SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

RESPONSABILIDADE DE TODOS

PRESIDENTE DA REPÚBLICA
Dilma Rouseff

MINISTRO DE ESTADO DO TRABALHO E EMPREGO
Carlos Roberto Lupi

SECRETÁRIO EXECUTIVO
Paulo Roberto dos Santos Pinto

SUBSECRETÁRIO DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO
Antônio Fernando Decnop Martins

COORDENAÇÃO-GERAL DE PLANEJAMENTO E GESTÃO ESTRATÉGICA
Maria Cristianna Barradas Carneiro

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Tiragem: 12000 exemplares
Reimpressão: 2000 exemplares - out/2011

Edição e distribuição:
Coordenação-Geral de Planejamento e Gestão Estratégica

Esplanada dos Ministérios – Bloco "F" – Ed. Sede – Sala 419 - Brasília – DF
CEP: 70059-900 - Fone: (61) 3317.6835
Impresso no Brasil / Printed in Brazil

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca. Seção de Processos Técnicos – MTE

S456 Segurança da Informação e Comunicações:Responsabilidade de Todos – Brasília: MTE, SPOA, CGPGE, 2011.
20 p. il.

Cartilha Institucional.

1. Segurança, Informação, Brasil. 2. Segurança dados,Comunicação, Brasil. I. Brasil. Ministério do Trabalho e Emprego. II. Brasil. Cartilha Segurança da Informação e Comunicações.

CDD 004.6

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 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 Trabalho e Emprego pela Portaria nº 1.327, de 11 de junho de 2010, publicou a sua Política de Segurança da Informação e Comunicações, 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 Trabalho e Emprego (MTE) 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

Saiba o que é

É o conjunto de ações que objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

O que é informação?

É todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Por que Segurança da Informação e Comunicações?

Porque a segurança da informação abrange o processo de transmissão e recepção da informação, desde a elaboração até seu descarte, não importando o meio utilizado para transmiti-la.

Fique Ligado

Devemos proteger o conjunto de dados ou informações em qualquer formato: mídias eletrônicas, papel e até mesmo em conversações pessoais ou por telefone, preservando o valor que possuem e garantindo que esses dados e informações estejam protegidos contra o acesso por pessoas não autorizadas e, consequentemente, estejam sempre disponíveis e confiáveis.

2. Propriedades Básicas da Segurança da Informação e Comunicações (DICA)

Disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade. Consiste na proteção da informação para que não seja alterada ou se torne indisponível, assegurando ao usuário o acesso à informação sempre que dela precisar. Isto pode ser chamado também de continuidade dos serviços.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. A integridade consiste em proteger a informação nas suas mais variadas formas contra alteração, sem a permissão explícita do proprietário daquela informação. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado.

Confidencialidade: propriedade de que a informação não esteja disponível ou seja revelada a nenhuma pessoa física, sistema, órgão ou entidade não autorizada ou não credenciada. Os dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. Está associada à identificação correta de um usuário ou do computador, à certificação e origem da informação. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital.

Fique de olho: quebra de segurança que comprometa a DICA implica responsabilidade administrativa, civil e penal!

3. Você e a SIC

3.1 O que a SIC tem a ver com você?

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

Para que toda a informação 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 e da comunicação.

Segurança da informação e comunicações vai muito além da tecnologia da informação e, mais que isso, está intimamente relacionada ao nosso comportamento, daí o porquê de se exigir, em tempos de inclusão digital, mudança de comportamento, haja vista o potencial lesivo da velocidade com que correm as informações na internet.

Todo servidor público tem um compromisso com a integridade, a confidencialidade, a autenticidade e a disponibilidade da informação. Por isso, é fundamental a conscientização de todos para necessidade da concretização desse compromisso, a partir da adoção de condutas pessoais e procedimentos padrões de segurança adotados no MTE.

3.2 Você sabia que também é seu dever implementar e zelar pela SIC no MTE?

Toda e qualquer ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações pode resultar em responsabilização do servidor nas esferas penal, civil e administrativa.

Conheça mais sobre a SIC, acessando o link:
http://intranetmte/2011/planejamento_gestao/politica-de-seguranca-da-informacao-e-comunicacoes-conheca-e-divulgue.htm

3.3 Você se preocupa com a SIC no seu local de trabalho?

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. Por isso, é preciso tomar cuidado e ficar atento para que as informações corporativas não sejam alteradas sem autorização ou que pessoas mal-intencionadas tenham acesso a dados ou informações sigilosas.

Com simples mudança de hábitos pessoais e funcionais, podemos contribuir para a implantação de uma nova cultura relacionada à segurança da informação e comunicações no âmbito do Ministério do Trabalho e Emprego.

3.4 Boas práticas de SIC que você pode adotar no trabalho

Equipamentos de informática

Alguns procedimentos simples podem evitar transtornos oriundos de códigos maliciosos que são programas especificamente desenvolvidos para executar ações maliciosas em computador, como vírus, cavalos de tróia, spyware:

a) Mantenha seu antivírus atualizado. A equipe técnica da Coordenação-Geral de Informática do Ministério irá se encarregar disso, mas em caso de problema, entre em contato com a mesma para que a situação possa ser corrigida;
b) Evite trazer CD, DVD, pen drives ou quaisquer outros dispositivos móveis de fora do Ministério. Você pode estar trazendo vírus de outros equipamentos para a sua estação de trabalho e consequentemente, poderá infectar não só o seu equipamento, como a rede interna do órgão; e
c) Suspeite de softwares que "você clica e não acontece nada".

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.

Uso de Senhas

É importante certos cuidados na criação, no uso e na guarda de senhas pessoais, pois, o proprietário da senha é o responsável legal por qualquer ação cometida no uso da mesma.

Lembre-se:

a) evite senhas simples, tipo: 12345, ABCDE, 8765...
b) não utilize informações que podem ser facilmente verificadas, como: nome, sobrenome, número de CPF, placa de carro, identidade, data de nascimento....
c) não utilize a mesma senha para diversas finalidades, por exemplo, para sistemas corporativos, conta bancária, correio eletrônico...)
d) utilize senhas de fácil memorização para não precisar anotá-la;
e) efetue a alteração de senha periodicamente; e
f) sua senha não deve jamais ser passada a terceiros, nem mesmo à equipe da área de informática.

Utilização do correio eletrônico corporativo

O correio eletrônico corporativo foi criado com o objetivo de ser usado para fins de trabalho.

Lembre-se:

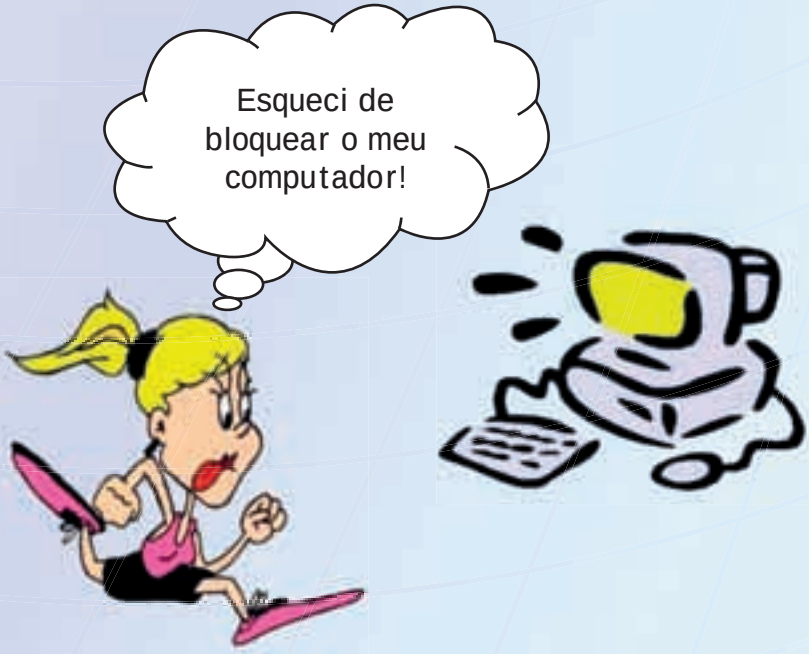
a) não clicar em links ou abrir anexos recebidos de pessoas desconhecidas;
b) não cadastrar e-mail institucional em listas de discussão;
c) não utilizar o e-mail institucional do MTE para assuntos pessoais;
d) não utilizar o e-mail do MTE para enviar ou repassar pornografia nem mensagem com conteúdo impróprio.
e) não repassar/enviar e-mails do tipo corrente; e
f) não enviar dados sigilosos para e-mail particular.

Ambiente de Trabalho

No ambiente de trabalho também devemos adotar certas atitudes para garantir a segurança da informação e comunicações.

Lembre-se:

a) ao deixar sua estação de trabalho, guarde todo documento que possa conter informação que não deva ser do conhecimento de todos;
b) lembre-se de desligar ou bloquear o computador, quando se ausentar; e
c) não deixe a sala aberta, facilitando o acesso de pessoas alheias a unidade.



Uso de Identidade Funcional

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 nas unidades do MTE, mas, também, para utilização enquanto permanecemos exercendo nossas atividades durante a jornada de trabalho diária. Isso facilita, inclusive, nossa identificação perante os cidadãos que demandam nossos serviços, bem como junto aos demais servidores.

Sigilo da informação

O servidor ou colaborador do MTE deve ser capaz de identificar a natureza do sigilo da informação que recebe e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

4. Ações que o MTE tem desenvolvido para garantir a Segurança da Informação e Comunicações

O MTE por intermédio da Portaria nº 1.177, de 30 de dezembro de 2008, cumprindo determinação do Governo Federal, instituiu o seu Comitê de Segurança da Informação e Comunicações - CSIC.

Como fruto do trabalho deste Comitê, por meio da Portaria nº 1.327, de 11 de junho de 2010, foi institucionalizada a Política de Segurança da Informação e Comunicações - POSIC, que objetiva fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação e Comunicações no Ministério.

A POSIC aborda questões referentes aos cuidados que os servidores e colaboradores do MTE devem ter na sua atuação dentro do órgão (crachá, uso de senhas, cuidados com equipamentos e informações que circulam na sua unidade),

inclusive questões referentes ao ingresso nas dependências e instalações do Ministério e a segurança da sua rede de informática e de comunicações.

E por meio da Resolução CSIC nº 1, de 30 de junho de 2010, instituiu a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR no âmbito do MTE.

Além disso, o MTE vem desenvolvendo ações disponibilizadas a todos os seus servidores e colaboradores, tendo como eixo principal a sensibilização, conscientização e formação de multiplicadores em torno da Segurança da Informação e Comunicações do órgão.

5. Estrutura de SIC no MTE

5.1 Comitê de Segurança da Informação e Comunicações – CSIC

Saiba o que é

É o grupo de representantes de unidades do MTE com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do Ministério.

5.2 Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR

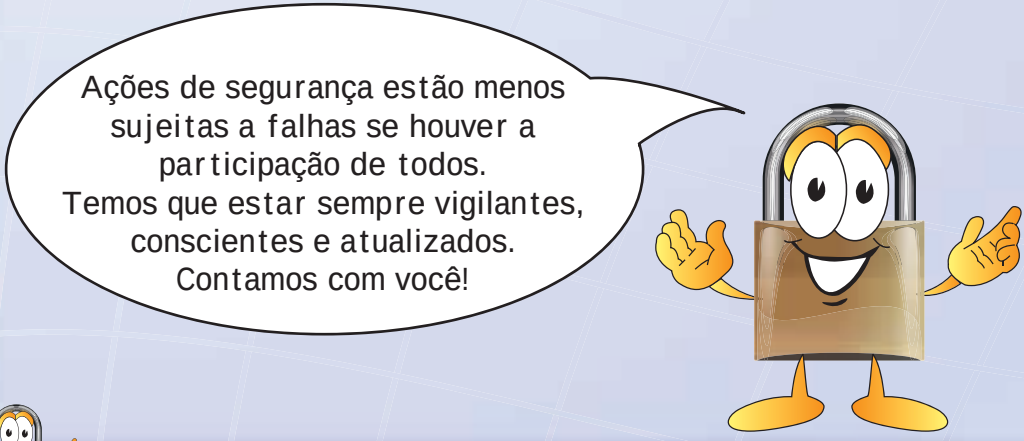
Quem é?

É uma equipe constituída por servidores da Coordenação-Geral de Informática, que tem a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

5.3 Gestor de Segurança da Informação e Comunicações

Quem é?

É o Coordenador-Geral de Planejamento e Gestão Estratégica, responsável pela promoção da cultura da segurança da informação e comunicações no âmbito do MTE. O Gestor de Segurança da Informação e Comunicações também é o coordenador do CSIC e responde pelo apoio às atividades da ETIR, no que se refere à infraestrutura e capacitação dos membros da Equipe.




MTE
Ministério do
Trabalho e Emprego


GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA