



Esta obra foi originalmente desenvolvida pelo CERT.br/NIC.br, com o propósito de promover a conscientização sobre o uso seguro da Internet e baseia-se nos materiais da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>).

Esta obra foi licenciada sob a licença Creative Commons Atribuição-NãoComercial-Compartilhável 4.0 Internacional (CC BY-NC-SA 4.0).

O CERT.br/NIC.br concede a Você uma licença de abrangência mundial, sem *royalties*, não-exclusiva, sujeita aos termos e condições desta Licença, para exercer os direitos sobre a Obra definidos abaixo:

- Reproduzir a Obra, incorporar a Obra em uma ou mais Obras Coletivas e Reproduzir a Obra quando incorporada em Obras Coletivas;
- Criar e Reproduzir Obras Derivadas, desde que qualquer Obra Derivada, inclusive qualquer tradução, em qualquer meio, adote razoáveis medidas para claramente indicar, demarcar ou de qualquer maneira identificar que mudanças foram feitas à Obra original. Uma tradução, por exemplo, poderia assinalar que “A Obra original foi traduzida do Inglês para o Português,” ou uma modificação poderia indicar que “A Obra original foi modificada”;
- Distribuir e Executar Publicamente a Obra, incluindo as Obras incorporadas em Obras Coletivas; e,
- Distribuir e Executar Publicamente Obras Derivadas.

Desde que respeitadas as seguintes condições:

- Atribuição** — Você deve fazer a atribuição do trabalho, da maneira estabelecida pelo titular originário ou licenciante (mas sem sugerir que este o apoia, ou que subscreve o seu uso do trabalho). No caso deste trabalho, deve incluir a URL para o trabalho original (Fonte – cartilha.cert.br) em todos os *slides*.
- NãoComercial** — Você não pode usar esta obra para fins comerciais.
- Compartilhável** — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Aviso — Em todas as reutilizações ou distribuições, você deve deixar claro quais são os termos da licença deste trabalho. A melhor forma de fazê-lo, é colocando um *link* para a seguinte página:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR

A descrição completa dos termos e condições desta licença está disponível em:


<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pt>

Agenda

- **A importância dos seus dados**
- **Como seus dados podem ser abusados**
- **Como se prevenir**
- **Reduza a quantidade de dados sobre você**
- **Informe-se sobre seus direitos**
- **Saiba mais**
- **Créditos**



Guardião Cibernético

 fonte: cartilha.cert.br

- **A importância dos seus dados:** apresenta alguns tipos de dados referentes a sua pessoa, os riscos a que estão sujeitos, exemplos de situações envolvendo esses riscos e ressalta a importância de proteger seus dados.
- **Como seus dados podem ser abusados:** apresenta formas como seus dados podem ser abusados e as consequências trazidas por esses abusos.
- **Como se prevenir:** apresenta dicas de como proteger seus dados.
- **Reduza a quantidade de dados sobre você:** apresenta a importância de reduzir os dados que você próprio divulga na Internet e os que são coletados sobre você.
- **Informe-se sobre seus direitos:** apresenta a Lei Geral de Proteção de Dados e como ela pode ajudar a proteger seus dados.
- **Saiba mais:** apresenta materiais de consulta onde você pode buscar mais informações e manter-se informado.
- **Créditos:** apresenta a lista de materiais usados como fonte das informações contidas nestes *slides*.

A importância dos seus dados (1/3)

- **Dados de cadastros, biográficos, profissionais, financeiros e de navegação são apenas alguns exemplos de dados referentes a você que, diariamente:**
 - circulam por diversas redes
 - são armazenados em diferentes sistemas, dispositivos e mídias
- **Infelizmente, há situações em que seus dados podem ser:**
 - perdidos
 - indevidamente acessados
 - coletados e vendidos sem que você tenha ciência disso

A importância dos seus dados (2/3)

- **Exemplos dessas situações incluem:**
 - **você perde o celular, computador ou mídia removível**
 - **seus dados são interceptados ao trafegarem na rede**
 - **há um vazamento envolvendo seus dados**
 - **suas contas de usuário e sistemas onde seus dados estão armazenados são invadidos**
 - **seus dados de navegação são coletados de forma não transparente e compartilhados sem seu consentimento**

A proteção de dados pode ser considerada um conjunto de mecanismos que visa assegurar que seus dados sejam tratados de forma adequada, a fim de garantir sua privacidade.

Algumas situações em que seus dados podem ser expostos e, conseqüentemente, sua privacidade, ocorrem quando eles são interceptados ao trafegarem na rede, quando há um vazamento de dados e quando suas contas de usuário, sistemas ou equipamentos em que estão armazenados são indevidamente acessados.

A importância dos seus dados (3/3)

- **Para proteger seus dados e assegurar que eles sejam tratados de forma adequada há um conjunto de mecanismos de segurança que podem ser usados**
 - exemplo: o uso de senhas fortes impede o acesso indevido às contas, a criptografia dificulta que seus dados sejam acessados e alterados indevidamente
- **Há situações em que os mecanismos de segurança sozinhos não protegem seus dados**
 - exemplo: quando eles são passados deliberadamente a outros sem sua autorização ou coletados sem necessidade
- **Adotar uma postura preventiva, tentando reduzir a quantidade de dados fornecida por você, é essencial**
- **Para coibir abusos, garantir seus direitos e agir adequadamente é importante conhecer a legislação vigente**

Guardião Cibernético

 fonte: cartilha.cert.br

Seus dados podem ser protegidos por meio do uso de mecanismos de segurança – por exemplo, senhas fortes e criptografia. Por isso, a segurança é considerada um dos pilares fundamentais para a proteção dos seus dados e para garantir sua privacidade. Há situações, entretanto, em que os mecanismos de segurança sozinhos não conseguem proteger seus dados; por exemplo, quando eles são passados deliberadamente a outros sem sua autorização ou são coletados sem necessidade. Para coibir abusos e esclarecer a forma de tratamento de dados, existe a legislação.

Como seus dados podem ser abusados



CERT.br/NIC.br



fonte: cartilha.cert.br

Como seus dados podem ser abusados

- **Pode ocorrer de diversas formas:**
 - acesso indevido
 - perda de dados
 - invasão de contas e golpes
 - coleta excessiva
- **O abuso de seus dados pode acarretar:**
 - prejuízos financeiros
 - restrição a direitos ou benefícios
 - invasão de privacidade

Acesso indevido

- **Seus dados podem ser indevidamente acessados:**
 - **por aplicativos e sites**
 - que processem seus dados além das finalidades informadas
 - **por atacantes ou códigos maliciosos**
 - que consigam acesso às suas contas, equipamentos ou mídias
 - **em casos de vazamentos de dados**



Perda de dados

- **Seus dados podem ser perdidos:**
 - pela ação de códigos maliciosos, como *ransomware*
 - pela ação de atacantes que consigam invadir seus equipamentos e mídias e venham a apagá-los



Ransomware é um programa que torna inacessíveis os dados armazenados em um equipamento e que exige pagamento de resgate para restabelecer o acesso ao usuário. Costuma ser recebido por meio de pastas compartilhadas em rede, pelo acesso a *sites* maliciosos ou invadidos e por mensagens eletrônicas em forma de anexo ou *link* para um arquivo a ser baixado.

O *ransomware* surgiu na década de 80 e suas primeiras versões espalharam-se por disquetes. Apesar de ter caído em desuso por algum tempo, nos últimos anos ele ressurgiu fortemente, impulsionado por alguns fatores, como o uso de criptomoedas, que facilitam a realização de transações bancárias, a quantidade cada vez maior de dados armazenados nos equipamentos, o alto valor desses dados e o grande número de usuários e de empresas que conectam seus equipamentos na Internet sem cuidados de segurança.


A única medida realmente eficaz para impedir a perda de dados causada pelo *ransomware* é fazer *backups* regularmente. Apesar de alguns antivírus serem capazes de detectar e remover certos tipos de *ransomware*, nem sempre eles conseguem recuperar todos os arquivos; além disso, podem rapidamente perder essa capacidade, por não acompanharem a evolução dos novos códigos maliciosos. O pagamento do resgate também não é uma boa opção, pois não garante que o acesso será restabelecido nem que todos os arquivos serão recuperados – além disso, pode incentivar os atacantes a fazerem novos pedidos de extorsão, já que obtiveram sucesso na tentativa anterior.

Existem casos de vítimas que tiveram problemas: ainda que houvessem realizado *backup* de seus dados e conseguido recuperá-los, os atacantes, por não receberem o pagamento do resgate, passaram a fazer novas tentativas de extorsão, como ameaça de vazar os dados coletados.

Invasão de contas e golpes

- **Seus dados podem ser usados:**
 - para adivinhar suas senhas e responder perguntas de segurança
 - em tentativas de golpes, como:
 - *phishing* direcionado e personalizado (*spear phishing*)
 - furto de identidade
 - extorsão



Guardião Cibernético  fonte: cartilha.cert.br

Furto de identidade, ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo a si uma falsa identidade, com o objetivo de obter vantagens indevidas.

Em seu dia-a-dia, sua identidade pode ser furtada, caso alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet, isso também pode ocorrer, se alguém criar um perfil em seu nome e enviar mensagens como se fosse você. Caso sua identidade seja furtada, você poderá arcar com consequências, como falta de crédito e perdas financeiras e de reputação. Além disso, pode levar muito tempo e ser bastante desgastante até que você consiga reverter os problemas causados pelo impostor.

Spear phishing é um tipo específico de *phishing* direcionado que explora tópicos e temas relativos a uma pessoa ou a um grupo específico, por exemplo os funcionários de uma determinada empresa. A grande quantidade de informações disponibilizadas na Internet permite que os golpistas criem mensagens personalizadas, com detalhes bastante convincentes, a fim de dificultar a detecção pelos usuários.

Coleta excessiva

- Muitos aplicativos e *sites* coletam dados extras sem o seu conhecimento e os utilizam para a elaboração de perfis de comportamento (*profiling*)
- Seu perfil pode, então, ser usado sem o seu consentimento:
 - de forma discriminatória
 - para fins como propagandas





Como se prevenir

Nos próximos *slides* veremos dicas sobre vários aspectos que podem prevenir a perda e o vazamento de dados.

- **Autenticação forte**
 - **Contas e senhas**
 - **Verificação em duas etapas**
 - Código de verificação
 - *Token* gerador de senhas
 - Cartão de segurança
 - Dispositivo confiável
 - Lista de códigos reserva/*backup*
 - Chave de recuperação
- **Cuidados no uso da tecnologia**
 - *E-mails* e mensagens eletrônicas
 - **Aplicativos**
 - **Equipamentos e mídias**
 - **Backups**
 - **Criptografia**

Contas e senhas

- **Crie senhas fortes e não repita senhas**
- **Habilite:**
 - **verificação em duas etapas**
 - especialmente em sistemas de armazenamento em nuvem
 - **notificações de login**
 - para ser mais fácil perceber acessos indevidos
 - **configurações de privacidade e segurança**
- **Ao usar equipamentos compartilhados:**
 - **lembre-se de sair de suas contas (*logout*)**



Guardião Cibernético  fonte: cartilha.cert.br

Uma senha, ou *password*, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui.

A sua conta de usuário é de conhecimento geral e é o que permite a sua identificação. Ela é, muitas vezes, derivada do seu próprio nome, mas pode ser qualquer sequência de caracteres que permita que você seja identificado unicamente, como o seu endereço de *e-mail*. Para garantir que ela seja usada apenas por você, e por mais ninguém, é que existem os mecanismos de autenticação.

