Guia de Segurança da Informação para

FUNCIONÁRIOS

SEGURANÇA DIGITAL
EDUCAÇÃO DO PARANÁ

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO

Ilustração

Debora Bacchi Camillo
Leandro Alves de Almeida
Will Stopinski

Projeto Gráfico/Diagramação

Joise Nascimento
Silvio Turra

Conteúdo e Elaboração

GOVERNADOR DO ESTADO DO PARANÁ
Carlos Massa Ratinho Junior

Secretário de Estado da Educação
Professor Roni Miranda Vieira

Diretor-Geral
João Luis Giona Junior

Diretor de Educação
Anderfábio Oliveira dos Santos

Diretor de Tecnologia e Inovação
Claudio Aparecido de Oliveira

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO

Este guia mostra como proteger informações no trabalho. Siga estas dicas para manter os dados seguros.

Controle de Acesso

Use senhas fortes e **verificação em duas etapas** para proteger suas contas

Proteção de Dados

Guarde dados importantes de forma segura e faça cópias de backup com frequência

Prevenção contra Golpes

Saiba **reconhecer emails falsos e links perigosos** para evitar ataques

Segurança de Equipamentos

Mantenha seus programas atualizados e cuide fisicamente dos equipamentos

Sumário

Introdução à Segurança da Informação

A segurança da informação é essencial para o funcionamento da administração pública. Os dados da Secretaria incluem informações sensíveis que devem ser protegidos contra ameaças.

Proteção de Dados Sensíveis

Os dados da Secretaria incluem informações de cidadãos, projetos governamentais e recursos públicos que precisam ser protegidos contra acessos não autorizados.

Integridade dos Sistemas

A manutenção da integridade dos sistemas utilizados é fundamental para evitar modificações indevidas e garantir a continuidade dos serviços públicos.

Confiança dos Cidadãos

A segurança da informação fortalece a confiança dos cidadãos nas instituições governamentais ao proteger dados contra divulgação ou destruição indevida.

Este guia oferece orientações práticas para proteger informações institucionais, melhorando a confiabilidade dos serviços prestados pela Secretaria.

Importância da Segurança da Informação

Proteção do Cidadão

As informações pessoais dos cidadãos representam uma responsabilidade crucial. Vazamentos podem causar prejuízos financeiros, danos à reputação e riscos à segurança física dos indivíduos.

Continuidade do Serviço Público

Falhas de segurança podem interromper serviços essenciais à população. A indisponibilidade de sistemas críticos afeta diretamente o atendimento ao cidadão e o funcionamento administrativo.

Conformidade Legal

A LGPD e outras leis estabelecem requisitos rigorosos para o tratamento de informações. O descumprimento pode resultar em severas penalidades para a instituição.

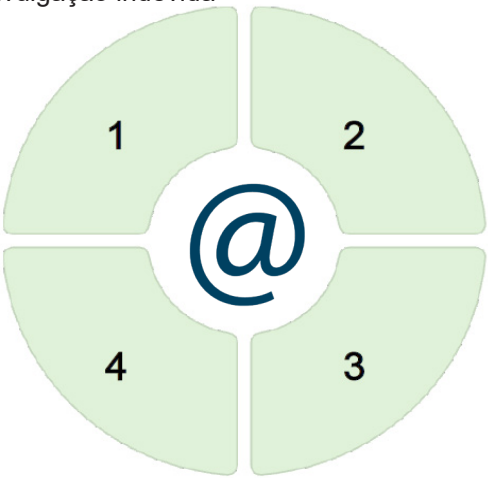
Princípios Básicos de Segurança da Informação

Confidencialidade

Garantir acesso restrito às informações apenas por pessoas autorizadas, evitando divulgação indevida

Integridade

Manter informações completas e inalteradas, preservando sua precisão e confiabilidade.



Autenticidade

Verificar identidades de usuários e origem das informações, confirmando sua legitimidade

Disponibilidade

Assegurar que sistemas e informações estejam acessíveis quando necessário, mantendo a continuidade dos serviços.

Estes quatro princípios fundamentam a segurança da informação e devem guiar o tratamento de dados e uso dos sistemas institucionais.

Responsabilidades do Funcionário

Cumprimento de Políticas

Conhecer e seguir as políticas de segurança da informação da Secretaria, participando dos treinamentos oferecidos.

Proteção de Credenciais

Proteger suas credenciais de acesso, **não compartilhá-las e utilizar senhas fortes** e únicas.

Vigilância Constante

Estar atento a vulnerabilidades ou incidentes de segurança, reportando-os imediatamente aos canais adequados.

Uso Consciente

Utilizar **recursos tecnológicos institucionais apenas para fins profissionais**, evitando exposição a riscos.

Cada funcionário é um elo essencial na segurança da informação. A conscientização e o comportamento responsável protegem os dados institucionais.

Controle de Acesso e Proteção de Dados

O controle de acesso adequado constitui a principal defesa na proteção de dados institucionais. Práticas seguras de autenticação e verificação garantem que apenas pessoas autorizadas acessem informações sensíveis.

A criptografia e outras ferramentas de segurança protegem os dados mesmo em casos de tentativas de acesso não autorizado. Esta seção apresenta as práticas recomendadas para um controle de acesso eficaz e proteção robusta dos dados da Secretaria.

Autenticação e Verificação

Autenticação Forte

Use senhas com mínimo de 12 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais. Evite utilizar dados pessoais identificáveis.

Dispositivos Confiáveis

Utilize apenas equipamentos institucionais para acessar sistemas internos. Evite computadores públicos e redes sem fio (wi-fi) não seguras.

Verificação em Duas Etapas (2FA)

Ative o 2FA em todos os sistemas disponíveis. Esta camada adicional protege o acesso mesmo se a senha for comprometida.

A autenticação adequada garante que somente pessoas autorizadas acessem dados institucionais. Proteja suas credenciais e nunca as compartilhe, mesmo com colegas.

Gerenciamento de Senhas

Use Senhas Únicas

Evite reutilizar senhas. Cada sistema deve ter uma senha exclusiva para minimizar riscos em caso de vazamento.

Utilize Gerenciadores

Use gerenciadores de senhas aprovados para armazenar credenciais com segurança e gerar senhas complexas automaticamente.

Atualize Periodicamente

Altere senhas regularmente, principalmente em sistemas com informações sensíveis, conforme política institucional.

Nunca Compartilhe

Jamais informe suas senhas por e-mail ou mensagens. O departamento de TI nunca solicitará sua senha por esses meios.

Proteção de Dados Sensíveis

A proteção de dados sensíveis exige medidas específicas para garantir confidencialidade e integridade. Use ferramentas de criptografia aprovadas pela instituição para arquivos confidenciais, principalmente ao compartilhá-los.

Classifique informações por sensibilidade (público, interno, confidencial, restrito) e aplique proteções adequadas a cada categoria. Em caso de dúvidas, consulte o departamento de segurança da informação.

Armazenamento Seguro

Servidores Institucionais

Armazene informações nos servidores oficiais da instituição, que contam com segurança e monitoramento regular.

Dispositivos Externos

Use apenas dispositivos fornecidos pela Secretaria, **evitando pendrives ou HD's externos pessoais**.

Nuvem Corporativa

Utilize somente soluções de nuvem aprovadas pela instituição, nunca serviços pessoais como Dropbox ou Google Drive.

Evite armazenar dados institucionais em dispositivos pessoais ou serviços não autorizados para não comprometer a segurança das informações.

Backups Regulares

Frequência Adequada

Realize backups dos dados conforme a periodicidade definida na política institucional para cada tipo de informação.

Verificação

Teste periodicamente a integridade dos backups para garantir sua correta restauração quando necessário.

Proteção

Armazene backups em locais seguros, separados fisicamente dos dados originais e protegidos contra acessos não autorizados.

Backups regulares são essenciais para a continuidade operacional em casos de falhas, ataques ou corrupção de dados.

Procedimentos para Backup de Sistemas Administrativos

Identificação

Identifique quais sistemas e dados precisam ser incluídos no backup, **priorizando informações críticas para o funcionamento da Secretaria**.

Agendamento

Configure backups automáticos para ocorrerem fora do horário de expediente, minimizando o impacto nas atividades diárias.

Armazenamento

Salve os backups em pelo menos dois locais diferentes, incluindo pelo menos um armazenamento offline ou em local fisicamente distante.

Documentação

Mantenha um **registro detalhado de todos os backups** realizados, incluindo data, conteúdo e localização, para facilitar a recuperação quando necessário.

PARANÁ GOVERNO DO ESTADO Secretaria da educação
SEGURANÇA DIGITAL EDUCAÇÃO DO PARANÁ

Uso de Computadores Institucionais

Uso Exclusivo para Sistemas Críticos

Utilize apenas computadores institucionais para acessar sistemas e processar informações da Secretaria, **nunca dispositivos pessoais**.

Proibição de Software Não Autorizado

Não instale softwares não autorizados nos equipamentos institucionais, preservando as medidas de segurança estabelecidas.

Configurações de Segurança

Mantenha as configurações de segurança definidas pelo departamento de TI, essenciais para a integridade do ambiente tecnológico.

Prevenção contra Golpes e Ameaças

A **engenharia social** é uma tática comum usada por criminosos para obter acesso não autorizado a sistemas governamentais. Aprenda a identificar e prevenir diferentes tipos de golpes digitais:

Phishing

E-mails fraudulentos que se passam por comunicações oficiais para obter dados sensíveis ou instalar malware em dispositivos institucionais.

Smishing

Mensagens de texto maliciosas que contêm links fraudulentos visando roubar informações pessoais ou credenciais de acesso.

Vishing

Ligações telefônicas onde criminosos se passam por instituições legítimas para manipular funcionários e obter informações confidenciais.

A vigilância constante é essencial para proteger dados institucionais e pessoais contra esses ataques cada vez mais sofisticados.

Identificação de E-mails Suspeitos

Remetente Desconhecido

Verifique o endereço de e-mail do remetente, especialmente ao solicitar informações sensíveis. Cibercriminosos usam domínios aparentemente legítimos com pequenas alterações.

Erros Gramaticais

Observe erros de português, formatação estranha ou inconsistências no estilo, que podem indicar fraude, mesmo quando aparentemente de contatos conhecidos.

Urgência Excessiva

Desconfie de mensagens que criam senso de urgência, pressionando para ações imediatas como “atualizar cadastro“ ou “confirmar senha”.

Anexos Inesperados

Não abra anexos não solicitados, principalmente com extensões .**bat, .exe, .zip, .msi, .scr ou .src**, mesmo se parecerem de fontes confiáveis.

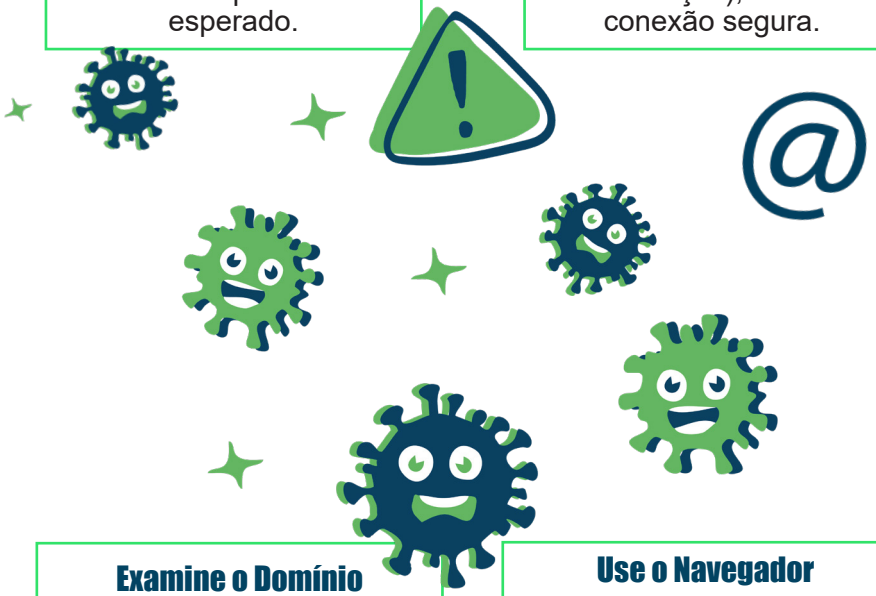
Como Identificar Links Maliciosos

Passe o Mouse

Antes de clicar em qualquer link, passe o cursor sobre ele (sem clicar) **para visualizar o endereço real** para onde ele direciona, verificando se corresponde ao esperado.

Verifique o Protocolo

Certifique-se de que **sites que solicitam informações sensíveis utilizem o protocolo HTTPS** (exibindo um cadeado fechado na barra de endereços), indicando conexão segura.



Examine o Domínio

Verifique cuidadosamente se o domínio corresponde exatamente ao oficial. Fraudadores frequentemente usam domínios semelhantes como "**secretaria-gov.com**" em vez de "secretaria.gov.br".

Use o Navegador Diretamente

Em caso de dúvida, em vez de clicar no link do e-mail, digite diretamente o endereço oficial no navegador ou use seus favoritos previamente salvos.

PARANÁ GOVERNO DO ESTADO Secretaria da educação
SEGURANÇA DIGITAL EDUCAÇÃO DO PARANÁ

Golpes Comuns Direcionados a Funcionários Públicos

Phishing Institucional

E-mails falsos imitando comunicações oficiais do governo que solicitam dados cadastrais ou credenciais de acesso a sistemas.

Vishing

Ligações fraudulentas de falsos profissionais de TI ou gestores pedindo informações sensíveis ou acesso remoto a equipamentos.

Documentos Falsos

Arquivos maliciosos disfarçados como documentos oficiais (planilhas, PDFs ou apresentações) contendo malware.

Smishing

SMS ou mensagens fraudulentas simulando alertas bancários ou notificações de RH com links maliciosos.

Canais de Comunicação Seguros

Comunicação Interna

Use apenas as ferramentas oficiais da instituição para assuntos de trabalho, evitando aplicativos pessoais de mensagens ou redes sociais.

Comunicação com Fornecedores

Utilize canais oficiais com fornecedores e confirme qualquer alteração solicitada (como dados bancários) por múltiplos canais antes de processar.

Comunicação Pública

Siga os protocolos institucionais para comunicações externas, verificando se as informações podem ser compartilhadas publicamente antes de enviá-las.

O uso de canais autorizados reduz riscos de vazamentos e ataques de engenharia social.

Monitoramento de Contas e Acessos

Revisão Regular

Verifique periodicamente as atividades em suas contas, observando acessos em horários incomuns ou de localizações desconhecidas.

Alertas de Segurança

Ative alertas para **receber notificações sobre logins** ou alterações importantes em suas contas.

Auditoria de Permissões

Revise periodicamente as permissões concedidas a aplicativos e serviços, revogando acessos desnecessários.

Reporte Anomalias

Informe imediatamente ao setor de segurança **qualquer atividade suspeita**, mesmo que pareça menor.

O Que Fazer em Caso de Suspeita de Acesso Não Autorizado

Isolamento

Desconecte o dispositivo da rede imediatamente para conter possíveis ameaças.

