CARTILHA DA SEGURANÇA

SIMPLES ATITUDES PODEM EVITAR GRANDES PROBLEMAS

SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES. UM COMPROMISSO DE TODOS.

DICA: MANTENHA A DISPONIBILIDADE, INTEGRIDADE, CONFIDENCIALIDADE E AUTENTICIDADE DA INFORMAÇÃO.

SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

MELHORES PRÁTICAS EM TECNOLOGIA DA INFORMAÇÃO

APRESENTAÇÃO

Todo servidor público tem um compromisso com a integridade, a confidencialidade, a autenticidade e a disponibilidade da informação. Por isso, deve estar atento aos padrões e procedimentos adotados na Presidência da República, às informações sobre segurança e às boas práticas em tecnologia da informação.

Esta cartilha, fruto de uma iniciativa do Comitê Gestor de Tecnologia da Informação da PR – CGTI/PR, além de informar, também tem como objetivo simplificar a utilização dos recursos tecnológicos disponíveis, estabelecendo mais um canal de comunicação entre o usuário de serviços de TI e a Diretoria de Tecnologia da Informação/Secretaria de Administração/Secretaria-Geral da Presidência da República – DIRTI.

O material está divido em sete capítulos:

1. Política de uso dos computadores – Conceitos importantes e restrições no uso de computadores;
2. Serviços disponíveis ao usuário – Informações sobre o uso de e-mail, intranet, sistemas, servidor de arquivos e cursos de capacitação;
3. Segurança – Conceitos, senhas, vírus, criptografia, certificação digital, e-mail, navegador e dicas sobre antivírus e backups;
4. Redes sem fio – Segurança no uso da rede sem fio e como usá-la na Presidência;
5. Onde obter mais informações – Referências externas sobre os tópicos abordados;
6. Referências legais – Legislação afeta à SIC e TI;
7. Os dez mandamentos da segurança da informação e comunicações.

Utilize ainda o índice remissivo no final do manual para encontrar assuntos específicos.

Boa leitura e bom trabalho!

SUMÁRIO

Introdução 11
1 Política de uso dos computadores 13
1.1 Aplicações 14
1.1.1 Para que serve uma política de uso? 14
1.1.2 Quais recursos computacionais devem seguir a política de uso? 14
1.2 Programas 14
1.2.1 O que posso instalar no computador? 14
1.3 Acessos 14
1.3.1 Que tipo de sítios posso acessar? 14
2 Serviços disponíveis ao usuário 15
2.1 Acesso à rede 16
2.1.1 Como solicitar o acesso à rede? 16
2.2 Programas 16
2.2.1 Como instalar um novo programa? 16
2.3 E-mail 17
2.3.1 Como criar uma conta de e-mail? 17
2.3.2 Posso escolher meu e-mail? 17
2.3.3 Quais os domínios do e-mail? 17
2.3.4 Como acesso meu e-mail? 17
2.3.5 Para que posso usar o e-mail da Presidência da República? 17
2.4 Intranet 18
2.4.1 Como posso divulgar uma informação na intranet? 18
2.5 Sistemas 18
2.5.1 Como obter acesso aos sistemas? 18
2.5.2 Como solicitar o desenvolvimento de um novo sistema? 18
2.6 Servidor de arquivos 18
2.6.1 Como acessar o servidor de arquivos? 18
2.6.2 Posso ter acesso a uma área privada? 19
2.6.3 Há uma política de backup? 19
2.6.4 Como recuperar no backup um arquivo perdido? 19

2.7 Cursos em informática 19
2.7.1 Quem é responsável pelo plano de capacitação da Presidência? 19
2.7.2 Como solicitar ou me inscrever nos cursos? 19
2.8 Equipamentos 20
2.8.1 Como solicitar um equipamento? 20
3 Segurança 21
3.1 Conceitos 22
3.1.1 O que pode ocorrer com um computador vulnerável? 22
3.2 Senhas 22
3.2.1 Quais senhas preciso para acessar os sistemas? 22
3.2.2 Como alterar minhas senhas? 22
3.2.3 O que posso usar como senha? 23
3.2.4 Minha senha foi bloqueada, o que eu faço? 24
3.2.5 Esqueci minha senha, o que eu faço? 24
3.2.6 Como utilizar minha senha com segurança? 25
3.3 Programas maliciosos 25
3.3.1 O que são programas maliciosos? 25
3.3.2 O antivírus protege contra programas maliciosos? 25
3.4 Certificação digital 26
3.4.1 O que é certificado digital? 26
3.4.2 Onde a Presidência utiliza certificação digital? 27
3.4.3 Como usar a certificação digital? 27
3.4.4 Como obter um certificado digital? 28
3.4.5 Por que devo usar um certificado digital? 28
3.4.6 Como instalar os programas necessários para o uso do “token”? 29
3.5 E-mail 29
3.5.1 Recebi um e-mail solicitando minha senha, devo responder? 29
3.5.2 Recebi um e-mail solicitando divulgação de um fato, o que faço? 29
3.5.3 Recebo periodicamente um e-mail com fotos. Devo abrir? 29
3.5.4 Afinal, quais e-mails posso ver? 29
3.6 Navegadores 30
3.6.1 Quais os riscos ao navegar na internet? 30
3.6.2 Quais cuidados devo ter ao efetuar transações financeiras? 30

3.7 Antivírus 30
3.7.1 Como verifico se um arquivo está com vírus? 30
3.7.2 Como "limpar" meu computador? 31
3.7.3 Existe alguma rotina automática para limpar meu computador? ... 31
3.8 Backups 31
3.8.1 Preciso fazer backup dos meus dados? 31
4 Redes sem fio 33
4.1 Definições 34
4.1.1 O que é rede sem fio? 34
4.2 Segurança de redes sem fio 34
4.2.1 Quais os riscos em utilizar rede sem fio? 34
4.2.2 É possível utilizar rede sem fio com segurança? 34
4.3 Rede sem fio na Presidência 34
4.3.1 Como posso habilitar um notebook da Presidência em rede sem fio? .. 34
4.3.2 Posso acessar a rede sem fio utilizando um equipamento pessoal? ... 34
4.3.3 Quais as áreas que têm acesso à rede sem fio? 35
5 Onde obter mais informações 37
5.1 Certificação digital 38
5.2 Criptografia 38
5.3 Redes sem fio 38
5.4 Ordens de serviço 38
5.4.1 Quem pode abrir uma ordem de serviço? 39
5.4.2 Como acompanhar uma ordem de serviço? 39
5.4.3 É possível obter suporte fora dos horários de trabalho? 39
5.4.4 A quem procurar em caso de problemas? 39
5.5 Política de segurança 40
5.6 Sobre a DIRTI 40
6 Referências legais 41
7 Os 10 mandamentos da segurança da informação e comunicações 43
Índice remissivo 45

INTRODUÇÃO

A tecnologia faz parte da vida das pessoas, empresas privadas e setor público. Do aluno da rede pública de ensino aos grandes centros de pesquisa, da dona de casa ao executivo, todos interagem de alguma forma com recursos de TI.

Para que toda a informação que circula possa servir somente ao seu propósito, que é o de informar, sem prejudicar quaisquer pessoas ou instituições, é necessária a gestão segura dos recursos disponíveis em tecnologia da informação.

Na Presidência da República não é diferente. Aliás, deve-se sempre adotar os procedimentos padrões, de modo a contribuir de forma positiva com a disponibilidade, integridade, confidencialidade e autenticidade da informação.

O desafio de fomentar a Segurança da Informação e Comunicações é grande, afinal, são milhares de computadores, servidores e usuários distribuídos em vários pontos e instâncias. Mas está longe de ser impossível, pois depende principalmente da atenção e da atitude das pessoas sobre as boas práticas de TI.

A partir de agora você tem acesso a informações fundamentais para um serviço público eficiente para o seu dia a dia e adaptado aos novos tempos.

1 POLÍTICA DE USO DOS COMPUTADORES

1.1 APLICAÇÕES

1.1.1 Para que serve uma política de uso?

Para estabelecer padrões e procedimentos que busquem a segurança, estabilidade e disponibilidade dos serviços computacionais.

1.1.2 Quais recursos computacionais devem seguir a política de uso?

Quaisquer equipamentos, programas, meios físicos de tráfego e sistemas de armazenamento digital inseridos no ambiente computacional da Presidência, incluindo notebooks, pen drives, HD externos, impressoras, além das estações de trabalho.

1.2 PROGRAMAS

1.2.1 O que posso instalar no computador?

A DIRTI distribui os computadores (estações de trabalho) instalados com sistemas e programas licenciados de acordo com o padrão adotado na PR. Então, por razões de padronização e segurança, o usuário não pode instalar aplicativos e programas sem a prévia autorização da DIRTI.

Em caso de necessidade específica de algum programa ou sistema, deve-se entrar em contato com a DIRTI (veja seção 2.2.1 para detalhes).

1.3 ACESSOS

1.3.1 Que tipo de sítios posso acessar?

É proibido acessar sítios ilícitos, com conteúdos indevidos ou inadequados ao ambiente de trabalho. Além disso, alguns sítios são bloqueados por razões de segurança. Em caso de necessidade de acesso a um sítio que esteja bloqueado, consulte a CENAU sobre a possibilidade de liberação (veja a seção 5.4).

2 SERVIÇOS DISPONÍVEIS AO USUÁRIO

2.1 ACESSO À REDE

2.1.1 Como solicitar o acesso à rede?

Para servidores ou estagiários, os passos são:

1. Obter uma cópia do formulário de credenciamento na Diretoria de Gestão de Pessoas (DIGEP);
2. Preencher e colher assinaturas do responsável pela área ou gestor da informação;
3. Enviar para a DIRTI;
4. Aguardar atendimento técnico.

Para colaboradores, consultores ou terceirizados, os procedimentos são:

1. Obter uma cópia do "formulário de credenciamento na rede" na intranet (http://intra/, "jogo rápido","credenciamento na rede","memorando de credenciamento");
2. Preencher e colher assinaturas do responsável pela área ou gestor da informação;
3. Enviar para a DIRTI;
4. Aguardar atendimento técnico.

2.2 PROGRAMAS

2.2.1 Como instalar um novo programa?

O responsável da área/setor deve abrir uma ordem de serviço (OS) junto à DIRTI (veja a seção 5.4). O atendimento à solicitação vai depender da existência de licenças e do domínio técnico do programa pela DIRTI. Ao preencher a solicitação, marcar "Informática" no campo "Área de Competência".

2.3 E-MAIL

2.3.1 Como criar uma conta de e-mail?

O e-mail é criado juntamente com o login que habilita o acesso à rede de dados da PR. Veja os procedimentos na seção 2.1.1.

2.3.2 Posso escolher meu e-mail?

O padrão de e-mail é:
nome.ultimoNome@planalto.gov.br ou nome.ultimoNome@presidencia.gov.br.
Em alguns casos, o usuário pode sugerir um e-mail diferente, no ato da entrega do formulário de credenciamento.

2.3.3 Quais os domínios do e-mail?

Os domínios oficiais para envio e recebimento de e-mails são planalto.gov.br e presidência.gov.br. Entretanto, há outros domínios que são utilizados para seus respectivos usuários, como: spmulheres.gov.br e portosdobrasil.gov.br.

2.3.4 Como acesso meu e-mail?

Na rede interna ou intranet, o acesso ao e-mail pode ser feito pelos aplicativos Outlook ou Thunderbird.Também pode ser feito pela internet nos endereços:
https://correio.planalto.gov.br,
https://correiopr.planalto.gov.br
ou https://correio.presidencia.gov.br.

2.3.5 Para que posso usar o e-mail da Presidência da República?

Os e-mails disponibilizados pela DIRTI devem ser utilizados estritamente para as atividades vinculadas ao trabalho exercido no órgão.

2.4 INTRANET

2.4.1 Como posso divulgar uma informação na intranet?

Na área de destaques da intranet há um serviço de veiculação de banners. Podem ser exibidos até seis banners simultaneamente. Pode-se ainda utilizar banners que abrem automaticamente na área de trabalho (desktop) dos usuários da rede PR, ao ligarem o computador. Essa publicação tem duração máxima de 3 (três) dias para o mesmo assunto.

A solicitação dos serviços deve ser feita por memorando com antecedência máxima de 03 (três) meses e mínima de 07 (sete) dias. Casos de conflitos de datas e prioridade de publicação serão tratados pela Diretoria de Tecnologia da Informação ou pela Secretaria de Administração.

2.5 SISTEMAS

2.5.1 Como obter acesso aos sistemas?

Entre em contato com o gerente de contas da sua área, por meio do ramal especificado na tabela 1.1. Ele irá orientá-lo sobre os sistemas a que você pode ter acesso e quais os procedimentos necessários para cada caso.

2.5.2 Como solicitar o desenvolvimento de um novo sistema?

Se for necessário desenvolver um novo sistema de informação, o responsável da área deve encaminhar o pedido à DIRTI, por meio de memorando.

2.6 SERVIDOR DE ARQUIVOS

2.6.1 Como acessar o servidor de arquivos?

Geralmente, cada órgão/setor da PR tem um espaço no servidor de armazenamento de dados para guardar arquivos. Durante o processo de logon na rede, o sistema mapeia automaticamente uma letra associada ao espaço correspondente ao seu

setor. Esse espaço é exclusivo para alocar arquivos que fazem parte do trabalho. Não se deve armazenar, nesse local, arquivos de cunho particular ou arquivos do tipo imagem, vídeo ou áudio. Necessidades específicas de armazenamento devem ser solicitadas à DIRTI, por meio de memorando.

2.6.2 Posso ter acesso a uma área privada?

Sim. Caso tenha necessidade de acesso restrito a uma pasta específica, solicite o serviço por meio de ordem de serviço junto à DIRTI (veja seção 5.4).

2.6.3 Há uma política de backup?

Sim. A DIRTI é responsável pelo salvamento dos dados armazenados nos servidores. Já os dados armazenados nas estações de trabalho devem ser salvos pelo próprio usuário em mídias fornecidas pela PR.

2.6.4 Como recuperar no backup um arquivo perdido?

Caso algum arquivo tenha sido excluído indevidamente do servidor da rede, é possível solicitar a restauração por meio de ordem de serviço junto à DIRTI (veja seção 5.4). É preciso informar o endereço completo do arquivo ou da pasta que se quer recuperar.

2.7 CURSOS EM INFORMÁTICA

2.7.1 Quem é responsável pelo Plano de Capacitação da Presidência?

O Plano de Capacitação da Presidência é gerido pela Diretoria de Gestão de Pessoas (DIGEP) por meio da Coordenação-Geral de Desenvolvimento de Pessoas (CODEP) e do Centro de Capacitação e Desenvolvimento (CECAD). A DIRTI participa sugerindo a inclusão de cursos em sua área de atuação.

2.7.2 Como solicitar ou me inscrever nos cursos?

Deve-se entrar em contato com o agente de gestão de pessoas da sua área.

2.8 EQUIPAMENTOS

2.8.1 Como solicitar um equipamento?

Para solicitar equipamentos de informática, o responsável pela área/setor deve encaminhar memorando com o pedido para a Diretoria de Tecnologia da Informação – DIRTI.

A solicitação deve ser detalhada para que a DIRTI avalie a melhor configuração a ser utilizada. O atendimento do pedido também depende da disponibilidade e da adequação à política de tecnologia da informação da PR.

3 SEGURANÇA

3.1 CONCEITOS

3.1.1 O que pode ocorrer com um computador vulnerável?

Entre outras coisas, pode ocorrer:

- Roubo de informação;
- perda de dados;
- redução de desempenho;
- uso do computador para atacar servidores e outros computadores.

Por isso, os cuidados com a segurança são importantes.

3.2 SENHAS

3.2.1 Quais senhas preciso para acessar os sistemas?

Na Presidência são utilizadas senhas para:

- Correio Expresso;
- rede Windows;
- aplicativo Lotus Notes.

Além dessas, podem ser necessárias outras para acessar aplicativos específicos.

3.2.2 Como alterar minhas senhas?

Para alterar suas senhas, veja os passos descritos a seguir para cada aplicativo:

- Correio Expresso
    1. Clique em “Minhas Preferências” no canto superior direito;
    2. clique em “Altere sua senha”;
    3. digite a senha atual, a nova senha e sua confirmação;
    4. clique em “Alterar”.
- Rede Windows / correio Exchange (Outlook)
    1. Pressione as teclas ctrl+alt+del;
    2. clique em “alterar uma senha”.
- Aplicativo Lotus Notes
    1. Acesse o menu “Arquivo”, “Segurança”, “Segurança do Usuário”;
    2. digite a senha atual;
    3. clique no botão “Alterar senha”;
    4. digite novamente a senha atual;
    5. digite duas vezes a nova senha e confirme clicando “OK”.

3.2.3 O que posso usar como senha?

Para proteger bem suas informações confidenciais e impedir que alguém descubra a sua senha, o ideal é nunca usar nomes próprios, datas, combinações simples de letras ou palavras existentes em dicionários. A senha deve ser segredo seu.

Misture caracteres especiais (ex.: @#$%¨&*()+=.;) e combinações entre números e letras minúsculas e maiúsculas.

Uma boa dica para criar uma senha segura e fácil de lembrar é pensar em uma frase e usar a primeira, segunda ou a última letra de cada palavra.

Ex.: "Batatinha quando nasce, se esparrama pelo Chão"

Exemplos de senhas consideradas seguras:

- &(aAccd383-#$!
- 9Unmytaquie
- NevdyWytjaw1k
- imcajFisk7
- evCuegUrvoc8

Exemplos de senhas consideradas frágeis:

- amor123
- daniele22
- jo4o
- s3gr3d0

3.2.4 Minha senha foi bloqueada, o que eu faço?

Por razões de segurança, após 5 (cinco) tentativas, sem sucesso, de acesso à rede, a senha do usuário é automaticamente bloqueada por 30 minutos. Neste caso, você deve ligar para a Central de Atendimento ao Usuário (CENAU) nos ramais 1000, 2000 ou 3400 e solicitar a liberação.

Importante: somente o próprio usuário pode solicitar a liberação do acesso ou uma nova senha.

3.2.5 Esqueci minha senha, o que eu faço?

Abra uma ordem de serviço junto à CENAU. Veja os detalhes na seção 5.4.

3.2.6 Como utilizar minha senha com segurança?

- Jamais compartilhe senhas com outras pessoas. Lembre-se que, a princípio, você é o responsável por tudo que ocorre com o uso de sua senha.
- Se você não consegue memorizar suas senhas e precisa anotar em algum lugar, dificulte o acesso das pessoas aos seus lembretes. Não deixe suas senhas anotadas em locais visíveis, de fácil acesso, expostas em cadernos, pastas ou marcadores em sua mesa de trabalho.
- A senha existe para evitar acessos não autorizados por outras pessoas a ambientes e sistemas que exigem segurança e controle, por isso, bloqueie sempre o seu computador em suas ausências, evitando o acesso indevido a informações sob sua responsabilidade. No Windows, utilize o conjunto de teclas <Ctrl> +<Alt>+<Del> ou <Windows> + <L> para bloquear rapidamente o computador.
- Utilize senhas também em celulares e notebooks, protegendo suas informações em caso de extravio, furto ou roubo do equipamento.
- Sempre que possível diversifique as senhas que possui, evitando que a descoberta de uma delas dê acesso a outras informações protegidas.

3.3 PROGRAMAS MALICIOSOS

3.3.1 O que são programas maliciosos?

São programas criados para executar ações maliciosas no computador, como captura de senhas e danificação de arquivos e programas. Os mais comuns são:

- Vírus – programa que infecta o computador utilizando-se de diversos meios. É replicado pela ação do computador infectado.
- Cavalo de troia – programa invasor que pode ler, copiar, apagar e alterar dados do sistema sem o conhecimento do usuário.

- Backdoors – programa que tenta obter controle de uma máquina aproveitando-se uma falha de segurança em um programa de computador ou sistema operacional, abrindo uma porta para seu invasor controlar o computador remotamente.
- Keylogger – programa capaz de capturar e armazenar as teclas digitadas pelo usuário.

3.3.2 O antivírus protege contra programas maliciosos?

Em geral, o antivírus detecta programas maliciosos oriundos de e-mails, disquetes, CDs, cartões de memória, pen drives etc. Contudo, é sempre bom tomar cuidado com todas as mídias que recebe. Verifique sempre se o antivírus está funcionando e atualizado.

Evite também executar programas ou abrir arquivos de origem duvidosa. Lembre-se que, por exemplo, joguinhos de computador aparentemente inofensivos, ao serem executados, poderão conter e instalar programas maliciosos, que poderão ocasionar danos irreversíveis aos seus arquivos, mau funcionamento do seu equipamento ou até mesmo furtar suas senhas. Muitas vezes, esses arquivos podem vir de amigos ou colegas de trabalho que desconhecem que seus arquivos possuem essa ameaça.

3.4 CERTIFICAÇÃO DIGITAL

3.4.1 O que é certificado digital?

O certificado digital é um documento eletrônico que possibilita comprovar a identidade de uma pessoa, uma empresa ou um site para assegurar as transações online e a troca eletrônica de documentos, mensagens e dados com presunção de validade jurídica. Para utilizá-lo, o usuário deve conectar o *token* no computador e digitar sua senha pessoal. Um *token* é um dispositivo eletrônico no qual são guardadas as informações do certificado digital.

3.4.2 Onde a Presidência utiliza certificação digital?

Atualmente a Presidência utiliza certificação digital em:

- Autenticação na estação de trabalho;
- autenticação no Correio Expresso;
- envio de e-mails assinados no Correio Expresso;
- autenticação em aplicações institucionais;
- envio de e-mails assinados no Exchange (Outlook).

