Segurança da

# INFORMAÇÃO

SAIBA COMO PROTEGER SEUS DADOS

## Guia prático de segurança de dados

INSTITUTO FEDERAL
Espírito Santo

# Introdução

O Guia prático de segurança da informação tem o objetivo de orientar os servidores acerca da proteção de dados pessoais e institucionais no âmbito do Instituto Federal do Espírito Santo (Ifes). Nele serão abordados temas como: uso adequado do e-mail institucional, como se proteger de ataques virtuais, cuidados ao utilizar computadores e programas e acesso à internet.

# Uso adequado do e-mail institucional

O e-mail institucional é a forma de comunicação oficial utilizada pelo Instituto Federal do Espírito Santo tanto para comunicação interna quanto externa. No entanto, o uso desta ferramenta também traz riscos quando utilizada de forma inadequada. Caso sejam desrespeitados aspectos profissionais, normativos, éticos e morais, o Ifes fica exposto a riscos, com repercussões sociais, políticas e econômicas.

Seguem algumas orientações:

**1** - Não utilize o e-mail institucional para tarefas não profissionais, como campanhas, promoções e redes sociais.

**2** - O sigilo da senha é responsabilidade do servidor.

**3** - A qualquer indício de anormalidade na conta, redefina sua senha.

**4** - Ao receber mensagens com conteúdos estranhos, que podem ser spams ou mensagens maliciosas, não clique no link e envie um e-mail para: spam@ifes.edu.br e DTI-Seguranca@ifes.edu.br.


# Senha

A senha é utilizada 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.

Há muitos perigos em expor a sua senha. Se outra pessoa souber a sua credencial de usuário e tiver acesso à sua senha, ela poderá utilizar essas informações e se passar por você na internet, realizando ações em seu nome, como:

**1** - Acessar a sua conta de correio eletrônico e ler seus e-mails, enviar mensagens de spam e/ou contendo phishing e códigos maliciosos, além de ter acesso à sua lista de contatos.

**2** - Pedir o reenvio de senhas de outras contas para esse endereço de e-mail (e assim conseguir acesso a elas).

**3** - Acessar o seu computador e obter informações sensíveis armazenadas nele, como senhas e números de cartões de crédito.

**4** - Utilizar o seu computador para esconder a real identidade dessa pessoa (o invasor) e, então, desferir ataques contra computadores de terceiros.

# Senha

## Alguns cuidados a serem tomados ao utilizar suas contas e senhas são:

**1** - Certifique-se de não estar sendo observado ao digitar suas senhas.

**2** - Não forneça suas senhas para outra pessoa, em hipótese alguma.

**3** - Certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senhas.

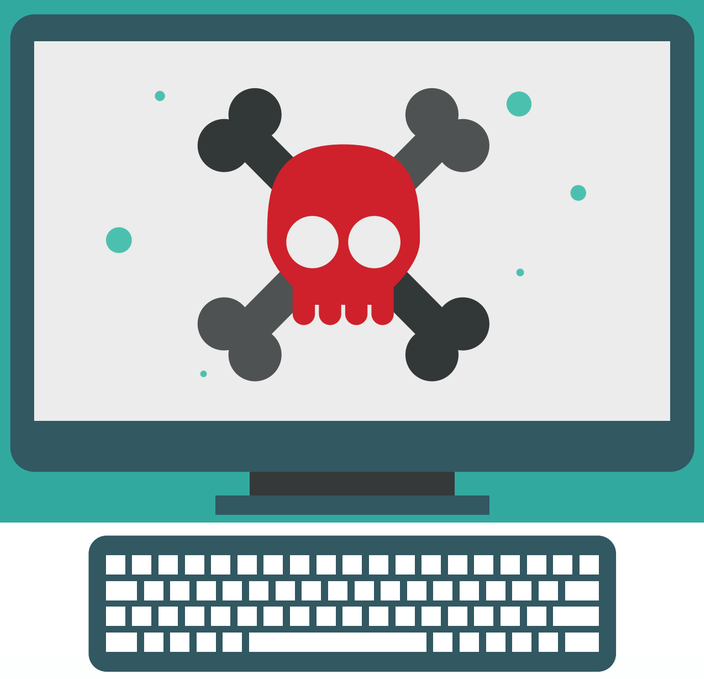
**4** - Utilize a opção de sair (logout), pois isso evita que suas informações sejam mantidas no navegador.

