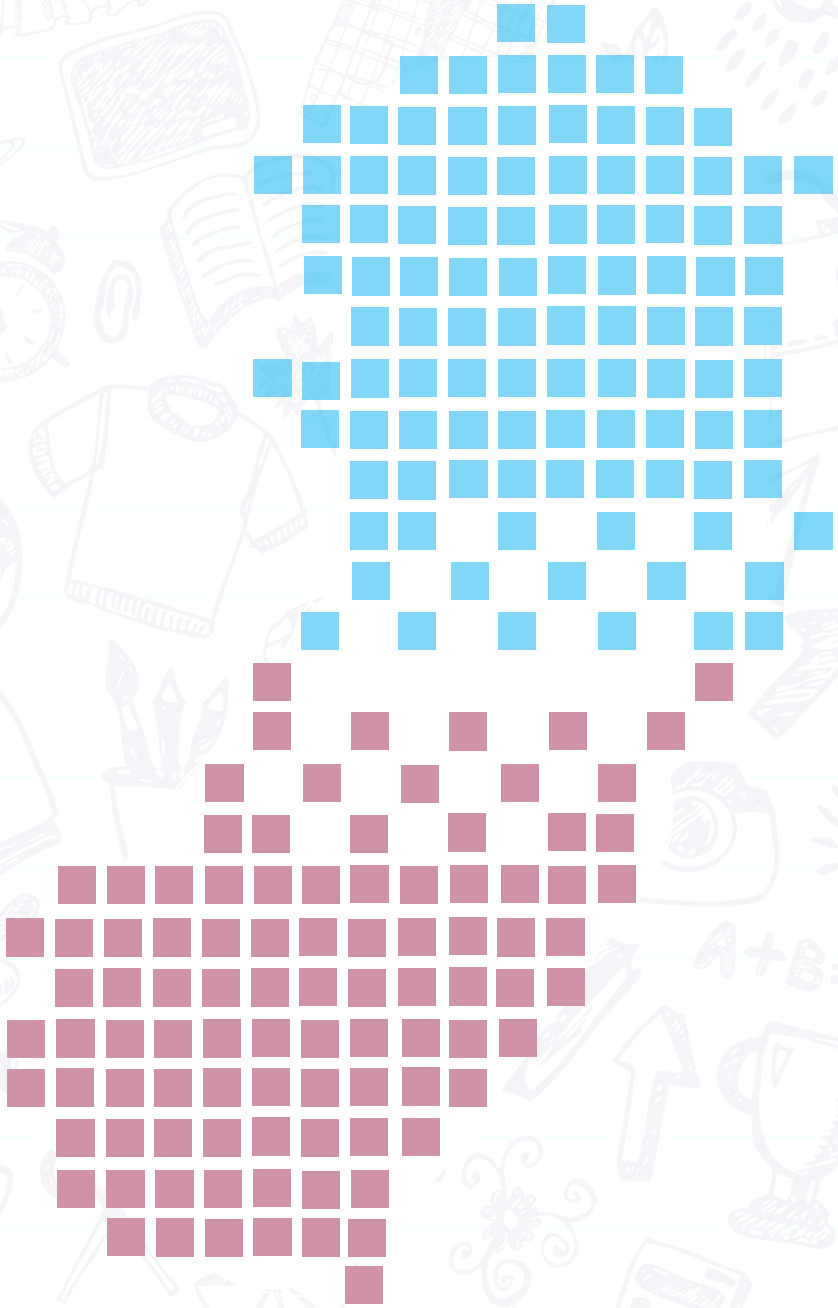


GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria da Educação

Boas Práticas de Segurança da Informação e Proteção dos Dados Pessoais na Educação

Vitória
2024

Expediente

Governador
Renato Casagrande

Vice-Governador
Ricardo de Rezende Ferraço

Secretário de Estado da Educação
Vitor Amorim de Angelo

Subsecretário de Estado de Administração e Finanças
Josivaldo Barreto de Andrade

Subsecretária de Estado de Articulação Educacional
Darcila Aparecida da Silva Castro

Subsecretária de Estado da Educação Básica e Profissional
Andréa Guzzo Pereira

Subsecretário de Estado de Planejamento e Avaliação
Marcelo Lema Del Rio Martins

Subsecretário de Estado de Suporte à Educação
André Melotti Rocha

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria da Educação

Versionamento

Data	Versão	Descrição	Responsável
15/03/2024	1.0	Elaboração a partir dos temas mais questionados pelas equipes SEDU.	Farley Correia Sardinha (EITDP/SEDU)
24/04/2024	1.1	Efetuadas alterações para melhoria de imagens, atualização de links corrompidos e a inclusão de link para o Alerta 7/2024 do CTIR Gov.	Farley Correia Sardinha (EITDP/SEDU)

Apresentação

Prezadas(os) servidoras(es),

É com grande satisfação que a **Secretaria de Estado da Educação - SEDU** lhes disponibiliza este guia contendo algumas informações e orientações importantes sobre as temáticas de **Segurança da Informação** e de **Proteção dos Dados Pessoais e da Privacidade**.

Em atendimento à **Política Estadual de Proteção dos Dados Pessoais e da Privacidade - PEPDP**, em consonância com a **Lei Geral de Proteção de Dados Pessoais – LGPD**, a SEDU, por meio de seu **Encarregado Interno pelo Tratamento de Dados Pessoais - EITDP**, tem a responsabilidade de lhes auxiliar na adequação de suas atividades à legislação vigente.

Assim, o objetivo deste material não é esgotar todas as medidas de boas práticas de segurança da informação e de proteção dos dados pessoais e da privacidade, mas dar algumas sugestões que promovam medidas individuais e coletivas para a segurança da informação e a proteção dos dados pessoais e da privacidade em cada unidade administrativa da SEDU.

O que você encontrará aqui?

❖ **Boas práticas para se adequar à LGPD:**

- ✓ Controle de acesso físico para setores que tratam informações sigilosas;
- ✓ Política de mesa limpa e tela limpa;
- ✓ Controle de acesso lógico, com a proteção de credenciais de acesso a sistemas;
- ✓ Práticas seguras para e-mail e apps de mensagens;
- ✓ Práticas seguras para E-Docs;
- ✓ Práticas seguras para formulários de inscrição/pesquisa;
- ✓ Práticas seguras para uso de foto e vídeo.

❖ **Obrigações a cumprir:**

- ✓ Registro das Atividades de Tratamento de Dados;
- ✓ Mapeamento de Riscos e Relatório de Impacto ao Tratamento de Dados Pessoais;
- ✓ Comunicação de incidentes de segurança ao Encarregado Interno da SEDU.

Pra começo de conversa ...

Se você ainda não conhece os principais termos da LGPD, agora **a ANPD lançou um Glossário**, que está disponível em seu site institucional.

Conheça as publicações da ANPD

Boas práticas para adequação à LGPD

O que podemos fazer para estar de acordo com a Lei Geral de Proteção de Dados Pessoais

Controle de acesso físico em locais que tratam dados pessoais

Todo setor que trata informações sigilosas, em especial os dados pessoais, deve realizar um controle efetivo de quem tem acesso ao ambiente de trabalho.

A **Lei Federal Nº 13.709/2018** (**Lei Geral de Proteção de Dados Pessoais - LGPD**) tem entre seus princípios:

Princípio da Segurança

Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

(Inciso VII do Artigo 6º da LGPD)

Princípio da Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

(Inciso VIII do Artigo 6º da LGPD)

Ou seja, se é possível prevenir danos e garantir a segurança dos dados com o simples controle de quem pode ou não entrar em uma sala, é nossa obrigação fazer!

Algumas dicas úteis para o controle de acesso físico

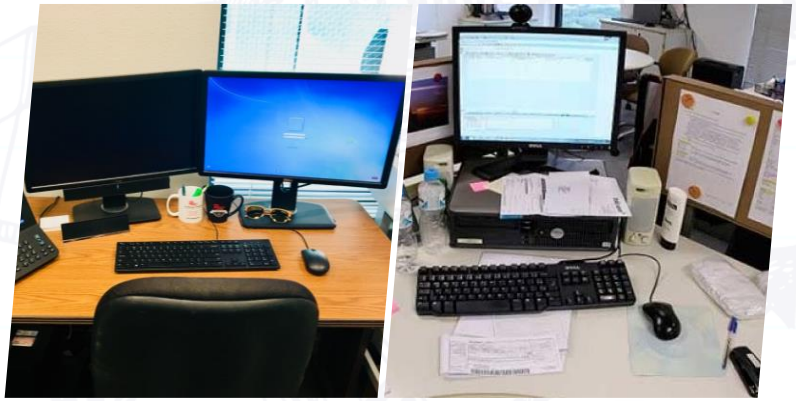
- **Trabalho a portas fechadas –** lembre-se que nessa "Era dos Dados", **os dados pessoais que o seu setor trata são de alto valor**! Assim, sempre que possível, mantenha a(s) porta(s) de seus setor fechadas, permitindo a entrada somente de pessoas autorizadas.
- **Não banalize as autorizações de acesso –** outro importante princípio da LGPD é o **Princípio da Necessidade**, o qual podemos estender para a importância de se permitir o acesso somente a quem tem real necessidade de estar nas dependências de seu setor, que trata dados pessoais.
- **Acesso de equipes terceirizadas –** é comum em nossa rotina a necessidade de acesso de equipes terceirizadas que prestam serviços em nossa unidade administrativa (limpeza, manutenção, desinsetização, etc.). Mesmo que o contrato desses serviços tenham regras claras para a atuação das equipes contratadas, é importante cada setor cuidar para que as informações sigilosas sejam protegidas de incidentes de segurança acidentais ou intencionais.

Saiba mais sobre a Era dos Dados

- **Supervisionar os acessos não é um excesso –** é importante que a chefia imediata de cada setor supervisione tanto as permissões de acesso concedidas, quanto as pessoas que realmente acessam seu setor de trabalho, que trata dados pessoais e outras informações sigilosas.
- **A Secretaria Escolar é o cofre dos dados pessoais tratados pela escola –** é na Secretaria Escolar que se encontram os dados de crianças e adolescentes, não só aqueles do sistema de gestão, mas também aqueles registrados no prontuário do estudante, em livros de ocorrência, etc. São dados pessoais e dados pessoais sensíveis de um público considerado prioritário para a LGPD. Por isso, o controle do acesso físico à Secretaria Escolar deve ser rigorosamente monitorado pela equipe gestora da escola.
- **Esteja preparado para as emergências –** a depender de cada setor, é preciso estabelecer procedimentos claros para situações de emergência (enchentes, incêndios, etc.), visando garantir que documentos sigilosos sejam protegidos durante esses incidentes.

Política de mesa limpa e tela limpa

Qual das fotos abaixo mais se parece com sua mesa de trabalho?



O título desta seção pode até nos induzir a pensar que basta deixar tudo como está na primeira foto. Mas, lembre-se que **informação é tudo aquilo que pode ser lido, compreendido e utilizado**.

Assim, no contexto da Segurança da Informação, para garantir que as informações tratadas pelas unidades administrativas da SEDU cumpram sua finalidade, devemos evitar que sejam acessíveis a pessoas não autorizadas.

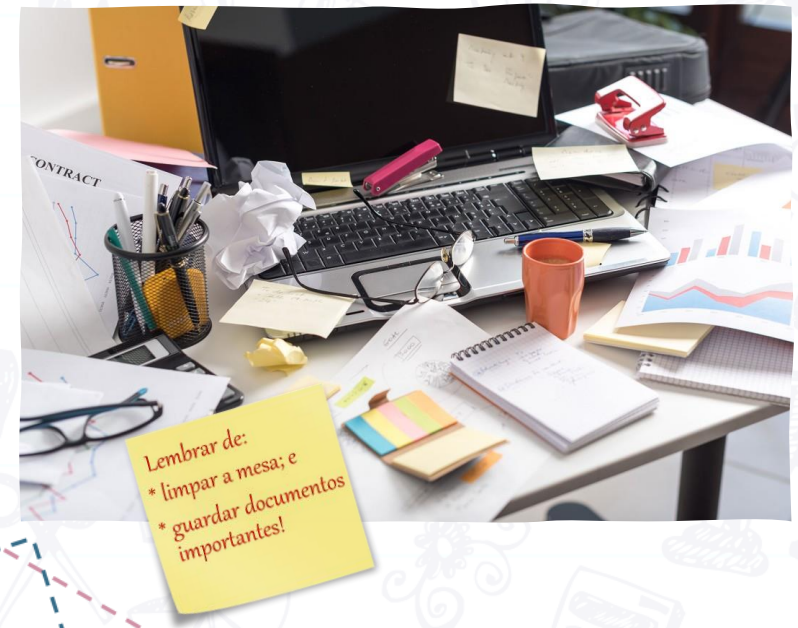
Ou seja, não importa se essas informações estão em sistemas digitais, ou em documentos impressos, ou mesmo em anotações em blocos adesivos.

Isso implica que, independentemente dos meios em que se encontram, as informações institucionais, em especial aquelas que contêm dados pessoais, devem ser protegidas de acesso e de manuseio indevidos (intencional ou acidental).

Mesa limpa e o ambiente em volta também!

Entrando em detalhes, a Política de Mesa Limpa nada mais é do que criar rotinas para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente.

Ou seja, estando você em sua mesa ou não, quaisquer pessoas não autorizadas, ou que não deveriam ter acesso a uma determinada informação, não devem conseguir ver (ou muito menos copiar!) o que tem escrito em documentos e informações sob sua guarda.



Informações deixadas sobre as mesas de trabalho são passíveis de serem danificadas ou destruídas de diversas formas.

Por isso, o objetivo da "Política de Mesa Limpa" é a redução dos riscos de uma violação de segurança, fraudes e roubo de informações, causadas por documentos que estão sendo deixados sozinhos nas instalações de qualquer unidade administrativa da SEDU.

Assim, essas rotinas simples de limpeza do ambiente de trabalho ajudam a prevenir o acesso não autorizado a informações sensíveis e a proteger os dados tratados pelo seu setor.

Além disso, a "Política de Mesa Limpa" está alinhada com normas internacionais de segurança da informação, tal como a **ISO 27001**.

Saiba mais sobre a norma ISO 27001

Algumas dicas úteis para manter a mesa e o ambiente de trabalho seguros

- **Não permita que documentos impressos contendo dados pessoais fiquem acessíveis para terceiros –** as cópias ou originais impressos de documentos e dados pessoais de estudantes e seus familiares, servidores ou de qualquer outra pessoa que entre em contato com seu setor devem ficar guardados em gavetas com chave ou em local de acesso restrito;
- **Não permita que quaisquer documentos impressos fiquem sobre a mesa –** além de demonstrar asseio com o ambiente de trabalho, tal atitude irá evitar que informações institucionais, especialmente aquelas de acesso restrito, sejam expostas de maneira indesejada;
- **Não permita que anotações e lembretes fiquem visíveis para terceiros –** Evite colar bilhetes adesivos em monitores ou mesas expondo atividades, senhas ou decisões. Se precisar lembrar de algo, anote em um caderno e mantenha-o fora da vista de terceiros;
- **Não exponha informações sensíveis em quadros de avisos –** quadros de aviso e quadros brancos devem ser usados para informações que podem ser expostas para o conhecimento de qualquer pessoa.
- **Mantenha guardados os documentos que não estão em uso –** os documentos impressos, agendas e cadernos de anotações com informações sensíveis ou com dados pessoais, quando não estiverem em uso, devem ser mantidos guardados em gavetas ou armários que possam ser trancados, especialmente fora do horário do expediente.
- **Imprima somente o que for necessário e quando for necessário –** a impressão de documentos contendo informações sensíveis ou confidenciais deve ser reservada para condições de absoluta necessidade. Os documentos devem ser visualizados, compartilhados e gerenciados eletronicamente sempre que possível.
- **Proteja as chaves de armários e gavetas onde guarda as informações sensíveis ou confidenciais –** chaves utilizadas para guardar documentos impressos, mídias eletrônicas, dentre outros, devem ser guardadas em local seguro e sob guarda da equipe de trabalho.
- **Cuidado com o quadro de aniversariantes –** evite expor a data de nascimento completa. O mês já é suficiente!

E a tal da Política de Tela Limpa?

Na era digital em que vivemos, as telas dos nossos computadores, tablets e smartphones se tornaram janelas para um mundo de informações.

No entanto, é essencial lembrar que essas janelas podem revelar muito mais do que gostaríamos, especialmente quando se trata de informações sensíveis ou sigilosas.

É por isso que é fundamental adotarmos uma "Política de Tela Segura (ou Tela Limpa)", cujos princípios são basicamente os mesmos da "Política de Mesa Limpa" e, por isso, são frequentemente trabalhadas com ações simultâneas.

A "Política de Tela Limpa" consiste em uma série de práticas destinadas a proteger informações sensíveis que podem ser exibidas na tela de dispositivos eletrônicos. Isso inclui **desde documentos confidenciais até dados pessoais** de estudantes e servidoras(es).

Por que a "Política de Tela Limpa" é tão importante?

Confidencialidade da Informação: A exposição indevida de informações confidenciais ou sensíveis na tela de computadores e outros dispositivos eletrônicos compromete a confidencialidade dessas informações. Isso as deixa suscetíveis a ataques de espionagem, de engenharia social, como o *"shoulder surfing"* (roubo de informações ao espiar por cima dos ombros da pessoa), e de roubo de identidade ou de credenciais de acesso.

Integridade da Informação: No caso de roubo de credenciais de acesso, também pode ocorrer de se comprometer a integridade dos dados, caso um agente malicioso acesse e altere ou exclua informações institucionais e dados pessoais de estudantes, servidores, funcionários terceirizados e visitantes.

Disponibilidade da Informação: Um agente malicioso de posse de credenciais de acesso válidas, pode comprometer a disponibilidade das informações institucionais e dados pessoais a que tiver acesso. Num caso mais extremo, a instituição pode ser vítima de um ataque de "ransomware" (os dados são criptografados e é exigido um resgate para restabelecer o acesso a eles).

Confiabilidade e Reputação da Instituição: Ao adotar práticas de segurança eficazes, a SEDU e suas unidades administrativas demonstram seu compromisso com a proteção das informações confidenciais, assim como os dados pessoais, o que pode aumentar a confiança da sociedade com relação aos serviços prestados para a população capixaba.

Economia de Recursos: Evitar vazamentos de informações confidenciais e/ou sensíveis resulta em economia de recursos financeiros e humanos que seriam necessários para lidar com os impactos negativos desses incidentes, como multas, processos judiciais e danos à reputação, tanto da secretaria, quanto das pessoas envolvidas no incidente.

Conformidade Regulatória: a LGPD e a LAI, assim como outras leis vigentes, exigem a implementação de medidas de segurança para proteger os dados pessoais. E a "Política de Tela Limpa e Segura" contribui para o cumprimento dessas regulamentações, garantindo que o seu setor esteja em conformidade.

Algumas dicas úteis para o uso seguro de dispositivos eletrônicos

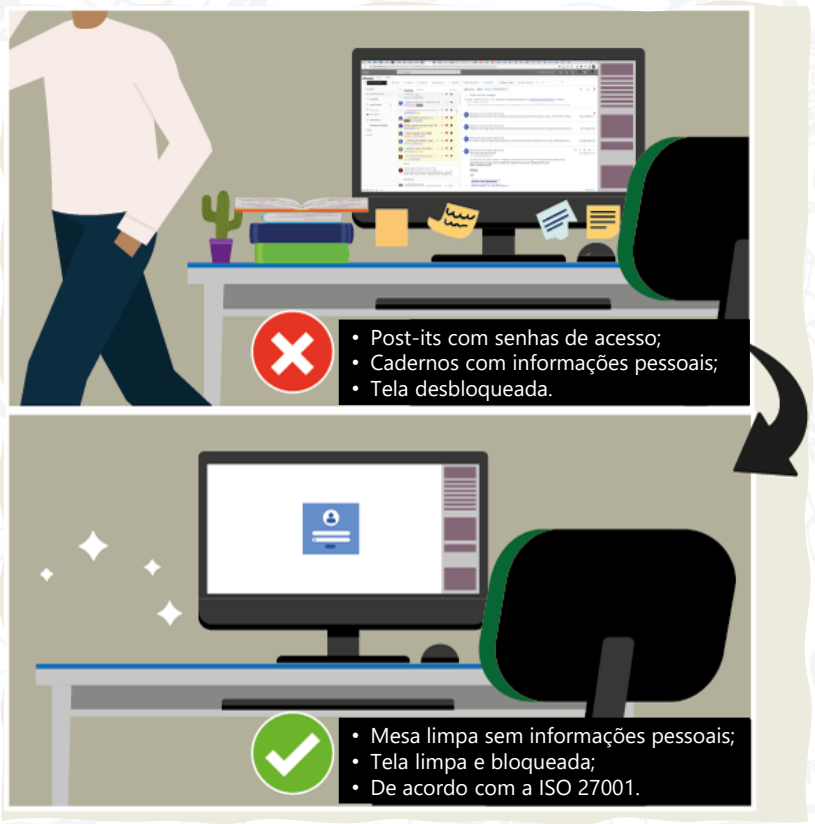
- **Manter abertos apenas arquivos e janelas de sistemas que estão em uso –** se você não estiver usando, evite manter abertos arquivos ou janelas de sistemas com informações confidenciais ou sensíveis, assim como dados pessoais de estudantes, servidores, funcionários terceirizados, fornecedores e/ou do público em geral.
- **Se vai sair temporariamente, bloqueie sua tela –** ao sair de sua mesa de trabalho, SEMPRE bloqueie a sua tela pressionando a tecla "**WINDOWS**" (⊞) ao mesmo tempo que pressiona a tecla "**L**". Assim, o computador bloqueia sua seção de usuário e exigirá as credenciais de acesso (login e senha) para desbloqueio.
- **Se deu a hora de ir embora, desligue o que deve ser desligado –** ao encerrar o seu expediente, lembre-se de encerrar a sua seção em sistemas críticos e desligue a sua estação de trabalho e outros dispositivos sob sua responsabilidade que não devem permanecer ativos.
- **Organize seu local de trabalho –** evite deixar visíveis para visitantes, ou até mesmo para a entrada da sala de trabalho, os monitores dos computadores que acessam informações confidenciais ou dados pessoais. Organize a disposição das mesas do seu ambiente de trabalho de modo a favorecer essa medida. Se isso não for possível, pode-se recorrer ao uso de protetores ou filtros de privacidade, que limitam o ângulo de visão da tela.
- **Fotocopiadoras e impressoras –** o uso de dispositivos como impressoras, fotocopiadoras e scanners deve ser restrito ao pessoal autorizado, conforme o setor de trabalho. Uma boa alternativa é o uso de bloqueio por senha, de modo que somente pessoas autorizadas tenham acesso ao material enviado a esses dispositivos.
- **Câmeras fotográficas –** o uso de câmeras fotográficas deve ser restrito aos locais autorizados. São úteis, por exemplo, os cartazes informando sobre a proibição de filmar e fotografar em ambientes onde são tratados dados pessoais e outras informações confidenciais (secretaria escolar, setor de RH, etc.).

Antes de mudar de assunto...

Os dispositivos de armazenamento portátil também devem ser protegidos – com a popularização do armazenamento de dados em nuvem, algumas pessoas já podem achar essa dica um pouco estranha. Mas, se o seu setor armazena dados em cartões de memória, unidades USB, HDs externos ou outro dispositivo semelhante, lembre-se de também mantê-los seguros. Não os conecte em máquinas desconhecidas e nem os deixe desprotegidos em cima da mesa, principalmente se contiverem informações confidenciais ou sensíveis e dados pessoais.

Documentos devem ser protegidos até quando viram lixo – os cuidados com documentos que contêm informações confidenciais e dados pessoais devem acompanhá-los até o descarte. Evite reutilizar papel usando o verso desses tipos de documentos e, ao descartar, lembre-se de rasgar o papel em pedaços tão pequenos quanto possível. Se seu setor descarta regularmente um grande volume de documentos impressos contendo dados pessoais, talvez deva considerar a aquisição de uma picotadora de papel.

Pra finalizar, veja o resumo com algumas dessas dicas no card elaborado pela **ETIR-UnB**.



Proteção de credenciais de acesso a sistemas e e-mails

Quando se trata das nossas credenciais de acesso (nome de usuário e senha) a sistemas e e-mails institucionais, **algumas práticas devem ser evitadas**, tais como:

- Senhas genéricas e fáceis
- Senhas reutilizadas em vários sistemas
- Compartilhamento das mesmas credenciais de acesso entre várias pessoas
- Credenciais anotadas em locais visíveis para qualquer pessoa que tenho acesso àquele ambiente

A razão disso é que essas credenciais abrem as portas para informações sigilosas e dados pessoais tratados por um setor ou pela secretaria como um todo e devem ser protegidas para garantir a segurança e integridade dessas informações.

Veja esse alerta do CTIR Gov

Nesta seção, abordaremos algumas dicas importantes para a proteção eficaz das credenciais de acesso.

Algumas dicas úteis para o uso seguro de credenciais de acesso

- **Sempre escolha usar senhas fortes –** utilize senhas que sejam únicas, complexas e difíceis de adivinhar, evite utilizar informações pessoais óbvias, como datas de nascimento ou nomes de familiares e, sempre que for permitido, combine letras maiúsculas e minúsculas, números e caracteres especiais para aumentar a complexidade da senha.
- **Cada um com sua credencial -** nunca compartilhe suas credenciais de acesso com colegas ou qualquer outra pessoa. Por mais que isso possa facilitar a execução de um trabalho, é uma prática que deve ser totalmente evitada. Cada usuário deve ter suas próprias credenciais individuais para acessar os sistemas e e-mails.
- **Autenticação de Dois Fatores (2FA) –** caso esteja disponível em seu sistema ou e-mail, ative a autenticação de dois fatores (*Two-Factor Authentication* - 2FA). Ela adiciona uma camada de segurança, exigindo uma segunda forma de verificação além da senha, como um código enviado por SMS ou gerado por um aplicativo autenticador.
- **Considere o uso de Gerenciadores de Senhas –** uma boa alternativa à prática pouco recomendável de anotar senhas em notas adesivas é usar os softwares e aplicativos gerenciadores de senhas. Existem versões acessíveis e confiáveis capazes de armazenar e gerar senhas complexas de forma segura. Além disso, eles facilitam a gestão de múltiplas credenciais sem comprometer a segurança.
- **A sua melhor senha também tem validade –** altere suas senhas regularmente. Isso ajuda a evitar que haja o comprometimento devido a vazamentos de dados ou ataques de agentes maliciosos.
- **Cuidado para não ser fisgado –** esteja atento àqueles e-mails suspeitos que solicitam informações de login, ou a atualização de suas credenciais de acesso ou que tenham links suspeitos exigindo urgência no seu acesso. Verifique sempre a autenticidade do remetente antes de clicar nesses links ou fornecer informações confidenciais e/ou dados pessoais, como suas credenciais de acesso.

Práticas seguras para o uso de e-mail

É indiscutível o quanto o e-mail facilita a comunicação agentes internos e externos à instituição, permitindo o compartilhamento de documentos e informações confidenciais ou sensíveis e dados pessoais.

Mas, como qualquer ferramenta poderosa, o e-mail também pode ser usado de forma inadequada ou perigosa. É importante estarmos cientes dos riscos e tomar medidas para proteger a nós mesmos, os dados a que temos acesso e a própria instituição.

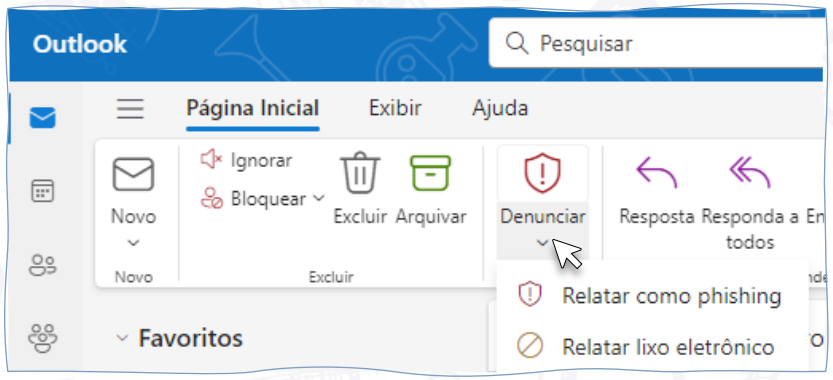
Além dos riscos envolvidos no compartilhamento de documentos e informações confidenciais ou sensíveis e dados pessoais, o e-mail também pode ser porta de entrada para uma técnica de manipulação que explora a confiança e a boa vontade das pessoas para obter àquelas informações confidenciais ou o acesso aos sistemas utilizados pela instituição. Essa técnica é conhecida como **engenharia social**.

Saiba mais sobre engenharia social

Recebimento seguro de e-mails

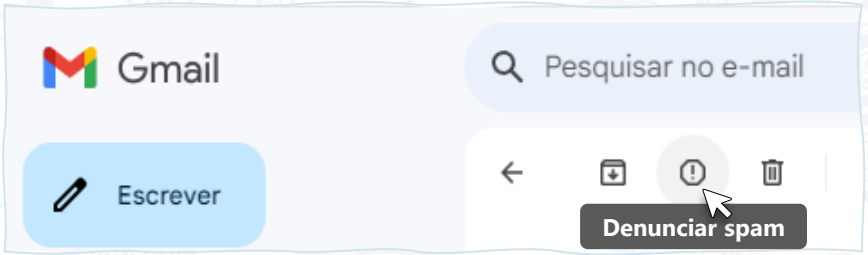
Cuidado ao receber e-mails suspeitos – Além dos e-mails de spam (aqueles chatos com propaganda) que recebemos, também estão mais frequentes os golpes com "phishing" (que nos induzem a revelar dados pessoais ou a instalar malwares nos dispositivos). Use as ferramentas disponíveis para bloquear esses e-mails. Se ainda assim você receber um e-mail suspeito, exclua-o sem clicar em nenhum link que ele indicar.

Se estiver utilizando o Microsoft Outlook - você ainda tem a opção de denunciar em ***"Relatar como phishing"*** ou ***"Relatar como lixo eletrônico"***:



Opções de denúncia de e-mail no Outlook (new).

Se estiver utilizando o Gmail – o Gmail também oferece opção semelhante:



Botão de denúncia de spam no Gmail.

