SECRETARIA DO
DESENVOLVIMENTO
ECONOMICO, CIÊNCIA
E TÉCNOLOGIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DEFINIÇÕES

Ativos: qualquer coisa que tenha valor para a organização. Exemplo: pessoas, processos, tecnologias e ambientes.

Autenticação: é o processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou que fazem parte de uma transação eletrônica.

Auditoria: é o processo de coleta de evidências de uso dos recursos, para identificar as partes envolvidas em um processo de acesso ou troca de informações.

Autorização: é o processo de concessão de permissão para acesso às informações, ativos, funcionalidades das aplicações, após a correta identificação e autenticação dos usuários ou dispositivos.

Autenticidade: é a garantia de que as partes envolvidas (usuários, dispositivos, informações), identificadas em um processo de comunicação como remetentes ou autores, sejam exatamente quem dizem ser.

Confidencialidade: o acesso e uso da informação devem ser limitados apenas às pessoas a quem são destinados.

Conformidade: é o processo de garantia de cumprimento de obrigações contratuais com investidores, empregados, credores e entre outros, com os aspectos legais e regulatórios relacionados à administração da companhia.

Criticidade: refere-se à gravidade ao impacto ao negócio, causado pela ausência de um ativo, interrupção de um serviço ou acesso não autorizado a informações.

Disponibilidade: toda informação criada ou adquirida por um indivíduo ou instituição deve ser sempre disponível no momento em que necessite.

Dispositivos Móveis: todo e qualquer dispositivo computacional portátil capaz de processar e armazenar informações.

Irretratabilidade: também conhecida como não repúdio, é a característica de informações que possuem a identificação de seu emissor, que o autentica como o autor de informações por ele enviadas e recebidas.

Incidente de segurança da informação: qualquer acontecimento adverso, confirmado ou sob suspeita, que impacte na segurança da informação dos ativos da organização.

Integridade: a informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la de alterações indevidas por pessoas não autorizadas.

Risco: efeito da incerteza nos objetivos.

Severidade: é a gravidade do dano que determinado ativo pode sofrer devido à exploração de uma vulnerabilidade.

Vulnerabilidades: são fragilidades presentes ou associadas a ativos que manipulam ou processam informações que, ao serem exploradas por uma ameaça, permitem a ocorrência de um incidente de segurança.

INTRODUÇÃO

A Tecnologia da Informação e Comunicação (TIC) modificou a forma como as organizações armazenam seus arquivos, entregam seus serviços e tratam de sua propriedade intelectual. As organizações tornaram-se dependentes de TIC em seus processos e a informação passou a ser regrada pelo seu próprio ciclo de vida.

Neste contexto, a Segurança da Informação é a área do conhecimento que se dedica ao estudo da proteção de ativos contra: acessos não autorizados, alterações indevidas e sua indisponibilidade. Além destes, existem outros aspectos importantes como: a autenticação, a conformidade, a autorização, a autenticidade, a severidade, a relevância do ativo, a relevância do processo de negócio, a criticidade e a irretratabilidade.

A segurança da informação é um processo, não se trata de um produto ou uma tecnologia, ela utiliza-se da implantação de controles adequados, que podem ser políticas, procedimentos, ferramentas de software e processos, que definem regras para o ciclo de vida da informação.

A Política de Segurança da Informação deverá ser seguida por todos os funcionários, diretoria, membros dos conselhos, estagiários, prestadores de serviço, fornecedores e clientes.

Este documento está sob a orientação das boas práticas das normas da "família" ISO 27000.

1. OBJETIVO

Os objetivos desta Política de Segurança da Informação da SDECT são:

- **1.1.** Estabelecer diretrizes que sejam adequados às necessidades de proteção legal da secretaria e do indivíduo para utilização de recursos de TIC (tais como estações de trabalho, internet, rede de dados, telecomunicações e correio eletrônico institucional), pelos seus servidores.
- **1.2.** Definir os papéis e responsabilidades dos responsáveis pela Segurança da Informação;
- **1.3.** Definir os papéis e responsabilidades dos servidores na segurança da informação;
- **1.4.** Possibilitar a criação de controles que contribuam para minimizar os riscos associados aos ativos de informação;
- **1.5.** Fomentar a criação de iniciativas relativas à Segurança da Informação.

Também é papel desta política informar a toda organização que poderão ser monitorados e gravados e utilizados para fins de auditoria todos os acessos aos sistemas, redes de dados, ambientes de trabalho e recursos computacionais da secretaria, conforme previsto na legislação brasileira.

2. PRINCÍPIOS

São princípios da Política de Segurança da Informação da SDECT:

- **2.1** Todos os públicos submetidos a esta política são responsáveis pela segurança da informação da SDECT, principalmente das informações que estão sob sua responsabilidade.
- **2.2** Os recursos computacionais da SDECT devem ser utilizados de maneira responsável e consciente para seu uso laboral.
- **2.3** Toda informação produzida ou recebida pela secretaria, em função da atividade desenvolvida pelos seus servidores, pertence à SDECT e por consequência, ao Governo do Estado do Rio Grande do Sul.
- **2.4** Todo o acesso a redes e sistemas utilizados na SDECT deverá ser feito por meio de login de acesso, pessoal e intransferível.

2.5 A SDECT pode utilizar ferramentas e tecnologias para controlar e monitorar o conteúdo e o acesso a quaisquer sistemas, informações e ambientes operacionais providos pela PROCERGS.

3 PAPÉIS E RESPONSABILIDADES

Definem-se como papéis e responsabilidades:

3.1 DIRETORIA ADMINISTRATIVA

3.1.1 Garantir que a segurança da informação seja tratada adequadamente por toda a organização, conforme esta Política.

3.1.2 Alocar recursos para financiar controles de segurança.

3.1.3 Assessorar a Divisão de TI na implementação das ações de segurança da informação.

3.1.4 Investigar os autores de eventuais transgressões as diretrizes da Política de Segurança da Informação.

3.1.5 Apoiar e avaliar a adequação de controles de segurança da informação para novos sistemas, processos ou serviços.

3.1.6 Acompanhar e tomar medidas necessárias para resolver incidentes de segurança da informação.

3.1.7 Agir nas não conformidades encontradas envolvendo as áreas quanto à Política de Segurança da Informação.

3.2 SERVIDORES, ESTAGIÁRIOS E TERCEIRIZADOS.

3.2.1 Manter-se atualizado em relação a esta Política de Segurança da Informação e às normas e instruções de serviços da Secretaria.

3.2.2 Responsabilizar-se por todo prejuízo ou dano que causar à SDECT devido à não obediência às diretrizes estabelecidas nesta Política de Segurança da Informação, bem como às demais normas, instruções de serviço e procedimentos estabelecidos pela Secretaria.

3.2.3 Fazer cumprir, quando chefia, a Política de Segurança da Informação, bem como acompanhar as suas atualizações.

3.3 ÁREA DE TECNOLOGIA DA INFORMAÇÃO

3.3.1 Configurar os recursos computacionais concedidos aos usuários, os de uso corporativo de forma segura, ou seja, com todos os controles necessários para cumprir as diretrizes estabelecidas nesta Política e no restante da documentação normativa da Secretaria.

3.3.2 Gerar e manter trilhas de auditorias com nível de detalhe suficiente para rastrear possíveis falhas e fraudes nos recursos computacionais.

3.3.3 Aplicar controles de segurança da informação nos ativos e informar chefias e aos donos dos ativos sobre os eventuais riscos residuais

3.3.4 Promover segurança para acesso aos sistemas, fazendo a guarda de todos os registros que permitam a rastreabilidade para fins de investigação ou auditoria.

3.3.5 Apresentar e apoiar iniciativas que visem a segurança dos ativos de informação da SDECT.

3.3.6 Investigar os autores de eventuais transgressões as diretrizes da Política de Segurança da Informação.

3.3.7 Apoiar e avaliar a adequação de controles de segurança da informação para novos sistemas, processos ou serviços.

3.3.8 Acompanhar e tomar medidas necessárias para resolver incidentes de segurança da informação.

3.3.9 Agir nas não conformidades encontradas envolvendo as áreas quanto à Política de Segurança da Informação.

3.3.10 Revisar periodicamente e propor alterações na Política de Segurança da Informação e nos demais documentos normativos da SDECT.

4 DIRETRIZES

As diretrizes contidas nesta Política de Segurança da Informação foram consideradas pensando nos riscos que a SDECT está submetida e que ainda não possuem controles descritos.

A partir das diretrizes criadas nesta política, deverão ser criadas novas normativas que estabeleçam adequadamente os melhores controles para os ativos e processos.

4.1 CLASSIFICAÇÃO DA INFORMAÇÃO

OBJETIVO

Estabelecer as diretrizes para a classificação, rotulação e tratamento das informações de acordo com sua sensibilidade e criticidade para a SDECT, visando o estabelecimento de níveis adequados de proteção.

NECESSIDADE DE ACESSO

Os Servidores da SDECT, seus estagiários e terceirizados, devem possuir somente acesso às informações que sejam necessárias ao desenvolvimento de suas atividades de trabalho e demais responsabilidades associadas.

DIRETRIZES

4.1.1 No processo de classificação da informação deve ser considerado o valor da informação, os requisitos legais, a sensibilidade, a criticidade, a vida útil, a necessidade de compartilhamento e restrição, a análise de riscos e os impactos para o estado.

4.1.2 O processo de classificação de uma determinada informação deve contemplar uma análise crítica periódica a intervalos regulares, para verificar se o nível de classificação e proteção está adequado.

NÍVEIS DE CLASSIFICAÇÃO

Níveis de Classificação	Características básicas
Pública	Informações que podem ou devem ser divulgadas publicamente.
Uso Interno	Informações internas que podem ou devem ser divulgadas a todos os servidores, desde que comprometidos com a confidencialidade das informações.
Restrita	Informações restritas que devem ser divulgadas a determinados grupos, áreas ou cargos.
Confidencial	Informações que requerem um tratamento especial e cuja divulgação não autorizada ou acessos indevidos pode gerar prejuízos financeiros, legais, normativos, ou na reputação de um ativo.

4.2 MESA LIMPA E TELA LIMPA

OBJETIVO

Reduzir o risco de perda, dano ou acesso não autorizado a informações, durante o horário de trabalho ou fora dele, de dados disponíveis em mídias, papéis ou outras formas de armazenamento, que possam estar sobre mesas, impressoras e outros locais.

DIRETRIZES

4.2.1 Informações internas, restritas e confidenciais sob a guarda dos Servidores, Estagiários e Terceirizados, devem ser armazenadas nos servidores de arquivo e sistemas oficiais da secretaria ou em gaveteiro com chave.

4.2.2 Documentos que contenham informação de uso interno, restritos ou confidenciais devem ser removidos da impressora imediatamente.

4.3 USO DA INTERNET

OBJETIVO

O acesso à Internet é fornecido, prioritariamente, para o desempenho das atividades profissionais. Para evitar abusos, esta diretriz estabelece os parâmetros aceitáveis para uso deste recurso.

Conforme estabelece a legislação brasileira, ficam cientes todas as partes que o acesso à Internet provido pela PROCERGS e monitorado pela DTI. Desta forma, poderão ser bloqueados os acessos a domínios que comprometam a segurança dos ativos da secretaria e/ou não digam respeito às atividades laborais realizadas na SDECT.

DIRETRIZES

É PERMITIDO NO USO DA INTERNET:

4.3.1 O uso da Internet pelos Servidores, Estagiários e Terceirizados é permitido, desde que seu uso seja aderente aos objetivos e atividades fins e das atividades de responsabilidade do colaborador.

4.3.2 O uso das redes sociais, segundo as regras definidas pelo Grupo de Tecnologia da Informação e Comunicação (TIC) da SDECT.

É VEDADO NO USO DA INTERNET:

4.3.3 O acesso, cópia, armazenamento e distribuição de conteúdo impróprio relativo à pornografia, racismo, xenofobia, violência, homofobia, incitação ao ódio, invasão de computadores, jogos de azar ou qualquer conteúdo que seja vedado pela legislação brasileira.

4.3.4 O download, o armazenamento, a cópia, o uso, a exibição e a transmissão de arquivos protegido por direito autoral, tais como: filmes, músicas, livros, entre outros conteúdos deste tipo, sem autorização do detentor de tais direitos.

4.3.5 A obtenção, o armazenamento e a distribuição de conteúdo ilegal, tais como senhas de terceiros, números de cartões de créditos de terceiros, entre outros.

4.3.6 O acesso, divulgação, armazenamento e distribuição de conteúdo sobre jogos de azar, correntes e pirâmides, investimentos em bolsa de valores e moedas eletrônicas.

4.3.7 A utilização da Internet para fazer difamação, injúria, calúnia ou ameaças.

4.3.8 Compartilhar informações confidenciais com outras pessoas.

4.4 USO DO CORREIO ELETRÔNICO

OBJETIVO

Estabelecer diretrizes para a utilização do correio eletrônico, que cumpre um papel importante nas comunicações e serviços prestados pelo Estado.

DIRETRIZES

4.4.1 O e-mail corporativo é o serviço de correio eletrônico disponibilizado pela Governo do Estado do Rio Grande do Sul (Via PROCERGS) ao seu quadro funcional, com a finalidade única e exclusiva de manter contato entre os órgãos que constituem o governo, além de empresas, instituições de ensino, órgãos federais, fornecedores e demais remetentes que digam respeito às atividades laborais realizadas na SDECT.