**5** - Não utilize a mesma senha para todos os serviços que acessa.

**6** - Elabore senhas fortes com no mínimo seis caracteres, alternando entre letras, números, caracteres especiais e:

- **a)** Não use qualquer tipo de dado pessoal.
- **b)** Não use sequências de teclado como: "1qaz2wsx" e "QwerTAsdfG".

Caso perceba qualquer sinal de comprometimento da segurança de credenciais ou de equipamento do Instituto, favor entrar em contato com a TI de sua unidade.



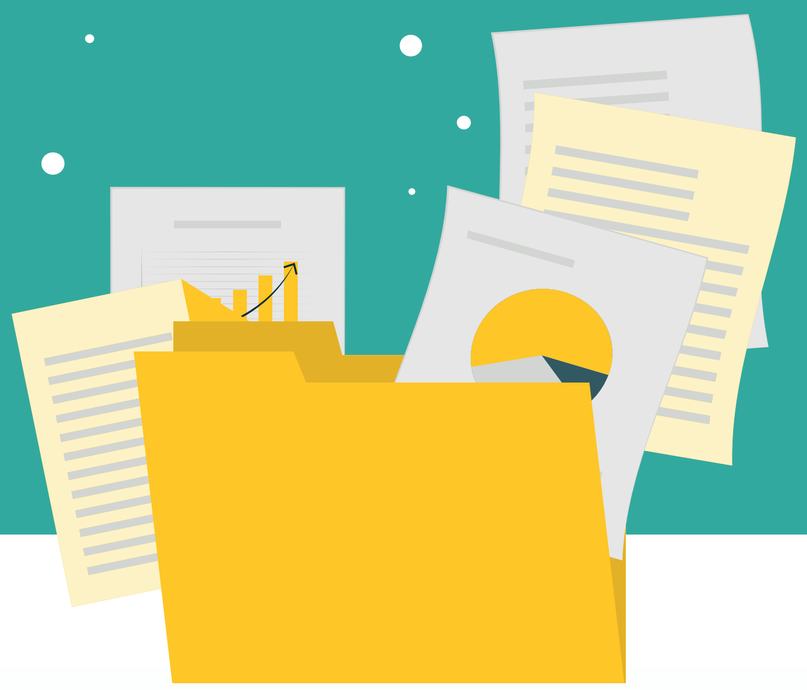
# Ataques virtuais

Como regra geral, a maioria dos ataques e fraudes na internet utiliza Engenharia Social, quando uma pessoa se passa por outra para convencer o usuário a clicar em links ou fornecer informações.

Isso acontece nos ataques de phishing, spam, links e banners maliciosos.

Além das dicas anteriores, fique atento ao que suas crianças fazem nas redes sociais. Pois, nesses casos, o perigo pode passar do mundo virtual para o real.

Desconfie de propostas ou contatos recebidos de pessoas em redes sociais, mesmo quando a pessoa é conhecida, pois a conta pode ter sido invadida.



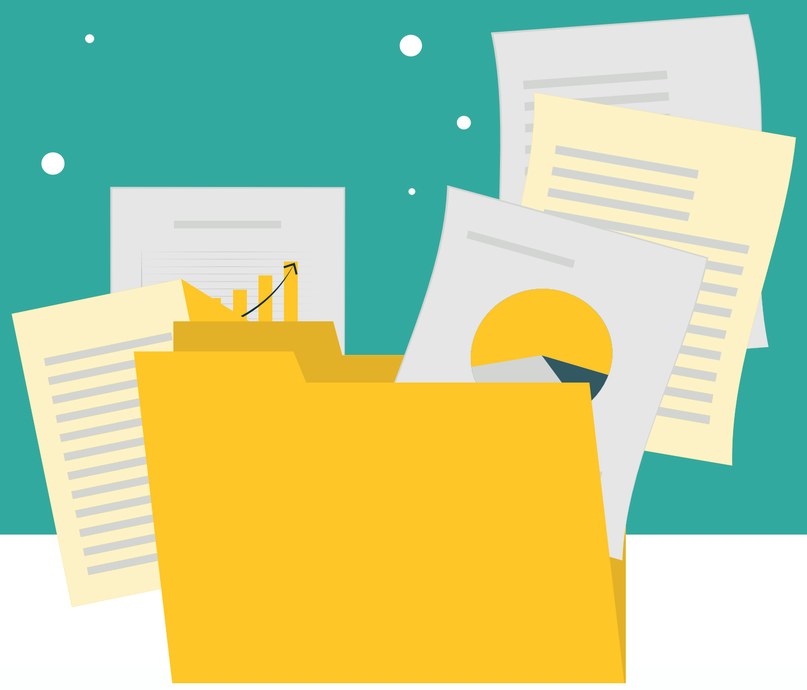
# Spam

Spam é o termo utilizado para se referir aos e-mails não solicitados. Geralmente possuem as seguintes características:

**1** - Apresentam no campo “Assunto” palavras com grafia errada ou suspeita.

**2** - Apresentam no campo “Assunto” textos alarmantes ou vagos como “Sua senha está inválida”, “A informação que você pediu” e “Parabéns”.

**3** - Contém mensagens de conteúdo duvidoso e pedem para acessar algum link.



# Spam

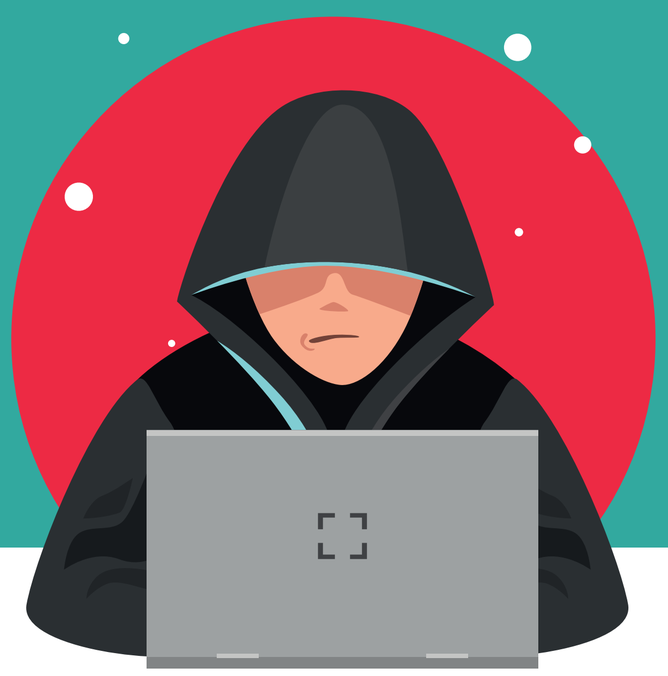
## Dicas de prevenção:

**1** - Não clique em links recebidos de usuários desconhecidos e não responda mensagens desse tipo (essas ações podem servir para confirmar que seu e-mail é válido).

**2** - Desabilite a abertura de imagens em e-mails HTML (o fato de uma imagem ser acessada pode servir para confirmar que a mensagem foi lida).

**3** - Crie contas de e-mail secundárias e forneça-as em locais onde as chances de receber spam são grandes, como ao preencher cadastros em lojas e em listas de discussão.

**4** - Respeite o endereço de e-mail de outras pessoas. Use a opção de CCO (Cópia Oculta) ao enviar e-mail para grande quantidade de pessoas. Ao encaminhar mensagens, apague a lista de antigos destinatários, pois mensagens reencaminhadas podem servir como fonte de coleta para spammers.



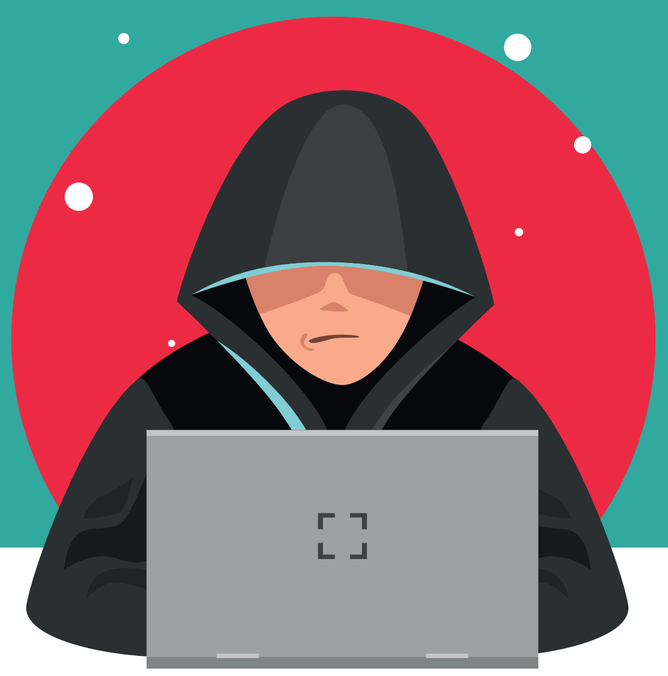
# Phishing

Phishing, phishing-scam ou phishing/scam é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social.

## Atenção!

Para atrair a atenção do usuário, as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento. Exemplos de situações envolvendo phishing são:

**1** - Páginas falsas de comércio eletrônico ou internet banking.
**2** - Páginas falsas de redes sociais ou de companhias aéreas.
**3** - Mensagens contendo formulários.
**4** - Solicitação de recadastramento.
**5** - Pedidos para acessar links de modo a aumentar a capacidade do e-mail.
**6** - Validação de informações de nota fiscal.



# Phishing

## Prevenção:

**1** - Fique atento às mensagens recebidas em nome de alguma instituição que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links.

**2** - Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança).

**3** - Fique atento às mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos.

**4** - Seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador web.

**5** - Verifique se a página utiliza conexão segura. Sites de comércio eletrônico ou internet banking confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados.

# Internet

## Ao acessar redes públicas

Dicas de segurança para conexões sem fio para manter você protegido enquanto usa o Wi-Fi público.

Em cafés, hotéis, shoppings, aeroportos e muitos outros locais que oferecem a seus clientes acesso a um Wi-Fi público é comum conferir e-mails, interagir nas redes sociais ou acessar a Internet durante o tempo livre. Entretanto, os criminosos virtuais costumam espionar redes Wi-Fi públicas e interceptar os dados transferidos pelo link. Dessa forma, o criminoso consegue acessar as credenciais bancárias, senhas de contas e outras informações valiosas dos usuários.

Seguem algumas dicas úteis da equipe de especialistas em segurança.

**Fique atento!**

Uma conexão Wi-Fi pública é basicamente desprotegida, então tome cuidado.

**Lembre-se: qualquer dispositivo pode estar em risco**

Laptops, smartphones e tablets são suscetíveis aos riscos de segurança de uma conexão sem fio.

# Internet

## Desconfie de todos os links no Wi-Fi

Não presuma que o link do Wi-Fi é legítimo. Pode ser um link falso, configurado por um criminoso virtual que tenta capturar informações pessoais valiosas de usuários mais desatentos. Questione tudo e não se conecte a pontos de acesso sem fio desconhecidos ou não reconhecidos.

## Verifique se a conexão sem fio é legítima

Alguns links falsos, configurados por usuários maliciosos, levam um nome de conexão deliberadamente semelhante ao do café, hotel ou local que oferece o Wi-Fi gratuito. Se você conversar com um funcionário do local que oferece a conexão Wi-Fi pública, peça informações sobre o ponto de acesso Wi-Fi legítimo, como nome e endereço IP da conexão.

## Use uma VPN (rede virtual privada)

Quando você usa uma VPN para se conectar a uma rede Wi-Fi pública, na verdade está usando um "túnel particular" que criptografa todos os dados que passam pela rede. Isso ajuda a evitar que criminosos virtuais, que ficam de tocaia na rede, interceptem seus dados.

# Internet

## Evite usar sites de tipos específicos

É sempre bom evitar se conectar a sites pelos quais os criminosos virtuais consigam capturar sua identidade, senhas ou informações pessoais, como redes sociais, serviços de banco on-line ou sites que armazenam informações de cartões de crédito.

## Pense em usar os dados do seu celular

Se for necessário acessar sites que armazenam ou exigem informações sigilosas, incluindo redes sociais, sites de compras on-line e bancos on-line, vale a pena acessá-los pela rede do seu celular, e não pela conexão Wi-Fi pública.

## Proteja seu dispositivo contra ataques virtuais

Garanta a proteção de todos os seus dispositivos com uma rigorosa solução de segurança e antimalware e mantenha-a sempre atualizada.

# Internet

## Ao navegar na internet

**1** - Fique atento aos conteúdos que saltam em sua tela (pop-ups).
**2** - Não clique nos anúncios de sites desconhecidos.
**3** - Navegue por sites considerados confiáveis.
**4** - Nunca insira senha ou credenciais em sites que não utilizem HTTPS (sites que não possuem o cadeado ao lado do endereço).

## Ao utilizar salas virtuais

### Exigir senhas

Como organizador da reunião, esta é a ação número 1 que você pode executar para proteger suas reuniões.

Torne as senhas obrigatórias para todas as suas reuniões para proteger contra pessoas não convidadas.

### Verificar participantes

Verifique a lista de participantes ao enviar o convite para a reunião e revise a lista de participantes durante a chamada. Remova qualquer pessoa que não deva fazer parte da reunião.

Para reuniões em que informações confidenciais estão sendo compartilhadas, como uma reunião completa da empresa, aumente a segurança exigindo que os participantes se autentiquem fazendo login antes de poderem participar da reunião.

# Internet

## Verifique os links da reunião

Ao receber um convite para uma reunião, verifique se é de um remetente conhecido e confiável.

Além disso, verifique o link da reunião antes de clicar,  e fique atento a links maliciosos com “.exe”, por exemplo.

Há um aumento acentuado nas tentativas de phishing usando links maliciosos com nomes dos fornecedores de videoconferência incorporados, mas eles o levam a sites de login falsos.

## Atualizações

Verifique se o software de videoconferência está atualizado com as atualizações mais recentes fornecidas pelo fornecedor e se há atualizações automáticas ativadas.

Quando se trata de softwares baseados em nuvem, utilizados via navegador, a atualização é feita de forma automática.

## Mantenha a confidencialidade

Mantenha conversas confidenciais em sigilo e verifique se você não compartilha acidentalmente nada de confidencial no laptop ou no plano de fundo.

Os fundos virtuais ganharam popularidade por uma mudança de cenário!

# Internet

## Compartilhamento de tela

Limite o recurso de compartilhamento de tela apenas para o administrador ou para alguém que seja selecionado. Isso evita a possibilidade de alguém compartilhar conteúdo por engano.

Ao compartilhar a tela, compartilhe apenas o aplicativo necessário, e não de toda a área de trabalho. Mesmo um ícone ou nome de arquivo em uma área de trabalho pode fornecer informações confidenciais.

O iOS da Apple produz capturas de tela usadas ao alternar tarefas entre aplicativos. Para estar protegido contra isso, incluindo a captura de informações confidenciais, verifique se o sistema de conferência pode desfocar esta imagem.

## Prevenção

Reserve um tempo para conhecer todas as opções de configurações disponíveis no sistema de videoconferência. Normalmente, existem muitos recursos e encontrar a configuração certa para o seu ambiente é uma tarefa importante e deve ser realizada para garantir que as comunicações da empresa permaneçam seguras.

Verifique a política de privacidade do serviço que você está usando. O ditado que diz “se é grátis, você é o produto” deve ser motivação suficiente para verificar se a empresa está coletando, vendendo ou compartilhando seus dados para financiar a prestação de seu serviço “gratuito”.

# Cuidados ao utilizar o computador/notebook

## Bloqueie a tela quando não estiver no mesmo ambiente do computador

Quando usar seu computador em locais públicos ou quando se ausentar do ambiente, é importante tomar cuidados para evitar que ele seja indevidamente utilizado por outras pessoas. Procure manter seu computador bloqueado quando você não estiver por perto (isso pode ser feito utilizando protetores de tela com senha; nos sistemas Windows a combinação das teclas "WIN + L" já é suficiente para habilitar essa proteção).

## Utilize apenas programas originais

A instalação de programas não originais, obtidos de mídias e sites não confiáveis ou via programas de compartilhamento de arquivos, pode incluir a instalação de códigos maliciosos, colocando em risco seu computador.

Caso deseje utilizar um programa proprietário, mas não tenha recursos para adquirir a licença, procure por alternativas gratuitas ou mais econômicas e que apresentem funcionalidades semelhantes às desejadas. Diga não à pirataria, é crime.

No ambiente do Ifes, caso haja necessidade de usar softwares proprietários, um processo de contratação deve ser aberto e encaminhado para a área de Tecnologia da Informação. A pirataria coloca o Instituto inteiro em risco e o servidor poderá ser punido de acordo com as sanções legais.

# Cuidados ao utilizar o computador/notebook

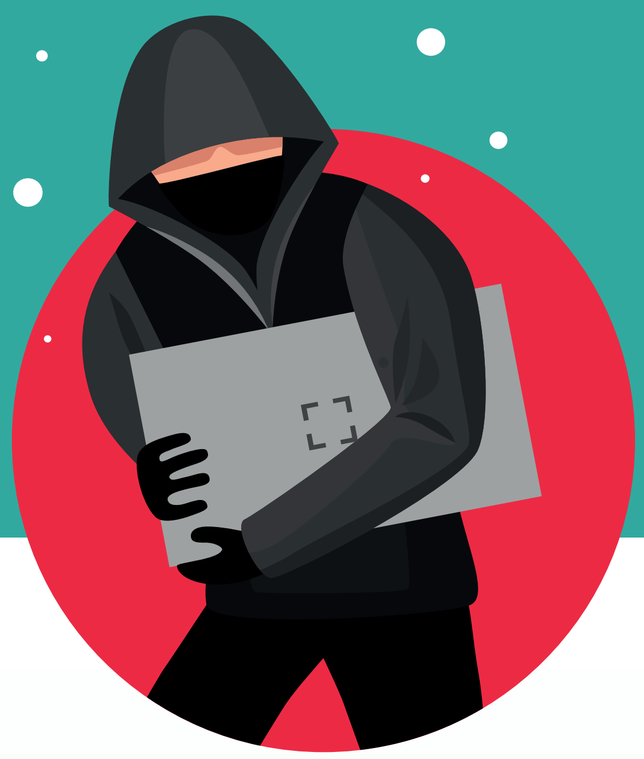
## Mantenha seus sistemas atualizados

Procure por atualizações automáticas diretamente nas opções do software ou sistema operacional, ou baixe as atualizações regularmente a partir do fornecedor oficial. Novas ameaças e vulnerabilidades são descobertas todos os dias. Logo, para se proteger, você deve manter seu sistema operacional e seus aplicativos sempre atualizados.

## Seja cuidadoso ao manipular arquivos

Alguns mecanismos, como os programas antimalware, são importantes para proteger seu computador contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas. Novos códigos maliciosos surgem a todo momento e nem sempre são acompanhados pela capacidade de atualização dos mecanismos de segurança. Por isso, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas.

**1** - Seja cuidadoso ao clicar em links, não importando como foram recebidos e quem os enviou;
**2** - Não considere que mensagens vindas de conhecidos são sempre confiáveis, pois o campo remetente pode ter sido falsificado ou elas podem ter sido enviadas de contas falsas ou invadidas;
**3** - Não abra ou execute arquivos sem antes verificá-los com seu antivírus.



# Cuidados ao utilizar o computador/notebook

## Perda ou furto de celular, notebook ou desktop

O que fazer em caso de perda ou furto de celular, notebook ou desktop?

**1** - Informe a sua operadora e solicite o bloqueio do seu número (chip).
**2** - Altere as senhas que possam estar armazenadas nele, como as de acesso ao e-mail, rede social e Sipac.
**3** - Bloqueie cartão de crédito cujo número esteja armazenado em seu dispositivo móvel.
**4** - Se estiver configurada a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados nele armazenados com auxílio de softwares especializados previamente instalados.

Diretoria de Tecnologia da Informação
Comitê Gestor de Segurança da Informação

INSTITUTO FEDERAL
Espírito Santo