Para evitar o *phishing*: você também pode evitar os golpes por *phishing* se atentando para e-mails de remetentes desconhecidos, evitando clicar em links suspeitos ou abrir anexos em e-mails suspeitos. E, se ficar na dúvida, verifique a URL do site antes de clicar no link ou botão.

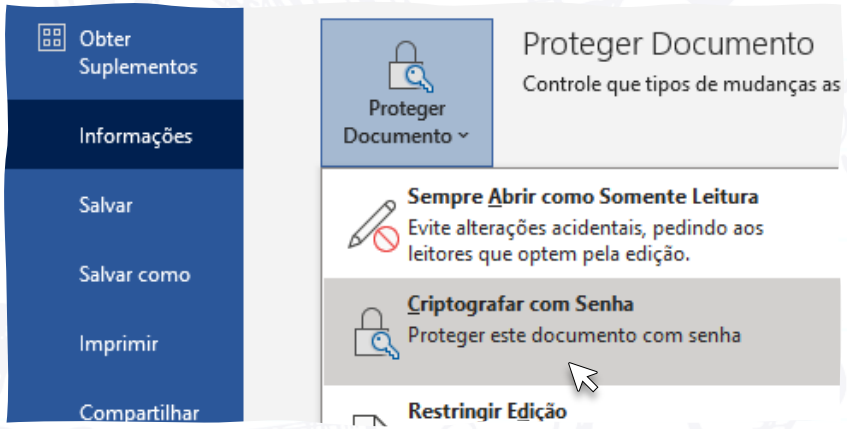
Veja dicas da Microsoft

Veja dicas da Google

Protegendo apenas os anexos dos seus e-mails

Proteja os anexos contendo informações confidenciais ou dados pessoais – Antes de encaminhar um e-mail contendo um documento anexo, busque formas de proteger esse documento antes de compartilhar por e-mail, em especial quando contiver dados pessoais.

Usando a criptografia do Microsoft 365 – qualquer app do Microsoft 365, na versão atualmente disponibilizada na SEDU, oferece a opção de "Criptografar com Senha", além de outras restrições:



Com o arquivo aberto, clique na aba "Arquivo" e depois em "Informações". A figura mostra um exemplo com o Word.

Usando outras ferramentas de encriptação – caso não esteja usando o Microsoft 365, ou queira proteger outro tipo de arquivo, ou até mesmo uma pasta com vários arquivos, você pode recorrer a outras ferramentas de encriptação. **Evite a tentação de recorrer a ferramentas online!**

Dica de software – uma alternativa gratuita é utilizar o software de compactação de arquivos **7-Zip** e utilizar a sua função de encriptação.

Existem outras alternativas mais adequadas e robustas para proteção de arquivos. As que estão sendo apresentadas aqui são apenas as mais facilmente encontradas nos computadores usados na maioria das unidades administrativas da SEDU.

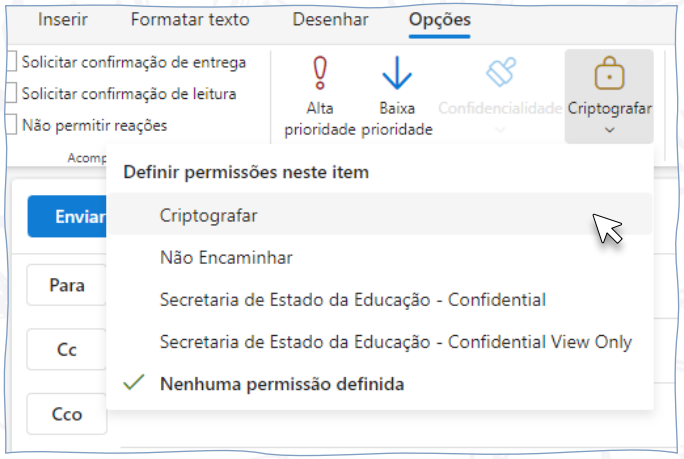
Veja o tutorial da Microsoft

Veja o tutorial da AVG sobre o 7-Zip

Protegendo o corpo do e-mail e seus anexos

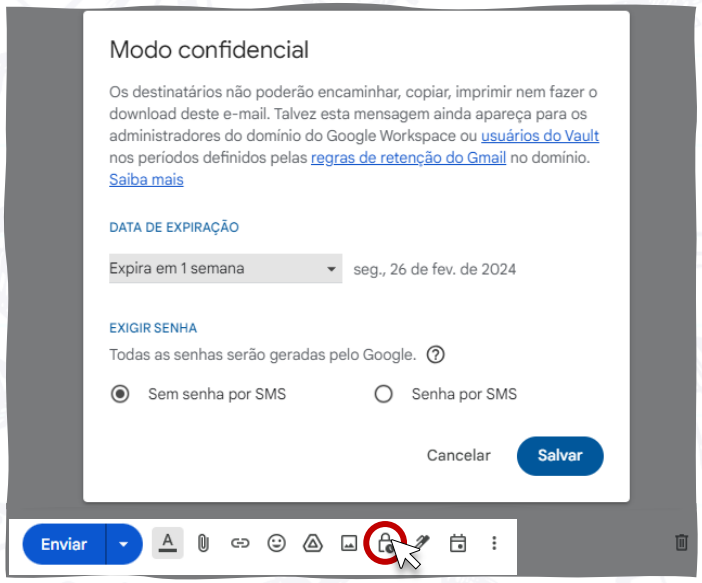
Proteja tanto o e-mail quanto seus anexos – Ao encaminhar um e-mail contendo informações confidenciais, em especial dados pessoais, seja no corpo do e-mail ou em um documento anexo, você também pode buscar formas de proteger o próprio e-mail, juntamente com seus anexos.

Se estiver usando o Microsoft Outlook – é possível usar a ferramenta de criptografia nativa, que oferece a diversas opções de restrição para envio de e-mail:



Escreva seu e-mail normalmente e, antes de enviar, clique na aba "Opções" e depois em "Criptografar". Na figura um exemplo com o Outlook (new).

Se estiver usando o Gmail – o Gmail também fornece uma opção de envio confidencial de e-mails.



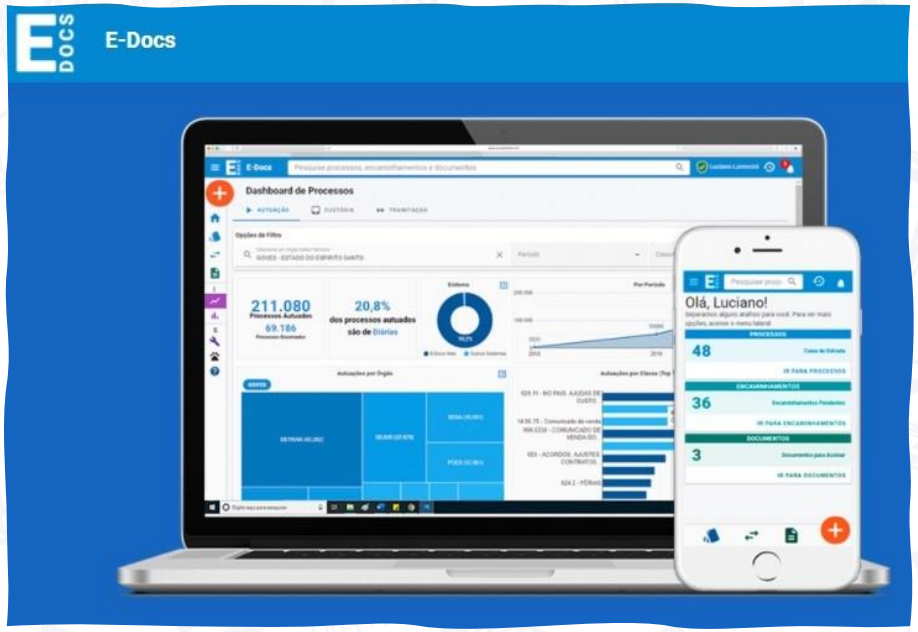
Escreva seu e-mail normalmente e, antes de enviar, clique no ícone de cadeado. Na figura um exemplo com o Gmail no navegador web.

Veja o tutorial da Microsoft

Veja o tutorial da Google

GOVERNO DO ESTADO DO ESPÍRITO SANTO
Secretaria da Educação

Práticas seguras para o uso do E-Docs



Acesse diversos tutoriais em vídeo e o manual SEDU sobre o E-Docs

Sempre que possível, será recomendável o uso do E-Docs para o compartilhamento de informações confidenciais e dados pessoais.

O e-mail deverá ser sempre a última opção para o compartilhamento de dados pessoais!

Como as técnicas sugeridas para a proteção dos anexos de e-mail não se aplicam aos documentos utilizados em encaminhamentos e processos no E-Docs, existem duas práticas recomendáveis:

- **controlar o Nível de Acesso de um documento específico**
- **controlar o credenciamento de novos usuários a documentos e processos**

Nesses casos, é importante pesar em que ponto cabe o direito de acesso à informação, previsto pela Lei Federal Nº 12.527/2011, que institui a **Lei de Acesso à Informação (LAI)** e em que ponto cabe o direito à privacidade, previsto tanto na LAI, quanto na Lei Federal Nº 13.709/2018, a **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

Controlando o Nível de Acesso aos documentos no E-Docs

Classificação da informação – seja um documento capturado ou gerado no sistema E-Docs, ele pode passar por um processo de classificação da informação, que estabelece níveis de restrição de acesso ao documento, conforme abaixo:

Níveis de Restrição de Acesso no E-Docs:

Público

O documento pode ser acessado por qualquer usuário logado no sistema E-Docs.

Organizacional

O documento pode ser acessado por qualquer servidor lotado em qualquer um dos órgãos por onde esse documento tramitar.

É selecionado por padrão pelo E-Docs.

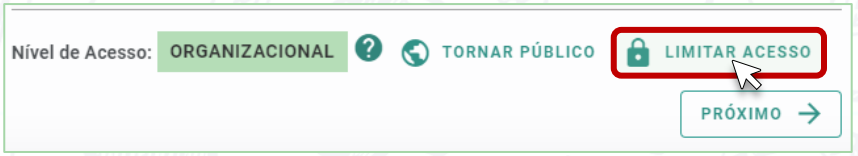
Sigiloso

O documento só pode ser acessado por quem o captura, assina, recebe (via encaminhamento ou processo administrativo), ou obtém credenciamento de leitura.

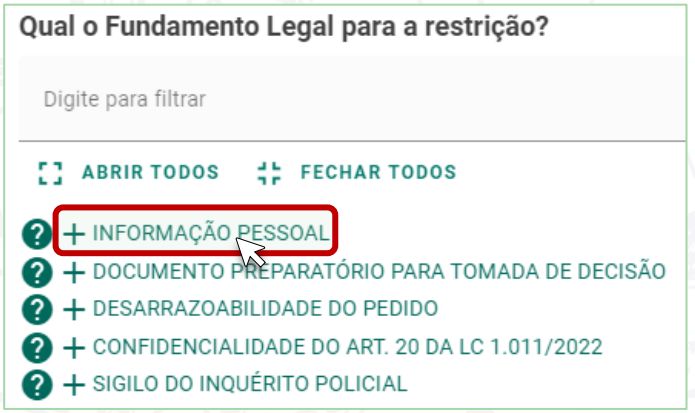
Classificado

O documento só pode ser acessado por quem tiver permissão para visualizar documentos classificados (**RESERVADO**, **SECRETO** ou **ULTRASSECRETO**).

Limitar acesso a documentos com dados pessoais – se você estiver tramitando documentos que contêm dados pessoais (vamos tratar aqui apenas desse caso), você deve iniciar a classificação assim que o E-Docs habilitar a seguinte seção:



Fundamento legal para restrição de acesso – ao clicar em "LIMITAR ACESSO" você será direcionado para a seguinte janela:



A informação pessoal é sigilosa – ao clicar na opção "Informação Pessoal", você estará classificando o documento como **SIGILOSO**. Essa proteção está prevista no artigo 22 da **Lei Estadual Nº 9.871/2012**, que regula o acesso à informação no âmbito estadual, no artigo 54 do **Decreto Estadual Nº 3.152-R/2012**, que a regulamenta, assim como na LGPD e na LAI.

Está explicado no próprio E-Docs – a definição para "documentos com informação pessoal" está descrita em texto explicativo no próprio sistema E-Docs:

> *"São documentos que trazem informações de determinada pessoa identificada ou identificável.*
>
> *A restrição de acesso respeita o disposto no art. 54 do Decreto nº 3.152-R/2012, que garante proteção às informações pessoais relativas à intimidade, vida privada, honra e imagem que estejam na posse dos órgãos e entidades.*
>
> *Nesse caso, as informações são restritas, por um prazo de 100 (cem) anos, aos agentes públicos legalmente autorizados e à própria pessoa."*

Acesse os vídeos com tutoriais do E-Docs – se você quiser saber mais sobre essa classificação, acesse o vídeo tutorial:

Controlando o credenciamento em documentos e processos no E-Docs

Existe previsão legal para o acesso aos dados pessoais contidos no documento ou processo? Sempre que alguém solicitar o acesso a um documento que você classificou como **sigiloso devido à existência de informações pessoais** em seu conteúdo, será necessário verificar as condições de cada caso concreto.

Veja o que diz a **Lei Estadual Nº 9.871/2012**, em conformidade a **Lei Federal Nº 12.527/2011**:

> As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem terão seu **acesso restrito**, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, **a agentes públicos legalmente autorizados e à pessoa a que elas se referirem**.
>
> *(Artigo 22, parágrafo 1º, inciso I)*

Então, se não se trata de agente público legalmente autorizado ou a própria pessoa a quem os dados se referem, **deverá ser considerada a restrição por sigilo devido à existência de informações pessoais**.

Existe alguma exceção a essa regra? Existe! E também encontra-se na **Lei Estadual Nº 9.871/2012**:

> As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem poderão ter autorizada sua divulgação ou acesso por terceiros **diante de previsão legal** ou **consentimento expresso da pessoa a que elas se referirem**.
>
> *(Artigo 22, parágrafo 1º, inciso II)*

Ou seja, **primeiro verifique se existe alguma previsão legal** para se conceder o acesso desses dados pessoais a terceiros.

Caso não exista uma previsão legal – nesse caso, consulte a pessoa a quem esses dados se referem e **solicite o seu consentimento** para compartilhar os dados com terceiros que lhe requisitam informações.

Lembre-se que esse consentimento deve ser **livre, esclarecido e claramente destinado ao que foi solicitado** (você ficará sabendo mais sobre consentimentos numa seção mais adiante!).

E se não existe previsão legal e a pessoa a quem os dados pessoais se referem negar o consentimento?
Nesse caso, cabe à Administração Pública garantir todas as medidas técnicas e administrativas cabíveis para que esses dados pessoais não sejam compartilhados ou acessados indevidamente.

Lembre-se que são direitos da pessoa a quem os dados se referem:

- ✓ Fornecer ou negar um consentimento; e
- ✓ Revogar um consentimento fornecido anteriormente.

Três boas alternativas são sugeridas no parágrafo 2º do artigo 7º da **Lei Estadual Nº 9.871/2012**:

Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de **certidão, extrato ou cópia com ocultação da parte sob sigilo**.

Certidão – É um documento oficial que transcreve o conteúdo original do documento ou processo solicitado, sem revelar as partes sigilosas.

Extrato – É um documento oficial que contém não uma transcrição parcial, mas sim trechos originais do(s) documento(s) ou do processo solicitado, que não contenham informações sigilosas.

Cópia com ocultação da(s) parte(s) sob sigilo – É uma cópia de um documento oficial original, editada para ocultar a(s) parte(s) que contenham dados pessoais. A ocultação dos dados pessoais em um documento, ou nas peças de um processo, nada mais é do que uma forma de anonimização, tal como previsto na LGPD.

Essa ocultação pode ser realizada:

- ✓ com a substituição das letras e/ou números por asteriscos (*), por exemplo ; ou
- ✓ a sobreposição de uma tarja preta sobre os dados a serem protegidos.

Ocultando informações sigilosas em documentos tratados no E-Docs

Como ocultar informações sigilosas, em especial os dados pessoais, que constam em documentos disponíveis no E-Docs? Nesse caso, a técnica a ser utilizada vai depender da disponibilidade do documento original editável, que deu origem ao documento disponível no E-Docs.

Também é importante que o novo documento com as informações ocultadas não perca a propriedade de ser pesquisável, caso ela exista no original.

Caso o documento original esteja acessível para edição – nesse caso, siga os seguintes passos:

1➤ **Faça uma cópia do arquivo –** renomeie essa cópia do arquivo incluindo ao final do nome original a "etiqueta" **[ANONIMIZADO]**.

(ex.: *Contrato Empresa XYZ [ANONIMIZADO].docx*)

2➤ **Acrescente um aviso no documento -** logo abaixo do nome do documento acrescente um aviso de que se trata de uma cópia com ocultação de informações sensíveis e/ou de dados pessoais.

3➤ **Faça a ocultação das informações sensíveis e/ou dos dados pessoais existentes –** para efetuar essa ocultação ou anonimização, você pode substituir as letras e/ou números por outros caracteres como os asteriscos (*). Veja o exemplo abaixo:

Trecho original → "... o aluno beneficiário, CPF 012.345.678-90, residente na Rua ABCDE, 01, XYZ, Vitória - ES ..."

Trecho anonimizado → "... o aluno beneficiário, CPF ***.345.678-**, residente na Rua *****, **, ***, ******* - ES ..."

Também é possível efetuar o **tarjamento**, que implica em cobrir as informações com uma tarja, ou seja:

- ✓ cobrir com uma forma geométrica, geralmente um retângulo na cor preta; ou
- ✓ cobrir com o realce de texto, função disponível na maioria dos editores de texto.

No entanto, essas duas técnicas não são recomendáveis, pois permitem selecionar o texto tarjado, copiar e colar em outro local. Consegue descobrir a solução sob as tarjas abaixo? 😉

4➤ **Faça o upload do arquivo censurado no E-Docs –** faça o upload do arquivo, mas lembre-se que o E-Docs exige que ele esteja no formato PDF. Por fim, faça o upload permitindo o acesso à pessoa solicitante.

Lembre-se de manter o documento original no E-Docs com o acesso restrito!

Veja como o Instituto Federal de São Paulo (IFSP) trata a questão do tarjamento de seus documentos institucionais

⚠ **Dados que sejam de interesse público não devem ser ocultados –** lembre-se que a Lei de Acesso à Informação exige que as informações necessárias ao controle da sociedade sobre o serviço público sejam fornecidas. Assim, alguns dados não podem classificados como informação sigilosa e, por isso, não podem ser ocultados.

O CPF e o Número Funcional de servidoras(es) são seus dados pessoais. Assim, sempre que cabível, **o CPF deve ser ocultado**.

No entanto, o Número Funcional é um dado que não se refere à vida privada, mas sim à vida funcional dos(as) servidores(as), sendo de interesse público.

Por isso, o **Número Funcional não deve ser ocultado**, inclusive para **garantir a identificação em casos de existência de homônimos**.

O CPF de pessoas físicas, Empresários Individuais (EI) e Microempreendedores Individuais (MEI), que utilizam esse documento como identificador em contratações com o poder público se torna uma informação de interesse público.

Por isso, **não podem ser classificados como sigilosos** e, consequentemente, **não podem ser ocultados no atendimento a solicitações de acesso à informação.**

Caso o documento original não esteja acessível – se não tiver acesso ao documento original, ou ele existir apenas em formato PDF, siga os seguintes passos:

1. **Obtenha uma cópia do documento –** faça um cópia do documento ou faça o download a partir do E-Docs. Em seguida, renomeie essa cópia incluindo a etiqueta **[ANONIMIZADO]**, como no caso anterior.
2. **O documento deve estar no formato PDF –** caso você tenha feito o download do E-Docs isso não será problema, mas se estiver preparando um documento para upload no E-Docs, deve se lembrar de fazer essa conversão.
3. **Abra o documento em uma ferramenta offline para edição de arquivos PDF –** caso você tenha acesso a um software pago, como o Adobe Acrobat Pro, ele terá a função de "Ocultar" disponível. Caso contrário, será necessário a instalação de um software gratuito que tenha essa função.

Dica de software – algumas universidades e institutos federais têm sugerido aos seus servidores o download e uso do software gratuito PDF24 Creator. Caso opte por essa ferramenta, abra um chamado junto à Gerência de Tecnologia da Informação e solicite a sua instalação.

Se o documento contém informações sigilosas, não caia na tentação de usar as alternativas online!

Lembre-se que assim você transferirá o documento que quer proteger para computadores de outra instituição.

Veja o tutorial do IFSP para o Adobe Acrobat Pro

Veja o tutorial do IFSP para o PDF24 Creator

4. **Faça o upload do arquivo anonimizado no E-Docs –** por fim, faça o upload no E-Docs, permitindo o devido acesso à pessoa solicitante.

Lembre-se de manter o documento original no E-Docs com o acesso restrito!

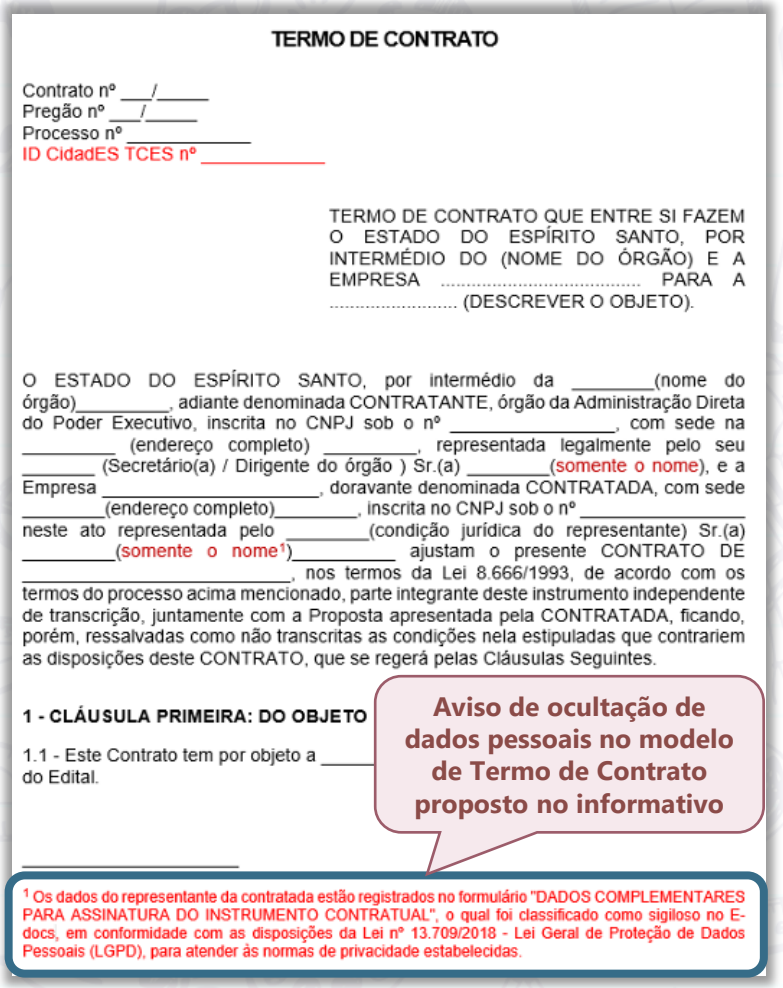
Tratando dados pessoais em novos contratos e convênios

Também podemos proteger os dados pessoais ainda durante a preparação dos documentos que irão pro E-Docs – Desde 2023 o Governo do Estado tem disponibilizado informativos relacionados à proteção dos dados pessoais, tanto no Portal de Contratos, quanto no Portal de Convênios. Dentre esses informativos vale destacar o:

- **Informativo de Convênios Nº 003/2023 –** Ajuste nos novos instrumentos de convênios para atender a Lei Geral de Proteção de Dados; e
- **Informativo de Contratos Nº 004/2023 –** Ajustes nos novos contratos para atender a Lei Geral de Proteção de Dados – LGPD

Veja os Informativos do Portal de Convênios

Veja os Informativos do Portal de Contratos



TERMO DE CONTRATO

Contrato nº ___/_____
Pregão nº ___/_____
Processo nº _____
ID CidadES TCES nº _____

TERMO DE CONTRATO QUE ENTRE SI FAZEM O ESTADO DO ESPÍRITO SANTO, POR INTERMÉDIO DO (NOME DO ÓRGÃO) E A EMPRESA ..... PARA A ..... (DESCREVER O OBJETO).

O ESTADO DO ESPÍRITO SANTO, por intermédio da _____(nome do órgão)_____, adiante denominada CONTRATANTE, órgão da Administração Direta do Poder Executivo, inscrita no CNPJ sob o nº _____, com sede na _____ (endereço completo) _____, representada legalmente pelo seu _____ (Secretário(a) / Dirigente do órgão) Sr.(a) _____(somente o nome), e a Empresa _____, doravante denominada CONTRATADA, com sede _____(endereço completo)_____, inscrita no CNPJ sob o nº _____ neste ato representada pelo _____(condição jurídica do representante) Sr.(a) _____(somente o nome[1])_____ ajustam o presente CONTRATO DE _____, nos termos da Lei 8.666/1993, de acordo com os termos do processo acima mencionado, parte integrante deste instrumento independente de transcrição, juntamente com a Proposta apresentada pela CONTRATADA, ficando, porém, ressalvadas como não transcritas as condições nela estipuladas que contrariem as disposições deste CONTRATO, que se regerá pelas Cláusulas Seguintes.

1 - CLÁUSULA PRIMEIRA: DO OBJETO

1.1 - Este Contrato tem por objeto a _____ do Edital.

_____

Aviso de ocultação de dados pessoais no modelo de Termo de Contrato proposto no informativo

[1] Os dados do representante da contratada estão registrados no formulário "DADOS COMPLEMENTARES PARA ASSINATURA DO INSTRUMENTO CONTRATUAL", o qual foi classificado como sigiloso no E-docs, em conformidade com as disposições da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), para atender às normas de privacidade estabelecidas.

Tratando dados pessoais coletados em formulários

Sejam formulários, impressos ou eletrônicos, destinados a inscrições, a pesquisas, ou mesmo a registros de presença, é importante observar mais três princípios da LGPD:

Princípio da Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

(Inciso I do Artigo 6º da LGPD)

Princípio da Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

(Inciso II do Artigo 6º da LGPD)

Princípio da Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

(Inciso III do Artigo 6º da LGPD)

Imagem de Storyset no Freepik

Adequando formulários à LGPD

- **Determine a finalidade do seu formulário –** Busque ajustar a finalidade do seu formulário às atribuições e competências legais do seu setor de atuação (**veja o artigo 5º da PEPDP**). Defina claramente a finalidade para a qual os dados serão coletados. Isso ajuda a garantir que apenas informações relevantes sejam solicitadas aos usuários.
- **Adeque o tratamento à finalidade –** Certifique-se de que o tratamento dos dados coletados esteja em conformidade com a finalidade para a qual foram obtidos. Ou seja, se você informa que se trata de um formulário de inscrição em um curso ou evento, os dados coletados não podem ser usados para gerar uma lista de contatos para divulgações da empresa que prestou o curso ou os serviços do evento.
- **Use somente os dados necessários –** Adote como regra a **minimização da coleta de dados**, limitando-se apenas ao que é estritamente necessário para a finalidade declarada. Evite solicitar informações sensíveis, a menos que sejam essenciais para o propósito do seu formulário.
- **Garanta a segurança dos dados coletados –** Implemente medidas que garantam a segurança dos dados pessoais coletados. Isso inclui controle de acesso às respostas do formulário, uso de pastas seguras, com senha e criptografadas para o arquivo de respostas de formulários eletrônicos, uso de armários/gavetas com chave para formulários impresso e monitoramento regular.
- **Informe se haverá uso posterior, diferente da finalidade original –** Se houver planos para utilizar os dados coletados para uma finalidade diferente da originalmente declarada, informe claramente a finalidade futura e solicite o consentimento explícito das pessoas que estão respondendo o formulário (pode ser até uma pergunta de marcar SIM ou NÃO).
- **Insira no formulário um Aviso de Privacidade –** Inclua um Aviso de Privacidade, preferencialmente no início formulário, descrevendo de forma clara e concisa como e quais dados serão utilizados, quem terá acesso a eles e quais são os direitos dos titulares dos dados no caso específico contemplado pelo formulário.

Um pouco mais sobre o Aviso de Privacidade

Observe o que determina a LGPD – o Aviso de Privacidade atende a um direito da pessoa titular dos dados de ter acesso à informação sobre o tratamento de seus dados pessoais, sendo que sua estrutura pode observar o que determina o **artigo 9º da LGPD**:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I. finalidade específica do tratamento;

II. forma e duração do tratamento, observados os segredos comercial e industrial;

III. identificação do controlador;

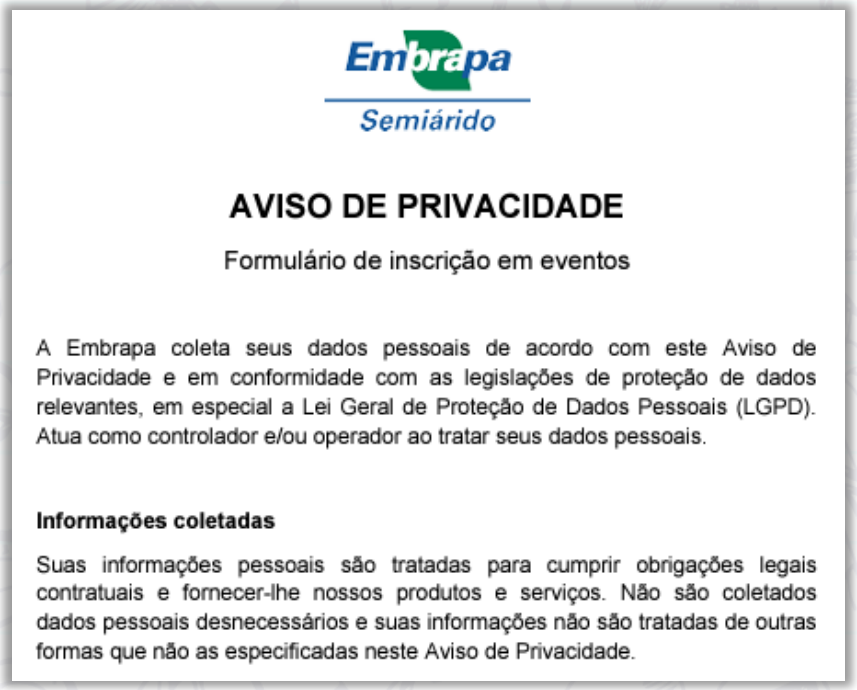
IV. informações de contato do controlador;

V. informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI. responsabilidades dos agentes que realizarão o tratamento; e

VII. direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Ex.: Formulário de inscrição em eventos da EMBRAPA:



Embrapa
Semiárido

AVISO DE PRIVACIDADE

Formulário de inscrição em eventos

A Embrapa coleta seus dados pessoais de acordo com este Aviso de Privacidade e em conformidade com as legislações de proteção de dados relevantes, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD). Atua como controlador e/ou operador ao tratar seus dados pessoais.

Informações coletadas

Suas informações pessoais são tratadas para cumprir obrigações legais contratuais e fornecer-lhe nossos produtos e serviços. Não são coletados dados pessoais desnecessários e suas informações não são tratadas de outras formas que não as especificadas neste Aviso de Privacidade.

Veja esse Aviso de Privacidade completo

Tratando dados pessoais que necessitam do consentimento da pessoa titular dos dados

Document illustration by Storyset

Como dito anteriormente, **o tratamento de dados pessoais por qualquer unidade administrativa da SEDU deve ser com o objetivo de atender a finalidade pública da Secretaria** e, mais especificamente, **considerando a conformidade com as atribuições e competências legais de cada setor de atuação**.

Quando a atividade de tratamento de dados ultrapassa esses limites, vale observar o que diz o **artigo 6º da PEPDP**:

> **Art. 6º** Em estrita observância e cumprimento de suas finalidades públicas, os agentes de tratamento poderão tratar dados pessoais, inclusive os dados pessoais sensíveis, **com dispensa de consentimento** dos respectivos titulares.
>
> **Parágrafo Único.** A **execução de atividades que ultrapassem as funções públicas condiciona-se à obtenção de consentimento dos titulares** dos dados pessoais, na forma do art. 8º da Lei Geral de Proteção de Dados.

Obtendo o consentimento da pessoa titular dos dados

O consentimento deve estar facilmente visível para quem assina - a LGPD permite que utilizemos outras formas de consentimento que não sejam mediante a assinatura de um Termo de Consentimento (artigo 8º da LGPD, § 1º). Mas, caso seja por um termo escrito (impresso ou digital), ele deve estar facilmente visível para a pessoa que o assina.

Além de estar visível, tem de ser claro - as informações sobre o tratamento de dados devem ser apresentadas previamente, com transparência e de forma clara e inequívoca (artigo 9º da LGPD, § 1º).

Se forem dados de crianças e adolescentes a clareza deve ser ainda maior – nesse caso, as informações "deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança" (artigo 14 da LGPD, § 6º).

A prova de conformidade legal do Termo de Consentimento é uma responsabilidade do setor emitente - se o seu setor solicitar o consentimento para tratamento de dados pessoais, automaticamente se tornará responsável por provar que ele foi obtido em conformidade com o disposto na LGPD e na PEPDP (artigo 8º da LGPD, § 2º). Importante notar que,

Tem que garantir que o consentimento seja dado pelo responsável, maior de 18 anos - se o consentimento se referir ao tratamento de dados de crianças e adolescentes, será responsabilidade de seu setor garantir que o consentimento seja dado por um dos pais ou responsável legal pela criança ou adolescente (artigo 14 da LGPD, § 5º).

O consentimento de menores de 18 anos não tem valor legal - deve-se sempre recorrer ao consentimento de ao menos um dos pais ou responsável legal. A depender do caso concreto e da capacidade cognitiva, uma criança ou adolescente pode assinar o termo conjuntamente com seu responsável, garantindo o seu direito de participação nessa tomada de decisão.

O artigo 9º também rege as informações contidas no Termo de Consentimento – para ser claro, o Termo de Consentimento também deve conter aquelas informações previstas no artigo 9º da LGPD:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I. finalidade específica do tratamento;

II. forma e duração do tratamento, observados os segredos comercial e industrial;

III. identificação do controlador;

IV. informações de contato do controlador;

V. informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI. responsabilidades dos agentes que realizarão o tratamento; e

VII. direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

A finalidade deve ser determinada e específica - se o Termo de Consentimento for fundamentado em uma finalidade genérica, se tornará automaticamente nulo (artigo 8º da LGPD, § 4º).

Alterações das informações contidas no Termo de Consentimento – caso ocorram alterações nas informações referidas nos incisos I, II, III ou V do artigo 9º da LGPD, seu setor deverá informar a cada uma dos titular que assinaram o Termo, destacando de forma específica o teor das alterações. Em caso de a pessoa titular desses dados discordar das alterações informadas, deve ser permitida a sua revogação (§ 6º do artigo 8º e § 2º do artigo 9º da LGPD).

Todo consentimento pode ser revogado – a pessoa titular dos dados pode revogar, a qualquer tempo, um consentimento que tenha fornecido anteriormente. Essa revogação deve se dar mediante manifestação expressa da pessoa titular, por procedimento gratuito e facilitado. O tratamento realizado anteriormente permanece válido, a menos que se solicite a eliminação dos dados (artigo 8º da LGPD, § 5º).

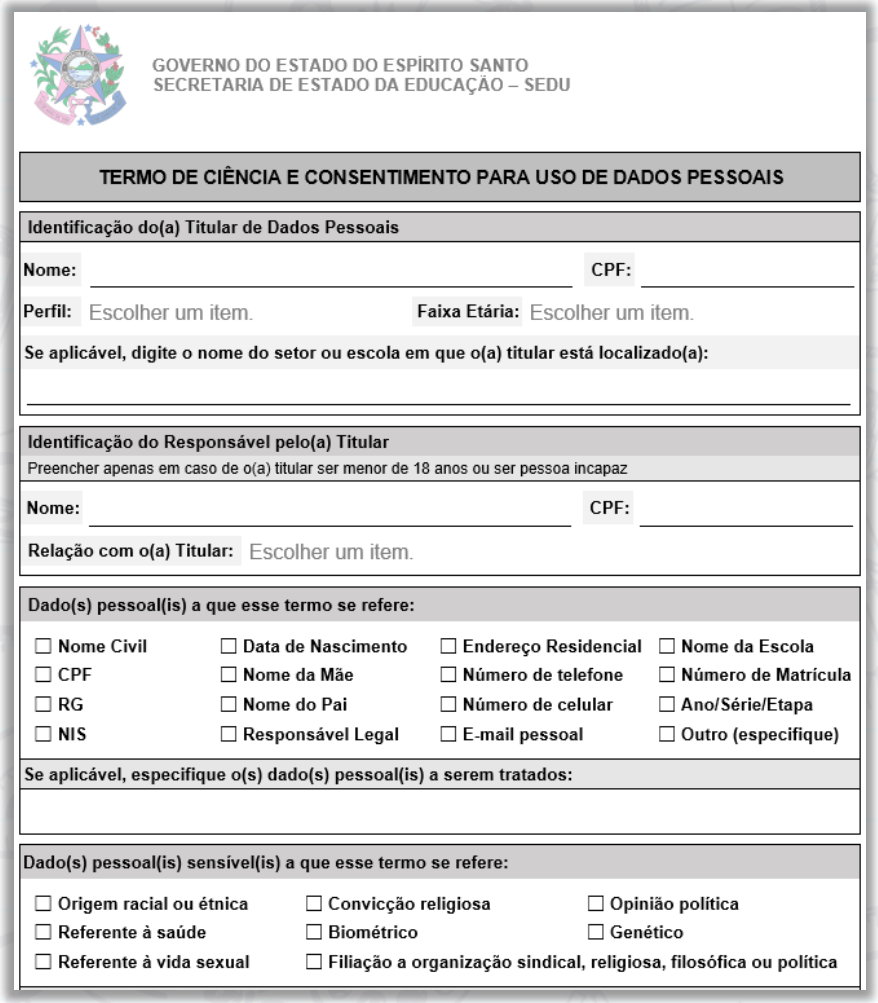
Modelos de Termo de Consentimento para a SEDU

Modelos de Termo de Consentimento – a SEDU disponibiliza em seu site institucional (na seção **"Privacidade e Proteção de Dados" > "Materiais e Publicações" > "Modelos de Documentos"**), dois modelos de Termo de Consentimento elaborados pelo Encarregado Interno pelo Tratamento de Dados Pessoais (EITDP) da Secretaria:

Termo de Ciência e Consentimento para Uso de Dados Pessoais – esse modelo serve para dar ciência e solicitar o consentimento para o tratamento de dados pessoais de tipos diversos (nome, CPF, endereço, etc.).

Termo de Ciência e Consentimento para Uso de Imagem – esse modelo serve para dar ciência e solicitar o consentimento para o tratamento de imagens, seja em formato de foto ou vídeo. As imagens são consideradas dados pessoais comuns, mas podem se tornar dados sensíveis se for possível utilizá-las, por qualquer meio técnico, para fins biométricos.

Acesse a página de materiais e publicações



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA EDUCAÇÃO – SEDU

TERMO DE CIÊNCIA E CONSENTIMENTO PARA USO DE DADOS PESSOAIS

Identificação do(a) Titular de Dados Pessoais

Nome: _____ CPF: _____

Perfil: Escolher um item. Faixa Etária: Escolher um item.

Se aplicável, digite o nome do setor ou escola em que o(a) titular está localizado(a):

_____

Identificação do Responsável pelo(a) Titular

Preencher apenas em caso de o(a) titular ser menor de 18 anos ou ser pessoa incapaz

Nome: _____ CPF: _____

Relação com o(a) Titular: Escolher um item.

Dado(s) pessoal(is) a que esse termo se refere:

☐ Nome Civil	☐ Data de Nascimento	☐ Endereço Residencial	☐ Nome da Escola
☐ CPF	☐ Nome da Mãe	☐ Número de telefone	☐ Número de Matrícula
☐ RG	☐ Nome do Pai	☐ Número de celular	☐ Ano/Série/Etapa
☐ NIS	☐ Responsável Legal	☐ E-mail pessoal	☐ Outro (especifique)

Se aplicável, especifique o(s) dado(s) pessoal(is) a serem tratados:

Dado(s) pessoal(is) sensível(is) a que esse termo se refere:

☐ Origem racial ou étnica	☐ Convicção religiosa	☐ Opinião política
☐ Referente à saúde	☐ Biométrico	☐ Genético
☐ Referente à vida sexual	☐ Filiação a organização sindical, religiosa, filosófica ou política	

Armazenamento dos Termos de Consentimento

Os Termos de Consentimento precisam ser mantidos arquivados e rastreáveis – A hipótese de tratamento de dados pessoais pelo consentimento possui muitas fragilidades para qualquer agente de tratamento. Por isso, garantir que haja um Termo de Consentimento legítimo e assinado por cada titular ou responsável legal, torna tudo um pouco mais seguro. Sendo assim, a partir do momento que seu setor obtém um Termo de Consentimento, é importante manter uma forma segura, tanto para armazenar, quanto para consultar os termos existentes.

Armazenando Termos de Consentimento impressos – Esse formato tende a se extinguir, mas se o seu setor mantém apenas versões impressas dos termos, será importante armazená-los em armários de arquivos que sejam protegidos e numa forma que seja possível pesquisar e encontrar qualquer termo existente, caso seja solicitado. No caso das escolas, também é possível armazenar os termos (ou suas cópias) juntamente com o prontuário do estudante (em caso de ainda haver uma versão impressa).

Armazenando Termos de Consentimento digitalizados – Nesse caso, os termos podem ser armazenados em qualquer pasta segura, seja offline ou mesmo online, desde que se garanta o acesso a todos os responsáveis pela ação. Dentre as opções disponíveis para as unidades administrativas da SEDU, temos:

Pasta nos servidores da SEDU/PRODEST – ao optar por essa forma de armazenamento, o setor deve estar atento para utilizar uma pasta acessível a todos, evitando o uso de pastas pessoais, mesmo que sejam institucionais. No entanto, apesar de esse método ser o mais comum entre os diversos setores da SEDU, ele não é acessível às escolas.

Pasta em serviços de armazenamento em nuvem – se o setor possui conta institucional da Microsoft, pode usar uma pasta no OneDrive, ou se possui uma conta institucional do Google, pode usar o Google Drive. Mas, assim como na opção anterior, cada setor também deve se atentar para o uso de uma pasta que não seja vinculada a uma conta pessoal, mesmo que seja institucional.

Processo no E-Docs – nesse caso o setor pode optar por entranhar os termos em um processo já existente e relacionado à ação específica que gerou a necessidade de solicitar consentimento das pessoas titulares. Outra opção é criar um processo específico para os Termos de Consentimento, onde será realizada toda a gestão do consentimento de uma determinada ação ou do setor em si mesmo.

Mantenha os Termos de Consentimento rastreáveis – Também é muito importante saber onde encontrar o(s) termo(s) assinado(s) por uma pessoa específica e onde estão os dados pessoais a que esse termo se refere. Lembre-se que é direito da pessoa titular saber sobre como você trata os dados dela, assim como é um direito poder revogar, a qualquer tempo, um consentimento dado anteriormente.

Assim, caso seja solicitado identificar se uma pessoa forneceu um consentimento e, em caso positivo, revogar o termo e remover todos os dados a ele associados, será preciso ter uma forma de rastreio que seja efetiva e funcional!

Use uma planilha de controle dos termos – uma solução bem simples para o controle dos Termos de Consentimento é registrar em uma planilha as informações necessárias para garantir o controle do setor, tais como:

- **Ação/Projeto –** qual a ação ou projeto a que o termo está associado?
- **Titular –** qual o nome da pessoa a quem os dados se referem?
- **Menor de idade –** SIM ou NÃO?
- **Responsável Legal –** se a pessoa titular é menor de idade, quem é seu responsável legal?
- **Dados Pessoais –** qual ou quais dados pessoais a que se refere o termo?
- **Localização do Termo –** onde o termo está armazenado? Se for online pode-se usar um link!
- **Localização dos dados –** onde estão os dados a que o termo se refere? Se for online pode-se usar um link!

Tratando dados de imagem por fotos ou vídeos

Nesta seção, vamos abordar como a LGPD se aplica ao uso de imagens de estudantes, servidores e demais pessoas que frequentam o ambiente de uma escola ou unidade administrativa.

Para começar, é importante lembrar que a LGPD considera como dado pessoal qualquer informação que possa identificar uma pessoa, seja ela direta ou indiretamente. Isso significa que fotos e vídeos que permitem identificar uma pessoa são considerados dados pessoais e, portanto, estão sujeitos às regras da LGPD. Além disso, se essa imagem puder, por qualquer técnica, ser usada para fins biométricos, **ela se torna um dado pessoal sensível**!

Assim, para garantir que você está utilizando as imagens de forma legal e ética, é importante se perguntar:

- A imagem é realmente necessária para a atividade proposta?
- Preciso do consentimento do titular dos dados para usar essa imagem?
- Quais medidas posso tomar para proteger a privacidade dos alunos e responsáveis?

Tirei foto de todos no evento de ontem e postei

Sem pedir a autorização de ninguém

Importante lembrar que **a LGPD não se aplica aos casos de tratamento de dados realizado por pessoa física, para fins exclusivamente particulares e não econômicos**! (LGPD, art. 4º, inciso I)

Ou seja, se um familiar tira fotos de estudantes durante um evento escolar, não deve ser impedido com base na LGPD. No entanto, vale orientar para que todos usem o bom senso, evitando postar fotos de outras pessoas em suas redes sociais, por exemplo, sem a devida autorização.

Dicas para o tratamento de imagens para documentos e cadastros oficiais

Fotos utilizadas para registro em documentos e cadastros oficiais - Fotos de estudantes, servidores e demais cidadãos, coletadas, armazenadas e utilizadas para documentos e cadastros oficiais (digitais ou impressos), sejam eles criados ou administrados pelo seu setor, são tratados visando a oferta do serviço público. Por isso, **não exigem o consentimento**.

Mantenha as pessoas titulares informadas sobre o tratamento de seus dados de imagem - Mantenha as pessoas titulares informadas sobre o uso de sua imagem, assim como dos outros dados pessoais tratados em conjunto. Pode ser usado um Termo de Ciência ou um Aviso de Privacidade específico para a ação que gerou esse cadastro.

Evite incluir novas finalidades para o tratamento de imagens - Não reutilize as fotos para outros fins, que não seja aquele informado previamente à pessoa titular, ou seja, para o registro em documentos e cadastros oficiais.

Imagens tratadas para documentos e cadastros oficiais não devem ser expostas em locais de grande circulação - Não exponha as imagens coletadas em locais que permitam o acesso ou a visualização por terceiros, sem as devidas autorizações.

Não publique as imagens em redes sociais – Se a finalidade informada às pessoas titulares foi a de usar a imagem na composição de um cadastro, seu setor não pode reutilizar essa imagem publicando-a em redes sociais institucionais ou pessoais.

Dicas para o tratamento de imagens de sistemas de videomonitoramento

Imagens obtidas a partir de sistemas de videomonitoramento - Imagens de estudantes, servidores ou de cidadãos, coletadas e armazenadas a partir de sistemas de videomonitoramento instalados nas unidades de ensino, nas SREs ou na Unidade Central da SEDU, têm como finalidade monitorar o ambiente da instituição pública, identificar seus frequentadores e registrar eventuais incidentes que coloquem em risco tanto sua segurança pessoal, quanto a segurança do patrimônio público. **Essa finalidade atende a expectativa dos titulares** de garantia da segurança e, por isso, **não exigem o consentimento**.

Mantenha as pessoas titulares informadas sobre o tratamento de seus dados de imagem - Mantenha as pessoas titulares informadas sobre o uso de sua imagem, assim como dos outros dados pessoais que eventualmente venham a ser usados no relatório. Pode ser usado um Termo de Ciência ou uma Política de Privacidade da ação/projeto.

Imagens coletadas por sistemas de videomonitoramento não devem ser expostas em locais de grande circulação – O ambiente que abriga a central de monitoramento deve ser uma sala protegida, preferencialmente mantida trancada e com acesso restrito.

Cuidados com solicitações de terceiros para visualização ou cópias dos arquivos de monitoramento – Caso receba essas solicitações:

- Não forneça cópias dos arquivos, se contiver imagens de outras pessoas além da pessoa solicitante;
- Oriente a pessoa solicitante que formalize Boletim de Ocorrência em uma Delegacia da Polícia Civil;
- No ato da lavratura do BO, a pessoa deve solicitar que a autoridade policial (delegado) requeira as imagens desejadas, informando o período e o local da(s) câmera(s).
- **A cópia do arquivo de imagem deve ser fornecida ao(à) Delegado(a)** ou outra pessoa por ele(a) designada e **nunca à pessoa solicitante, mesmo que ela apresente o BO**.

Dicas para o tratamento de imagens para fins de prestação de contas de projetos

Imagens de foto ou vídeo utilizadas para fins de prestação de contas - Imagens de estudantes, docentes e demais profissionais da educação, obtidas com a finalidade de gerar evidências fotográficas da prestação de um serviço ou para produzir um relatório fotográfico da realização de uma ação ou projeto realizado pela escola, pela SRE ou pela Unidade Central da SEDU, atendem a exigências legais de controle e transparência na prestação do serviço público. Por isso, **não exigem o consentimento** da pessoa titular.

Mantenha as pessoas titulares informadas sobre o tratamento de seus dados de imagem - Informe sobre o uso da imagem, assim como dos outros dados pessoais tratados em conjunto. Pode ser usado um Termo de Ciência ou um Aviso de Privacidade específico para a ação que gerou essa necessidade de registro.

Evite incluir novas finalidades para o tratamento de imagens - Não reutilize as fotos para outros fins, que não seja aquele informado previamente à pessoa titular, ou seja, para o registro e prestação de contas de uma determinada ação ou projeto que participaram.

Imagens tratadas para registro e prestação de contas não devem ser expostas em locais de grande circulação - Não exponha as imagens coletadas em locais que permitam o acesso ou a visualização por terceiros, sem as devidas autorizações.

Se vai para o E-Docs, classifique como SIGILOSO – Se a prestação de contas será tramitada pelo E-Docs, dê preferência para colocar as fotos em um ANEXO que possa ser entranhado como uma peça separada para ser classificada como SIGILOSA. Caso isso não seja possível, crie duas versões do arquivo, **uma em nível SIGILOSO**, com as imagens devidamente expostas para a prestação de contas **e outra em nível ORGANIZACIONAL**, com as imagens anonimizadas.

Não publique as imagens em redes sociais – Se a finalidade informada às pessoas titulares foi a de usar a imagem para registro e prestação de contas, seu setor não pode reutilizar essa imagem publicando-a em redes sociais institucionais ou pessoais. Se julgar necessário, solicite o consentimento das pessoas, cujas imagens foram capturadas na foto ou vídeo.

Dicas para o tratamento de imagens para fins de registro e/ou divulgação de eventos ou atividades educacionais

Imagens utilizadas para registro e/ou divulgação de eventos ou atividades educacionais - Imagens de servidores e demais cidadãos, obtidas para fins de registro e/ou divulgação de eventos ou atividades esportivas, culturais ou científicas, realizadas pela escola, pela SRE ou pela Unidade Central da SEDU, atendem a um interesse legítimo da Secretaria, mas que pode ferir os direitos e liberdades fundamentais da pessoa titular. Por isso, **esses casos podem exigir a solicitação do consentimento**.

Considere, em primeiro lugar, os direitos e liberdades fundamentais da pessoa titular – O tratamento de imagens, seja na forma impressa (quadros, cartazes, etc.) ou digital (filmes, apresentações, sites, redes sociais, etc.), deverá levar em conta sempre o direito das pessoas nelas expostas:

- Informe, de forma clara e ao nível de entendimento de cada um, como e onde as imagens serão usadas;
- Se não é essencial para a oferta do serviço público, a pessoa pode se recusar a ter sua imagem capturada;
- Menores de 18 anos, caso tenham interesse e compreensão dos fatos, possuem o direito de participar da decisão sobre a captura de sua imagem em uma foto ou vídeo.

Se os direitos e liberdades fundamentais são respeitados - Nesse caso, considera-se o legítimo interesse da SEDU em registrar e divulgar as ações desenvolvidas para a população, assim como o sucesso das(os) estudantes e o que eles desenvolvem na escola.

- As pessoas deverão ser informadas, verbalmente ou por escrito, que durante o evento/atividade serão obtidas imagens que poderão ser divulgadas em sites e/ou redes sociais institucionais, estando livres para recusar sua participação nas fotos ou vídeos.

Se houver risco de algum direito ou liberdade fundamental não ser respeitado - Pode ser solicitado o consentimento da pessoa titular ou de seu responsável legal, mediante assinatura do Termo de Consentimento, cujo modelo encontra-se no site da SEDU (veja as regras para o consentimento na seção anterior!).

Dicas para o tratamento de imagens realizado por terceiros, contratados ou não

Imagens tratadas por terceiros contratados – Caso a escola, ou qualquer outra unidade administrativa contrate uma empresa ou uma pessoa profissional da área de audiovisual (fotógrafos, cinegrafistas, etc.), é necessário estabelecer em contrato todos os cuidados com dados pessoais, em especial os dados de imagem.

Observe as Minutas Padronizadas da PGE - A Procuradoria-Geral do Estado do Espírito Santo – PGE/ES mantém em seu site minutas padronizadas para casos que envolvem a LGPD, tanto na seção **TÓPICOS EXTRAS** , quanto na na seção **OUTROS**. Verifique se o contrato do serviço que pretende celebrar se adequa a algum dos casos apresentados pela Procuradoria!

Deixe claras as responsabilidades de cada um – Independentemente do documento contratual utilizado, é importante deixar claro o papel de cada um. Seja uma pessoa física ou uma pessoa jurídica, a LGPD entende se tratar de um OPERADOR, que atua sob ordens da SEDU, sendo seu setor o representante da Secretaria. Então, cuide para estabelecer os padrões mínimos de qualidade e segurança do serviço a ser prestado.

Imagens tratadas por terceiros voluntários – Caso uma pessoa, profissional da área de audiovisual ou não, se voluntarie para tratar imagens, entende-se que não haverá, necessariamente, um contrato de prestação do serviço. No entanto, ainda é necessário estabelecer os padrões mínimos de segurança com os dados pessoais a serem tratados.

Use um Termo de Confidencialidade – trata-se de um complemento do instrumento contratual, mas suficiente neste caso do voluntário. Ele deve conter o padrão de segurança necessário para garantir que todas as imagens sejam integralmente entregues ao responsável ao final do serviço prestado voluntariamente.

Seja um terceiro contratado ou um voluntário, caso seja programada a entrega das imagens diretamente aos titulares, estabeleça medidas de segurança para que cada um tenho acesso somente às suas próprias imagens.

Ou seja, evite compartilhar uma pasta online com todas as fotos/vídeos dos participantes de um evento, por exemplo, para cada um procurar por conta própria e salvar em seu computador ou dispositivo móvel.

Exemplo – Imagem em Plano Geral

Estudantes da EEEFM Aldy Soares Merçon Vargas em apresentação para o projeto "Descoloniza Aldy".
Fonte: Assessoria Especial de Comunicação da Sedu.

- **São as mais adequadas ao caso de legítimo interesse da SEDU -** Imagens com grande quantidade de pessoas e que capturam um plano mais geral são as mais adequadas para ampla divulgação e em caso de uso da hipótese de tratamento do legítimo interesse por qualquer unidade administrativa da Secretaria.
- **Não necessitam de consentimento –** Nesses casos não é necessário solicitar a assinatura de um Termo de Consentimento, mas as pessoas precisam ter ciência de que o evento/atividade está sendo filmado e/ou fotografado.
- **Informe e dê a oportunidade de se recusar –** As pessoas precisam ter a oportunidade de se recusar a ter sua imagem capturada, seja por foto ou por vídeo. Um simples aviso verbal pode ser o suficiente para que as pessoas presentes se posicionem como desejarem.
- **Pode publicar essas imagens em sites e redes sociais institucionais –** Imagens assim, podem ser divulgadas em redes sociais, sites, etc.

Exemplo – Imagem de pequenos grupos de pessoas

Estudantes da EEEFM Narceu de Paiva Filho apresentam trabalhos de Projeto de Vida. Fonte: Assessoria Especial de Comunicação da Sedu.

Imagens de pequenos grupos de pessoas exigem maior atenção - Em especial quando se tratam de imagens de crianças e adolescentes! Nesse caso, há o risco de todos serem facilmente identificáveis por seus conhecidos. Na maioria das situações, são imagens mais adequadas para uso em registros internos e em relatórios de prestação de contas de ações e projetos.

A necessidade de consentimento depende de cada caso – Se o evento ou atividade estiver relacionada diretamente ao serviço público na área da Educação, NÃO será necessário o consentimento. Mas, se for uma atividade que NÃO é própria da Educação, ou da função pública da SEDU, a assinatura de um Termo de Consentimento é obrigatória.

Informe e dê a oportunidade de se recusar – De todo modo, as pessoas precisam ter ciência de que o evento ou atividade está sendo filmado e/ou fotografado. E lembre-se de dar a oportunidade de se recusar a ter sua imagem capturada, seja por foto ou por vídeo. Um simples aviso verbal ou por escrito no convite do evento pode ser o suficiente.

Estudantes da rede pública estadual no evento do "Projeto Boas-vindas", que marcou o início dos cursos de Educação Profissional Técnica Concomitante ao Ensino Médio, em parceria com o IFES.
Fonte: Assessoria Especial de Comunicação da Sedu.

Solicite o consentimento antes de usar imagens em sites e redes sociais – Se quiser divulgar essas imagens em sites e redes sociais institucionais, seu setor deverá solicitar o consentimento. Lembrando que em casos de crianças e adolescentes o consentimento deve ser fornecido por um dos pais ou pelo responsável legal.

Ao divulgar externamente, evite associar outros dados pessoais às imagens – Será mais fácil garantir o direito à privacidade de cada um se as fotos não forem associadas a outros dados, como nome, idade, turno escolar ou de trabalho, etc. Use apenas os dados necessários para divulgar o evento ou atividade.

Imagens de servidores no exercício da função podem ser divulgadas institucionalmente – Imagens de servidores durante participações em eventos e ações institucionais, podem ser divulgadas em redes sociais e sites institucionais, desde que o objetivo seja garantir a transparência e a prestação de contas dessa ação ou evento. Sempre que possível, as pessoas deverão ser informadas da possibilidade de recusar-se a participar da foto ou vídeo.

Exemplo – Imagem ocultada ou anonimizada

Estudantes da EEEM Misael Pinto Netto participam de aula no recém-inaugurado Laboratório de Ciências e Cultura Maker. (imagem alterada)
Fonte: Assessoria Especial de Comunicação da Sedu.

Caso o consentimento seja negado ou revogado – Cada pessoa tem o direito de determinar o que será feito com seus dados pessoais. Quando visamos garantir o acesso a serviços públicos, nem sempre isso é possível, mas sempre que for, deve ser respeitado!

Ao divulgar externamente, use recursos de anonimização – Caso o consentimento ou autorização para a exibição da imagem não sejam obtidos, uma solução possível é a anonimização ou a ocultação do rosto das pessoas que não autorizaram, de modo que não seja possível identificá-las. No exemplo ao lado, a foto original, obtida no site da SEDU, foi copiada no Microsoft Powerpoint e pra cada pessoa foi usado um tipo de ocultação (dá pra fazer alguns deles também direto nos apps das redes sociais ou de imagem):

- Ícone temático;
- Emoji temático;
- Desfoque (este é o mais trabalhoso, mas dependendo do uso da imagem pode ter um melhor resultado estético).

Exemplo – Foto ou vídeo individual

Aluna posando com vestido de festa junina. Fonte: Revista Crescer.

- **Trate esse tipo de imagem somente após o consentimento da pessoa ou de seu responsável –** Esse tipo de imagem merece o total cuidado, principalmente quando for de crianças ou adolescentes! Trate as fotos de estudantes sozinhos apenas após obter a autorização dos pais ou responsáveis e se for para:
  - Registro e/ou divulgação de uma atividade didática, científica, cultural ou esportiva; ou
  - Composição de portfólio da(o) estudante ou de seu acervo pessoal e/ou de seus familiares.
- **Use apenas para a finalidade informada –** As imagens não devem ser usadas para outra finalidade além da informada às pessoas e/ou seus responsáveis legais.
- **Proteja de acessos não autorizados –** As fotos não devem ser expostas para terceiros sem autorização da pessoa e de seus responsáveis legais.
- **Dê publicidade apenas após autorização –** Essas imagens só podem ser compartilhadas em sites e redes sociais sob autorização ou se a pessoa já tiver publicado em sua própria rede social, marcando a escola na postagem, por exemplo.

Tratando dados pessoais por aplicativos de mensagem

Em meio ao cenário atual, os aplicativos de mensagens instantâneas desempenham um papel fundamental, tanto em nossa comunicação interna, quanto externa. Por isso, é crucial reforçar as medidas de segurança para a proteção dos dados pessoais eventualmente compartilhados nessas plataformas.

Neste contexto, é imperativo garantir que o compartilhamento de dados pessoais (listas nominais, fichas com dados escolares, atestados médicos, imagens, etc.), seja tratado com o máximo de cautela e responsabilidade.

Por mais práticos que sejam esses aplicativos, a segurança vem em primeiro lugar. Então, sempre que puder utilizar um dos meios mais seguros, já citados nas seções anteriores, faça isso!

Lembre-se que é responsabilidade de cada setor adotar as medidas técnicas e administrativas mais adequadas às suas atividades de tratamento de dados!

Dicas para o tratamento de dados pessoais em aplicativos de mensagens

- **Use apenas para o que precisa ser instantâneo –** Se a mensagem não necessita de uma resposta instantânea, ou possui uma grande quantidade de informações, ou ainda precisa estar acessível facilmente a todos, evite o uso de aplicativos de mensagens. Talvez um e-mail possa lhe atender mais adequadamente nesses casos.
- **Se possível, use apps institucionais –** Além de garantir maior eficiência na comunicação e colaboração entre equipes, eles podem auxiliar na segurança dos dados e informações sigilosas, e garantir a conformidade regulatória para o seu setor.
- **Se seu setor tem acesso ao plano institucional da Microsoft –** nesse caso, você e sua equipe pode ter acesso ao Microsoft Teams institucional. Além de diversas ferramentas colaborativas do Microsoft 365, os arquivos podem ser compartilhados pelo OneDrive.
- **Se seu setor tem acesso ao plano institucional da Google –** nesse caso, o Gmail institucional fornece a ferramenta Google Chat incorporada a ele, e que também tem bons recursos de segurança e colaboração.
- **Se o único recurso for um aplicativo vinculado à sua conta pessoal –** Se, por exemplo, seu setor necessita de efetuar um contato com alguém externo à rede estadual, talvez lhe reste como opção usar um aplicativo vinculado a uma conta pessoal. Ainda assim é possível garantir o mínimo de segurança!
- **Ative o recurso de criptografia de ponta a ponta –** verifique se o aplicativo da sua preferência oferece o recurso de criptografia de ponta a ponta, que garante maior proteção dos dados durante a transmissão. Então ative esse recurso e oriente a pessoa que vai receber a mensagem a fazer o mesmo.
- **Proteja arquivos com criptografia e senha –** você pode usar os mesmo recursos de proteção já indicados para o envio de e-mail, como a proteção por senha.
- **Envie a mensagem somente pra quem deve e pode receber a informação –** Cuidado para não compartilhar informações sigilosas com a pessoa ou com o grupo errado. Esse é um dos mais simples incidentes de segurança que podem ocorrer com dados pessoais!

Práticas Obrigatórias definidas pela LGPD

O que não pode deixar de ser feito para estarmos de acordo com a Lei Geral de Proteção de Dados Pessoais

Registrando atividades de tratamento de dados pessoais

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal Nº 13.709/2018) exige dos agentes de tratamento:

> O controlador e o operador **devem manter registro das operações de tratamento de dados pessoais que realizarem**, especialmente quando baseado no legítimo interesse.
>
> *(Artigo 37 da LGPD)*

Esse **Registro das Operações de Tratamento de Dados Pessoais**, foi posteriormente designado pela Secretaria de Governo Digital e pela ANPD como:

- **Inventário de Dados Pessoais (IDP) –** descrito em 2021, no **Guia de Elaboração do Inventário de Dados Pessoais**, como documento primordial para atendimento do artigo 37 da LGPD. Já possui uma 2ª versão, de 2023.
- **Registro das Atividades de Tratamento (RAT) –** descrito, em 2022, na **Resolução CD/ANPD Nº 02/2022**, como um documento a ser usado de forma simplificada por agentes de tratamento de pequeno porte.

Como elaborar o RAT das atividades de tratamento de dados do seu setor?

Planeje o seu registro – Como o RAT é um documento crucial para identificar quais dados são tratados (e como são tratados) em seu setor, é importante planejar corretamente. Uma boa ferramenta para isso é o **diagrama SIPOC**, cujo nome vem de:

- **SUPPLIER** (FORNECEDOR) → É a pessoa, setor ou instituição que fornece os insumos para o processo
- **INPUT** (ENTRADA) → Série de passos em que os insumos são convertidos em produtos
- **PROCESS** (PROCESSO) → Série de passos em que os insumos são convertidos em produtos
- **OUTPUT** (SAÍDA) → É o conjunto de produtos ou serviços gerado após os insumos passarem pelo processo
- **COSTUMER** (CONSUMIDOR) → É a pessoa, setor ou instituição que recebe o produto ou serviço

Adequando o SIPOC à LGPD (seria um SIPPOC?) – para que fique mais adequado à LGPD, o diagrama precisa de mais um campo:

- **FORNECEDOR** → De onde vêm os dados?
- **ENTRADA** → Quais dados são necessários?
- **FINALIDADE** → Qual o objetivo a ser alcançado com esses dados?
- **PROCESSO** → Quais atividades de tratamento de dados serão realizadas?
- **SAÍDA** → Qual será o produto dessas atividades de tratamento?
- **CONSUMIDOR** → Quem consumirá o produto dessas atividades de tratamento?

Lembre-se que o SIPOC (ou SIPPOC) é uma etapa prévia, que prepara para o RAT – em uma organização mais simples, pode ser até um modelo de RAT. Mas, em nosso caso, é uma ferramenta de planejamento para o RAT, **que não é obrigatória**. O RAT segue a mesma lógica, mas é uma planilha com mais campos a preencher, como será visto a seguir.

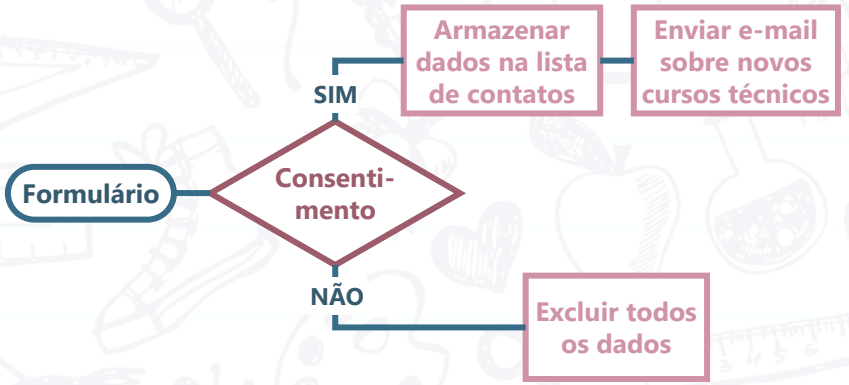
Como usar o SIPPOC? – se seu setor optar por utilizar o diagrama, pode ser mesmo no formato de um diagrama ou já partir para o formato de planilha eletrônica, usando os campos como colunas da tabela:

FORNECEDOR	ENTRADA	FINALIDADE	PROCESSO	SAÍDA	CONSUMIDOR

Saiba mais sobre o SIPOC

Elabore um fluxograma da atividade de tratamento a ser registrada no RAT – Essa é outra ferramenta importante para planejamento do RAT! No entanto, ela é quase que obrigatória para atividades de tratamento mais complexas. Ou seja, a depender da complexidade da atividade, o fluxograma pode não ser feito, pode ser feito antes do RAT, ou ainda pode ser uma parte dele.

O fluxograma deve considerar o Ciclo de Vida dos Dados (CVD) – cada atividade de tratamento pode conter algumas ou todas as etapas do CVD, ou até mesmo ser uma etapa de um CVD mais amplo. O fluxograma pode ajudar a entender essa estrutura.



Agora vamos ao RAT – Como já foi dito, atualmente existem dois modelos vigentes e aplicáveis:

- **Inventário de Dados Pessoais (IDP) –** modelo mais completo, que consta no **Guia de Elaboração do Inventário de Dados**, do Ministério da Gestão e da Inovação em Serviços Públicos.
- **RAT para ATPP –** modelo mais simplificado, sugerido pela **Autoridade Nacional de Proteção de Dados Pessoais – ANPD** para uso pelos Agentes de Tratamento de Pequeno Porte - ATPP.

Conheça o IDP

Conheça o RAT para ATPP

O modelo RAT-SEDU – devido à complexidade dos dados tratados pelas unidades administrativas da SEDU, em especial os dados de crianças e adolescentes, o modelo adotado será uma adaptação do IDP para a área da Educação, com uma complexidade intermediária entre os dois modelos oficiais.

Quem deve preencher o RAT-SEDU – o responsável pelo preenchimento do RAT será sempre o(a) gestor(a) da unidade escolar ou administrativa responsável por demandar a atividade de tratamento de dados, ou uma pessoa por ele(a) designada.

Como preencher o RAT-SEDU do meu setor – enquanto não temos um sistema que centralize essas informações, **o Encarregado Interno pelo Tratamento de Dados Pessoais da SEDU se responsabilizará por centralizar todos os RAT-SEDU**, utilizando os recursos do OneDrive ou Google Drive institucionais. Assim, para preencher o RAT-SEDU, o(a) gestor(a) de cada setor deve solicitar o seu acesso ao formulário, ou da pessoa que designou para essa atividade, pelo e-mail:

encarregado.interno@sedu.es.gov.br

Observação: Alguns setores da Unidade Central já possuem um registro realizado anteriormente e que está sendo adaptado para o modelo atual.

Relatório de Impacto ao Tratamento de Dados Pessoais (RIPD)

O RIPD está definido na Lei Federal Nº 13.709/2018 (LGPD) da seguinte forma:

> Relatório de Impacto à Proteção de Dados Pessoais é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
>
> *(Artigo 5º da LGPD, inciso XVII)*

Ou seja, trata-se de mais um importante documento a ser elaborado por quem trata dados pessoais. E podemos extrair três características importantes dessa definição:

- **É uma documentação do controlador –** ou seja, somente o setor que tem o poder de decisão sobre o tratamento dos dados é que tem essa obrigação.
- **Descreve processos que podem gerar riscos –** é um documento que se origina a partir do mapeamento dos riscos que podem ser causados aos titulares.
- **Descreve como mitigar os riscos –** parte do princípio de que, se o risco é conhecido, é possível encontrar uma solução para eliminá-lo ou suavizar seu impacto.

O gestor do projeto relendo o RIPD e descobrindo como o incidente de segurança foi possível.

Como elaborar o RIPD para uma atividade de tratamento de dados pessoais?

Comece pelo RAT – Se seu setor já possui o Registro das Atividades de Tratamento devidamente elaborado, ele será o ponto de partida para a elaboração do Relatório de Impacto.

Quanto mais detalhado o RAT, mais fácil será para elaborar o RIPD!

Avalie se há possibilidade de riscos – a partir do detalhamento da atividade no RAT, faça um mapeamento das possibilidades de risco de:

Descumprimento de obrigações legais – existe risco de descumprir alguma exigência da LGPD ou de alguma outra legislação ou regulamento vigente e aplicável ao caso?

Desrespeito aos direitos da pessoa titular – existe risco de desrespeito a algum direito da pessoa titular dos dados pessoais previsto na LGPD ou em alguma outra legislação ou regulamento vigente e aplicável ao caso?

Falhas de segurança – existe risco (interno ou externo) de roubo, perda de acesso, acesso indevido, alteração indevida ou destruição/eliminação de dados, sejam acidentais ou intencionais, inclusive dentre aqueles provocados por causas naturais?

Registre as medidas adotadas para a gestão dos riscos identificados – A identificação e análise dos fatores de risco devem ser documentadas e justificadas para que possam demonstrar que foram tomadas as medidas mais adequadas com base nas informações disponíveis. A avaliação de risco dificilmente irá representar a totalidade dos fatores de risco envolvidos na atividade de tratamento, mas será sempre melhor do que o total desconhecimento desses fatores.

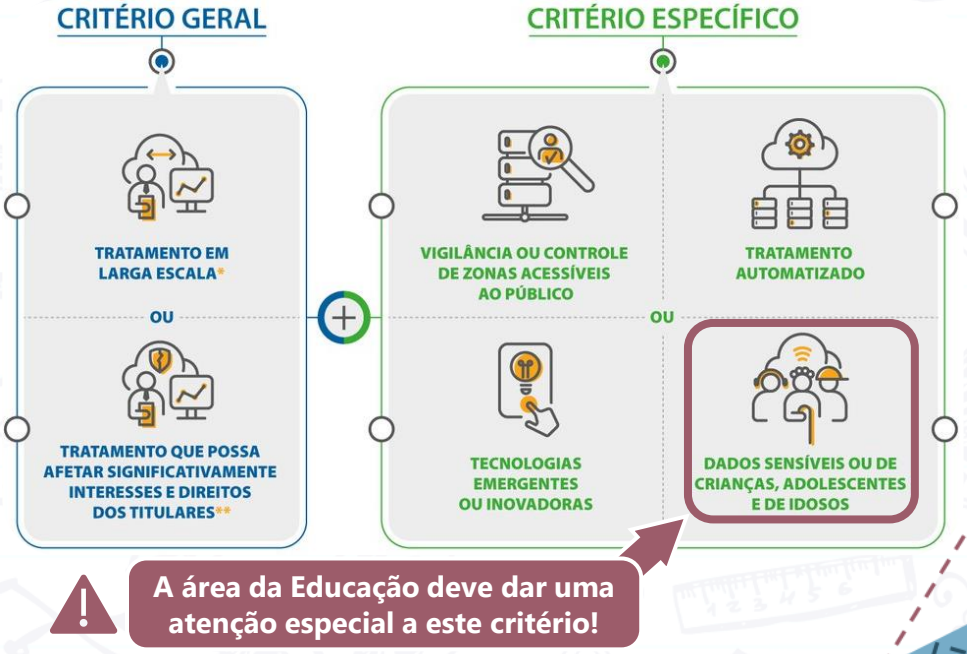
Cabe ao controlador identificar o maior número possível de fatores de risco – para cada fator identificado, seu setor deve estimar a probabilidade de materialização do risco e o impacto inerente. Esse impacto dependerá dos danos que possam ser causados aos titulares, em particular no âmbito dos seus direitos e liberdades.

Avalie os efeitos de múltiplos riscos – a existência de múltiplos fatores de risco pode aumentar o nível de risco da atividade de tratamento. Nesse caso, também é necessário interpretar como esses fatores podem interagir entre si para aumentar o nível de risco do tratamento, analisando suas dependências e efeitos combinados ou as suas interações mútuas.

Registre as medidas de mitigação dos riscos – Assim como registrou os fatores de risco, seu setor deve registrar o planejamento com relação às medidas, salvaguardas e mecanismos de mitigação dos riscos identificados.

Não tente reinventar a roda – a gestão de riscos pode ser feita por diferentes metodologias e a inovação é sempre bem-vinda! No entanto, recomenda-se adotar aquelas medidas que já são reconhecidas como boas práticas pela comunidade técnica de segurança, privacidade e proteção de dados. E, se surgirem dúvidas sobre qual medida adotar, peça apoio das equipes especialistas (GTI, Encarregado Interno da SEDU, etc.).

Há casos de "alto risco" para fins de elaboração do RIPD? – Na falta de um regulamento específico sobre o RIPD, podemos adotar, no que couber, o conceito de alto risco definido no artigo 4º da Resolução CD/ANPD Nº 02/2022 (Regulamento dos ATPP). Ou seja, o alto risco existirá se for verificada a presença de, ao menos, um critério geral e um critério específico:



Pode ser feito um RIPD único para todas as atividades de um setor? – Em geral, um RIPD deve corresponder a cada projeto/processo que contenha um conjunto de atividades de tratamento voltadas para uma mesma finalidade. Em alguns casos, isso pode se traduzir em relatórios diferentes para cada atividade de tratamento, especialmente se o seu setor possuir atividades muito distintas.

Dependendo da complexidade é melhor optar por vários RIPD – Ao elaborar relatórios separados para um conjunto de atividades de tratamento que possuam a mesma finalidade, é possível visualizar melhor as atividades realizadas e identificar com maior precisão os riscos associados a elas.

Em caso de haver semelhanças entre as atividades, um único RIPD pode ser elaborado – se o seu setor realiza múltiplas atividades de tratamento, que sejam **similares em termos de natureza, finalidade e riscos**, é razoável que seja elaborado apenas um RIPD que inclua todas essas atividades de tratamento.

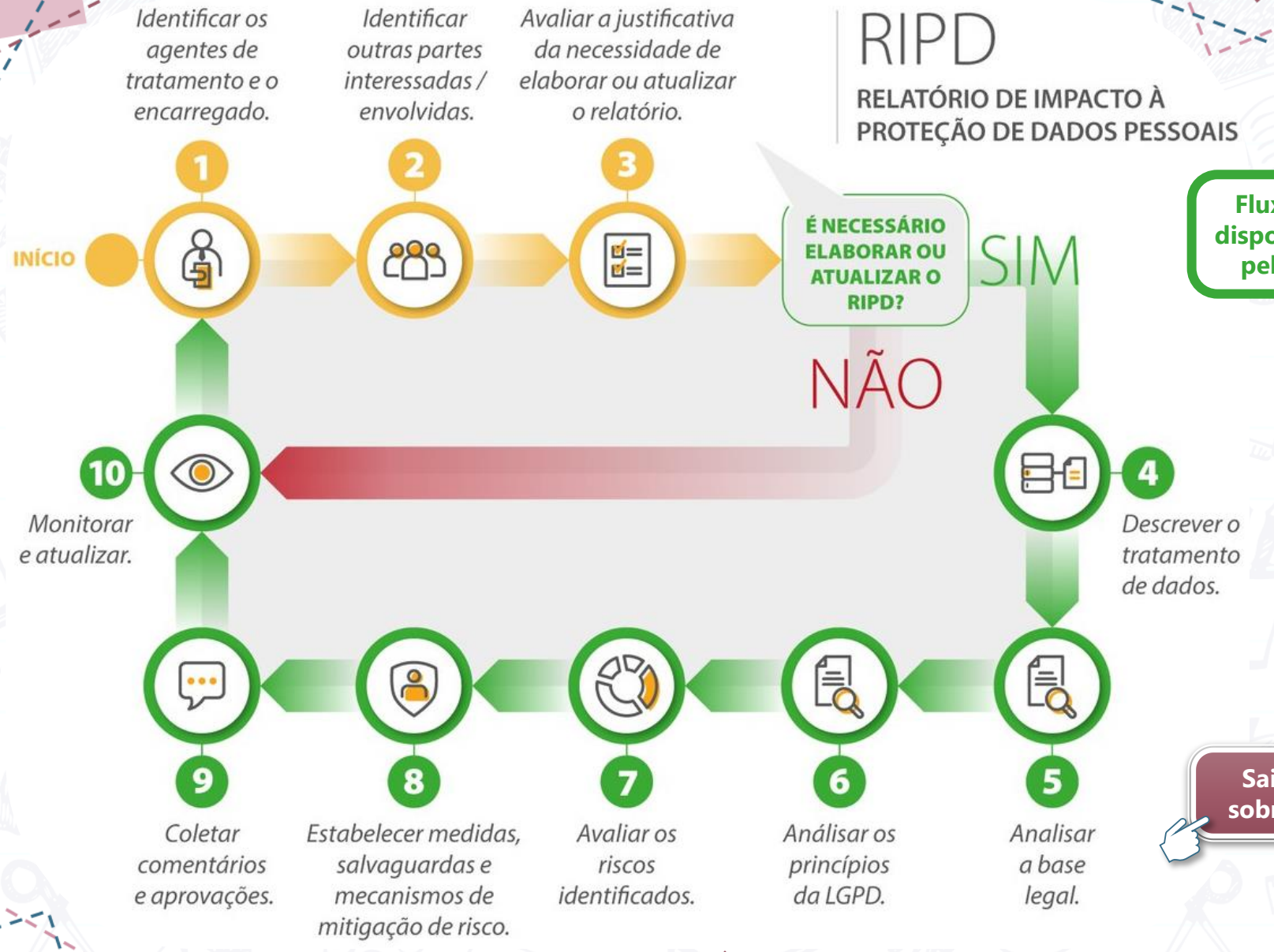
Se outro setor ou órgão/instituição também tiver poder de decisão, cada um faz o seu RIPD – em cenários em que há compartilhamento de dados pessoais entre diferentes controladores (Controladoria Conjunta), cada controlador poderá ser responsável por um RIPD, **ainda que utilizem uma plataforma compartilhada**, uma vez que as finalidades das atividades de tratamento de cada um podem ser distintas.

O operador não tem obrigação, mas pode auxiliar na elaboração do RIPD – eventuais operadores envolvidos na atividade de tratamento não são obrigados a elaborar um RIPD. No entanto, seu apoio pode ser solicitado para a elaboração do RIPD do seu setor.

Qual o modelo de elaboração do RIPD? – A ANPD disponibilizou um único modelo de RIPD, que também foi adaptado para atender as necessidades da SEDU e de suas unidades escolares e administrativas. Assim ao solicitar credenciamento para acessar a pasta com o formulário do RAT-SEDU, também receberá o acesso ao formulário do RIPD.

RIPD

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS



Fluxograma disponibilizado pela ANPD

Saiba mais sobre o RIPD

Comunicação de incidentes de segurança

A Lei Federal Nº 13.709/2018 (LGPD) determina, em caso de incidentes de segurança:

> O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> *(Artigo 48 da LGPD, caput)*

No entanto, a **Política Estadual de Proteção de Dados Pessoais e da Privacidade – PEPDP** (Decreto Estadual Nº 4.922-R/2021) determina que todos os órgãos e entidades do Poder Executivo Estadual realizem essa comunicação ao **Comitê Encarregado Central** (**CEC**) que, por sua vez, cumprirá as determinações do artigo 48 da LGPD:

> O controlador, **através do Comitê Encarregado Central**, deverá comunicar à ANPD e aos titulares dos dados a ocorrência de qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos moldes do art. 48, §1º da Lei Geral de Proteção de Dados.
>
> *(Artigo 19 da PEPDP)*

Como relatar um incidente de segurança no tratamento de dados pessoais?

O que é um incidente de segurança? – Uma boa definição a ser seguida pelas unidades escolares e administrativas da SEDU foi disponibilizada pelo Comitê Encarregado Central na **Resolução CEC Nº 02/2022**:

> Para os fins da presente Resolução, considera-se "incidente de segurança da informação" (ou simplesmente "incidente de segurança") o **evento que, envolvendo o tratamento de dados pessoais** no âmbito Administração Pública Direta e Indireta do Estado do Espírito Santo, **possa comprometer quaisquer dos direitos garantidos pela LGPD aos titulares dos dados** pessoais objeto do incidente.
>
> *(Artigo 4º da Resolução CEC Nº 02/2022)*

Comunique imediatamente o Encarregado Interno da SEDU – Imediatamente após tomar conhecimento do incidente de segurança, comunique o Encarregado Interno pelo Tratamento de Dados Pessoais da SEDU.

Como comunicar? – solicite ao Encarregado o link do Formulário de Comunicação de Incidente pelo e-mail **encarregado.interno@sedu.es.gov.br**.

Quais informações são fornecidas no comunicado? – visando atender o que é solicitado ao Encarregado Interno pelo CEC em sua Resolução CEC Nº 02/2022, o Formulário de Comunicação de Incidente solicita:

- **Identificação do comunicante –** identificação e dados de contato de quem está relatando o incidente, incluindo o setor de atuação.
- **Localização do incidente –** identificação e dados de contato do setor onde ocorreu o incidente de segurança.
- **Resumo do incidente –** breve relato sobre como foi o incidente.
- **Data/hora do incidente –** quando o incidente ocorreu e quando foi detectado.
- **Descrição das informações afetadas –** descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de titulares afetados.
- **Riscos relacionados ao incidente –** indicação dos possíveis riscos relacionados a esse incidente e das consequências e efeitos negativos sobre os titulares.

- **Medidas de preventivas –** quais foram as medidas de segurança, técnicas e administrativas tomadas pelo setor, de acordo com a LGPD, para evitar esse tipo de incidente.
- **Medidas de resposta ao incidente –** resumo das medidas implementadas até o momento para controlar os possíveis danos.
- **Tipo de Comunicação de Incidente –** pode ser do tipo PRELIMINAR, ADICIONAL ou COMPLETA. Se tiver todas as informações acima, marque a opção COMPLETA. Caso não seja possível fornecer todas as informações, marque a opção PRELIMINAR. Nesse último caso, o setor deverá encaminhar novo formulário com as informações faltantes, marcando a opção ADICIONAL.

A Comunicação Adicional, contendo as informações que faltavam na Comunicação Preliminar, deverá ser encaminhada pelo setor no prazo máximo de 05 (cinco) dias úteis, contados da comunicação preliminar, salvo impossibilidade devidamente justificada.

Operadores também são obrigados a relatar incidentes ao Encarregado – conforme determina o artigo 20 da PEPDP, eventuais operadores (instituições contratadas ou parceiras que executam atividades de tratamento de dados sob ordens da SEDU, ou da SRE, ou da escola) **deverão comunicar ao Encarregado Interno da SEDU, no prazo máximo de 48 horas, a ocorrência de incidente de segurança** que possa acarretar riscos ou danos relevantes aos titulares.

O Encarregado comunica o incidente ao CEC – conforme determina a Resolução CEC Nº 02/2022, o Formulário de Comunicação de Incidente será revisado e encaminhado ao Comitê Encarregado Central pelo Encarregado Interno da SEDU.

O CEC comunica a ANPD – após ser notificado pelo Encarregado Interno, o Comitê Encarregado Central avalia e encaminha a comunicação de incidente para a ANPD.

Saiba mais sobre a comunicação de incidentes para a ANPD

Por enquanto ficamos por aqui! Mas, lembre-se que a Proteção dos Dados Pessoais e da Privacidade é um jogo que se joga junto!

Se precisar de apoio ou se notar algo incorreto, ou que falta no guia, não hesite em entrar em contato com o Encarregado Interno da SEDU:

encarregado.interno@sedu.es.gov.br

(27) 99902-2249

Grupo de Trabalho: "EITDP"

Imagem criada com IA (Bing / Dall-E)

Tu te tornas eternamente responsável pelos dados pessoais que tratas.

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria da Educação

Referências

- BRASIL. Presidência da República. **Lei Federal Nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD).
- CEARÁ. Governo do Estado. ÍRIS - Laboratório de Inovação e Dados do Governo do Ceará. **A Era dos Dados para o setor público: uma nova cultura organizacional analítica**.
- BRASIL. Universidade de Brasília. Comitê de Governança Digital. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR). **Mesa Limpa e Tela Limpa**.
- BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov). **Alertas e Recomendações do CTIR Gov**.
- KASPERSKY. Centro de Recursos. **O que é engenharia social?**.
- MICROSOFT. Central de Suporte. **Proteja-se contra phishing**.
- GOOGLE. Central de Ajuda do Gmail. **Denunciar spam no Gmail**.
- MICROSOFT. Central de Suporte. **Proteger um documento com senha**.
- AVG. Blog AVG Signal. **Como proteger um arquivo ou pasta com senha no Windows**.
- MICROSOFT. Central de Suporte. **Criptografar mensagens de e-mail**.
- GOOGLE. Central de Ajuda do Gmail. **Enviar e abrir e-mails confidenciais**.
- ESPÍRITO SANTO. Governo do Estado. Secretaria da Educação. **Informações sobre o E-Docs**.
- BRASIL. Presidência da República. Casa Civil. **Lei Federal Nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação (LAI).
- ESPÍRITO SANTO. Governo do Estado. **Lei Estadual Nº 9.871, de 09 de julho de 2012**. Regulamenta a LAI para a Administração Pública Estadual.

GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria da Educação

- ESPÍRITO SANTO. Governo do Estado. **Decreto Estadual Nº 3.152-R, de 26 de novembro de 2012**. Regulamenta a Lei Estadual Nº 9.871/2012.
- BRASIL. Ministério da Educação. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP). Manuais IFSP. **Tarjando (anonimizando) dados pessoais/sensíveis**.
- ESPÍRITO SANTO. Governo do Estado. Portal de Convênios. **Informativo SUBCONV/GECOV**.
- ESPÍRITO SANTO. Governo do Estado. Secretaria de Estado de Gestão e Recursos Humanos (SEGER). Portal de Contratos. **Informativos**.
- ESPÍRITO SANTO. Governo do Estado. **Decreto Estadual Nº 4.922-R, de 9 de julho de 2012**. Institui a Política Estadual de Proteção de Dados Pessoais e da Privacidade do Poder Executivo Estadual (PEPDP).
- BRASIL. Ministério da Gestão e da Inovação em Serviços. Governo Digital. Programa de Privacidade e Segurança da Informação. **Guias e Modelos**.
- BRASIL. Ministério da Gestão e da Inovação em Serviços. Governo Digital. Programa de Privacidade e Segurança da Informação. **Guia de Elaboração do Inventário de Dados**.
- BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados (ANPD). **ANPD divulga modelo de registro simplificado de operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP)**.
- BRASIL. Ministério da Gestão e da Inovação em Serviços. Governo Digital. Programa de Privacidade e Segurança da Informação. **Guia de Boas Práticas - LGPD**.
- BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados (ANPD). **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**.
- ESPÍRITO SANTO. Governo do Estado. **Decreto Estadual Nº 2.884-R, de 21 de outubro de 2011**. Institui a Política Estadual de Segurança da Informação no âmbito do Poder Executivo do Estado (PESI).

- ESPÍRITO SANTO. Governo do Estado. Secretaria de Estado do Governo. Comitê Encarregado Central. **Resolução CEC Nº 2, de 29 de novembro de 2022**. Disciplina, no âmbito da Administração Pública Direta e Indireta do Estado do Espírito Santo, os procedimentos administrativos a serem adotados em casos de incidente de segurança da informação no tratamento de dados pessoais.
- BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados (ANPD). **Comunicação de Incidente de Segurança**.

GOVERNO DO ESTADO DO ESPÍRITO SANTO

Secretaria da Educação