Contas e senhas

<p>Use:</p> <ul style="list-style-type: none">• números aleatórios<ul style="list-style-type: none">– quanto mais ao acaso forem os números melhor• grande quantidade de caracteres e palavras<ul style="list-style-type: none">– quanto mais longa for a sua senha melhor• diferentes tipos de caracteres<ul style="list-style-type: none">– quanto mais “bagunçada” for a sua senha melhor	<p>Evite usar:</p> <ul style="list-style-type: none">• dados pessoais<ul style="list-style-type: none">– nome, sobrenome– contas de usuário, datas– números de documentos, de telefones ou de placas de carros• dados disponíveis em redes sociais e páginas web• sequências de teclado<ul style="list-style-type: none">– “1qaz2wsx”, “QwerTAsdfG”• palavras presentes em listas publicamente conhecidas<ul style="list-style-type: none">– músicas, times de futebol– personagens de filmes– dicionários de diferentes idiomas
--	--

Guardião Cibernético fonte: cartilha.cert.br

Uma senha boa, bem elaborada, é aquela difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha simples de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Elementos que você **NÃO DEVE** usar ao criar suas senhas:


- **Qualquer tipo de dado pessoal:** evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas.
- **Qualquer tipo de dado relativo ao serviço:** evite palavras associadas ao serviço no qual a senha será usada, como o nome da rede social ou *webmail*.
- **Sequências de teclado:** evite senhas associadas à proximidade entre os caracteres no teclado, como “123456”, “1qaz2wsx” e “QwerTAsdfG”.
- **Palavras que façam parte de listas publicamente conhecidas:** evite nomes de músicas, times de futebol, personagens de filmes e palavras presentes em dicionários de diferentes idiomas.

Elementos que você **DEVE** usar ao criar suas senhas:

- **Números aleatórios:** quanto mais ao acaso forem os números usados, melhor.
- **Grande quantidade de caracteres:** quanto mais longa for a senha, mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas o são facilmente.
- **Diferentes tipos de caracteres:** quanto mais “bagunçada” for a senha, mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação dificulta que ela seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Dicas práticas para elaborar boas senhas

- **Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra**
Frase: “O Cravo brigou com a Rosa debaixo de uma sacada”
Senha: “?OCbcaRddus”
- **Escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres**
Senha: “1 dia ainda verei os aneis de Saturno!!!”
- **Invente um padrão de substituição próprio**
Padrão: substituir “o” por “0” e duplicar as letras “s” e “r”
Frase: “Sol, astro-rei do Sistema Solar”
Senha: “SS0l, asstrr0-rrei d0 SSistema SS0larr”

Guardião Cibernético  fonte: cartilha.cert.br

Algumas dicas práticas que você pode usar na elaboração de boas senhas são:

- **Selecione caracteres de uma frase:** baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase “O Cravo brigou com a Rosa debaixo de uma sacada” você pode gerar a senha “?OCbcaRddus” (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).
- **Utilize uma frase longa:** escolha uma frase longa, que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas à você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha “1 dia ainda verei os aneis de Saturno!!!”.
- **Faça substituições de caracteres:** invente um padrão de substituição baseado, por exemplo, na semelhança visual (“w” e “vv”) ou de fonética (“ca” e “k”) entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras “s” e “r”, substituindo “o” por “0” (número zero) e usando a frase “Sol, astro-rei do Sistema Solar” você pode gerar a senha “SS0l, asstrr0-rrei d0 SSistema SS0larr”.

Contas e senhas

- **Não exponha suas senhas**
 - certifique-se de não estar sendo observado ao digitá-las
 - não as deixe anotadas em locais onde outros possam ver
 - um papel sobre sua mesa ou colado em seu monitor
 - evite digitá-las em computadores e dispositivos móveis de terceiros
- **Não forneça suas senhas para outras pessoas**
 - cuidado com *e-mails*/telefonemas pedindo dados pessoais
- **Use conexões seguras quando o acesso envolver senhas**


Contas e senhas

- **Evite:**
 - **salvar as suas senhas no navegador web**
 - **usar opções, como:**
 - “Lembre-se de mim”
 - “Continuar conectado”
 - **usar a mesma senha para todos os serviços que acessa**
 - basta ao atacante conseguir uma senha para ser capaz de acessar as demais contas onde ela seja usada
- **Não use senhas de acesso profissional para acessar assuntos pessoais (e vice-versa)**
 - **respeite os contextos**

Contas e senhas

- **Crie grupos de senhas, de acordo com o risco envolvido**
 - **crie senhas:**
 - únicas, fortes, e use-as onde haja recursos valiosos envolvidos
 - únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior
 - simples e reutilize-as para acessos sem risco
- **Armazene suas senhas de forma segura:**
 - **use programas gerenciadores de contas/senhas**
 - **anote-as em um papel e guarde-o em local seguro**
 - **grave-as em um arquivo criptografado**

Guardião Cibernético

 fonte: cartilha.cert.br

Crie grupos de senhas, de acordo com o risco envolvido:

- crie senhas únicas e fortes e use-as onde haja recursos valiosos envolvidos. Exemplo: para acesso a *Internet Banking* ou *e-mail*;
- crie senhas únicas, um pouco mais simples, para casos nos quais o valor dos recursos protegidos é inferior. Exemplo: *sites* de comércio eletrônico, desde que as informações de pagamento não sejam armazenadas para uso posterior;
- crie senhas simples e reutilizadas para acessos sem risco. Exemplo: baixar um arquivo.

Armazene suas senhas de forma segura:

- anote-as em um papel e guarde-o em local seguro: este método é preferível a usar senhas fracas pois, é mais fácil garantir que ninguém terá acesso ao papel do que evitar que uma senha fraca seja descoberta;
- grave-as em um arquivo criptografado: mantenha-a um arquivo criptografado e use-o para cadastrar manualmente suas contas e senhas;
- use programas gerenciadores de contas/senhas: programas deste tipo permitem armazenar grandes quantidades de contas/senhas em um único arquivo, acessível por meio de uma chave mestra.

Contas e senhas

- **Altere suas senhas:**
 - **imediatamente: se desconfiar que tenham sido descobertas ou usadas em computadores invadidos ou infectados**
 - **rapidamente:**
 - se perder um computador onde elas estejam gravadas
 - se usar:
 - um padrão de formação e desconfiar que alguma tenha sido descoberta
 - uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles
 - ao adquirir equipamentos acessíveis via rede
 - eles podem estar configurados com senha padrão

Você deve alterar a sua senha:

- **Imediatamente:** sempre que desconfiar que ela pode ter sido descoberta ou que o computador no qual você a utilizou pode ter sido invadido ou infectado.
- **Rapidamente:**
 - se um computador onde a senha esteja armazenada seja furtado/perdido;
 - se usar um padrão para a formação de senhas e desconfiar que uma delas tenha sido descoberta (tanto o padrão como todas as senhas elaboradas com ele devem ser trocadas pois, com base na senha descoberta, um atacante pode conseguir inferir as demais);
 - se usar uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles (esta senha deve ser alterada em todos os lugares nos quais é usada);
 - ao adquirir equipamentos acessíveis via rede, como roteadores Wi-Fi e e *modems* ADSL (muitos destes equipamentos são configurados de fábrica com senha padrão, facilmente obtida na Internet e por isto, se possível, deve ser alterada).

Contas e senhas

- **Configure opções de recuperação de senhas:**
 - endereço de *e-mail* alternativo, pergunta de segurança, dica de segurança, número de telefone celular
- **Ao usar perguntas de segurança:**
 - evite escolher questões cujas respostas sejam facilmente adivinhadas
 - procure criar suas próprias questões
- **Ao usar dicas de segurança, escolha aquelas que sejam:**
 - vagas o suficiente para que ninguém consiga descobri-las, e
 - claras o bastante para que você consiga entendê-las
- **Ao solicitar o envio de suas senhas por *e-mail*:**
 - procure alterá-las o mais rápido possível
 - cadastre um *e-mail* que você acesse regularmente
 - para não esquecer a senha desta conta também

Guardião Cibernético



fonte: cartilha.cert.br

Ao usar perguntas de segurança:

- evite cadastrar questões que possam ser facilmente descobertas, como o nome do seu cachorro ou da sua mãe;
- procure criar suas próprias perguntas e, de preferência, com respostas falsas. Exemplo: caso você tenha medo de altura, pode criar a pergunta "Qual seu esporte favorito?" e colocar como resposta "paraquedismo" ou "alpinismo".

Ao usar dicas de segurança, escolha aquelas que sejam vagas o suficiente para que ninguém consiga descobri-las e claras o bastante para que você consiga entendê-las. Exemplo: se usar a senha "SS0l, asstr0-rrei d0 SSistema SS0larr", cadastre a dica "Uma das notas musicais", isso o fará se lembrar de "Sol" e se recordar da senha.

Ao solicitar o envio de suas senhas por *e-mail*:

- procure alterá-las o mais rápido possível. Muitos sistemas enviam as senhas em texto claro, ou seja, sem nenhum tipo de criptografia e elas podem ser obtidas caso alguém tenha acesso à sua conta de *e-mail* ou use *sniffers*;
- certifique-se de cadastrar um *e-mail* de recuperação que você acesse regularmente para não esquecer a senha desta conta também;
- procure não depender de programas gerenciadores de senhas para acessar o *e-mail* de recuperação (caso você esqueça sua chave mestra ou, por algum outro motivo, não tenha mais acesso às suas senhas, o acesso ao *e-mail* de recuperação pode ser a única forma de restabelecer os acessos perdidos);
- preste muita atenção ao cadastrar o *e-mail* de recuperação para não digitar um endereço que seja inválido ou pertencente a outra pessoa. Para evitar isto, muitos *sites* enviam uma mensagem de confirmação assim que o cadastro é realizado. Tenha certeza de recebê-la e de que as eventuais instruções de verificação tenham sido executadas.

Verificação em duas etapas

- Também chamada de:
 - *two-factor authentication*
 - verificação ou autenticação em dois fatores
 - aprovação de *login*
 - verificação ou autenticação em dois passos
-
- Recurso opcional oferecido por diversos serviços:
 - *webmail, redes sociais, Internet Banking, serviços em nuvem*
 - ao ser habilitada aumenta a segurança de sua conta
 - pode ser desabilitada



Guardião Cibernético

 fonte: cartilha.cert.br

A verificação ou autenticação em duas etapas (*two-factor authentication*, também chamada de aprovação de *login*, verificação ou autenticação em dois fatores ou, ainda, verificação ou autenticação em dois passos) adiciona uma segunda camada de proteção no acesso a uma conta, dificultando que ela seja indevidamente acessada, mesmo com o conhecimento da senha.

A verificação em duas etapas costuma ser uma configuração opcional de segurança e pode ser desativada quando não mais desejada. Ao habilitá-la você estará aumentando a segurança de sua conta e, caso não deseje mais utilizá-la, basta que você a desabilite.

Na verificação em duas etapas são utilizados dois passos de checagem, ou seja, é feita uma dupla verificação. Adicionando uma segunda etapa de verificação fica mais difícil a invasão de uma conta de usuário. Mesmo que um atacante venha a descobrir uma senha ela, isoladamente, não será suficiente para que ele consiga acessar a conta. O atacante necessitará executar a segunda etapa, o que tornará a invasão mais difícil de ser realizada.

Verificação em duas etapas

- **Dificulta o acesso indevido de contas de usuário**
- **Para que o acesso ocorra é necessário que o atacante realize com sucesso duas etapas**
 - primeira etapa: geralmente a senha do usuário
 - segunda etapa: informações adicionais
- **Segunda etapa pode envolver:**
 - **algo que apenas você sabe**
 - outra senha, perguntas de segurança, número PIN, alguma informação pessoal
 - **algo que apenas você possui**
 - código de verificação, cartão de senhas bancárias, *token* gerador de senhas, acesso a determinado computador ou dispositivo móvel
 - **algo que você é**
 - informações biométricas: impressão digital, palma da mão, rosto

Guardião Cibernético



fonte: cartilha.cert.br

Existem três grupos básicos de mecanismos de autenticação, que se utilizam de: aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho), aquilo que apenas você possui (como seu cartão de senhas bancárias e um *token* gerador de senhas) e, finalmente, aquilo que apenas você sabe (como perguntas de segurança e suas senhas).

A escolha do mecanismo a ser usado depende de questões como o “valor” da informação que está sendo protegida e o custo de implementação e manutenção da solução. Mecanismos que envolvam biometria, por exemplo, podem necessitar de equipamentos especiais de reconhecimento. Por outro lado, o envio de um código de verificação para um telefone celular, via mensagem de texto, pode ser bem mais simples devido à facilidade de acesso e à popularização destes dispositivos.

Verificação em duas etapas: Código de verificação

- **Código individual**

- **criado pelo serviço e enviado de forma que apenas você possa recebê-lo**
 - por *e-mail*, chamada de voz, mensagem SMS
 - pode ser gerado por um aplicativo autenticador instalado em seu dispositivo móvel

Cuidados a serem tomados:

- **mantenha atualizados seus dados para recebimento**
 - números de telefones celulares alternativos podem ser cadastrados, caso o seu principal não esteja disponível
- **certifique-se de estar com seu telefone celular, caso tenha configurado:**
 - o envio via SMS ou o uso do aplicativo autenticador
 - aplicativo autenticador deve ser usado em casos onde não é possível receber mensagens SMS

Código de verificação é um código individual criado pelo serviço e enviado de forma que apenas você possa recebê-lo, por exemplo por *e-mail*, chamada de voz ou mensagem de texto (SMS) para o telefone celular que você cadastrou. Também pode ser gerado por um aplicativo autenticador, instalado em seu dispositivo móvel.

Verificação em duas etapas: Token gerador de senhas

- **Chave eletrônica**
 - tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade
- **Cada código é válido por um determinado período**
 - geralmente alguns segundos, após esse tempo um novo código é gerado
 - código pode ser gerado automaticamente ou necessitar que você clique em um botão para ativá-lo

Cuidados a serem tomados:

- **guarde seu *token* em um local seguro**
- **não informe o código mostrado no *token* por *e-mail* ou telefone**
- **caso perca seu *token* ou ele seja furtado:**
 - avise imediatamente o responsável pelo serviço no qual ele é usado

Token gerador de senhas, também chamado de chave eletrônica, é um tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade. Cada código é válido por um determinado período, geralmente alguns segundos, e após esse tempo um novo código é gerado. O código pode ser gerado automaticamente ou necessitar que você clique em um botão para ativá-lo.

Verificação em duas etapas: Cartão de segurança

- **Cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta**

Cuidados a serem tomados:

- **guarde seu cartão em um local seguro**
- **nunca forneça os códigos do cartão por *e-mail* ou telefone**
- **forneça apenas uma posição do seu cartão a cada acesso**
- **verifique se o número de identificação do cartão apresentado pelo serviço corresponde ao que está no seu cartão**
 - caso sejam diferentes entre em contato com o serviço
- **desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição do cartão**

Verificação em duas etapas: Dispositivo confiável

- **Computador ou dispositivo móvel usado para acessar suas contas**
- **No primeiro acesso:**
 - pode ser necessário inserir um código de segurança
 - ele não será necessário nos demais acessos, pois seu dispositivo será “lembrado”, caso você assim o configure

Cuidados a serem tomados:

- não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles
- pode ser necessário habilitar a opção de *cookies* em seu navegador *web* para que seu dispositivo seja memorizado

Dispositivo confiável é um computador ou dispositivo móvel que você frequentemente usa para acessar suas contas. Pode ser necessário inserir um código de segurança no primeiro acesso. Ele não será necessário nos demais, pois seu dispositivo será “lembrado”, caso você assim o configure.

Verificação em duas etapas: Lista de códigos reserva/*backup*

- **Lista de códigos que devem ser usados de forma sequencial e uma única vez**

Cuidados a serem tomados:

- **anote ou imprima a lista e a mantenha em um local seguro**
- **não a armazene em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes**
 - caso não esteja criptografada
- **caso perca a lista ou desconfie que alguém a acessou você deve gerá-la novamente ou revogá-la**
 - anulando assim a anterior

Verificação em duas etapas: Chave de recuperação

- **Número gerado pelo serviço quando você ativa a verificação em duas etapas**
- **Permite que você acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis**

Cuidados a serem tomados:

- **anote ou imprima a chave e a mantenha em um local seguro**
- **não a deixe anotada em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes**
 - caso não esteja criptografada
- **caso perca ou desconfie que alguém acessou a sua chave você deve gerá-la novamente**
 - substituindo assim a anterior

E-mails e mensagens eletrônicas

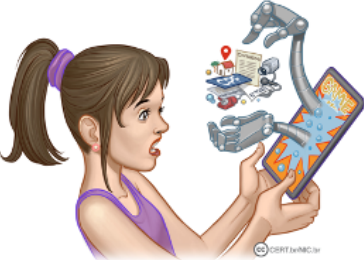
- **Desconfie de *links* ou pedidos de pagamentos recebidos via mensagens eletrônicas**
 - mesmo que vindos de pessoas conhecidas
 - podem ter sido enviadas de perfis falsos ou invadidos
- **Evite:**
 - **clicar/seguir *links* recebidos via mensagens eletrônicas**
 - procure digitar a URL diretamente no navegador
 - **usar *sites* de busca para acessar serviços que requeiram senhas, como seu *webmail* e sua rede social**
- **Seja cuidadoso ao acessar *links* reduzidos:**
 - use complementos que permitam expandir o *link* antes de clicar sobre ele


Fique atento a mensagens que tentem induzi-lo a fornecer informações, instalar/executar aplicativos ou clicar em *links*. Desconfie de mensagens que apelem demasiadamente por sua atenção e que o ameacem, caso você não execute os procedimentos descritos.

Não considere uma mensagem confiável baseando-se apenas na confiança que você deposita em quem a enviou. Essa pessoa pode não ter percebido que se tratava de um golpe ou ter encaminhado sem verificar o conteúdo. Além disso, a mensagem pode ter sido enviada de uma conta invadida, de um perfil falso ou, ainda, ter sido forjada.

Aplicativos

- **Instale aplicativos somente de fontes e lojas oficiais**
 - antes de instalar, verifique as telas e o nome do aplicativo
 - muitos falsos aplicativos se assemelham aos oficiais
- **Observe:**
 - se o desenvolvedor é confiável
 - quantas pessoas instalaram o aplicativo
 - qual a opinião delas sobre o aplicativo
- **Fique atento às permissões:**
 - forneça apenas as que considerar necessárias
 - limite quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização
- **Apague os aplicativos que não usa mais**



Guardião Cibernético  fonte: cartilha.cert.br

Configure permissões de sistemas e aplicativos de maneira a minimizar os acessos que eles tem aos seus dados. Preferencialmente, permita apenas o necessário e enquanto estiver usando, a fim de reduzir a coleta e exposição ampla e contínua dos dados.


Remova versões antigas e aplicativos que você não usa mais, eles tendem a ser esquecidos e a ficar potencialmente vulneráveis.

Equipamentos e mídias

- **Atualize o sistema e os aplicativos**
- **Utilize mecanismos de segurança**
- **Cuidado para não perder *pen drives* e discos externos**
- **Antes de se desfazer de seus equipamentos e mídias apague os dados armazenados**
- **Ao enviar equipamentos para manutenção escolha empresas com boa reputação**
- **Seja cuidadoso ao usar equipamentos de terceiros ou potencialmente infectados**



Guardião Cibernético

 fonte: cartilha.cert.br

Mantenha os programas instalados com as versões mais recentes e com todas as atualizações aplicadas. Fabricantes costumam lançar novas versões e atualizações quando há recursos a serem adicionados, ajustes a serem feitos e vulnerabilidades e erros a serem corrigidos. Sempre que uma nova versão ou atualização é lançada, ela deve ser prontamente instalada, pois isso ajuda a proteger seus equipamentos da ação de atacantes e códigos maliciosos. Além disso, alguns fabricantes deixam de dar suporte e de desenvolver atualizações para versões antigas, o que significa que novas vulnerabilidades não serão corrigidas.

Use mecanismos de segurança, como programas *antispam*, *antimalware* e *firewall* pessoal, e assegure-se de mantê-los atualizados.

Backups

Backups protegem seus dados em caso de mau funcionamento de equipamentos, da perda de dispositivos e da ação de códigos maliciosos, especialmente *ransomware*

- **Faça regularmente *backup* dos seus dados**
- **Programe seus *backups* para serem feitos automaticamente**
- **Teste periodicamente seus *backups***
 - para ter certeza de que estão sendo feitos corretamente
- **Mantenha pelo menos um *backup off-line***



Guardião Cibernético

 fonte: cartilha.cert.br

Você já imaginou o que aconteceria se, de uma hora para outra, perdesse alguns ou até mesmo todos os dados armazenados em seu computador? E se fossem todas as suas fotos ou os dados armazenados em seus dispositivos móveis? E se, ao enviar seu computador para manutenção, você o recebesse de volta com o disco rígido formatado? Para evitar que estas situações aconteçam, é necessário que você aja de forma preventiva e realize cópias de segurança (*backups*).

Muitas pessoas, infelizmente, só percebem a importância de ter *backups* quando já é tarde demais, ou seja, quando os dados já foram perdidos e não se pode fazer mais nada para recuperá-los.

Backups são extremamente importantes, pois permitem:

- **Recuperação de versões:** você pode recuperar uma versão antiga de um arquivo alterado, como uma parte excluída de um texto editado ou a imagem original de uma foto manipulada.
- **Arquivamento:** você pode copiar ou mover dados que deseja ou que precisa guardar, mas que não são necessários no seu dia a dia e que raramente são alterados.
- **Proteção de dados:** você pode preservar seus dados para que sejam recuperados em situações como falha de disco rígido, atualização malsucedida do sistema operacional, exclusão ou substituição acidental de arquivos, ação de códigos maliciosos/atacantes e furto/perda de dispositivos.

Arquivos

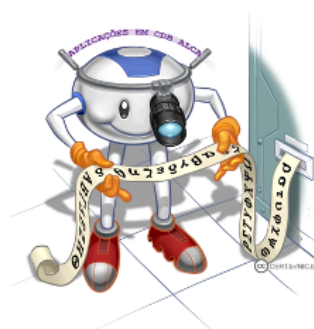
- **Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados**
- **Crie uma partição criptografada ou use outros recursos de criptografia para armazenar seus arquivos de forma segura**
- **Seja cuidadoso ao abrir arquivos enviados por terceiros**



Criptografia

A criptografia ajuda a tornar as transmissões de dados mais seguras, detectar alterações em seus dados e impedir que sejam lidos indevidamente

- **Use criptografia para proteger os dados armazenados em seus equipamentos e mídias**
 - em caso de perda ou furto será mais difícil deles serem acessados
- **Ative as configurações de criptografia em seus discos e mídias**
 - como *pen drives* e discos externos
- **Use conexões seguras**




Guardião Cibernético

 fonte: cartilha.cert.br

A criptografia é considerada a ciência e a arte de escrever mensagens em forma cifrada ou em código. A primeira vista, ela até pode parecer complicada, mas, para usufruir dos benefícios proporcionados por ela, você não precisa estudá-la profundamente nem ser nenhum matemático experiente. Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à maioria dos sistemas operacionais e aplicativos e, muitas vezes, é usada de forma imperceptível ou requer que você realize algumas configurações básicas.

Reduza a quantidade de dados sobre você



 fonte: cartilha.cert.br

Rastros digitais

- **Você sabia que todas as vezes que acessa seus equipamentos e “entra na Internet” alguns de seus dados são de alguma forma fornecidos?**
- **Cada vez que acessa um site, assiste a um vídeo ou compra algo, deixa marcas de sua passagem**
 - **essas marcas são chamadas vestígios, rastros ou pegadas digitais**
 - **permitem criar sua reputação *online* e definir seu perfil comportamental**



Guardião Cibernético



fonte: cartilha.cert.br

Você já imaginou que todas as vezes que acessa seus equipamentos e “entra na Internet” fornece informações sobre você? Cada vez que você acessa um *site*, assiste a um vídeo ou compra algo, está deixando marcas de sua passagem – essas marcas são chamadas vestígios, rastros ou pegadas digitais (*digital footprinting*).

Os vestígios digitais costumam ser de dois tipos: ativos e passivos. Enquanto os vestígios digitais ativos são deixados intencionalmente por você, como parte de suas ações (por exemplo quando curte uma foto, posta algo ou envia um *e-mail*); os vestígios digitais passivos são coletados sobre você, sem que você saiba ou tenha controle sobre isso (por exemplo os que você deixa quando navega na Internet ou os que são coletados por seus aplicativos).

Sua reputação *online* é aquilo que “a Internet diz sobre você”. Basta pesquisar pelo seu nome para verificar os resultados – quanto mais resultados forem apresentados, mais detalhada será sua reputação *online*.

Assim como você provavelmente pesquisa sobre a reputação de uma empresa cujos serviços deseja contratar, algumas empresas fazem o mesmo quando pretendem contratar um novo funcionário ou conceder algum tipo de crédito.

Caso queira conhecer e gerenciar sua reputação *online* é importante criar o hábito de pesquisar seu nome na Internet. Alguns *sites* de buscas permitem que você configure buscas específicas para serem executadas de tempos em tempos, a fim de emitirem alertas caso encontrem algum resultado novo: você pode criar buscas sobre seu nome e ser alertado quando novos resultados aparecerem.

Dados que você divulga

- **Pense bem antes de divulgar algo**
 - depois será difícil de excluir
- **Seja seletivo ao aceitar seus contatos nas redes sociais**
- **Ao preencher cadastros questione-se sobre a necessidade:**
 - de fornecer todos os dados solicitados
 - da instituição retê-los

Quanto mais informações você divulga, mais fácil é, para um golpista, furtar sua identidade, pois ele tem mais dados disponíveis e, provavelmente, será mais convincente. Para coletar seus dados, inclusive suas senhas, o golpista pode usar outros tipos de golpes (como códigos maliciosos) e de ataques (como força bruta e interceptação de tráfego).

Pense bem antes de postar algo, pois não há possibilidade de arrependimento. Uma frase ou imagem fora de contexto pode ser mal interpretada e causar mal-entendidos. Após uma informação ou imagem se propagar, dificilmente poderá ser totalmente excluída.

Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa, tanto agora quanto futuramente.

Sempre que alguém solicitar dados sobre você ou quando preencher algum cadastro, procure se perguntar o motivo de pedirem determinada informação, se ela é realmente necessária no contexto a que se destina e evite fornecê-la, caso conclua que a solicitação é abusiva ou desnecessária.

Dados coletados sobre você

- Use conexões seguras
- Seja seletivo ao baixar aplicativos
- Observe as configurações de privacidade de seus aplicativos e navegadores
- Ao acessar *sites*, procure limitar a coleta de dados por *cookies*
 - preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão
- Limpe frequentemente o histórico de navegação

Inicialmente, grande parte da navegação *web* não envolvia o tráfego de informações sigilosas e costumava ser feita por meio do protocolo HTTP, que não oferece criptografia (as informações trafegam em texto claro), não garante que o usuário esteja se comunicando com o *site* desejado nem que os dados não possam ser interceptados, coletados, modificados ou retransmitidos. Com o passar do tempo, a oferta de serviços via Web envolvendo informações sigilosas tem aumentado, assim como os tipos de ataques e as técnicas usadas pelos atacantes. Com isso, as características do protocolo HTTP mostraram-se insuficientes para garantir a segurança e seu uso passou a ser gradativamente substituído pelo HTTPS.

O protocolo HTTPS usa certificados digitais para assegurar a identidade tanto do *site* de destino como a do usuário que está navegando. Também usa métodos criptográficos e outros protocolos, como SSL e TLS, para assegurar a confidencialidade e a integridade das informações. Atualmente, conexões usando o protocolo HTTP (quando o endereço do *site* começa com “http://”) são chamadas **conexões inseguras ou não seguras**, ao passo que aquelas que usam o HTTPS (quando o endereço do *site* começa com “https://”) são chamadas **conexões seguras**.



O titular dos dados pessoais tem diversos direitos garantidos pela LGPD, como a revogação do consentimento, a exclusão de dados, a portabilidade para outro fornecedor ou serviço e a correção de dados incompletos, inexatos ou desatualizados. É importante que você conheça essa lei para que possa detectar mais facilmente os casos e agir da forma que considerar mais adequada.

Lei Geral de Proteção de Dados (LGPD)

- **Criada para que:**
 - o indivíduo tenha controle sobre seus dados pessoais
 - saiba como esses dados são tratados por organizações públicas, privadas e terceiros
- **Dados pessoais, segundo a LGPD:**
 - informações relacionadas a pessoa natural identificada ou identificável
- **Como titular de dados pessoais você tem diversos direitos garantidos pela LGPD, como os definidos no art. 18**
- **Informe-se sobre a LGPD, conheça seus direitos e saiba como agir de forma adequada:**
 - <https://www.gov.br/anpd/pt-br/legislacao>

A “Lei Geral de Proteção de Dados Pessoais” (LGPD), que regulamenta o tratamento de dados em território brasileiro, foi criada para coibir o uso indiscriminado de dados pessoais.

Um dos pressupostos fundamentais da LGPD é que o tratamento de dados pessoais só pode ser realizado em determinadas hipóteses, como mediante o fornecimento de consentimento pelo seu titular, e deve observar princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Benefícios e direitos trazidos pela LGPD (1/2)

- **A LGPD:**
 - **dá a você o direito de saber:**
 - como seus dados são exatamente tratados
 - quais dados são coletados
 - o porquê e com quem seus dados são compartilhados
 - **traz maior segurança jurídica**
 - ao fornecer mecanismos para que você tenha controle sobre quais dados seus são coletados e como são usados
- **Organizações públicas e privadas devem disponibilizar informações claras que o ajudem a compreender:**
 - **os termos de consentimento**
 - **as bases legais que apoiam o tratamento dos seus dados**

Benefícios e direitos trazidos pela LGPD (2/2)

- **Caso a instituição responsável pelo tratamento de seus dados pessoais não atenda a um de seus direitos de titular sem uma justificativa legal:**
 - **você tem o direito de peticionar uma reclamação para a Autoridade Nacional de Proteção de Dados – ANPD**
 - **https://www.gov.br/anpd/pt-br/canais_atendimento**

A Autoridade Nacional de Proteção de Dados – ANPD é um órgão vinculado à Presidência da República, dotada de autonomia técnica e decisória, que tem a competência de zelar pela proteção dos dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto na Lei nº 13.709, de 14 de agosto de 2018, a LGPD. Mais informações em <https://www.gov.br/anpd> .

Saiba mais

- Consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet: cartilha.cert.br
- Confira os demais materiais sobre segurança para os diferentes públicos: internetsegura.br
- Acompanhe novidades e a dica do dia no Twitter do CERT.br twitter.com/certbr



Guardião Cibernético

fonte: cartilha.cert.br

Novidades e dicas diárias podem ser obtidas por meio do RSS da Cartilha e do Twitter do CERT.br:

- Twitter: <https://twitter.com/certbr>
- RSS: <https://cartilha.cert.br/rss/cartilha-rss.xml>

No *site* da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>) você encontra diversos materiais, como dicas rápidas sobre vários assuntos e outros fascículos, com temas como Boatos, *Internet Banking*, Senhas e Verificação em Duas Etapas, entre outros.

No *site* Internet Segura (<https://internetsegura.br/>) você encontra materiais de interesse geral e para diversos públicos específicos, como crianças, adolescentes, pais, educadores, pessoas com mais de 60 anos e técnicos. Além dos materiais produzidos pelo NIC.br, há também iniciativas de outras entidades e instituições, com diversas informações sobre uso seguro da Internet.

Créditos

- **Cartilha de Segurança para Internet**
 - ▶ Fascículo Proteção de Dados
 - ▶ Fascículo Senhas
 - ▶ Fascículo Verificação em Duas Etapascartilha.cert.br/guardiao

- **Livro Segurança na Internet**
cartilha.cert.br/livro



Apoio de Divulgação:  Produção: cert.br nic.br cgib.br

ESTE SLIDE NÃO PODE SER REMOVIDO. DEVE SER EXIBIDO EM TODAS AS REPRODUÇÕES, INCLUSIVE NAS OBRAS DERIVADAS.

Esta obra foi originalmente desenvolvida pelo CERT.br/NIC.br, com o propósito de promover a conscientização sobre o uso seguro da Internet e baseia-se nos materiais da Cartilha de Segurança para Internet (<https://cartilha.cert.br/>).

Esta obra foi licenciada sob a licença Creative Commons Atribuição-NãoComercial-Compartilhual 4.0 Internacional (CC BY-NC-SA 4.0).

O CERT.br/NIC.br concede a Você uma licença de abrangência mundial, sem *royalties*, não-exclusiva, sujeita aos termos e condições desta Licença, para exercer os direitos sobre a Obra definidos abaixo:

- a. Reproduzir a Obra, incorporar a Obra em uma ou mais Obras Coletivas e Reproduzir a Obra quando incorporada em Obras Coletivas;
- b. Criar e Reproduzir Obras Derivadas, desde que qualquer Obra Derivada, inclusive qualquer tradução, em qualquer meio, adote razoáveis medidas para claramente indicar, demarcar ou de qualquer maneira identificar que mudanças foram feitas à Obra original. Uma tradução, por exemplo, poderia assinalar que “A Obra original foi traduzida do Inglês para o Português,” ou uma modificação poderia indicar que “A Obra original foi modificada”;
- c. Distribuir e Executar Publicamente a Obra, incluindo as Obras incorporadas em Obras Coletivas; e,
- d. Distribuir e Executar Publicamente Obras Derivadas.

Desde que respeitadas as seguintes condições:

- **Atribuição** — Você deve fazer a atribuição do trabalho, da maneira estabelecida pelo titular originário ou licenciante (mas sem sugerir que este o apoia, ou que subscreve o seu uso do trabalho). No caso deste trabalho, deve incluir a URL para o trabalho original (Fonte – cartilha.cert.br) em todos os *slides*.
- **NãoComercial** — Você não pode usar esta obra para fins comerciais.
- **Compartilhual** — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Aviso — Em todas as reutilizações ou distribuições, você deve deixar claro quais são os termos da licença deste trabalho. A melhor forma de fazê-lo, é colocando um *link* para a seguinte página:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.pt_BR

A descrição completa dos termos e condições desta licença está disponível em:

<https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.pt>