4.4.2 A SDECT presume que toda informação recebida, criada, armazenada e transmitida através do correio eletrônico corporativo não é de caráter pessoal.

4.4.3 É vedado o uso do correio eletrônico corporativo para fins particulares, tais como: cadastro em redes sociais, sites comerciais, sites de relacionamento, cadastro para receber milhagens, dentre outros usos particulares.

4.4.4 É proibido o envio e recebimento de mensagens de conteúdo impróprio relativo a pornografia, racismo, xenofobia, violência, homofobia, incitação ao ódio, invasão de computadores, propagando político-partidária, jogos de azar, correntes e pirâmides, investimentos em bolsa de valores e moedas eletrônicas, através da estrutura de correio eletrônico da PROCERGS. Normas específicas de uso do Correio Eletrônico encontram-se na Política de Uso do Expresso.

4.5 USO DE DISPOSITIVOS MÓVEIS

OBJETIVO

Gerenciar os riscos decorrentes do uso de dispositivos móveis para assegurar que as informações do negócio não sejam comprometidas.

DIRETRIZES

4.5.1 Servidores e gestores devem assinar um termo que estabeleça suas responsabilidades quanto à proteção do equipamento, atualização do software e confidencialidade das informações.

4.5.2 Não é permitido trabalhar com dispositivos móveis particulares (smartphones, notebooks ou qualquer dispositivo que armazene e processe informações). Qualquer dispositivo particular deverá permanecer com a sua configuração de uso pessoal, sem ingressar no domino da secretaria ou acessar os dados em rede.

4.5.3 Dispositivos móveis particulares (smartphones, notebooks ou qualquer dispositivo que armazene e processe informações) são de responsabilidade do servidor, a Divisão de TI não está compelida a prestar qualquer tipo de suporte, manutenção ou consultoria aos servidores e seus dispositivos para finalidade particular.

4.6 GESTÃO DOS ATIVOS

OBJETIVO
Identificar os ativos da SDECT, definindo responsáveis e as responsabilidades pela proteção dos ativos.

DIRETRIZES

4.6.1 Servidores, Estagiários e Terceirizados da SDECT devem desenvolver suas atividades laborais somente com ativos da própria secretaria.

4.6.2 Cada ativo deve possuir um responsável, que deve classificá-lo levando em consideração critérios como: a criticidade, valor financeiro, entre outros.

4.6.3 A área de patrimônio deve garantir que o ativo seja: corretamente inventariado, assegure a correta classificação e proteção, assegure o correto tratamento quando o ativo for excluído ou destruído.

4.6.4 Servidores e partes terceiras que fazem uso ou têm acesso aos ativos de informação da SDECT, devem ser responsáveis pelo uso de qualquer recurso de processamento da informação que utilizem.

4.6.5 Todos os Gestores, Servidores, Estagiários e Terceirizados, devem devolver todos os ativos sob guarda da SDECT que estejam em sua posse, após o encerramento de suas atividades ou do contrato.

4.7 CONTROLE DE ACESSO, USO DE SOFTWARE E SEGURANÇA DOS DADOS

OBJETIVO
Limitar o acesso à informação e aos recursos de processamento, transmissão e armazenamento da informação, estabelecer controle na instalação de software nos recursos computacionais e proteger a secretaria contra a perda de dados.

DIRETRIZES

4.7.1 Deve ser mantida uma norma de controle de acesso, baseada nos requisitos de segurança da informação que determine as regras apropriadas do controle de acesso, direitos de acesso e restrições para usuários acessarem ativos.

4.7.2 Os aspectos principais que orientam o controle de acesso são:

- NECESSIDADE DE CONHECER: será concedida permissão de acesso apenas à informação necessária para desempenhar as tarefas de trabalho;
- NECESSIDADE DE USO: será concedido permissão somente aos ativos de processamento, transmissão e armazenamento de informação necessários para o desempenho das tarefas de trabalho;
- TEMPORALIDADE: as permissões deverão ser concedidas por tempo determinado, quando necessárias da execução de atividades específicas;

4.7.3 A norma de controle de acesso deve estabelecer os seguintes requisitos básicos:

- Requisitos para a autorização formal de pedidos de acesso;
- Um procedimento para a remoção de direitos de acesso;
- Estabelecer regras bem definidas para o acesso privilegiado.

4.7.4 No acesso às redes e aos serviços de rede devem ser observados:

- O estabelecimento de procedimentos para a autorização de acesso a redes e serviços de redes;
- Uma descrição dos meios para acessar as redes e serviços de rede, por exemplo: VPN, redes sem fio, etc.
- Monitoramento do uso dos serviços de rede.
- Os servidores devem possuir privilégio mínimo (preferencialmente nenhum) para a instalação de softwares. Toda necessidade de

instalações em recursos computacionais deve ser encaminhada através de requisição de serviço para a Divisão de TI (DTI).

- A Divisão de TI pode estabelecer uma lista de softwares que podem ser instalados pelos colaboradores, tais como: instalação de patches nos softwares existentes e programas para uso pessoal (desde que homologado pela área responsável).
- Os servidores não podem instalar softwares não autorizados pela DTI.
- Os servidores não podem armazenar ou compartilhar dados corporativos em aplicativos que armazenam dados em nuvens.
- O uso dos sistemas de proteção, como antivírus e sistema de detecção de intrusão, nos recursos computacionais da SDECT, quando disponíveis, é obrigatório. Não sendo admitido, sob nenhuma circunstância, a remoção destas sem a autorização da DTI.
- Não é permitido ao servidor a troca do sistema operacional instalado nos recursos computacionais que faz uso na SDECT. Toda e qualquer necessidade de manutenção deve ser encaminhada a DTI.
- A DTI será responsável em fornecer através da PROCERGS as cópias de segurança das informações salvas em rede, dos seus sistemas e serviços.
- Não será realizado salvamento de dados (BACKUP) e documentos das estações de trabalho. Qualquer dado que o servidor deseja preservar, deverá ser salvo em rede.
- Os servidores têm a responsabilidade de notificar qualquer incidente de segurança da informação. Também possuem a responsabilidade de estarem cientes sobre os procedimentos para notificar incidentes de segurança da informação.

4.8 POLÍTICA DE SENHAS E ACESSOS

OBJETIVO

Definir a forma de utilização e armazenamento das senhas.

DIRETRIZES

4.8.1 É vedada a utilização de credenciais de outro servidor, estagiário ou terceirizado.

4.8.2 Todos os recursos computacionais adquiridos pela SDECT devem ter suas senhas padrões alteradas.

4.8.3 As senhas não devem ser anotadas em papel ou armazenadas nas estações de trabalho em arquivos eletrônicos sem criptografia.

4.8.4 Todas as senhas de administração devem ser armazenadas num ambiente seguro.

4.8.5 As senhas devem ter validade temporária.

4.9 DATA CENTER (PASTA DADOS)

OBJETIVO

Garantir os procedimentos para acesso ao Data Center.

DIRETRIZES

4.9.1 O acesso às dependências da Pasta Dados é restrito para a execução das atividades de cada Departamento/Divisão.

4.9.2 Seu uso para armazenamento de qualquer material ou trabalho referente as atividades de cada Departamento/Divisão é obrigatório. Deste modo, a Divisão de TI fica desobriga a garantir a integridade dos dados em casos

críticos ou de manutenção do equipamento utilizado pelo servidor caso os esses tenham sido armazenados fora da rede (Disco c:).

4.9.3 O acesso de pessoas que não fazem parte do quadro funcional da secretaria para utilização da Pasta Dados, deve ser previamente autorizado pela Diretoria ou responsável do setor.

5 REFERÊNCIAS LEGAIS E NORMATIVAS

CLASSIFICAÇÃO	DENOMINAÇÃO	PUBLICAÇÃO	ASSUNTO
Decreto Estadual	52.616	19/10/2015	Política de Tecnologia da Informação e Comunicação.
Decreto Estadual	53.927	21/02/2018	Compartilhamento de Dados na Administração Pública Estadual.
Decreto Estadual	53.164	10/08/2016	Procedimentos para a classificação de informações.
Lei Federal	2.848	07/12/1940	Código Penal
Lei Federal	9.610	19/02/1998	Dispõe sobre o Direito Autoral.
Lei Federal	12.965	23/04/2014	Marco Civil da Internet no Brasil.
Lei Federal	12.527	18/11/2011	Regula o acesso a informações.
Lei Federal	12.737	30/11/2012	Tipificação criminal dos delitos cibernéticos.
Lei Federal	13.303	30/06/20116	Dispõe sobre o estatuto jurídico da companhia pública, da sociedade de economia mista e de suas subsidiárias.
Norma Estadual	PGOV 03/2016	28/11/2016	Padrão de Governança em Segurança da Informação.
Resolução PROCERGS	Reestruturação Organizacional	05/04/2013	Resolução da Diretoria da PROCERGS que cria a Coordenação de Segurança (CSEG).