das operações de tratamento de dados pessoais na SICDHAS conforme LGPD.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação da SICDHAS.

Promover a conscientização dos usuários em relação à relevância da segurança da informação para as atividades da SICDHAS, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Para garantir as regras mencionadas nesta PSI a SICDHAS poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede - a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Realizar, a qualquer tempo, inspeção física nos equipamentos da rede;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

8.0 CORREIO ELETRÔNICO

O objetivo desta norma é informar aos usuários da SICDHAS quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

8.1 O uso do correio eletrônico da SICDHAS é para fins corporativos e relacionados às atividades do usuário dentro da Instituição.

8.2 É proibida ao usuário a utilização do correio eletrônico da SICDHAS para:

- a. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Instituição;
- b. Enviar mensagem por correio eletrônico pelo endereço de sua lotação ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- c. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a SICDHAS ou suas unidades vulneráveis a ações cíveis ou criminais;
- d. Divulgar informações não autorizadas ou imagens, dados pessoais do cidadão, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- e. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- f. Produzir, transmitir ou divulgar mensagens que:
 - Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
 - Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
 - Vise obter acesso não autorizado a outro computador, servidor ou rede;
 - Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
 - Vise burlar qualquer sistema de segurança;
 - Vise vigiar secretamente ou assediar outro usuário;
 - Vise acessar informações que possam causar prejuízos a qualquer pessoa;
 - Tenha conteúdo impróprio, obsceno ou ilegal;



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, dentre outros;
- Possua conteúdo preconceituoso baseado em orientação sexual, raça, cor, credo, incapacidade física ou mental;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

9.0 INTERNET

As regras estabelecidas nesta PSI visam o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da Instituição com a internet ofereça um grande potencial de benefícios, ela abre possibilidades para riscos significativos para os ativos de informação.

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites e downloads e uploads de arquivos.

A PROCERGS fará a homologação dos navegadores para a utilização de sistemas/aplicativos utilizados pela SICDHAS autenticados ou não pelo SOEWEB, (COE, CFV, SEO, GPE, FPE, RHE, SGM, GSS, SEG DAS, CAU, dentre outros).

9.1 São procedimentos considerados proibidos na Rede Informatizada da SICDHAS:

- a. Utilizar mídias de armazenamento removíveis sem conhecimento da DTI
- b. Utilizar os recursos da SICDHAS para fazer o download/upload ou distribuição de software ou dados não legalizados;
- c. Colaboradores não podem efetuar upload (envio) de qualquer software licenciado à SICDHAS ou de dados de propriedade, sem a expressa autorização do responsável pelo software ou pelos dados;
- d. Divulgação de informações confidenciais da SICDHAS em grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida;
- e. Utilização de arquivos que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
- f. Acesso a domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
- g. Utilização de softwares de compartilhamento peer-to-peer (P2P), tais como Ares, Emule, Vuze, Utorrent e afins;
- h. Acessar, expor, armazenar, distribuir, editar, imprimir ou gravar materiais de cunho sexual por qualquer recurso
- i. Utilização de site que burlam o controle de acesso da internet, tais como Web Proxy, UltraSurf, etc.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

9.2 O acesso à Internet é dividido em 4 (quatro) grupos:

- Básico, Intermediário, Avançado e Irrestrito.

	Básico	Intermediário	Avançado	Irrestrito
Bancos				
Governo				
Universidades/Cursos	B			
Comunicação Instantânea	B	B		
Streaming	B	B	B	
Redes Sociais	B	B	B	
Jogos Online	B	B	B	

B = Bloqueado

O uso da internet será monitorado pela DTI, mediante ferramentas específicas.

10.0 IDENTIFICAÇÃO

10.1 A presente norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os usuários.

10.2 Os dispositivos de identificação e senhas protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SICDHAS e/ou terceiros.

10.3 Sendo a DRH (Divisão de Recursos Humanos da SICDHAS) responsável pelo ingresso dos servidores e estagiários, cabe a mesma solicitar a criação de login, email e SOE, informando o local de lotação do servidor ou estagiário, bem como, informar os desligamentos, para que a DTI providencie o bloqueio de acesso.

10.4 Nas situações de troca de lotação de colaboradores o DRH deverá comunicar a DTI, para que essa providencie as alterações necessárias nos sistemas informatizados.

10.5 É proibido o compartilhamento de login para quaisquer atividades.

10.6 É de responsabilidade de cada colaborador a utilização de sua própria senha, sendo ela pessoal e intransferível.

10.7 Os usuários podem alterar a própria senha, devendo fazê-lo caso orientados ou por suspeita que terceiros tenham obtido acesso indevido.

10.8 Caso o usuário suspeite que sua senha tenha sido obtida por terceiros indevidamente, o mesmo deve comunicar imediatamente sua Gestão e a DTI.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

10.9 Caso o usuário esqueça sua senha no login de rede, ele deverá requisitar formalmente a sua alteração à DTI.

10.10 Dos Colaboradores em Regime Temporário será concedido apenas acesso à rede e e-mail, pelo prazo de 30(trinta) dias, mediante solicitação do gestor da área. As utilizações dos sistemas da Secretaria serão liberadas após sua nomeação e criação de sua identificação organizacional. Caso seja necessário, o Gestor da área poderá prorrogar o prazo inicial.

10.11 A certificação digital é a forma de demonstrar e certificar a identidade do titular da assinatura digital, portanto é de responsabilidade exclusiva de cada usuário a sua utilização, devendo a DTI zelar por sua instalação periférica para sistemas homologados pela mesma.

11.0 COMPUTADORES E RECURSOS TECNOLÓGICOS

11.1 Os equipamentos disponíveis aos usuários são de propriedade da SICDHAS, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas chefias responsáveis.

11.2 É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação sem o conhecimento prévio e o acompanhamento de um técnico da DTI ou de quem está determinar.

11.3 Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida homologação da DTI e depois de sua disponibilização pelo fabricante ou fornecedor.

11.4 Os sistemas e computadores devem ter versões do software antivírus adotado pela SICDHAS instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a DTI mediante registro de chamado ou email.

11.5 A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte, somente poderá ser realizada com a devida identificação do solicitante e com a real necessidade do destinatário.

11.6 Arquivos pessoais e/ou não pertinentes às atividades da SICDHAS não deverão ser copiados/movidos para os drives de rede, pois sobrecarregarão o armazenamento nos servidores. Caso identificada a existência desses arquivos, os mesmos serão excluídos.

11.7 Documentos pertinentes e imprescindíveis para as atividades de cada usuário da SICDHAS deverão ser salvos nos seguintes locais:



GOVERNO DO ESTADO
RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

Unidade U: (<setor>)	Armazenar arquivos pertinentes as atividades do setor ao qual o colaborador está lotado. A responsabilidade dos documentos contidos na pasta é do setor, ficando para a DTI a responsabilidade de backup desta conforme item 13 deste documento.
Unidade P: <Público>	Área pública para compartilhamento de arquivos na Secretaria. A responsabilidade dos documentos contidos na pasta é do setor porém o acesso é de todas as áreas .

11.8 Arquivos gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

11.9 Os arquivos contidos nas pastas de escaneamento serão removidos da mesma toda sexta-feira, para fins de boa pratica de uso de armazenamento.

11.10 No uso dos computadores, equipamentos e recursos de informática, as seguintes regras devem ser atendidas:

- Os usuários devem informar à DTI qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio para qualquer tipo de reparo que não seja realizado por um técnico da DTI ou por terceiros devidamente contratados para o serviço.
- É expressamente proibido o consumo de alimentos e bebidas próximo aos equipamentos.
- Qualquer servidor deverá bloquear os terminais de computador quando não estiver próximo do mesmo. O mesmo deve ser feito caso perceba a ausência de outro usuário.

11.9 É proibido o uso de computadores e recursos tecnológicos da SICDHAS nas situações a seguir:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

- qualquer método ilícito ou não autorizado.
- f. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
 - g. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
 - h. Utilizar software sem as devidas licenças do fabricante ou detentor dos direitos (comumente chamado *de pirata*).
 - i. Transferir dados pessoais dos cidadãos à entidades privadas em situações não previstas na LGPD.
 - j. Tratar dados pessoais dos cidadãos para atividades que não estejam dentro das atribuições legais da SICDHAS.

12.0 DISPOSITIVOS MÓVEIS E ARMAZENAMENTO EM NUVEM

Para fins desta PSI, entende-se por "dispositivo móvel" qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da Instituição ou de terceiros, desde que aprovado e permitido pela DTI, como: notebooks, smartphones, tablets etc.

Para fins desta PSI, entende-se por "armazenamento em nuvem" qualquer tecnologia que permita armazenar e tratar dados na internet através de um servidor online, fora da rede local.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e armazenamento em nuvem e deverá ser aplicada a todos os usuários que utilizem tais equipamentos e recursos.

121 O usuário assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SICDHAS, mesmo depois de terminado o vínculo mantido com a Instituição.

12.2 A SICDHAS reserva-se o direito de inspecionar os equipamentos de sua propriedade a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

12.3 O suporte técnico dos dispositivos móveis de propriedade da SICDHAS e aos seus usuários deverá seguir o mesmo fluxo de suporte adotado pela Instituição para os demais equipamentos da rede.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

12.4 Todo usuário deverá utilizar senhas de bloqueio automático para seu dispositivo móvel e se responsabilizar pela segurança dos dados armazenados em nuvem.

12.5 Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da DTI e sem a condução, auxílio ou presença de um de seus técnicos.

12.6 O usuário deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da DTI.

12.7 A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela Instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

12.8 É permitido o uso de rede banda larga de locais conhecidos pelo usuário, como sua casa, hotéis e fornecedores.

12.9 O usuário deverá estar ciente de que o uso indevido do dispositivo móvel e armazenamento em nuvem caracterizarão a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à SICDHAS e/ou a terceiros.

12.10 O usuário é responsável por todos os acessórios que acompanham ou fazem parte dos dispositivos móveis, devendo mantê-los sempre junto aos mesmos.

12.11 Recomenda-se fortemente que materiais e documentos que contenham dados pessoais do cidadão não sejam armazenados e transportados em dispositivos móveis. A perda, extravio ou roubo de dispositivos com este tipo de informação deve ser informada, por chamado, imediatamente a DTI.

12.12 É proibido que arquivos e documentos que contenham dados pessoais do cidadão e trabalhos com informações sensíveis e sigilosas da SICDHAS sejam tratados em nuvem sem o consentimento e aviso através de chamado do Gestor da área, da DTI e da alta administração da SICDHAS. A invasão ou perda por qualquer motivo da conta pessoal que contenha estes tipos de dados em nuvem deverá ser informada imediatamente ao Gestor e, mediante chamado, a DTI.

12.13 A DTI não é responsável pela manutenção, configuração ou qualquer outra ação de contas pessoais de serviços em nuvem utilizados pelos usuários.

12.14 Dispositivos móveis pessoais não são de responsabilidade da DTI.

13.0 BACKUP

As rotinas de backup dos dados da SICDHAS são de responsabilidade da PROCERGS, através de contrato de prestação de serviços.



GOVERNO DO ESTADO RIO GRANDE DO SUL

SECRETARIA DA IGUALDADE
CIDADANIA, DIREITOS HUMANOS E
ASSISTÊNCIA SOCIAL

São executadas as rotinas diárias, semanais e mensais dos tipos diferencial e full.

As solicitações de restauração de arquivos devem conter: Nome do arquivo, pasta de armazenamento e a provável data de exclusão.

As operações de restauração de arquivos serão efetuadas num prazo de 48 horas, após a solicitação via chamado, podendo ser informado pela DTI a ampliação do prazo.

Arquivos que permaneçam menos de 24h no servidor não serão possíveis de restauração.

Não existe garantia de restauração de arquivos removidos a mais de 30 dias.

Também é possível que o usuário reverta para uma versão anterior de um arquivo específico ou um grupo de arquivos em uma pasta, através do recurso "Versão Anterior". Essa ferramenta tem uma temporalidade diferente e menor, e depende que o arquivo ou o grupo de arquivos, seja alterado no intervalo de tempo.

Somente serão passíveis de restauração os arquivos pertinentes ao serviço e que estejam salvos na unidade de rede "S".

14.0 DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura organizacional interna da SICDHAS. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela Instituição.

Política de Segurança de TI DOE 11-01-2022 - Matéria 664612

[Documento na Integra](#)