UNIVERSIDADE Correios

TLT

SEGURANÇA DA INFORMAÇÃO

Ficha Técnica

Assunto	Área	Carga horária
Segurança da informação	Tecnologia da informação e comunicação	50 min

Objetivo

Citar ações que contribuam efetivamente com a segurança da informação.

Indicador Estratégico

Promover cultura de segurança da informação de TIC.

Conteúdo

- Importância da segurança da informação.
- Pilares da segurança da informação.
- Ameaças mais comuns.
- Como se proteger de golpes e ataques.

Público-Alvo

Empregados da área de atendimento, tratamento e distribuição.

Recursos Instrucionais

Roteiro de TLT e flip chart, se houver.

Bibliografia

CERTBR. **Cartilha de Segurança para Internet, versão 4.0/CERT.br** - São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf> Acesso em 03 de mar. de 2019.

CORREIOS. **Manual de Tecnologia**. Brasília, 2019. Disponível em: <http://intranet/ect-normas/mantic>. Acesso em 11 de jul. de 2019.

ÉPOCA NEGÓCIOS. **Dados são o petróleo da atualidade, diz futurista**. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/06/dados-sao-o-petroleo-da-atualidade-diz-futurista.html.> Acesso em 24 de mai. de 2019.

ANDERSON, Ross. **Security Engineering**: A Guide to Building Dependable Distributed Systems Second Edition. Willey Publishing, Indianapolis, 2008.

Validação

Área responsável pela validação do conteúdo: CS/DIEFI/SUTIC/DEARP/GRIS

Conteudistas: Ricardo Pereira Garcia; Enise Regina Willms Passos; Lara Lemes dos Santos Ferreira; Silvio do Espírito Santo.

Responsável pela Validação: Leonardo Resende Carvalho

Publicação UniCorreios: 03/2020

AÇÕES DO FACILITADOR DO TLT

Para ministrar a sessão de ensino programada, o Facilitador do TLT deve:

- Familiarizar-se com o material instrucional e preparar a aula com antecedência, buscando esclarecimento para as dúvidas que surgirem;
- Estar no local alguns minutos antes do grupo;
- Receber os participantes de forma descontraída. Isso deixa o grupo mais à vontade e cria empatia;
- Começar no horário marcado, mesmo que todos os participantes não tenham chegado. Os presentes não podem ser penalizados;
- Explicar o(s)objetivo(s) de desempenho que os participantes deverão demonstrar ao final da sessão de ensino do TLT;
- Falar sobre a importância do conteúdo que será trabalhado na sessão de ensino;
- Seguir o Roteiro do TLT, onde os assuntos são tratados de forma crescente, do mais simples para o mais complexo.
- Trabalhar apenas um Módulo do TLT em cada sessão de ensino de 50 minutos;
- Tratar o treinando pelo nome;
- Ser claro, paciente e objetivo;
- Criar oportunidades para que os participantes façam perguntas e **evitar**:
  - Monopolizar discussões;
  - Desviar do foco do treinamento;
  - Discussões fora do assunto e debates longos entre participantes.
  - Comprovar a compreensão do treinando a respeito do conteúdo, fazendo perguntas;
  - Responder sempre o que for questionado;
  - Administrar bem o tempo disponível para o repasse de conteúdo;
  - Respeitar o horário de término da sessão de ensino.

Olá pessoal!

Hoje vamos estudar sobre a importância da **segurança da informação** e o cuidado que devemos ter com os dados e as informações físicas e virtuais que circulam na empresa; sejam elas de clientes, empregados, fornecedores, franqueados, parceiros ou mesmo informações estratégicas da organização.

E para começar o estudo, segue uma reflexão:

Reflita

Muitos de nós, empregados dos Correios, vivemos grande parte da vida sem telefone fixo, sem computador, sem celular e, acredite, sem *Whatsapp!*

Pergunta

E hoje, você consegue imaginar sua vida sem esses dispositivos?

Na empresa, um simples pico de energia e pronto! Temos que reduzir ou até mesmo paralisar nossas atividades, pois em grande parte estão relacionadas à tecnologia e, por conseguinte, à segurança da informação!

Mas segurança da informação não se resume somente à tecnologia. Diz respeito à proteção de um conjunto de coisas ou informações que possuem valor para um indivíduo ou uma organização, sejam elas físicas: documentos, objetos postais, ambientes físicos ou virtuais.

Lembrando que o sigilo profissional independe de qualquer dispositivo tecnológico. Desde que ingressamos na empresa, sabemos que é proibido divulgar nomes de pessoas que se correspondem, número de caixa postal, informar o endereço de alguém que tenhamos tomado conhecimento devido às nossas atividades, informar dados dos empregados... enfim, são inúmeras as informações que se forem reveladas indevidamente, causarão muitos problemas.

Já deu para perceber que segurança da informação é um assunto estratégico para as organizações e exige muitos cuidados, não é mesmo?

Reflexão

Imagine vazar dados da empresa para a concorrência ou dados de clientes e empregados! Além de problemas jurídicos, indenizações, risco à imagem, pode ameaçar a sobrevivência da organização. Assim, a responsabilidade de todos em relação à segurança da informação é fundamental!

Capacitação, câmeras, senhas e mais senhas, medidas e sistemas de segurança fazem parte do nosso dia a dia, mas há algo fundamental nisso tudo: o ser humano.

De nada adiantam os mais modernos sistemas de segurança da informação se nós, empregados, não os utilizamos de maneira correta ou se descumprimos nossos deveres, que aliás, estão contidos no Código de Conduta Disciplinar, disponível no MANPES.

Segundo o futurólogo Gerd Leonhard "dados são o novo petróleo", por isso criminosos pagam muito por esses ativos e a forma de alcançar essa fonte de renda é por meio de roubos, por exemplo: de carga, de dados, da bolsa do carteiro, golpes diversos, clonagem de cartões de crédito, trote pelo celular, ataques organizados à rede corporativa, enfim, são muitas formas!

Provavelmente você já ouviu notícias de empresas que sofreram invasões e ataques de *cibercriminosos* (pronuncia-se "saibercriminosos"). Mas não apenas as empresas correm este risco. Qualquer pessoa pode ser vítima, principalmente se não estiver preparada para enfrentar ataques.

Atenção

O elo mais forte para que a segurança da informação se realize plenamente, somos nós, as pessoas.

Por isso, precisamos ter consciência do quanto é importante:

- guardar sigilo das informações;
- utilizar senhas fortes;
- bloquear o computador ao se ausentar da estação de trabalho;
- manter gaveteiros, armários e cofres trancados, sobretudo nas agências;

- vigiar para que somente pessoas autorizadas acessem locais, equipamentos e dispositivos da empresa;
- não fornecer informações pessoais e profissionais a pessoas estranhas ou não autorizadas;
- não conversar sobre assuntos relacionados ao trabalho em barzinhos, supermercados, restaurantes e lugares públicos em geral, pois a conversa pode ser ouvida por pessoas mal intencionadas, além de expor a empresa;
- utilizar crachá quando estiver nas dependências da empresa e nos locais previstos;
- manter portas e portões trancados nos locais onde isso é necessário, entre outras medidas pontuais.
- ter muito zelo na utilização do smartphone durante a entrega, pois os aparelhos eletrônicos são muito visados por ladrões e os parelhos contém informações da empresa e dos clientes.

Como você pode perceber, o rol de cuidados que devemos ter é fundamental para a nossa proteção individual e de toda a organização.

E quando falamos em tecnologia, um conceito muito importante que devemos ter em mente, diz respeito aos **pilares da segurança da informação,** vamos conhecê-los.

É fácil entender, veja só: ao buscar informação sobre dados de entrega de uma encomenda no SRO, o CEP de uma rua ou o seu contracheque, por exemplo, você deseja que a informação esteja a seu dispor, não é mesmo? O nome desse pilar é **disponibilidade.**

Mas não basta a informação estar disponível, é preciso garantir que não haja violação dos dados, que eles não sejam alterados ou excluídos, acidental ou propositalmente. O nome desse pilar é **integridade.**

Então a informação precisa estar disponível e íntegra, mas todas as informações devem estar acessíveis a todos? Não. Imagina todos poderem acessar seu prontuário médico, sua ficha cadastral ou informações estratégicas dos Correios? Por isso, o uso de senhas pessoais e intransferíveis para garantir a **confidencialidade** das informações.

E o último pilar da segurança da informação é a **autenticidade,** ou seja, garantir que as informações que transitam na rede veio da fonte anunciada e sejam acessadas por quem de direito, por meio do registro das ações feitas pelos usuários na rede e nos sistemas.

Então, para os Correios, há quatro pilares da segurança da informação:

- **disponibilidade**
- **integridade**

- **confidencialidade e**
- **autenticidade.**

Embora esses sejam os pilares mais comuns, você poderá encontrar na literatura, algumas variações.

Atenção

Cada empregado tem especial responsabilidade na manutenção dos pilares, pois caso venha a descumprir deveres ou proibições, pode colocar em risco a segurança da informação de toda organização: pessoas e processos.

Para manter os pilares da segurança da informação os Correios contam com uma série de mecanismos: manuais, políticas e códigos. Uma dessas políticas é a **POSIC - Política de Segurança da Informação e Comunicação**.

A POSIC é um documento que estabelece os princípios e diretrizes para proteção dos dados, informações e conhecimentos gerados nos Correios e para os Correios. Visa conscientizar e orientar os usuários para o uso seguro de sistemas e informações, físicos e informatizados.

A POSIC – Política de Segurança da Informação e Comunicação dos Correios, está contida no MANTIC – Manual de Tecnologia da Informação e Comunicação, Módulo 1 – Capítulo 2 – Anexo 2, disponível no Correios Normas.

Dica

Todos os colaboradores devem zelar pela proteção de ambientes, equipamentos, dispositivos, sistemas, documentos, informações, de maneira a impedir que pessoas não autorizadas tenham acesso a esses ativos e possam fazer mau uso.

Hoje em nossa sociedade, há muitos riscos de roubos e ataques, tanto físicos, quanto cibernéticos. Conheça alguns.

Pergunta

Já ouviu falar de “engenharia social” e phi*shing*?

Atualmente, há duas ameaças que merecem muita atenção: a engenharia social e as tentativas de golpes realizados por meio de *phishing* (pronuncia-se “fiching”).

Engenharia social é um método de ataque onde um *cibercriminoso* por meio da persuasão (envolvimento), abusando da ingenuidade, inocência, boa-fé ou confiança do usuário, busca obter informações, aparentemente simples, que podem ser utilizadas para ter acesso não autorizado a computadores, celulares ou informações a respeito de pessoas, horários, rotinas, procedimentos, funcionamento do local entre outras.

Os meios mais utilizados na prática da engenharia social são: contato por telefone, envio de *e-mails*, vasculhação de lixo, invasão de aplicativos de conversas, acompanhamento de postagens em redes sociais (*Facebook*, *Instagram*) e *sites* de relacionamento.

O *phishing* é o ato de “pescar”, roubar informações dos usuários, que via de regra sequer tem noção disso. É uma técnica virtual muito utilizada, como se fosse uma carta (isca), enviada a um alvo, normalmente por *e-mail* ou celular, e a mensagem pode conter algum tipo de arquivo malicioso que contamina o equipamento. É o fato de clicar nessa “isca” em forma de mensagem, que abre as portas do computador ou celular, redes e sistemas para os invasores.

O que pode acontecer? Dependerá de qual tipo de arquivo malicioso está contido na mensagem.

Os “programas maliciosos” podem acessar secretamente um dispositivo sem o conhecimento do usuário, extrair informações pessoais ou senhas e a partir daí o acesso à conta bancária, compras em nome do usuário por meio do cartão de crédito, bloqueio total ou parcial de acesso do proprietário ao próprio aparelho celular, por exemplo.

Os golpes baseados em *phishing* são frequentes e de fácil utilização pelos criminosos, pois, assim como a engenharia social, tem um aspecto comportamental envolvido. Normalmente, as mensagens são atraentes, curiosas, chamam a atenção e oferecem, em geral, emprego, vantagens, sorteios, brindes, prêmios, lucro fácil ou anunciam novidades.

!!! Atenção

Os ataques relacionados à engenharia social possuem as mais variadas características, mas aqui evidenciamos 4 técnicas mais comuns:

1. **Ataque estruturado:** um engenheiro social não aplica golpes indiscriminadamente. Para alcançar seus objetivos planeja seus ataques de modo estruturado. Invade redes próximas ao local ou coloca câmeras de vídeo para estudar a redondeza. O ataque final é só o momento da ação, mas o golpe foi pensado com antecedência e teve planejamento meticuloso.

2. **Coleta de informações:** toda informação é importante, tendo isso em mente, é necessário estar atento aos detalhes. A coleta de informações é parte necessária para que um ataque estruturado aconteça. Por isso, os criminosos utilizam métodos variados de perguntas simples em uma ligação telefônica, por meio de e-mail, coletam dados em redes sociais, vasculham lixo. Toda atenção precisa ser dispensada. Quando um golpe acontece e os criminosos obtém êxito, não foi obra do acaso e sim fruto de muita pesquisa mal intencionada.

3. **Elicitação:** é a extração sutil de informação durante uma conversa, aparentemente normal e inocente. Muito utilizada para montar quebra-cabeças para um futuro golpe ou refinar esses ataques. Como as pessoas, na sua maioria, gostam de conversar, de serem elogiadas e também de demonstrar que sabem algo, a elicitação é esse método de conversa em que parcelas de informações são cedidas, sem que se suspeite do interlocutor.

4. **Pretexto:** é a criação de cenários falsos para aumentar a credibilidade do golpe e induzir as pessoas a colaborar. É uma ação planejada em que as táticas de convencimento são as mais variadas. De técnico pirata da área de tecnologia a um suposto diretor da empresa, de páginas falsas de bancos a lojas inteiras de e-commerce, os *cibercriminosos* conseguem simular um pouco de tudo e a atenção é a única chance para escapar aos golpes.

Importante ressaltar que em muitos casos, somos nós mesmos, pela nossa falta de informação ou descuido, que acabamos por fornecer informações aos criminosos.

Pergunta

Como se proteger de golpes e ataques?

1. **Conhecimento é o melhor mecanismo para evitar golpes. Pessoas que utilizam computadores, *tablets* e *smartphones* e não sabem dos riscos envolvidos no processo, são vítimas potenciais para os golpes.**
2. **Tenha uma senha forte, composta por letras maiúsculas e minúsculas, números e caracteres especiais como por exemplo: *, #, $, @ e memorize-a.**
3. **Senha é pessoal e intransferível. Não empreste sua senha, nem utilize a de outras pessoas, mesmo que sejam colegas e gestores.**
4. **Utilize o e-mail corporativo, apenas para atividades do trabalho.**
5. **De modo algum clique em *links*, acesse sempre pela página indicada.**
6. **Desconfie de produtos, ofertas ou oportunidades com preços e condições excelentes demais.**

Dicas

Conheça mais dicas que o ajudarão a se proteger de golpes e ataques:

- Ao acessar contas bancárias ou demais sites, onde ocorra a troca de informações, verifique a existência de conexão segura, indicada pelo protocolo “https” e pelo cadeado na barra de endereço do navegador.

- Em qualquer interação pela internet, seja por redes sociais, mensageiros instantâneos ou chats, fique atento para determinar quais informações serão passadas por meio desses canais, assim como irá tratar as informações recebidas.

- Nunca forneça informações sensíveis (aquelas que contenham dados sobre política, origem racial e étnica, religiosa, sobre saúde, filiação sindical, e etc.) em *sites*, pelo telefone ou por mensagem de celular, sem que você tenha solicitado o serviço.

Verifique atentamente, peça informações, entre em contato com o estabelecimento ou solicite ajuda de alguém de confiança, antes de passar qualquer informação.

- Sempre desconfie de mensagens recebidas de bancos, Receita Federal ou de lojas, sobretudo por SMS ou no aplicativo de mensagens (WhatsApp) no seu celular, ou por e-mail, solicitando atualização de cadastro ou recadastramento de senha. Certifique-se de que a mensagem é de fato daquela instituição, antes de fornecer qualquer tipo de informação. Normalmente esse tipo de mensagem vem acompanhada de uma "ameaça" como: se você não fizer o "recomendado", sua conta será encerrada, seu pagamento bloqueado ou cairá na malha fina. Mantenha a calma e verifique a procedência da mensagem.

- Cuidado ao fornecer/disponibilizar informações pessoais em *sites* de relacionamento, por exemplo: telefone, CPF, endereço, escola dos filhos, fotos com uniforme, são informações preciosas aos criminosos.

Bom, como você pode perceber, o assunto é super atual, interessante e muito importante tanto para a vida pessoal, quanto profissional. Aproveite e compartilhe as informações com outros colegas de trabalho, amigos e familiares.

Caso queira se aprofundar no assunto, acesse o **Curso Segurança da Informação**, disponível no ambiente virtual, na página da Unicorreios.

Verificação da Aprendizagem

Caro facilitador,

O objetivo da verificação da aprendizagem é reforçar a compreensão do conteúdo. Assim, para se certificar que houve aprendizado, favoreça a participação, o envolvimento e valorize cada resposta.

Para concluir o desenvolvimento do conteúdo, inclua a verificação da aprendizagem para confirmar se o desempenho esperado, indicado no objetivo, foi alcançado.

1. Solicite aos participantes que relembrem algumas ações que colaboram efetivamente com a segurança da informação:

Respostas possíveis:

a) guardar sigilo das informações; b) utilizar senhas fortes; c) bloquear o computador ao se ausentar da estação de trabalho; d) manter gaveteiros, armários e cofres trancados, sobretudo nas agências; e) vigiar para que somente pessoas autorizadas acessem locais, equipamentos e dispositivos da empresa; f) não fornecer informações pessoais e profissionais a pessoas estranhas ou não autorizadas; g) não conversar sobre assuntos relacionados ao trabalho em barzinhos, supermercados, restaurantes e lugares públicos em geral, pois a conversa pode ser ouvida por pessoas mal intencionadas, além de expor a empresa; h) utilizar crachá quando estiver nas dependências da empresa e nos locais previstos; i) manter portas e portões trancados nos locais onde isso é necessário, entre outras medidas pontuais.

2. Como se prevenir de possíveis golpes?

Respostas possíveis:

Conhecimento é o melhor mecanismo para evitar golpes.
Tenha uma senha forte, composta por letras maiúsculas e minúsculas, números e caracteres especiais, e memorize-a.
Senha é pessoal e intransferível.
Utilize o e-mail corporativo, apenas para atividades do trabalho.
De modo algum clique em *links*, acesse sempre pela página indicada.
Desconfie de produtos, ofertas ou oportunidades com preços e condições excelentes demais.

Obrigado(a) a todos pela presença e participação.

Ícone	Finalidade
	Chamar a atenção para determinado assunto
	Informar a carga horaria do curso
	Fornecer uma dica
	Apresentar exemplo para contextualizar o assunto
	Informar os objetivos de aprendizagem
	Fornecer as orientações gerais sobre o curso
	Apresentar perguntas para reflexão ou para introdução de um assunto
	Listar as referências bibliográficas
	Resumir o conteúdo estudado
	Sugerir fontes para complementar conteúdos na forma de “saiba mais”

	Apresentar uma citação
	Promover uma reflexão
	Público
	Curso