3.4.3 Como usar a certificação digital?

- Autenticação na estação de trabalho
    1. Na tela de solicitação de usuário e senha, insira o "token" de acesso;
    2. digite a senha do certificado.
- Autenticação no Correio Expresso
    1. Insira o "token" no computador;
    2. na tela de autenticação, clique em "Utilizar o meu Certificado para logar";
    3. confirme as possíveis perguntas de autenticidade, selecionando "Para sempre confiar no conteúdo deste sítio";
    4. aguarde;
    5. digite a senha do certificado, quando solicitada, e confirme.
- Envio de e-mails assinados no Correio Expresso
    1. Na primeira vez, altere as configurações:

(a) Acesse o Correio Expresso com a senha normal;

(b) clique em “Minhas Preferências”no canto superior direito;

(c) clique em “Preferências” na seção “Expresso Mail”;

(d) selecione “SIM” para “Possibilitar assinar/cifrar digitalmente a mensagem?”;

(e) clique em salvar.

2. Insira o “token” no computador;
3. ao enviar uma mensagem, selecione “Assinar digitalmente a mensagem?”;
4. clique em enviar a mensagem;
5. digite a senha do certificado e confirme.

3.4.4 Como obter um certificado digital?

Para a emissão do certificado digital, encaminhe sua solicitação por meio de memorando endereçado à DIRTI.

3.4.5 Por que devo usar um certificado digital?

É com o uso de um certificado digital que se pode assinar um documento em meio eletrônico, possibilitando a comprovação de sua autoria e a integridade de seu conteúdo. Conforme a Medida Provisória 2.200-2, os documentos digitais terão a mesma validade jurídica que os documentos em papel assinados manualmente se forem assinados com certificado emitido pela ICP-Brasil ou com a utilização de certificados emitidos por outras infraestruturas de chaves públicas, desde que as partes que assinam reconheçam previamente a validade destes.

3.4.6 Como instalar os programas necessários para uso do “token”?

Solicitar a instalação por meio da abertura de uma ordem de serviço (consulte a seção 5.4). Caso seja administrador da estação de trabalho, acesse os procedimentos descritos no endereço http://www.planalto.gov.br/ACPR/.

3.5 E-MAIL

3.5.1 Recebi um e-mail solicitando minha senha, devo responder?

Não! Nunca se deve informar senhas e dados pessoais por e-mail. Há uma prática maliciosa conhecida como “phishing”, que consiste em solicitar informações ou ações do usuário. Existe um controle de spams na Presidência que coíbe essa prática. Entretanto, como essas mensagens se assemelham a e-mails verdadeiros, é possível o recebimento de algum e, por isso, deve-se estar sempre atento.

3.5.2 Recebi um e-mail solicitando divulgação de um fato, o que faço?

É comum algumas mensagens do tipo “Ajude essa criança com câncer” ou “Previna-se do novo vírus” solicitando divulgação (“envie para todos da sua lista”). A maioria dessas mensagens é boato e não deve ser passada adiante.

3.5.3 Recebo periodicamente um e-mail com fotos. Devo abrir?

Vários vírus são disseminados por meio de links em textos ou em fotos. Não se deve, portanto, abrir anexos ou links recebidos de remetentes desconhecidos.

3.5.4 Afinal, quais e-mails posso ver?

Confie nas mensagens de remetentes conhecidos e com conteúdo esperado. E-mails suspeitos devem ser enviados para análise da DIRTI, pelo endereço cenaupr@planalto.gov.br.

3.6 NAVEGADORES

3.6.1 Quais os riscos ao navegar na internet?

Alguns sítios exploram vulnerabilidades dos navegadores e acabam instalando programas maliciosos no computador do usuário. Por isso, é importante manter os aplicativos atualizados e não fazer download de arquivos em sítios desconhecidos.

3.6.2 Quais cuidados devo ter ao efetuar transações financeiras?

Verifique se o endereço do sítio da sua instituição está escrito corretamente na barra de endereços. Nunca clique em referências recebidas por e-mail ou de fontes não confiáveis. Certifique-se de que a conexão é criptografada. Para isso veja se há "https://" antes do endereço do sítio.

3.7 ANTIVÍRUS

3.7.1 Como verifico se um arquivo está com vírus?

Sempre que um arquivo é acessado, a ferramenta de antivírus instalada nos computadores da Presidência da República verifica automaticamente se há vírus ou não. Caso queira verificar manualmente um arquivo, efetue os seguintes passos:

1. Clique sobre o ícone do arquivo com o botão direito do mouse e escolha a opção "Fazer varredura para encontrar ameaças";
2. confirme clicando em "Limpar";
3. aguarde enquanto a ferramenta efetua a varredura;
4. ao terminar clique no botão "Fechar".

3.7.2 Como “limpar” meu computador?

Para executar uma varredura completa no computador, faça o seguinte:

1. Clique em Iniciar Programas McAfee Varredura por solicitação;
2. ao abrir a janela, clique em “Iniciar” e aguarde a conclusão da varredura;
3. com o término da varredura, clique em “Fechar”.

3.7.3 Existe alguma rotina automática para limpar meu computador?

Sim. Todas as quartas-feiras, a partir de uma hora da madrugada, é executada uma rotina de verificação em todos os computadores da rede PR. Por isso, sugerimos manter o computador ligado de terça para quarta-feira.

3.8 BACKUPS

3.8.1 Preciso fazer backup dos meus dados?

Sim. A DIRTI é responsável pelo salvamento dos dados armazenados nos servidores. Quanto aos dados armazenados nas estações de trabalho, o próprio usuário é responsável pelo seu salvamento.

4 REDES SEM FIO

4.1 DEFINIÇÕES

4.1.1 O que é rede sem fio?

É uma rede que pode ser acessada sem a necessidade de conexões por fios metálicos. A mais comum utiliza radiofrequência na comunicação entre os computadores. Essa tecnologia é indicada quando se necessita de mobilidade, como no uso de notebooks. Embora a rede sem fio permita mobilidade, a rede com cabo é mais estável e mais rápida.

4.2 SEGURANÇA DE REDES SEM FIO

4.2.1 Quais os riscos em utilizar rede sem fio?

Como o acesso à rede é feito sem a necessidade de contato físico, é possível alguém acessá-la mesmo estando fora das dependências do órgão. Isso pode ser utilizado para roubo de informações.

4.2.2 É possível utilizar rede sem fio com segurança?

Sim. Há tecnologias de criptografia e autenticação que garantem que apenas usuários certificados possam acessar a rede.

4.3 REDE SEM FIO NA PRESIDÊNCIA

4.3.1 Como posso habilitar um notebook da Presidência em rede sem fio?

Abra uma ordem de serviço solicitando a ativação. Para isso, veja a seção 5.4.

4.3.2 Posso acessar a rede sem fio utilizando um equipamento pessoal?

Por razões de segurança, não é permitido ter acesso à rede interna por meio da tecnologia wireless em computadores pessoais. Para estes, é permitido apenas o acesso à Internet como usuário visitante.

4.3.3 Quais as áreas que têm acesso à rede sem fio?

Atualmente há cobertura de rede sem fio apenas para a a área do Palácio do Planalto. Está em fase de implantação nas demais unidades da Presidência da República.

5 ONDE OBTER MAIS INFORMAÇÕES

5.1 CERTIFICAÇÃO DIGITAL

- Sítio http://www.iti.gov.br – na aba Certificação Digital;
- Sítio http://pt.wikipedia.org/wiki/Certificado_digital – Definições;
- Contato com o gerente de contas que atende sua área (veja tabela 1.1);
- Norma VIII 501 rev.01. Na intranet, menu "Conheça a PR", link "Normas Internas".

5.2 CRIPTOGRAFIA

- Sítio http://pt.wikipedia.org/wiki/Criptografia – Definições.

5.3 REDES SEM FIO

- Sítio http://pt.wikipedia.org/wiki/Wireless – Definições;
- Sítio http://www.microsoft.com/business/smb/pt-br/products/howto/setupwireless.mspx – Dicas da Microsoft para a configuração de rede sem fio no Windows.

5.4 ORDENS DE SERVIÇO

Para acionar o suporte de informática, é necessário abrir uma ordem de serviço. Para isso, os usuários credenciados na rede PR devem entrar em contato com a Central de Atendimento diretamente pelos ramais 1000, 2000 ou 3400 ou via intranet (http://intra, menu "Jogo Rápido", link "Ordem de Serviço").

5.4.1 Quem pode abrir uma ordem de serviço?

Somente usuários da rede PR. Caso seja servidor da PR ainda não credenciado como usuário, solicite à sua chefia o encaminhamento da solicitação de credenciamento de usuário à DIRTI.

5.4.2 Como acompanhar uma ordem de serviço?

Acesse o sítio http://intra/jogo_rapido/ordem-de-servico ou ligue para a Central de Atendimento ao Usuário (CENAU) nos ramais 1000, 2000 e 3400.

5.4.3 É possível obter suporte fora dos horários de trabalho?

Sim. Está disponível um plantão de apoio à informática em ocasiões excepcionais. Para verificar os telefones, acesse o documento: http://intra/groups/DIRTI/arquivos/Plantao.pdf.

5.4.4 A quem procurar em caso de problemas?

A COATE é a Coordenação-Geral de Atendimento a Usuários, cujo atendimento é feito pela Central de Atendimento ao Usuário (CENAU), por meio da abertura de uma ordem de serviço (consulte a seção 5.4).
A COATE presta apoio de:

- Suporte no uso do computador;
- configuração de aplicativos;
- problemas no acesso à rede;
- acesso a sistemas.

O atendimento também pode ocorrer de forma personalizada por meio de um gerente de conta.

Veja na tabela abaixo os ramais dos gerentes de contas e respectivas áreas de atendimento. Para outras informações sobre os serviços prestados pela DIRTI acesse o link "Tecnologia da Informação" no menu "Infraestrutura" da Intranet.

Área	Ramal
SRI / SAF / SUPAR / SEDES SIP / SECOM / SAE	2268
CISET / CASA CIVIL SE / SAM / SAJ / SAG	2816
GSI / SPMULHERES CONSEA / VPR / SEPPIR	2355
SECRETARIA DE ADMINISTRAÇÃO SECRETARIA DE PORTOS	2638
CERIMONIAL / AJUDÂNCIA DE ORDENS ASSESSORIA ESPECIAL / DDH PALÁCIO ALVORADA / TORTO	1525
SECRETARIA-GERAL / GABINETE PR	1351

Tabela 1.1

5.5 POLÍTICA DE SEGURANÇA

- Sítio http://intra/conheca_a_pr/normas – Acesso à norma de uso seguro de recursos computacionais ("NORMA VIII-101");

5.6 SOBRE A DIRTI

- Sítio http://intra/infra_estrutura/tecnologia-da-informacao/tecnologia-da-informacao – Informações diversas.

6 REFERÊNCIAS LEGAIS

Referência	Descrição
Lei 8.429/92	Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências.
MP 2200-2/01	Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia e dá outras providências.
Decreto 1.171/94	Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.
Decreto 3.505/00	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto 4.081 de 11 de janeiro de 2002	Institui o Código de Conduta Ética dos Agentes Públicos em exercício na Presidência e Vice-Presidência da República.
Decreto 4.553/02	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
IN-GSI Nº 1/08 e normas complementares	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Portaria 310/09	Dispõe sobre Política de Segurança de Tecnologia da Informação da Presidência da República.
Norma VIII-101rev02/10	Uso seguro de recursos computacionais.
Norma VIII-501rev03/10	Norma de Gestão de Certificados Digitais.

Tabela 1.2

7 OS 10 MANDAMENTOS DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1. Utilize senhas difíceis de serem descobertas
2. Altere sua senha periodicamente
3. Tome cuidado com downloads
4. Tome cuidado com e-mails de remetentes desconhecidos
5. Evite sítios com conteúdos duvidosos
6. Não abra anexos de e-mails desconhecidos
7. Tome cuidado com compras na internet
8. Tome cuidado ao acessar sítios de bancos
9. Não revele informações sobre você na internet
10. Ao informar dados em sítios, verifique se a página é segura (com prefixo “https”)

ÍNDICE REMISSIVO

A
abrir uma 38, 39
acessos 14, 16,17, 18
alterar 22, 23
antivírus 25, 30
área privada 18
arquivos 18, 25

B

backup 19, 31
boato 29

C

capacitação 19
certificação digital 26, 27
COATE 39
criptografia 25, 26, 34
cursos 19

D

decreto 42
desenvolvimento 18
DIRTI 14, 16, 17, 18, 19, 31, 39, 40

E

e-mail 17, 26, 27, 28, 29, 44
equipamentos 14, 19

I

inscrição 45
intranet 16, 17

O

ordem de serviço 16, 18, 19, 24, 34, 38, 39

P

phishing 29
plano de capacitação 19
política de uso s14
programas 14, 16
programas Maliciosos 25

R

recuperar 19
Redes sem fio 33, 34, 35, 38

S

segurança 22, 23, 24, 34, 35, 40, 42
senha 22, 23, 24, 25, 26, 27, 28, 29, 44
servidor 18,19, 22
sistemas 14, 18, 22, 39
solicitação 19, 27, 30

T

token 27, 28

W

wireless 39

GOVERNO FEDERAL

BRASIL

PAÍS RICO É PAÍS SEM POBREZA