SIC

# Segurança da Informação e Comunicações

## ORIENTAÇÕES PARA O SERVIDOR

**Ministério do Planejamento, Orçamento e Gestão**

**Ministra do Planejamento, Orçamento e Gestão**
MIRIAM APARECIDA BELCHIOR

**Secretária Executiva**
EVA MARIA CELLA DAL CHIAVON

Cartilha editada pelo Comitê de Segurança de Informação e Comunicações – CSIC

**Redação e revisão:**
ESSE MARQUES MOREIRA
FÁBIO HITSUKI NITTO
GILSON FERNANDO BOTTA
GRAZIELLE SEABRA DURÃES AGUIAR
LÊNIO SILVA FONSECA DE FIGUEIREDO
RAMON GOMES BRANDÃO
REGINA CARLA OLIVEIRA FRAZÃO
RONALDO BALESTRA CHOZE

Projeto gráfico, diagramação e ilustração:
ROGÉRIO FERNANDES GUIMARÃES

**Referências de sites utilizados nas pesquisas:**
Site Certbr: http://cartilha.cert.br/

Cartilha de Segurança da Informação do MTE:
portal.mte.gov.br/data/files/8A7C812D32DC09BB0132EF32761F30CE/segurancadainformacao.pdf

Artigo Cuidado com Pen Drives e HDs Externos:
http://www.oabes.org.br/artigos/555083/

**Leitores podem entrar com contato pelos e-mails:**
cetra@planejamento.gov.br
abuse@planejamento.gov.br

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES


# Segurança da Informação e Comunicações

## ORIENTAÇÕES PARA O SERVIDOR

BRASÍLIA - DF
2014

# Apresentação

A Segurança da Informação e Comunicações não está restrita apenas a sistemas computacionais, informações eletrônicas ou qualquer outra forma mecânica de armazenamento. Ela está relacionada com a proteção existente ou necessária sobre dados, informações ou documentos que possuem valor para alguém ou uma organização.

A segurança é obtida através de padrões e medidas de proteção capazes de neutralizar ameaças contra alguém ou alguma coisa. Possui como propriedades básicas: disponibilidade, integridade, confidencialidade e autenticidade da informação. Por isso, torna-se da maior importância a educação para o uso ético, seguro e legal das tecnologias e das informações, pois o seu uso inadequado pode criar vulnerabilidades que comprometam as instalações, serviços e bens, comprometendo assim as propriedades básicas da informação.

Ciente da importância estratégica em controlar e garantir a proteção da informação e manter e zelar pela integridade e sigilo dos dados corporativos, o Ministério do Planejamento, Orçamento e Gestão, pela Portaria nº 27, de 03 de fevereiro de 2012, publicou a sua Política de Segurança da Informação e Comunicações (POSIC), que é uma declaração formal do órgão acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob guarda, devendo ser cumprida por todos os seus servidores e colaboradores.

Nesta cartilha, abordaremos os principais aspectos que possam levar a cada um dos servidores e demais colaboradores do Ministério do Planejamento, Orçamento e Gestão (MP) a uma reflexão para mudança de atitudes pessoais e profissionais que assegurem a proteção dos recursos de informação e comunicações do Ministério.

# Sumário

# 1 A Segurança da Informação e Comunicações – SIC

- **O que é informação?**

  É todo e qualquer conteúdo dotado de valor para uma pessoa ou organização.

- **Qual o valor da informação?**

  Na sociedade atual, muitas vezes referenciada como Sociedade da Informação ou Sociedade do Conhecimento, a informação é um ativo estratégico, apontada como o principal patrimônio de uma organização. E, como tal, permanece sob constante risco.





- **Qual o papel da Segurança da Informação e Comunicações – SIC?**

  A SIC compreende um conjunto de iniciativas cujo objetivo é assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações. Deve contemplar todo o ciclo de vida da informação, desde a elaboração, transmissão, recepção e tratamento até seu descarte, independente dos meios empregados nestes processos.

# 2 Propriedades básicas da Segurança da Informação e Comunicações – SIC

Para referenciar as propriedades da segurança da informação é comum utilizar o acrônimo DICA (Disponibilidade, Integridade, Confidencialidade e Autenticidade).


**Disponibilidade:** propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade. Proteger essa propriedade significa assegurar ao usuário o acesso à informação, sempre que dela precisar.

**Integridade:** propriedade de que a informação não seja modificada ou destruída de maneira não autorizada ou acidental. Protegê-la significa assegurar que nada foi acrescentado, retirado ou modificado sem a explícita permissão do seu proprietário.

**Confidencialidade:** propriedade de que a informação não seja revelada ou disponibilizada a indivíduo, entidade, órgão ou sistema, não autorizado ou não credenciado. Dados privados ou com algum grau de sigilo devem ser apresentados somente ao(s) seu(s) dono(s) ou ao(s) grupo(s) com a devida permissão para tal.

**Autenticidade:** propriedade de que a informação seja produzida, expedida, modificada ou destruída por indivíduo, entidade, órgão ou sistema, devidamente identificado ou certificado.

## FIQUE LIGADO

**Ações que venham a comprometer a DICA importam em responsabilidade administrativa, civil e penal!**

# 3 O que eu tenho a ver com a SIC?

A segurança de uma determinada informação pode ser afetada por fatores comportamentais, pelo ambiente ou infraestrutura que a cerca ou ainda por pessoas mal-intencionadas, que tem o objetivo de furtar, destruir ou modificar os dados para fins ilícitos.

Para que toda informação possa servir adequadamente ao seu propósito, sem prejudicar quaisquer pessoas ou instituições, é necessária a gestão segura dos recursos que lidam com essas informações.

A SIC vai muito além da tecnologia da informação. Mais do que isso, ela está intimamente relacionada ao nosso comportamento





e nossas atitudes. Assim, exige-se, em tempos de inclusão digital, uma mudança de comportamento, tendo em vista o potencial lesivo da velocidade com que correm as informações nos meios digitais, como a Internet, por exemplo.

Torna-se necessário que os conceitos relacionados à segurança da informação sejam compreendidos e seguidos por todos os servidores, autoridades e colaboradores do MP, na vida pessoal e profissional. Todos devem ter um compromisso com a disponibilidade, integridade, confidencialidade e autenticidade (DICA) das informações da nossa instituição.

## 3.1 – A SIC na vida pessoal

- **Você consegue ficar sem suas informações?**

  Na era da tecnologia, somos "bombardeados" diariamente por diversas informações, as quais gravamos em nossa mente, computadores, dispositivos móveis e o restante em outros lugares (mesa, gaveta, armário...).

  E se, de repente, você as perdesse, o que faria? Conseguiria ficar sem as suas informações? Quais os prejuízos que você teria?

- **Celulares e tablets sem senha ou sistema de bloqueio. O que pode acontecer se eu deixar assim?**

  Os celulares e *tablets* têm sido cada vez mais utilizados para armazenamento de dados. Agenda de contatos, mensagens com conversas pessoais, e-mails e arquivos, dentre outros, podem estar facilmente disponíveis para alguém mal-intencionado utilizar, caso você não faça uso de senhas ou sistemas de bloqueio da tela. Para que você consiga utilizar estes recursos, disponíveis na maioria dos dispositivos atuais, leia o manual do equipamento ou entre em contato com o suporte técnico e solicite orientações sobre como implementar esta simples, mas importante medida preventiva.

**FIQUE LIGADO**

**Projeta a sua informação pessoal! Ela também pode proteger você! Coloque senha e bloqueio de tela em seus dispositivos pessoais. É simples!**





- **Engenharia Social: O que é e como me afeta?**

  São ações feitas por pessoas mal intencionadas, para obter acesso a informações importantes ou sigilosas de pessoas ou organizações, por meio da enganação ou exploração da confiança dos indivíduos.

  Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade e até fingir que é um profissional de determinada área. Ele explora as emoções e fragilidades das pessoas que, quando não treinadas ou preparadas para se defender desses ataques, podem ser facilmente manipuladas. Na dúvida, não passe suas informações! Elas podem ser indevidamente divulgadas e trazer sérios riscos à você e sua família.



**FIQUE LIGADO**

**Cuide das informações sob sua responsabilidade. Só lembramos da real importância quando perdemos ou quando precisamos dela. As suas estão seguras?**

**Não dê informações pessoais por telefone, e-mail ou mensagem, a não ser que você tenha absoluta certeza de quem está pedindo. Oriente seus familiares e seus funcionários!**

# SAIBA MAIS

**Você consegue, ao entrar em um site, identificar se é falso? Saiba como se proteger em http://cartilha.cert.br/golpes**

## Phishing

**Do inglês *"fishing"*, vem de uma analogia criada pelos fraudadores, onde "iscas" (mensagens eletrônicas) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.**

- **Comprar ou transacionar via internet pode ser muito prático e fácil! Mas e se o site for falso?**

  As opções de compras e de transações bancárias via internet estão cada vez mais numerosas, acessíveis e amigáveis. Contudo, existem *sites* maliciosos que simulam os *sites* reais para roubar informações e dinheiro dos usuários (conhecido como *phishing – veja ao lado*). Se desconfiar de qualquer coisa, feche imediatamente o navegador e contate a empresa através do telefone fixo para confirmar o endereço e os dados apresentados.





- **Pen drive e HDs externos com informações pessoais. E se eu perder?**

  Com o aumento de capacidade das mídias removíveis, é cada vez maior a quantidade de informações que estão gravadas em HDs externos e nos pequenos Pen-drives.

  Todas estas mídias podem se tornar um ponto fraco na segurança dos seus dados. Imagine um Pen-drive recheado de informações particulares (ou mesmo sensíveis para sua empresa) "dando sopa" por aí. Nada agradável, certo?

  Exatamente pensando nisto alguns fornecedores criaram aplicativos que permitem que você defina uma senha de acesso para estas informações gravadas. Assim, mesmo no caso de perda ou roubo do dispositivo, suas informações estarão a salvo.

# FIQUE LIGADO

**Tenha os dispositivos móveis (pen drives e HDs externos) sempre com você ou guarde-os em local seguro, sem se esquecer da utilização de ferramentas que protegem os dados neles armazenados.**

# FIQUE LIGADO

**Defina senhas para acesso a sua rede sem fio (Wi-fi) doméstica! Saiba como se proteger em: http://cartilha.cert.br/redes/**

- **Rede sem fio (Wi-Fi) em casa. Como devo me proteger?**

  Redes Wi-Fi se tornaram populares pela mobilidade que oferecem, pela conveniência e facilidade de uso em diferentes tipos de ambientes. Por terem instalação bastante simples, muitas pessoas as instalam em casa sem qualquer cuidado com configurações mínimas de segurança.

  Pessoas mal intencionadas podem fazer uso de sua rede de forma não autorizada e, inclusive, ter acesso a dados e arquivos dos computadores e dispositivos de sua rede doméstica.





- **Contas e formulários financeiros disponíveis com seus dados. Será que alguém pode se aproveitar?**

  O fim do mês chega e, junto com ele, contas e mais contas para pagar. Mas o que fazemos com os recibos, boletos e afins? Guardamos em ambientes seguros? Nestes documentos existem informações valiosas, como, por exemplo, seu endereço residencial, o seu CPF e identidade e, em alguns casos, seus telefones pessoais. Esses dados podem ser utilizados por pessoas mal intencionadas das mais variadas formas (falsificação de documentos, fraudes, assaltos, sequestros, entre outros). Lembra-se da Engenharia Social?

- **E-mails suspeitos ou fraudulentos, spams e com vírus. Como posso me proteger?**

  Quem nunca recebeu um e-mail com um suposto alerta do SERASA ou da Receita Federal, de atualização de cadastro de banco ou de uma promoção absurdamente imperdível, com um *link* “clique aqui”? Em sua grande maioria, são e-mails maliciosos, conhecidos como



FIQUE LIGADO

**Seus dados e informações pessoais deixados por aí podem ser usados para os mais diversos fins maliciosos, inclusive contra você!**

**Atenção aos e-mails recebidos! Analise a origem, a mensagem e, na dúvida, não clique em nenhum link. Mantenha seus programas antivírus sempre atualizados e faça uso dos filtros de spam da sua caixa de e-mail.**

# SAIBA MAIS

**Phishing Scam**

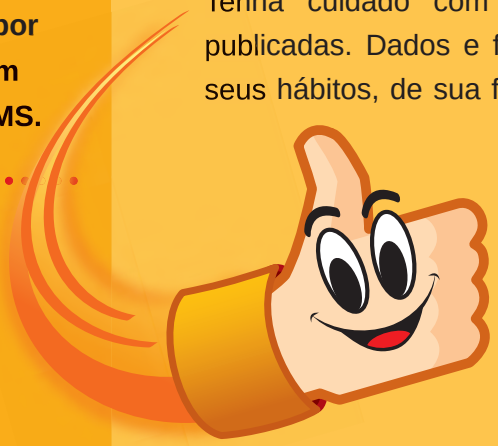
**Forma de fraude eletrônica, caracterizada por tentativas de adquirir fotos, músicas e outros dados pessoais ao se fazer passar por uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial. Isso ocorre de várias maneiras, principalmente por email, mensagem instantânea e SMS.**

*phishing scams (veja ao lado)*, cujo objetivo é adquirir seus dados pessoais e financeiros. Usam as mais diversas técnicas como simular um *site* legítimo ou instalar um programa malicioso (vírus e cavalos-de-tróia, por exemplo) em seu computador.

- **Uso de Redes Sociais e Blogs. Devo me preocupar?**

As redes sociais e *blogs* fazem parte de nosso cotidiano. Eles permitem que você se informe sobre os assuntos do momento, saiba o que seus amigos e ídolos estão fazendo, pensando e os lugares que estão frequentando. Entretanto, a grande popularidade das redes sociais também chama a atenção de pessoas mal-intencionadas.

Tenha cuidado com as informações publicadas. Dados e fotos sobre você, seus hábitos, de sua família, seus amigos, seus bens, informações do seu trabalho e lugares frequentados podem ser usadas indevidamente, tanto para causar danos à sua imagem e reputação, como para o uso criminoso em tentativas de sequestro e furto.



Se você tem filho(s) ou crianças próximas, tenha cuidado redobrado e os oriente para que se protejam dos riscos das redes sociais. Saiba que tipo de conteúdo acessam em sua navegação e, sobretudo, oriente para não se relacionarem com estranhos e nem forneçam informações pessoais na rede.

### 3.2 – A SIC no ambiente de trabalho

Com a simples mudança de hábitos pessoais e funcionais, podemos contribuir para a implantação de uma nova cultura de SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES no Ministério do Planejamento, Orçamento e Gestão.

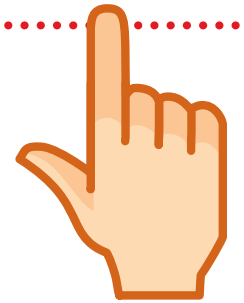
Todos os dias pessoas, empresas e organizações governamentais são vítimas de tentativas de ataques, cujo objetivo é a captura ou destruição de dados ou informações importantes. Por isso, é preciso tomar cuidado e ficar atento para que as informações corporativas não sejam colocadas em risco.





# FIQUE LIGADO

**Pense bem antes de divulgar algo nas suas redes sociais, pois tudo o que você publicar pode ser lido ou acessado por qualquer pessoa, e assim você não terá mais controle do que pode ser feito com aquela informação. Não é possível voltar atrás! Oriente seus filhos!**



Existem inúmeras situações de insegurança que podem afetar as informações e os sistemas que as gerenciam, tais como: incêndios, alagamentos, problemas elétricos, fraudes, uso inadequado, engenharia social, guerras e seqüestros. Apesar de não serem totalmente gerenciáveis, podem ter seu impacto bastante reduzido com a tomada de ações preventivas.

**Equipamentos de Informática**

a) Mantenha atualizado o antivírus de sua estação de trabalho. A equipe técnica da Diretoria de Tecnologia da Informação do MP irá se encarregar disso, mas, em caso de problema, entre em contato com o ***suporteti@planejamento.gov.br*** para que a situação possa ser corrigida;

b) Evite trazer CDs, DVDs, *pen drives* ou quaisquer outros dispositivos móveis de fora do MP para utilização no computador do trabalho. Você pode estar trazendo vírus de outros equipamentos para sua estação e, consequentemente, poderá infectar não só o seu equipamento, mas toda a rede interna do órgão; e

c) Suspeite de softwares e *link*s recebidos por e-mail em que você clica e não acontece nada.

**Uso de Senhas**

É importante termos certos cuidados na criação, no uso e na guarda de senhas pessoais. Você é o responsável legal por qualquer ação cometida com a sua senha.





**Você protege suas senhas assim:**

a) evite senhas simples, tipo: 12345, ABCDE, 8765, que podem ser rapidamente descobertas. Busque mesclar letras minúsculas, maiúsculas, números e caracteres especiais (*,&,¨%,$,#);

b) não utilize informações pessoais que podem ser facilmente descobertas, tais como: nome, sobrenome, número de CPF, telefone, placa de carro, identidade, data de nascimento e similares;

c) não utilize a mesma senha para diversas finalidades, por exemplo, para sistemas corporativos, conta bancária, correio eletrônico, etc.

d) altere suas senhas periodicamente; e

e) jamais repasse sua senha a terceiros, nem mesmo ao seu chefe ou à equipe da área de informática.

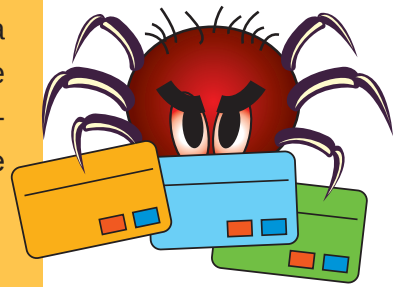
**Utiliza**

O e-mail institucional foi criado e disponibilizado a você com o objetivo de ser usado para o propósito do seu trabalho. Assim, não utilize o e-mail institucional do MP para assuntos pessoais e não utilize e-mail pessoal para fins de trabalho.



## FIQUE LIGADO

**Pessoas mal intencionadas utilizam-se de códigos maliciosos para obter informações sobre senhas, dados bancários, número do cartão de crédito e do CPF, além de poder colocar em risco informações sensíveis do seu trabalho.**



# FIQUE LIGADO

**Você é responsável pelas informações enviadas pela Internet! O e-mail institucional é um recurso importante e está sujeito a monitoramento e investigação.**

**Ao utilizar seu e-mail institucional:**

a) não clique em *link*s e não abra anexos recebidos de remetentes desconhecidos;

b) não cadastre o e-mail institucional em listas de discussões não ligadas ao trabalho;

c) não envie e nem repasse mensagens com conteúdo impróprio, ofensivo e do tipo corrente;

d) não envie dados sigilosos do MP para seu e-mail particular.

**Uso da Identidade Funcional (crachá)**

A utilização da identidade funcional integra o conjunto de medidas de segurança adotado por este Ministério. Sua utilização é obrigatória não apenas para o ingresso em todas as unidades do MP, mas, também, para utilização enquanto exercemos nossas atividades durante a jornada de trabalho.

Isso facilita nossa identificação junto aos demais servidores, áreas de acesso e, inclusive, perante os cidadãos que demandam nossos serviços.





**Informações restritas e sigilosas**

Todos os servidores e colaboradores são responsáveis pelo sigilo das informações que recebem ou tratam no âmbito do MP e devem conhecer e obedecer às restrições de acesso e divulgação associadas.

**E não se esqueça:**

a) ao deixar sua estação de trabalho, guarde todo documento que possa conter informação que não deva ser de conhecimento alheio;

b) não deixe sua sala aberta, facilitando o acesso de pessoas alheias à unidade;e

c) ao se ausentar, lembre-se de desligar ou bloquear o computador. Já imaginou as implicações de alguém não autorizado utilizando a sua conta, acessando e divulgando indevidamente informações sob sua responsabilidade?

FIQUE LIGADO

**O uso do crachá é obrigatório nas dependências do MP. Trata-se de uso pessoal e em nenhuma hipótese deve ser emprestado ou usado por outro que não seja você!**

**Lembre-se: não esqueça documentos em impressoras ou fotocopiadoras. Informações em papéis ou mídias devem ser manuseadas e descartadas de forma adequada.**

# FIQUE LIGADO

**Conheça e pratique a Politica de Segurança da Informação e Comunicações do MP. Ajude a promover uma cultura de segurança da informação. Dissemine essa ideia!**

### 3.3 – Você sabia que também é seu dever zelar pela SIC do Ministério do Planejamento, Orçamento e Gestão – MP?

É dever de todos nós zelar pela Segurança das informações e comunicações do MP. Toda e qualquer ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC pode resultar em responsabilização do servidor nas esferas penal, civil e administrativa.

### 3.4 – O que posso fazer para melhorar a SIC?

Sua participação é fundamental e indispensável para o sucesso da segurança da informação e comunicações, tanto na vida pessoal quanto na profissional. Cultive um comportamento seguro, oriente as pessoas e colegas de seu convívio, reveja sempre as dicas dessa cartilha e busque conhecer os riscos aos quais você se expõe.





**Em caso de suspeitas ou denúncias de quebra de segurança, ou ainda sugestões de melhoria, entre em contato pelo e-mail: cetra@planejamento.gov.br**

# 4 Ações que o MP desenvolve para garantir a Segurança da Informação e Comunicações

Em cumprimento ao determinado pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR, o MP instituiu, por intermédio da Portaria nº 625, de 16 de julho de 2010, seu Comitê de Segurança da Informação e Comunicações – CSIC/MP.

Como principal resultado dos vários trabalhos do CSIC, foi instituída, para todo o MP, a Política de Segurança da Informação e Comunicações – POSIC/MP, pela Portaria nº 27, de 3 de fevereiro de 2012.





A POSIC/MP estabelece diretrizes, critérios e controles indispensáveis à implementação e manutenção da SIC do MP, sobretudo no que diz respeito aos cuidados e responsabilidades que os servidores e colaboradores do ministério devem ter na sua atuação dentro do órgão ou unidade, tais como uso de identificação pessoal, cuidados com os ativos de informação, uso responsável dos recursos de tecnologia e de comunicações.

Outra importante ação foi a instituição, por meio da Portaria SLTI nº 13, de 25 de março de 2011, do Centro de Tratamento e Resposta a Ataques na Rede MP – Cetra/MP, cuja equipe é responsável por tratar adequadamente os incidentes de SIC na rede computacional do MP.

Além disso, o CSIC vem desenvolvendo ações de divulgação, sensibilização, conscientização e formação de multiplicadores no tema da Segurança da Informação e Comunicações, para todos os servidores e colaboradores do MP, abrangendo todas as suas unidades.

# 5 Estrutura de SIC do MP

## 5.1 – Comitê de Segurança da Informação e Comunicações - CSIC

Constituído por representantes de diversas áreas do MP, o CSIC trabalha assessorando a implementação das ações de Segurança da Informação e Comunicações, além de constituir grupos de trabalho e propor soluções e normas específicas sobre SIC. Trabalha também nas proposições, revisões e alterações da POSIC.





## 5.2 – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - CeTRA/MP

Constituído por servidores do Departamento de Tecnologia da Informação – DTI/SE, o Centro de Tratamento de Resposta a Ataques da Rede MP – CeTRA/MP é responsável por receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação e comunicações.

## 5.3 – Gestor de Segurança da Informação e Comunicações

O gestor de SIC é o Coordenador do Comitê de Segurança da Informação e Comunicações – CSIC. É responsável pela promoção da cultura da segurança da informação e comunicações no âmbito do Ministério, apóia as atividades do CeTRA/MP, no que se refere à infraestrutura e capacitação dos membros da equipe e representa o MP nos assuntos de SIC.

# 6 A quem posso recorrer em caso de dúvidas, suspeita, denúncia ou problema relacionado à SIC no MP?

Um incidente isolado, que aparentemente apresenta pouco risco, pode representar parte de uma operação de maior abrangência e maior potencial de risco.





- **É importante informar todo e qualquer incidente identificado ao Cetra/MP: cetra@planejamento.gov.br**
- **Em casos específicos de suspeita de e-mails maliciosos, encaminhe-os para: abuse@planejamento.gov.br**

**Nesta cartilha, encontramos os principais aspectos que possam levar a cada um dos servidores e demais colaboradores do Ministério do Planejamento, Orçamento e Gestão a uma reflexão para mudança de atitudes pessoais e profissionais que assegurem a proteção dos recursos de informação e comunicações do Ministério**

CSIC Comitê de Segurança da Informação e Comunicações

Ministério do **Planejamento**

GOVERNO FEDERAL

BRASIL

PAÍS RICO É PAÍS SEM POBREZA