Comunicação

Notifique o departamento de segurança através dos canais oficiais estabelecidos.

Documentação

Registre horário, ações realizadas e comportamentos anômalos observados.

Seguir Orientações

Aguarde e **siga as instruções da equipe de segurança**, evitando iniciativas não autorizadas.

Segurança no Uso de Equipamentos

A segurança dos equipamentos que acessam informações institucionais é essencial para proteger dados sensíveis. Dispositivos desatualizados ou sem proteção adequada criam vulnerabilidades facilmente exploráveis.

Esta seção apresenta as práticas recomendadas para garantir a segurança dos dispositivos no ambiente de trabalho, incluindo atualizações de software e configurações de proteção contra ameaças digitais.

Atualizações de Software

Sistema Operacional

Mantenha o sistema operacional atualizado, aplicando as atualizações de segurança assim que disponibilizadas pela TI.

Aplicativos

Atualize todos os aplicativos regularmente, principalmente navegadores, leitores de PDF e ferramentas que processam arquivos externos.

Firmware

Aplique atualizações de firmware em roteadores, impressoras e demais equipamentos conectados à rede institucional.

Políticas de Atualização

Siga as políticas de atualização da instituição, incluindo janelas específicas para evitar interrupções nos serviços.

Proteção contra Malware

Antivírus

Mantenha o **antivírus sempre ativo e atualizado**. Nunca desative a proteção em tempo real por qualquer motivo.

Verificações Regulares

Execute **verificações completas periodicamente**, especialmente após mudanças, conectar dispositivos externos ou baixar arquivos.

Navegação Segura

Use as **extensões de segurança** recomendadas para identificar sites maliciosos e downloads perigosos.

A proteção contra malware previne infecções que podem comprometer dados sensíveis e sistemas institucionais.

Uso de Firewall

O firewall é um componente essencial da segurança institucional, funcionando como barreira de proteção entre dispositivos e possíveis ameaças da internet.

Funcionamento do Firewall

O firewall atua como barreira de proteção, monitorando e bloqueando constantemente o tráfego de rede conforme regras de segurança estabelecidas pela instituição.

Não Desative o Firewall

Nunca desative o firewall nos equipamentos institucionais, mesmo que temporariamente, para evitar exposição desnecessária a ameaças de rede.

Alteração de Configurações

Caso precise modificar configurações do firewall para uso específico de aplicações, consulte previamente o departamento de TI para orientações seguras.

Configurações de Segurança

Bloqueio Automático

Configure dispositivos para **bloquearem após curtos períodos de inatividade** (máximo 5 minutos), exigindo biometria ou senha para desbloqueio.

Criptografia de Disco

Use soluções de criptografia fornecidas pela instituição para proteger dados armazenados localmente, principalmente em dispositivos móveis.

Autenticação na Inicialização

Habilite autenticação obrigatória na inicialização dos dispositivos, impedindo acessos não autorizados em caso de perda ou roubo.

Restrição de Instalação

Mantenha restrições para instalação de aplicativos, permitindo apenas softwares aprovados e licenciados pelo departamento de TI.

Dispositivos Móveis

Separação de Contas

Mantenha **perfis separados para uso pessoal e profissional**, utilizando as funcionalidades de perfil de trabalho quando disponíveis.

Aplicativos Seguros

Instale apenas aplicativos de fontes oficiais e verifique as permissões solicitadas, especialmente para acesso a armazenamento, contatos, câmera ou microfone e localização.

Rastreamento e Limpeza Remota

Configure a localização e limpeza remota para ações rápidas em caso de perda ou roubo do dispositivo.

Dispositivos móveis representam um desafio para a segurança por transitarem entre ambientes pessoais e profissionais, exigindo cuidados específicos.

Proteção Física de Equipamentos

Trava de Segurança

Utilize travas físicas para notebooks em áreas de trabalho compartilhadas ou quando precisar se ausentar temporariamente, especialmente em espaços com acesso público.

Supervisão Visual

Mantenha os dispositivos institucionais sempre à vista ou armazenados em locais seguros quando não estiverem em uso, evitando deixá-los desacompanhados em áreas públicas.

Proteção contra Visualização

Utilize filtros de privacidade na tela de dispositivos utilizados em locais públicos ou áreas de atendimento para prevenir a visualização das informações por pessoas não autorizadas.

Condições Ambientais

Proteja os equipamentos contra condições ambientais adversas como calor excessivo, umidade ou poeira, que podem causar danos físicos e comprometer o funcionamento seguro.

Gerenciamento de Redes Sociais e Comunicação

As redes sociais e canais digitais são essenciais para interação pública, porém apresentam riscos quando mal gerenciados. Compartilhamentos inadequados podem comprometer operações, expor dados sensíveis e danificar a imagem institucional.

Esta seção apresenta práticas recomendadas para o gerenciamento seguro de contas oficiais, proteção contra divulgação indevida e configurações de segurança para presença institucional nas redes sociais.

Uso de Contas Oficiais

Autenticação Reforçada

Implemente **verificação em duas etapas para todas as contas oficiais** em redes sociais e plataformas de comunicação, reduzindo o risco de acesso não autorizado.

Credenciais Compartilhadas

Utilize ferramentas de gerenciamento de redes sociais aprovadas pela instituição e que permitam acesso diferenciado por perfil de usuário, evitando o compartilhamento de senhas.

Separação de Contas

Mantenha contas pessoais e profissionais estritamente separadas, nunca utilizando perfis pessoais para comunicações oficiais ou vice-versa.

Aprovação de Conteúdo

Implemente um processo de revisão e aprovação para publicações institucionais, especialmente para informações sensíveis ou durante situações de crise.

Divulgação de Informações

Classificação

Identifique o nível de sensibilidade da informação antes de compartilhá-la (pública, interna, confidencial, restrita).

Autorização

Verifique se você tem autorização para divulgar a informação conforme políticas institucionais.

Contexto

Avalie como a informação pode ser interpretada em diferentes contextos ou quando isolada de seu contexto original.

Revisão

Submeta informações sensíveis à revisão pelos canais apropriados antes da divulgação pública.

Impacto

Considere as possíveis consequências da divulgação para indivíduos, processos institucionais e segurança pública.

Orientação sobre Compartilhamento de Informações

Tipo de Informação	Compartilhável?	Canal Adequado	Cuidados
Informações públicas oficiais	Sim	Redes sociais, e-mail, canais oficiais	Verificar atualizações/ retificações
Dados pessoais de cidadãos	Não	Nunca compartilhar	Sujeito à LGPD
Documentos administrativos	Restrito	Apenas sistemas internos	Verificar classificação/ autorização
Fotos de ambientes institucionais	Restrito	Com autorização específica	Evitar exposição de dados sensíveis

Gestão de Permissões de Acesso

Inventário de Contas

Mantenha um registro centralizado de todas as contas institucionais em plataformas de mídia social e comunicação, incluindo responsáveis e níveis de acesso.

Revisão Periódica

Realize **auditorias regulares das permissões concedidas**, removendo acessos de colaboradores que mudaram de função ou deixaram a instituição.

Privilégio Mínimo

Conceda apenas o **nível mínimo de acesso necessário para cada função**, limitando permissões de administrador ao estritamente necessário.

Revogação Imediata

Estabeleça um **processo para revogação imediata** de acessos **quando um funcionário se desliga da instituição** ou muda de função.

Resposta a Incidentes em Redes Sociais

Detecção

Monitore regularmente as contas para identificar rapidamente atividades suspeitas, publicações não autorizadas ou interações anômalas.

Comunicação

Informe as partes relevantes (departamento de segurança, comunicação institucional e, se necessário, o público) sobre o incidente de forma transparente e responsável.

Contenção

Em caso de comprometimento, **altere imediatamente a senha, desconecte sessões ativas** e, se necessário, solicite à plataforma o bloqueio temporário da conta.

Recuperação

Restaure o controle seguro da conta, **verificando e corrigindo publicações** comprometidas e reforçando medidas de segurança para prevenir recorrências.

Proteção de Dados Pessoais em Comunicações Públicas

A LGPD estabelece diretrizes rigorosas para o tratamento de dados pessoais em comunicações institucionais. Verifique sempre a base legal antes de compartilhar qualquer conteúdo contendo informações pessoais, mesmo que parcialmente.

Não compartilhe capturas de tela de sistemas, documentos ou comunicações com dados pessoais identificáveis. Quando indispensável, utilize técnicas de anonimização ou pseudonimização para proteger a privacidade dos indivíduos.

Segurança em Videoconferências

Controle de Acesso

Utilize salas de espera e senhas para reuniões confidenciais, verificando a identidade dos participantes antes de permitir acesso à videoconferência.

Compartilhamento Seguro

Ao compartilhar tela, feche documentos e programas não relacionados à apresentação para evitar a exposição acidental de informações confidenciais.

Ambiente Controlado

Realize **videoconferências** que tratarão de temas sensíveis **em ambientes privados**, verificando o que está visível no plano de fundo e utilizando recursos de desfoque quando apropriado.

Gravações

Obtenha consentimento explícito de todos os participantes antes de gravar reuniões e estabeleça protocolos claros para o armazenamento e compartilhamento das gravações.

Vazamento de Dados: Como Proceder

Identificação

Documente os dados expostos, quando e como ocorreu o vazamento, registrando todas as informações relevantes para análise posterior.

Comunicação Interna

Notifique imediatamente o DPO e a equipe de segurança da informação, seguindo o protocolo do plano de resposta a incidentes.

Contenção

Limite a exposição removendo conteúdos indevidos, revogando acessos comprometidos e isolando sistemas afetados.

Resposta Oficial

Comunique as autoridades competentes dentro dos prazos estabelecidos pela LGPD, seguindo diretrizes institucionais.

Treinamento e Conscientização

A segurança da informação é um esforço coletivo que depende do engajamento e do conhecimento de todos os funcionários.

Participação Ativa em Treinamentos

Participar ativamente dos treinamentos oferecidos pela instituição é fundamental para desenvolver e manter as habilidades necessárias para identificar e responder adequadamente a ameaças à segurança da informação.

Compartilhamento de Conhecimentos

É importante compartilhar conhecimentos e alertas relevantes com colegas, contribuindo para uma cultura de segurança sólida dentro da Secretaria.

Cultura de Segurança

O **investimento em conscientização é uma das medidas mais eficazes** para prevenir incidentes de segurança na administração pública.

Recursos de Aprendizagem Disponíveis

Cursos Internos

Acesse os **cursos de segurança da informação na plataforma** de ensino à distância corporativa.

Workshops Práticos

Participe de simulações de ameaças reais como phishing para desenvolver habilidades de identificação de riscos.

Boletins de Segurança

Acompanhe os boletins periódicos com alertas sobre novas ameaças distribuídos pelo departamento de TI.

Base de Conhecimento

Acesse tutoriais, FAQs e procedimentos detalhados **na base de conhecimento interna** sobre segurança.

Contatos e Canais de Suporte

Tipo de Ocorrência	Canal de Contato	Horário
Phishing ou golpes	seguranca@ secretaria.gov.br	24h x 7 dias
Perda/roubo de dispositivos	(XX) XXXX-XXXX	24h x 7 dias
Dúvidas sobre segurança	suporte@ secretaria.gov.br	8h às 18h (dias úteis)
Vazamento de dados	dpo@secretaria. gov.br e (XX) XXXX-XXXX	24h x 7 dias
Solicitação de acesso	Sistema de chamados interno	8h às 18h (dias úteis)

Para emergências com dados sensíveis ou sistemas críticos, use os canais 24h mesmo fora do horário comercial.

Checklist de Segurança da Informação

Use esta lista regularmente para avaliar que você segue as práticas de segurança recomendadas. Identifique os itens já implementados e trabalhe para incorporar os demais à sua rotina.

Realize esta avaliação mensalmente e sempre após mudanças em seus dispositivos, responsabilidades ou sistemas. Em caso de dúvidas, consulte o departamento de segurança da informação.

Checklist Diário de Segurança

- Uso apenas **conexões seguras (https://)** para acessar sistemas com dados sensíveis.

- **Bloqueio meu computador (teclas Win + L) ao me afastar, mesmo que brevemente**

- **Avalio e-mails recebidos**, verificando o remetente antes de abrir anexos ou links.

- Uso somente **mídias removíveis fornecidas pela instituição** para dados de trabalho.

- **Observo o ambiente ao manipular informações sensíveis** em locais públicos

- Evito discutir assuntos confidenciais em ambientes públicos ou áreas movimentadas

- **Guardo documentos sensíveis em locais trancados** ao final do expediente.

- Mantenho "mesa limpa", **sem documentos sensíveis expostos**.

Checklist Mensal de Segurança

- **Atualizar senhas principais** (12+ caracteres com letras maiúsculas/minúsculas, números e símbolos).

- **Revisar configurações de privacidade** e permissões nos dispositivos institucionais.

- Executar backup completo de dados conforme procedimento padrão.

- **Confirmar atualizações de antivírus e software** em todos dispositivos.

- Revisar acessos de aplicativos terceiros nas contas institucionais.

- **Ativar autenticação em duas etapas** em todas contas sob minha responsabilidade.

- **Descartar informações desnecessárias** seguindo a política de retenção de dados.

- Verificar disponibilidade de novos treinamentos de segurança na plataforma institucional.

Considerações Finais

A proteção efetiva dos dados e sistemas institucionais só é possível quando cada indivíduo incorpora a segurança da informação como parte integrante de suas responsabilidades profissionais diárias.

Responsabilidade Compartilhada

A segurança da informação é responsabilidade de todos os funcionários da Secretaria. Cada indivíduo desempenha um papel crucial na proteção dos dados e dos serviços prestados à população.

Cultura de Segurança

O desenvolvimento de uma cultura de segurança depende do compromisso contínuo com as boas práticas apresentadas neste guia e da disposição para aprender e se adaptar às novas ameaças que surgem constantemente.

Melhoria Contínua

As ameaças digitais evoluem rapidamente, assim como as tecnologias para combatê-las. **Mantenha-se atualizado através dos canais oficiais e contribua com sugestões para a melhoria** dos processos de segurança da instituição.

SEGURANÇA DIGITAL
EDUCAÇÃO DO PARANÁ

Termo de Responsabilidade

Declaro que recebi, li e compreendi o Guia de Segurança da Informação da Secretaria e estou ciente da minha responsabilidade em seguir as diretrizes e procedimentos nele estabelecidos.

Entendo que o descumprimento das normas de segurança da informação pode resultar em incidentes que comprometem a integridade, disponibilidade e confidencialidade dos dados institucionais, podendo ocasionar danos à instituição e aos cidadãos atendidos, além de possíveis consequências administrativas conforme previsto nas normas internas e na legislação vigente.

Comprometo-me a participar dos treinamentos de segurança da informação oferecidos e a consultar o departamento responsável em caso de dúvidas sobre os procedimentos adequados para situações específicas.

Nome: _____

Matrícula: _____ Data: ___/___/_____

Assinatura: _____

Anotações

Guia de Segurança da Informação para

FUNCIONÁRIOS

SEGURANÇA DIGITAL
EDUCAÇÃO DO PARANÁ

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO