

CONFIDENCIAL

Cartilha de Segurança da Informação

Versão 1.0 – **Anonimizada para fins de portfólio.**

São Paulo

2022

SOBRE O AUTOR

Flávio F Cunha atua como consultor de segurança da informação e docente desde 2002. Durante este período esteve em empresas dos mais variados setores, liderando projetos de segurança da informação e implementando soluções *FOSS (Free and Open Source Software)*. Atualmente exerce a função de especialista em segurança da informação para o grupo XXX.

AGRADECIMENTOS

Agradeço ao meus colegas de *tech* e ao meu gestor yyyy pela confiança e apoio durante o desenvolvimento deste trabalho.

PREFÁCIO

Esta cartilha foi elaborada para informar e conscientizar os colaboradores sobre as melhores práticas de segurança da informação.

O conhecimento das principais ameaças e técnicas utilizadas pelos cibercriminosos é fundamental para criação de medidas preventivas de segurança, afinal, não podemos nos proteger daquilo que não conhecemos.

todos os programas e ativos tecnológicos podem apresentar falhas de segurança passíveis de serem exploradas por um invasor para obtenção de um acesso não autorizado. Além disso, técnicas de manipulação e convencimento social conhecidas como engenharia social, também são usadas para persuadir os colaboradores a passarem informações sensíveis da empresa e de seus ativos. Portanto, as organizações devem estar preparadas para tratar tanto as falhas tecnológicas, quanto os riscos que podem surgir de informações sensíveis passadas através de ataques de engenharia social.

Esperamos que os temas descritos neste material ajudem de forma significativa a aumentar o conhecimento dos colaboradores sobre segurança da informação.

Boa leitura!

Sumário

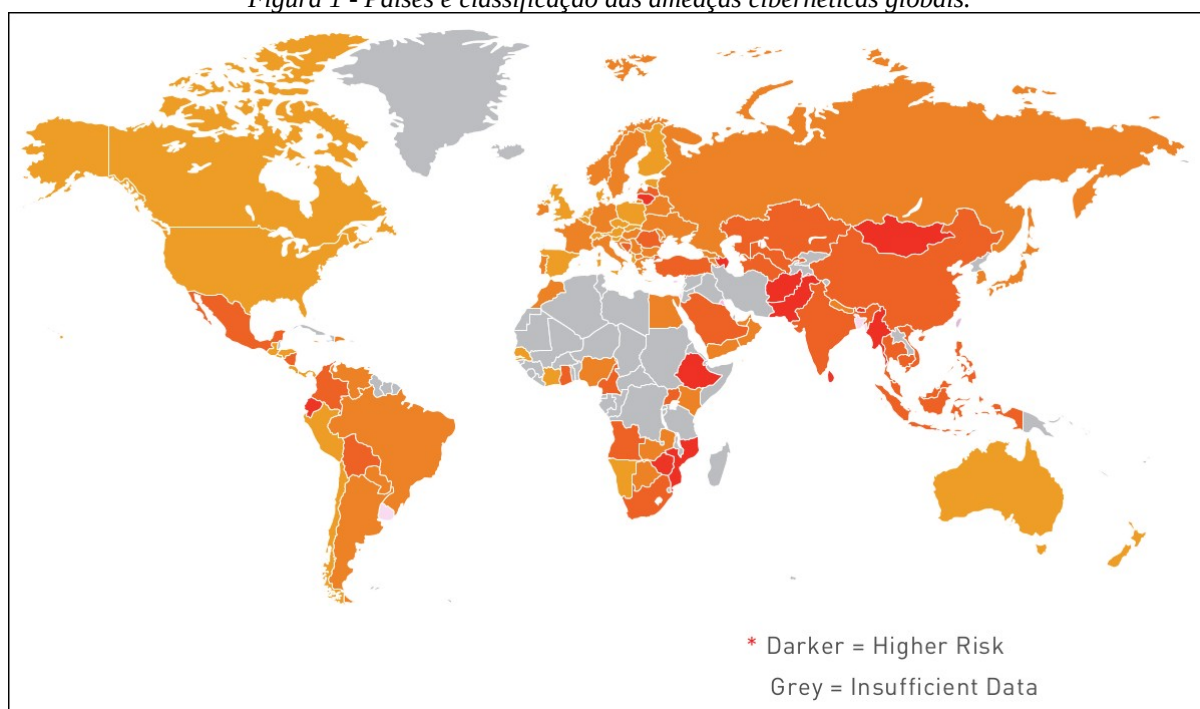
| | |
|---|----|
| 1 INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO..... | 1 |
| 1.1 Propriedades fundamentais da segurança da informação..... | 2 |
| 1.2 Gestão da segurança da informação e o cubo de <i>McCumber</i> | 5 |
| 2.0 GERENCIAMENTO DE SENHAS..... | 6 |
| 2.1 O que é uma senha segura?..... | 6 |
| 2.2 Política de senhas para os colaboradores VÍSSIMO..... | 8 |
| 3.0 IDENTIFICAÇÃO, AUTENTICAÇÃO, AUTORIZAÇÃO E AUDITORIA..... | 10 |
| 3.1 MFA - <i>Multi Factor Authentication</i> | 10 |
| 4.0 CONTROLE DE ACESSO E POLÍTICA DO PRIVILÉGIO MÍNIMO..... | 15 |
| 5.0 SEGURANÇA PARA AS ESTAÇÕES DE TRABALHO..... | 16 |
| 5.1 Política para instalação e remoção de programas..... | 16 |
| 5.2 Principais riscos..... | 17 |
| 5.3 Cuidados a serem tomados..... | 17 |
| 6.0 SEGURANÇA NA INTERNET..... | 18 |
| 6.1 Segurança em conexões <i>web</i> | 18 |
| 6.2 Mas o que é criptografia e como ela funciona?..... | 18 |
| 6.2.1 Criptografia assimétrica..... | 20 |
| 6.3 Protegendo informações sensíveis nos <i>sites</i> da internet..... | 21 |
| 6.3.1 Como verificar se o <i>site</i> é protegido por criptografia?..... | 21 |
| 6.3.2 Como detectar <i>sites</i> sem suporte a criptografia?..... | 22 |
| 6.3.3 Como detectar sites falsos, maliciosos ou com o certificado expirado?..... | 22 |
| 7.0 BACKUPS..... | 24 |
| 8.0 ENGENHARIA SOCIAL..... | 26 |
| 8.1 Tipos de engenharia social..... | 27 |
| 8.1.2 Exemplos de abordagens..... | 27 |
| 8.1.3 Como se proteger da engenharia social..... | 30 |
| 9.0 MALWARES..... | 31 |
| 9.1 Definição de <i>Malware</i> | 31 |
| 9.1.2 Principais tipos de <i>Malware</i> | 31 |
| 9.2 Contramedidas para proteção contra <i>Malwares</i> | 35 |
| 10 RANSOMWARE..... | 36 |
| 10.1 Estatísticas do <i>Ransomware</i> pelo mundo..... | 36 |
| 10.2 Métodos de infecção..... | 37 |
| 10.3 Mecanismos de defesa e contramedidas contra <i>ransomwares</i> e <i>malwares</i> em geral..... | 40 |
| 11 CONSIDERAÇÕES FINAIS..... | 42 |

1 INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Diante de um cenário global onde as ameaças digitais representam enormes riscos para as organizações, as iniciativas de segurança da informação se tornaram fundamentais e estratégicas para manter a infraestrutura tecnológica dos setores público e privado funcionando adequadamente.

O relatório *Cyber Security Report 2021* da *Check Point Research* exibe o índice de risco das ameaças cibernéticas globais. Onde o Brasil é classificado como país de alto risco, conforme podemos observar na figura 1.

Figura 1 - Países e classificação das ameaças cibernéticas globais.



1.1 Propriedades fundamentais da segurança da informação

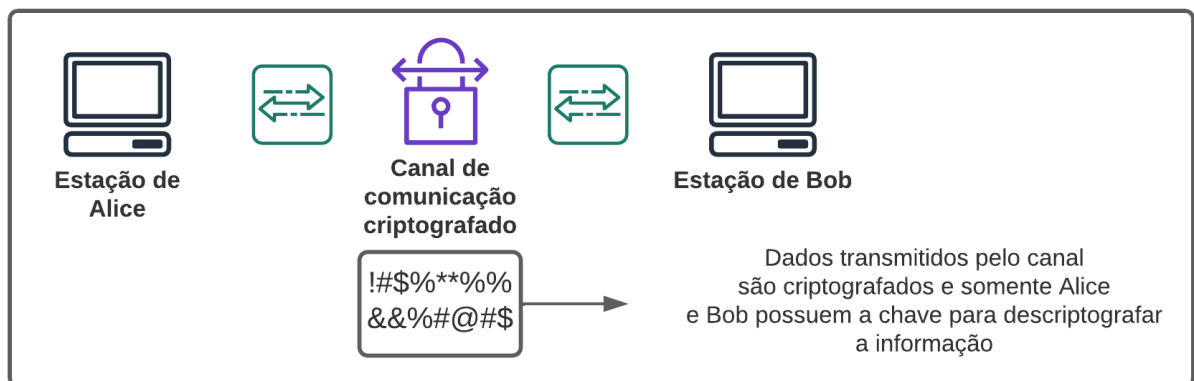
A segurança da informação deve garantir que todo o fluxo que envolva o armazenamento, processamento, transmissão e entrega da informação seja protegido de acordo com as suas propriedades mais importantes, que são: confidencialidade, integridade e disponibilidade. No ambiente tecnológico o acrônimo CIA é utilizado para fazer referência a estas três propriedades.

Confidencialidade

A confidencialidade garante o acesso à informação apenas para as pessoas com permissões para acessá-la.

Esquemas de permissões de acesso e criptografia são usados para garantir esta propriedade. Na figura 2 o canal criptografado estabelece confidencialidade para a comunicação entre Alice e Bob.

Figura 2 - Canal criptografado estabelecendo confidencialidade para a comunicação.

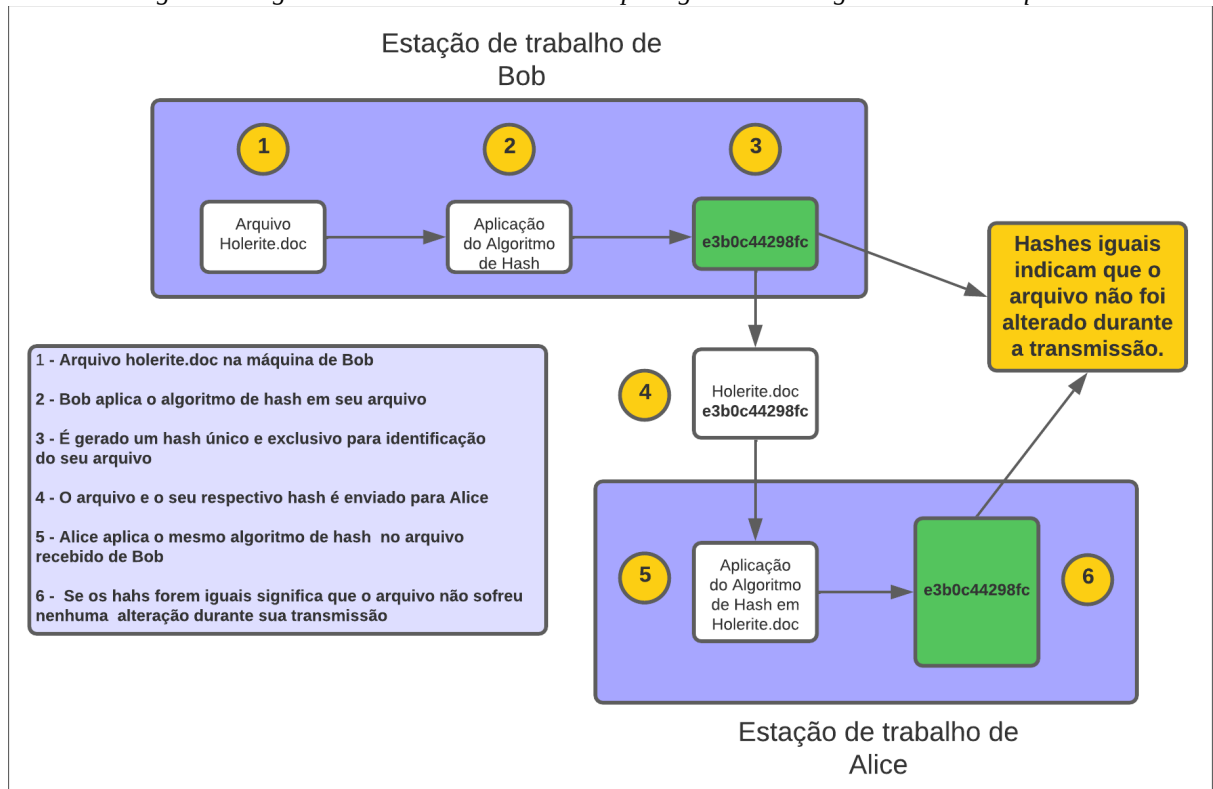


Integridade

A integridade garante que a informação chegue de forma íntegra ao usuário, ou seja, sem alterações no seu conteúdo original.

As tecnologias de *Hash* fornecem uma assinatura única e exclusiva para cada informação, desta forma, podem garantir que a mesma não foi corrompida ou sofreu alterações durante o seu ciclo de vida. A figura 3 mostra um algoritmo de *hash* sendo usado para garantir que um arquivo enviado de Bob para Alice chegue sem modificações durante sua transmissão.

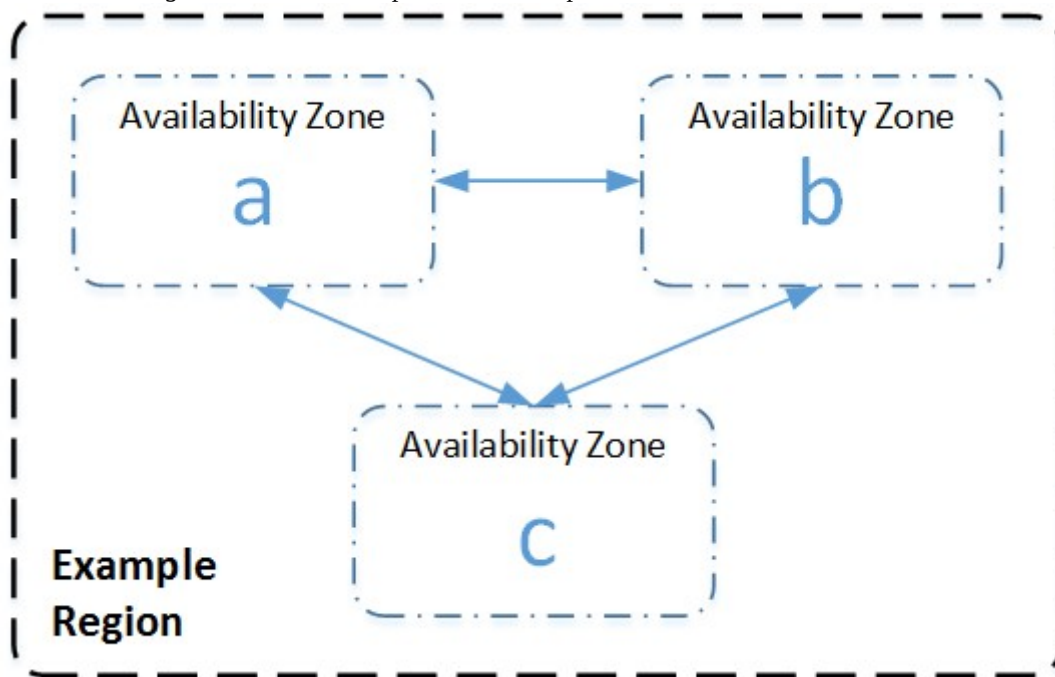
Figura 3 - Algoritmo de hash sendo utilizado para garantir a integridade de um arquivo.



Disponibilidade

A disponibilidade garante que a informação esteja disponível sempre que o usuário necessitar. Mecanismos de redundância, *load balancing*, *auto scaling* e *backups* são usados para atingir a alta disponibilidade. Um exemplo seria a plataforma de *Cloud Amazon AWS*, que fornece 3 diferentes zonas de disponibilidade dentro de uma mesma região. Desta forma, uma aplicação pode estar disponível simultaneamente nas zonas **A** e **C**. Se a zona **A** ficar indisponível a zona **C** continuará mantendo a disponibilidade da aplicação. A figura 4 apresenta o modelo de zonas de disponibilidade da *Amazon AWS*.

Figura 4 - Zonas de disponibilidade do provedor de nuvem Amazon AWS.



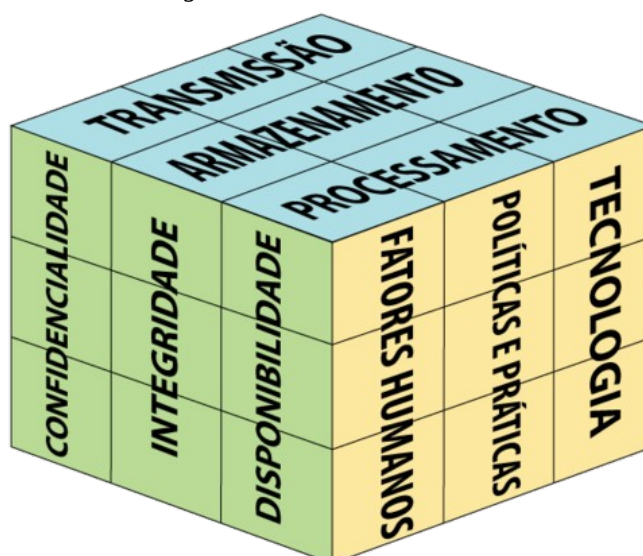
1.2 Gestão da segurança da informação e o cubo de *McCumber*

A figura 5 apresenta o cubo de segurança cibernética ou cubo de *McCumber*.

Este cubo mostra como as propriedades de segurança da informação interagem com os estados que a informação pode assumir e com as estratégias para sua proteção.

A primeira dimensão do cubo inclui as três propriedades da segurança da informação (confidencialidade, integridade e disponibilidade). A segunda dimensão apresenta os estados que as informações ou dados podem assumir, ou seja, a informação pode estar armazenada em algum lugar (sistema de arquivos ou banco de dados), sendo transmitida de um ponto para outro ou em processamento por alguma aplicação. Por fim, a terceira dimensão, identifica as áreas de conhecimento necessárias para proteger a informação (tecnologia, políticas e práticas e fatores humanos).

Figura 5 - Cubo de *McCumber*.



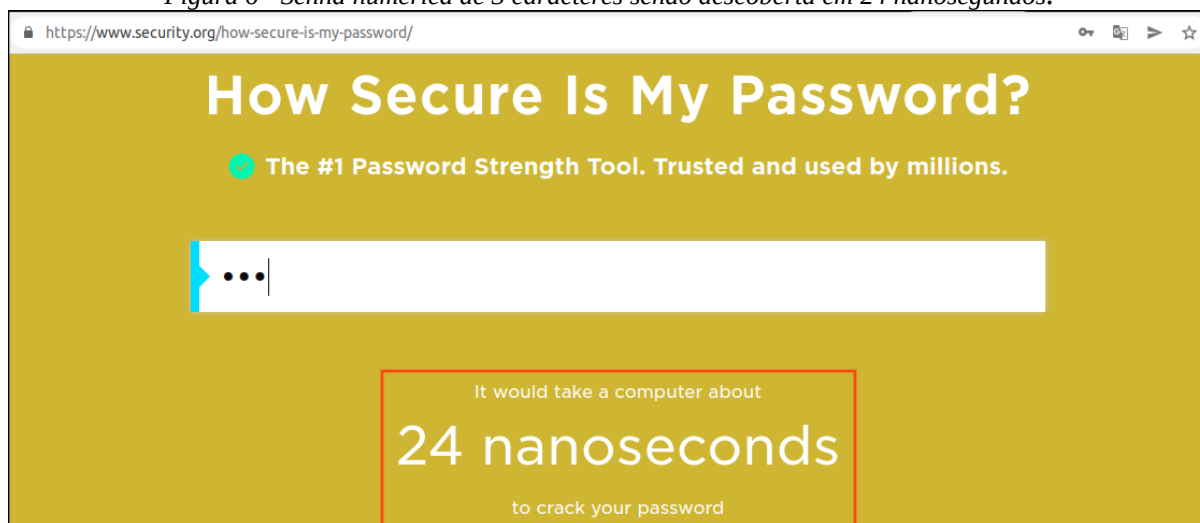
2.0 GERENCIAMENTO DE SENHAS

Apesar de todos os avanços tecnológicos, o processo de autenticação com senhas ainda se destaca como um dos mais comuns e utilizados. Portanto, é fundamental que um critério para geração de senhas seguras seja definido. Normalmente, o processo que estabelece as regras para criação de senhas chama-se: política de senhas.

2.1 O que é uma senha segura?

Por exemplo, vamos considerar a senha 123. Esta senha possui apenas 3 caracteres numéricos e utiliza o sistema decimal (base 10), logo, teremos 10^3 (1000) combinações possíveis. De 000 até 999. Um programa de computador levaria apenas **24 nanosegundos** para testar as 1000 possibilidades possíveis e descobrir este tipo de senha. Portanto, trata-se de uma senha muito fraca que nunca deve ser utilizada. A aplicação web *“How Secure Is My Password?”* exibida na figura 6, mostra o tempo necessário para descobrir uma senha de 3 caracteres numéricos.

Figura 6 - Senha numérica de 3 caracteres sendo descoberta em 24 nanosegundos.

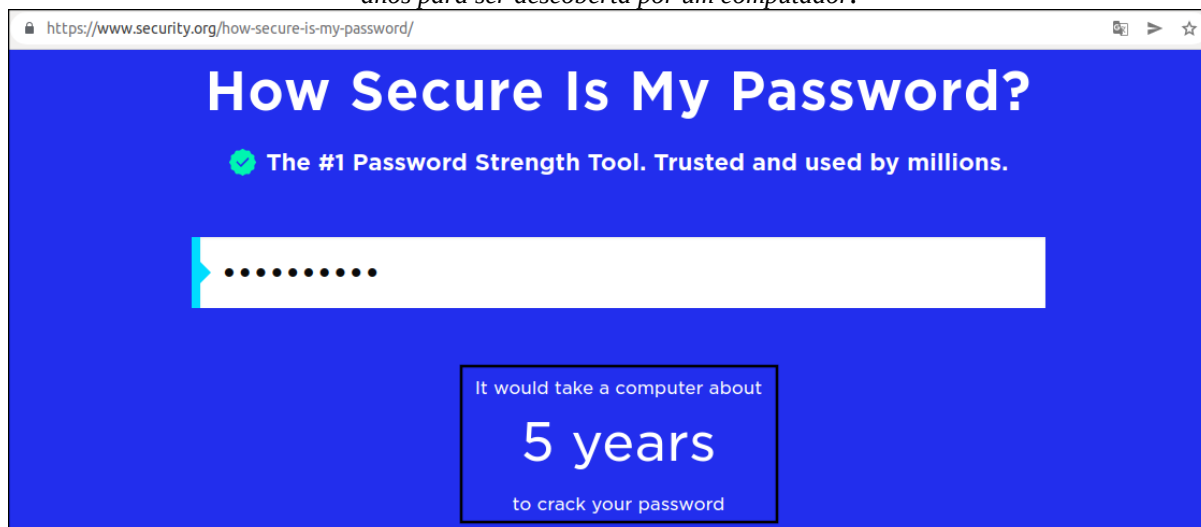


Outro exemplo: a palavra bola. Uma senha de 4 caracteres alfabéticos e minúsculos. O alfabeto tem 26 letras, logo, uma senha de 4 caracteres minúsculos possui 456.976 ($26 \times 26 \times 26 \times 26$) combinações possíveis. Um programa de computador levaria apenas **11 microsegundos** para descobrir uma senha com estas características.

Conforme mostram os exemplos, senhas curtas e que não possuem diversidade de caracteres (letras maiúsculas e minúsculas, caracteres especiais e números) são facilmente descobertas pelos programas de quebra de senhas. **Portanto, uma senha com um nível de segurança aceitável deve possuir no mínimo 10 caracteres e usar letras maiúsculas, minúsculas, números e caracteres especiais.**

A senha **Tatu#37@Bo** é considerada uma senha forte pois atende aos requisitos mínimos estabelecidos e levaria **5 anos** para um programa executando em um computador descobrir a mesma, conforme mostra a figura 7.

Figura 7 - Senha de 10 caracteres com letras minúsculas, maiúsculas, números e símbolos, levaria cerca de 5 anos para ser descoberta por um computador.



2.2 Política de senhas para os colaboradores

É preciso que seja estabelecido um padrão seguro para criação de senhas nas aplicações da empresa, a fim de evitar acessos não autorizados e roubo de informações.

Assim sendo, todos os colaboradores devem seguir os critérios estabelecidos na tabela 1.

Tabela 1 - Política de senhas para os colaboradores do grupo.

- As senhas devem ter um tamanho mínimo de 10 caracteres, letras minúsculas, letras maiúsculas, números e caracteres especiais.
- Cada colaborador deve possuir uma identificação de usuário nominal exclusiva e única (ID), para que responsabilidades possam ser atribuídas. Não é permitido que um usuário compartilhe seus dados de acesso (usuários, senhas, chaves, *tokens* e demais credenciais) com outras pessoas.
- As senhas temporárias deverão ser modificadas no primeiro acesso ao sistema.
- As senhas possuem um prazo de duração de 3 meses. Após este período os sistemas solicitarão que os colaboradores informem uma nova senha.
- As senhas devem ser armazenadas e transmitidas de forma segura. Desta maneira, fica proibido o envio de senhas por *e-mail*, FTP (*File Transfer Protocol*) ou qualquer outro protocolo sem suporte a criptografia. Quando novas senhas forem criadas pelo departamento de tecnologia, as mesmas, serão comunicadas de forma verbal ou utilizando programas homologados pela equipe de TI.
- Os usuários deverão utilizar o programa *Lastpass* para gerenciamento de suas senhas. Lembrando que, a qualquer tempo e de acordo com critérios técnicos, a área de segurança da informação poderá adotar outro programa. No caso de adoção de outro *software* para gerenciamento de senhas todos os colaboradores serão notificados e orientados.

3.0 IDENTIFICAÇÃO, AUTENTICAÇÃO, AUTORIZAÇÃO E AUDITORIA

3.1 MFA - *Multi Factor Authentication*

Durante muito tempo o processo de autenticação utilizou apenas um fator (senha) para confirmar a identidade dos usuários. Porém, com o surgimento de novas e eficientes técnicas de ataque para descoberta de senhas, ficou evidente que apenas um fator não era mais suficiente para proteger o acesso das pessoas. Isto posto, outros fatores foram adicionados para aumentar a segurança do processo de autenticação.

Instituições bancárias, por exemplo, costumam trabalhar com três fatores de autenticação para que o usuário possa fazer uma operação. São eles:

- O que eu tenho
- O que eu sei
- O que eu sou

O que eu tenho

Autenticação baseada em algo que a pessoa tenha. Exemplos: cartões bancários, códigos de verificação e *tokens* de acesso. Figura 8.

Figura 8 - Autenticação baseada em algo que a pessoa tenha. Como um cartão bancário.



O que eu sei

Autenticação baseada em algo que somente a pessoa saiba: Exemplos: usuário/senha e número PIN. Figura 9

Figura 9 - Autenticação baseada em algo que a pessoa saiba. Como usuário e senha.

A imagem mostra uma interface de login web. No topo, há o texto "Informe suas credenciais de acesso". Abaixo, há dois campos de entrada: o primeiro é rotulado "USUÁRIO" e contém o texto "Usuário"; o segundo é rotulado "SENHA" e contém o texto "Senha". Abaixo dos campos, há um botão azul com o texto "Entrar".

O que eu sou

Autenticação baseada em características do corpo de uma pessoa (biometria). Exemplos: palma da mão, reconhecimento facial, digitais e retina dos olhos. Figura 10

Figura 10 - Autenticação baseada nas características de uma pessoa (biometria).



A companhia utiliza a plataforma *Google Cloud* para serviços de *e-mail*, pastas compartilhadas, vídeo chamadas (*Meet*), entre outros. E para segurança adicional destes aplicativos, o *MFA (Multi Factor Authentication)* é habilitado. Para acessar um *site* ou

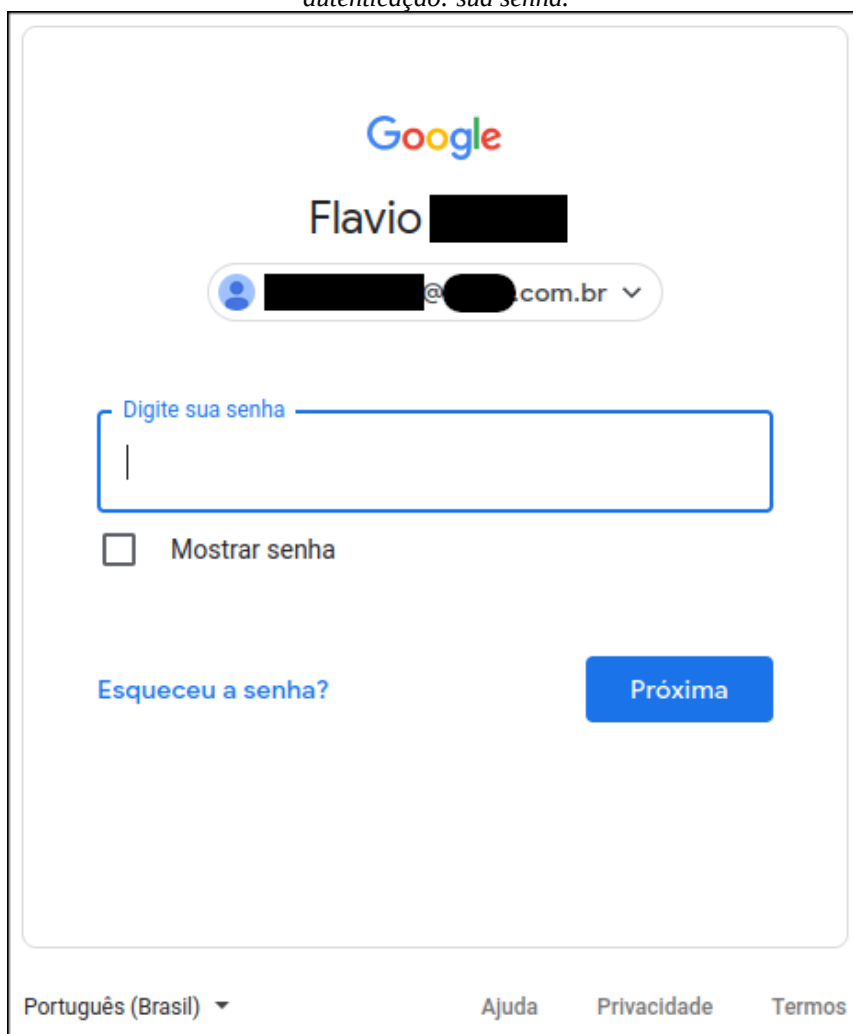
aplicativo com *MFA* o usuário deve fornecer dois ou mais fatores para comprovar a sua identidade. A tabela 2, mostra como o *MFA* funciona.

Tabela 2 - Fatores do MFA.

| | |
|-----------------|--|
| 1º Fator | Senha |
| 2º Fator | Número aleatório gerado por um <i>token</i> Código enviado por SMS Entre outros |

A figura 11 apresenta a tela de *login* do *Google workspace*, onde o colaborador da empresa se identifica com seu nome de usuário e se autentica com seu primeiro fator, no caso, sua senha.

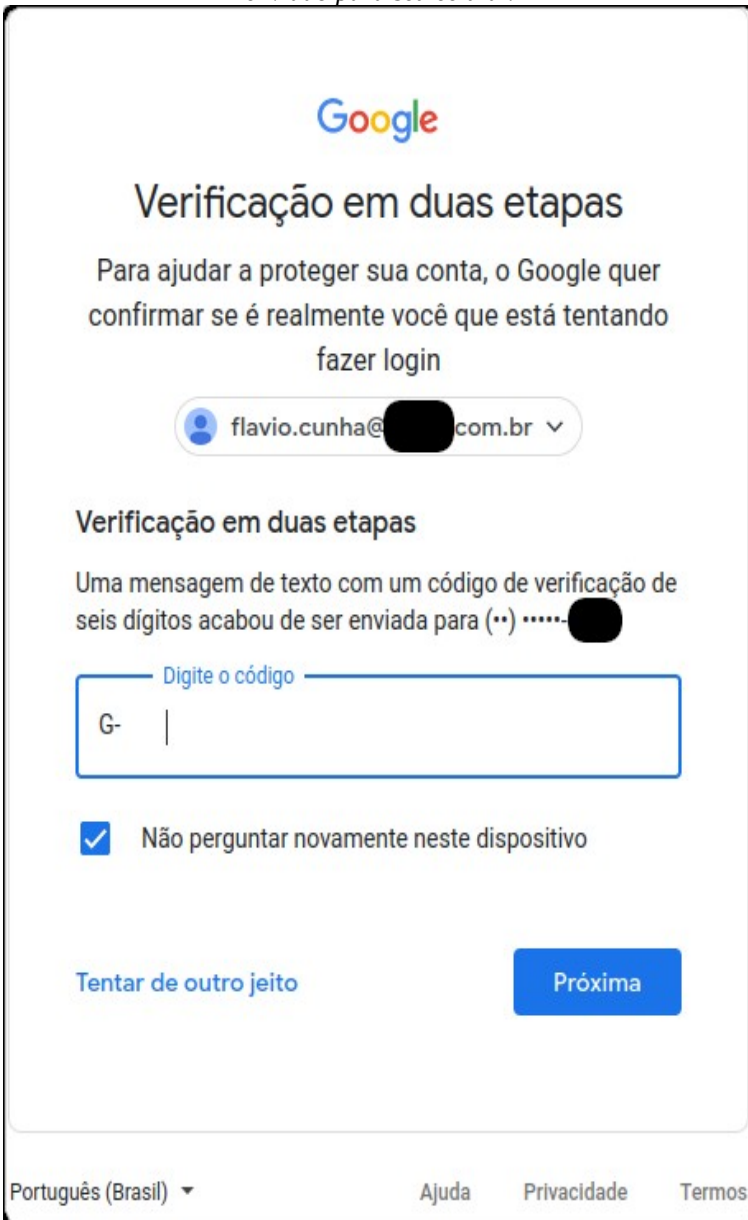
Figura 11 - Colaborador da empresa entrando no Google com seu primeiro fator de autenticação: sua senha.



The image shows the Google login interface. At the top is the Google logo. Below it, the name "Flavio" is displayed next to a blacked-out profile picture. Underneath is a rounded rectangle containing a blue person icon, a blacked-out email address, and ".com.br" with a dropdown arrow. Below this is a large text input field with the placeholder text "Digite sua senha". To the left of the input field is a small checkbox labeled "Mostrar senha". Below the input field is a blue link that says "Esqueceu a senha?". To the right of the link is a blue button labeled "Próxima". At the bottom of the interface, there is a footer with "Português (Brasil)" and a dropdown arrow on the left, and "Ajuda", "Privacidade", and "Termos" on the right.

Posteriormente, um segundo fator de autenticação é pedido para completar o processo. Um código aleatório e de uso único é enviado via *SMS* para o *smartphone* do colaborador, que digita o mesmo para ter acesso à plataforma. A figura 12 mostra o funcionamento do processo.

Figura 12 - Colaborador da empresa fornecendo seu segundo fator de autenticação: um SMS enviado para seu celular.




The image shows a Google account login screen for two-step verification. At the top is the Google logo. Below it, the title "Verificação em duas etapas" is displayed. A message explains that Google wants to confirm the user's identity. The user's email address, "flavio.cunha@[REDACTED].com.br", is shown in a dropdown menu. The section "Verificação em duas etapas" follows, stating that a six-digit code has been sent via SMS to a phone number "[REDACTED]". A text input field with the placeholder "Digite o código" and a "G-" label is provided for the user to enter the code. Below the input field is a checked checkbox with the text "Não perguntar novamente neste dispositivo". At the bottom, there are two links: "Tentar de outro jeito" and a blue "Próxima" button. The footer contains the language selection "Português (Brasil)" and links for "Ajuda", "Privacidade", and "Termos".

Google

Verificação em duas etapas

Para ajudar a proteger sua conta, o Google quer confirmar se é realmente você que está tentando fazer login

 flavio.cunha@[REDACTED].com.br ▼

Verificação em duas etapas

Uma mensagem de texto com um código de verificação de seis dígitos acabou de ser enviada para (..) [REDACTED]

Digite o código

G- |

☒ Não perguntar novamente neste dispositivo

[Tentar de outro jeito](#) [Próxima](#)

Português (Brasil) ▼ [Ajuda](#) [Privacidade](#) [Termos](#)

4.0 CONTROLE DE ACESSO E POLÍTICA DO PRIVILÉGIO MÍNIMO

Grande parte das invasões e violações de segurança da informação acontecem com o uso de credenciais administrativas ou que possuem altos privilégios de autorização sobre os ativos da companhia. Desta forma, é fundamental a utilização de uma política de gestão para controle de acesso dos colaboradores.

A base para as políticas de controle de acesso da companhia se baseiam na *premissa do menor privilégio*, onde o colaborador tem acesso somente aos recursos necessários para desempenhar o seu trabalho.

Figura 13 - Colaborador atribuindo permissões para um documento no Confluence apenas para as pessoas com necessidade de acesso.

Restrições [Inspeccionar permissões](#)

Apenas pessoas específicas podem visualizar ou editar

Digite um nome de usuário ou grupo

| Usuário | Permissão | Ação |
|-----------------|----------------|-------------------------|
| Todos | Não tem acesso | |
| FC Flavio Cunha | Pode editar | |
| DP Diego | Pode vis... | Remover |
| J jose | Pode vis... | Remover |

Nunca dê acesso público para um documento confidencial. Atribua as permissões pertinentes no documento (leitura, edição) somente para as pessoas autorizadas.

5.0 SEGURANÇA PARA AS ESTAÇÕES DE TRABALHO

Impulsionada pela pandemia, as práticas de teletrabalho se popularizaram nas organizações. Muitos colaboradores que antes trabalhavam nas dependências da empresa e tinham suas estações de trabalho gerenciadas pela equipe de TI, agora estão desempenhando suas tarefas em casa e sem supervisão.

Este novo paradigma de trabalho também trouxe novas preocupações quanto à segurança da informação, pois abre espaço para que os colaboradores acessem arquivos e aplicações da empresa a partir de seus equipamentos pessoais.

Portanto, é importante separar o uso pessoal do uso profissional.

Visando fortalecer a segurança da informação neste cenário, a empresa passou a fornecer equipamentos atualizados, com antivírus e todas as aplicações necessárias para que os colaboradores desempenhem suas tarefas. *Assim sendo, para fins de teletrabalho, é obrigatório o uso do equipamento fornecido pela empresa. E para objetivos pessoais, os colaboradores deverão usar seus próprios dispositivos.*

5.1 Política para instalação e remoção de programas

É proibida a instalação e a remoção de programas nos equipamentos fornecidos pela empresa. A área de suporte é responsável por entregar o equipamento com todos os programas que o colaborador necessita para desempenhar suas funções. Para instalação de programas adicionais deverá ser feita uma solicitação para o *help desk*.

5.2 Principais riscos

- *Malwares* em geral podem comprometer o equipamento do usuário.
- Um vírus pode causar lentidão e mal funcionamento do sistema operacional e aplicativos.
- Técnicas de engenharia social como *e-mails Phishing* enganam o usuário e o induzem a acessar *sites* maliciosos contendo arquivos *Ransomware*.
- Programas sem as atualizações de segurança podem ser explorados por invasores para realização de acesso não autorizado no computador do usuário.

5.3 Cuidados a serem tomados

Para manter o computador seguro e diminuir os riscos envolvidos no uso da *Internet* os colaboradores devem adotar as seguintes práticas:

1. Instalar um programa antivírus e mantê-lo sempre atualizado.
2. Manter o sistema operacional sempre atualizado com as últimas atualizações de segurança (usuários de sistemas *Windows* devem sempre instalar as correções de segurança do *Windows Update*).
3. Habilitar o *firewall* do Windows.

6.0 SEGURANÇA NA INTERNET

6.1 Segurança em conexões web

A confidencialidade das informações que trafegam entre o navegador do usuário e o *site* acessado é garantida pelos recursos de criptografia.

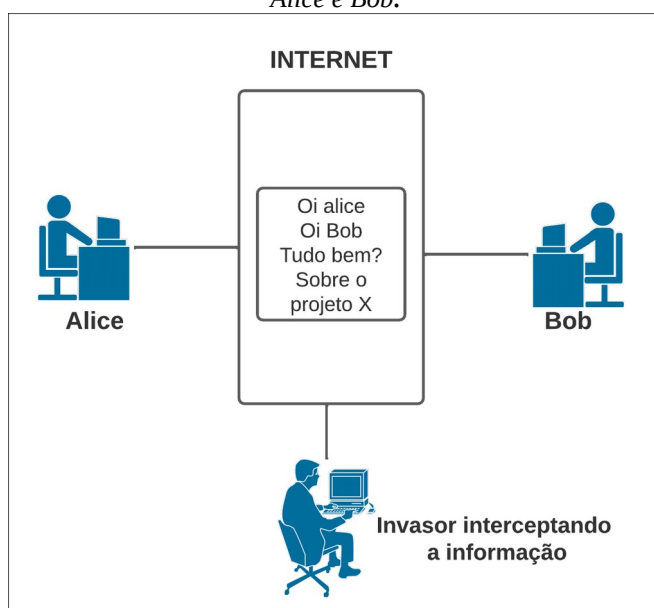
6.2 Mas o que é criptografia e como ela funciona?

Criptografia é a ciência de esconder o significado de uma mensagem.

Considere um cenário onde Alice e Bob precisam trocar informações usando a Internet. Se as informações forem transmitidas de forma legível, ou seja, em um formato que tecnicamente é conhecido como “*clear text*” (que significa sem criptografia) qualquer pessoa que interceptar a comunicação terá acesso a mesma.

A figura 14 mostra um invasor interceptando a comunicação entre Alice e Bob e obtendo acesso ao conteúdo da informação.

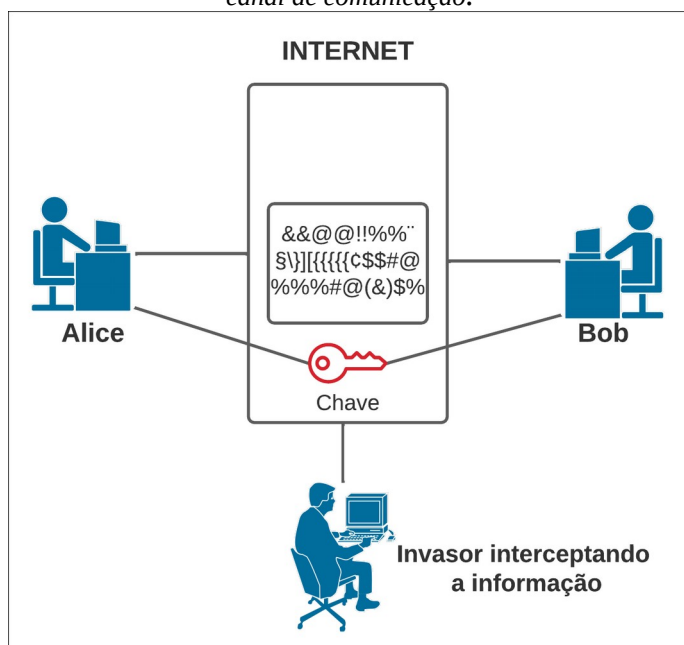
Figura 14 - Invasor interceptando a comunicação entre Alice e Bob.



Em contrapartida, um *site* que possui suporte a recursos de criptografia torna a informação ilegível para todas as outras pessoas que não estiverem participando da comunicação. Deste modo, mesmo que um invasor capture o tráfego criptografado a informação permanecerá oculta. A figura 15 mostra Alice e Bob utilizando uma chave para criptografar o canal de comunicação.

A técnica de criptografia que utiliza uma única chave para encriptar e decriptar mensagens é chamada de “criptografia simétrica”.

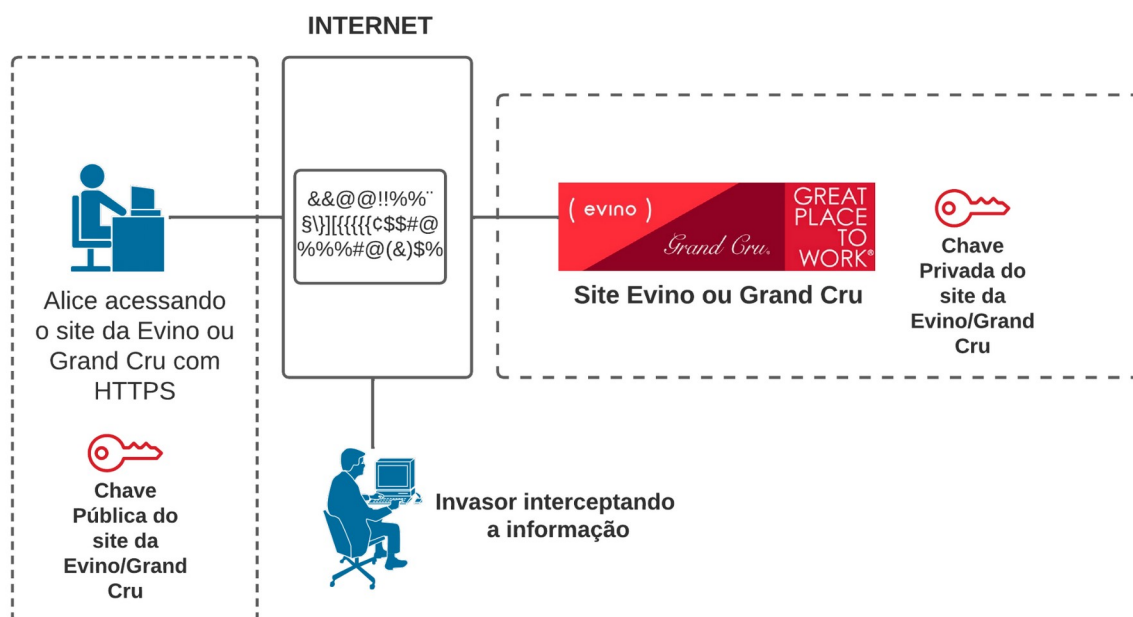
Figura 15 - Uso de chave de criptografia para criptografar o canal de comunicação.



6.2.1 Criptografia assimétrica

A criptografia assimétrica utiliza um par de chaves para realizar o processo de cifragem das mensagens. Uma chave pública e uma chave privada. Os *sítes* da Internet fazem uso desta técnica para trafegar informações confidenciais. Neste modelo, a chave privada fica armazenada de forma segura no servidor *web* e a chave pública é disponibilizada para os usuários do site. Sendo que, as mensagens que são encriptadas com a chave pública só podem ser decriptadas com a chave privada. A figura 16 mostra o funcionamento do processo. Neste cenário, mesmo que o invasor tenha acesso ao canal de comunicação a informação estará ilegível.

Figura 16 - Os sites da figura disponibilizam acesso criptografado para seus clientes e colaboradores através do protocolo *https*.



6.3 Protegendo informações sensíveis nos *sites* da internet

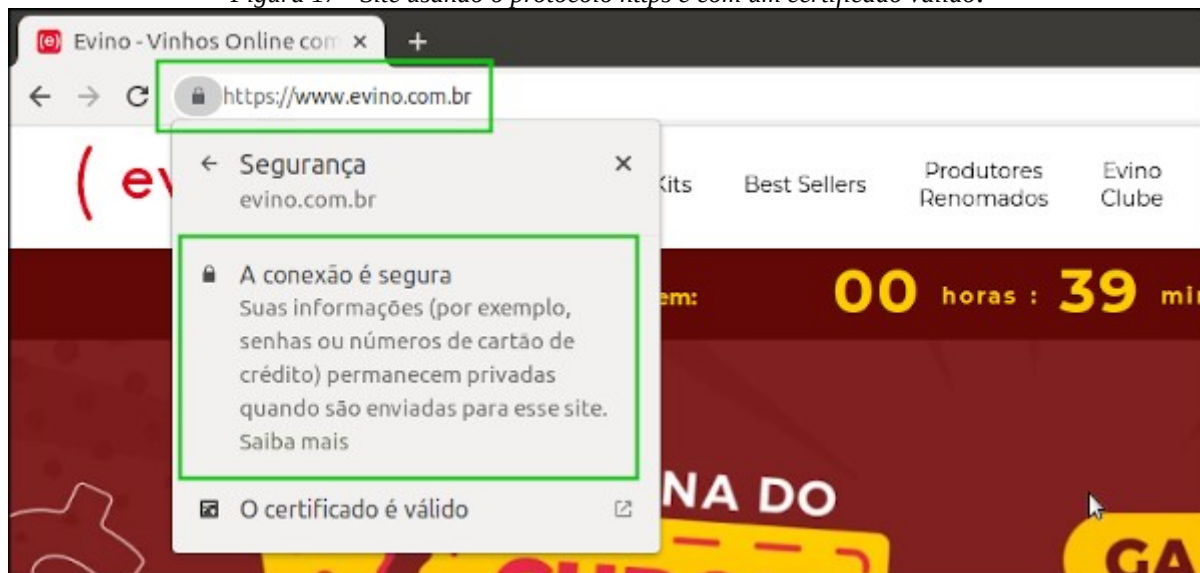
De forma geral, os *sites* da *Internet* utilizam dois protocolos: HTTP (*Hypertext transfer protocol*) e HTTPS (*Hypertext transfer protocol secure*) sendo que, o HTTPS fornece suporte a criptografia e o HTTP não.

Sites que transmitem informações sensíveis e confidenciais como: números de cartões de crédito, credenciais de acesso, chaves e tokens de sessão devem fazer uso do protocolo **https**.

6.3.1 Como verificar se o *site* é protegido por criptografia?

Instituições bancárias, financeiras e *e-commerces* em geral fazem uso do protocolo *https* em seus *sites* para proteger as informações dos seus clientes. Desta maneira, sempre verifique na barra de endereços do navegador se o *site* começa com **https://** e se o ícone do “**cadeado fechado**” aparecerá, conforme exibido na figura 17.

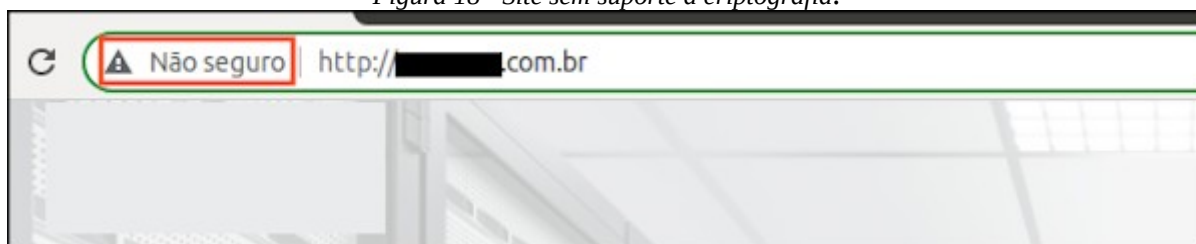
Figura 17 - Site usando o protocolo *https* e com um certificado válido.



6.3.2 Como detectar *sites* sem suporte a criptografia?

Sites sem suporte a criptografia usam somente o protocolo **http**, o navegador *Google Chrome* apresenta a mensagem **não seguro** para todos endereços que não utilizam o protocolo **https**, conforme mostra a figura 18.

Figura 18 - Site sem suporte a criptografia.

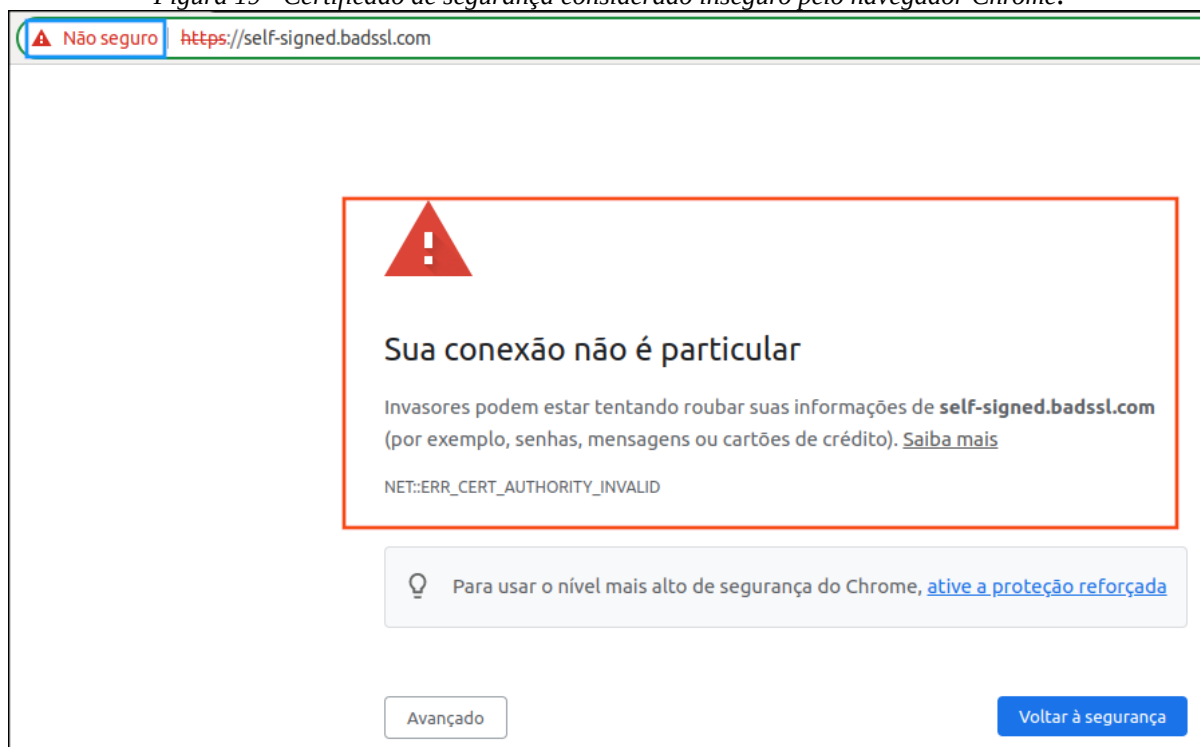


6.3.3 Como detectar sites falsos, maliciosos ou com o certificado expirado?

Os navegadores mais populares geralmente exibem um alerta dizendo que a conexão não é particular ou que o certificado não é válido para o *site* em questão. Nestes casos, o *Google Chrome* também marca o *site* como “Não seguro” na barra de endereços.

Caso tente navegar em um *site* e apareça algum alerta com relação ao certificado de autenticidade ou à segurança da conexão jamais prossiga com o acesso (adicionando o *site* como exceção de segurança ou algo similar). Diante desta situação, notifique imediatamente o departamento de segurança da informação. A figura 19, mostra um alerta do navegador *Chrome* para um certificado que foi classificado como inseguro.

Figura 19 - Certificado de segurança considerado inseguro pelo navegador Chrome.



7.0 BACKUPS

Muitos iniciantes confundem o processo de cópia de arquivos com *backup*. Apesar das semelhanças, são coisas distintas.

O *Backup* é a cópia de dados de um local para outro. Portanto, quando um arquivo é copiado de uma pasta para outra dentro da mesma unidade de disco, não estamos realizando um *backup*, e sim, a cópia de um arquivo, pois se a unidade de disco for danificada tanto o arquivo original quanto a sua cópia serão perdidos.

Figura 20 - Cópia de um arquivo dentro da mesma unidade de disco não é *backup*.

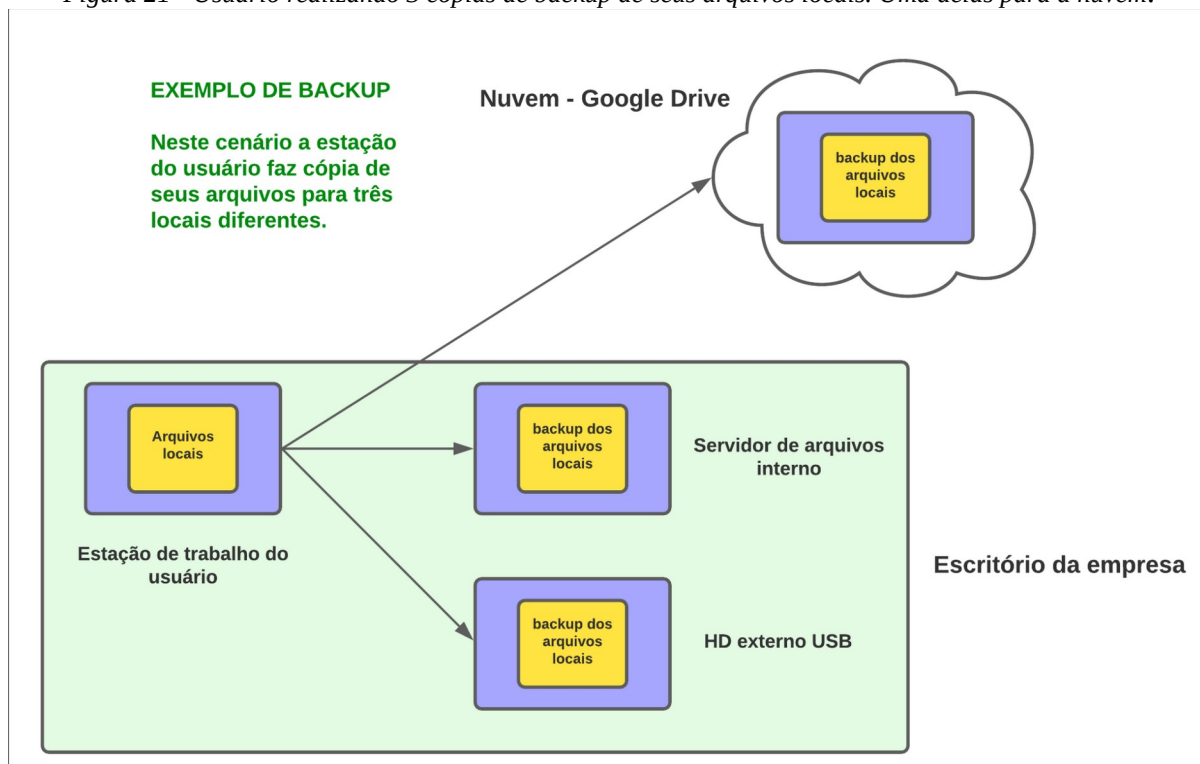


O processo de *backup* consiste em criar e armazenar cópias de segurança de arquivos digitais de um local para outro, de maneira que, seja possível realizar a sua restauração caso os arquivos originais sejam perdidos. Na figura 21, a estação de trabalho do usuário faz cópias de segurança de seus arquivos para três locais distintos: servidor de arquivos e HD USB na rede interna do escritório da empresa e também para um repositório externo na nuvem do Google (*Google Drive*). Este exemplo é uma boa

estratégia para *backups*, pois se um evento destruir o escritório da empresa, ainda haverá uma cópia dos dados na nuvem.

Uma regra de *backup* recomendada por especialistas consiste em armazenar pelo menos 3 versões de seus dados em duas mídias diferentes, uma delas em outro local.

Figura 21 - Usuário realizando 3 cópias de backup de seus arquivos locais. Uma delas para a nuvem.



8.1 Tipos de engenharia social

- **Baseada em pessoas:** Não faz uso de programas computacionais. Praticada por pessoas que utilizam técnicas de convencimento social para alcançar os seus objetivos. *Crackers*, farsantes, golpistas e estelionatários são alguns exemplos.
- **Baseada em computadores:** Neste cenário, as técnicas utilizadas precisam de programas computacionais para serem concretizadas, golpes que envolvem técnicas de *phishing* e implantação de *backdoors* se encaixam nesta categoria.

8.1.2 Exemplos de abordagens

Golpe do *Pen Drive*

Neste tipo de prática, o engenheiro social coloca um *pen drive* nas dependências da empresa (estacionamento, banheiro, entre outros) rotulado com algo que chame a atenção, como: folha de pagamento e reajuste de colaboradores. Dentro desta mídia é inserido um arquivo malicioso que contém um *malware*. Determinado colaborador acha o *pen drive* e insere em sua estação de trabalho corporativa e movido pela curiosidade, executa o arquivo. A partir deste momento, a máquina é infectada com o *malware*. Em casos de *ransomware* ou *worm*, eles tentam se espalhar para todas as outras máquinas da rede, intensificando os danos e prejuízos para a organização.

Vishing

Nesta abordagem o criminoso liga para um colaborador se passando por um funcionário de uma grande companhia ou da própria organização onde a vítima trabalha, e seu objetivo é obter informações sensíveis para invadir sistemas da empresa, realizar acessos em nome da vítima, compras e até transferências de dinheiro para sua conta.

Nesta abordagem o criminoso liga para um colaborador se passando por um funcionário de uma grande companhia ou da própria organização onde a vítima trabalha, e seu objetivo é obter informações sensíveis para invadir sistemas da empresa, realizar acessos em nome da vítima, compras e até transferências de dinheiro para sua conta.

As figuras 23,24 e 25 mostram como a técnica é empregada pelos cibercriminosos.

Figura 23 - cibercriminoso se passando por funcionário do help desk para descobrir usuários e senhas de sistemas.

Golpista - Olá meu nome é Lucas. Sou o novo funcionário do Help Desk e vou trabalhar junto com o Diego. Estamos fazendo um atualização de sistema. Pode por gentileza, passar seu usuário e senha do Windows pra mim?

Vítima – Claro. Meu usuário é patricialimaflores@grandcru.com.br e minha senha é FG@sinx92

Figura 24 - Cibercriminoso induzindo um colaborador a instalar um malware em sua máquina.

Golpista – Olá aqui é o Flávio de segurança da informação. Estamos instalando uma nova ferramenta de segurança nas estações. Vou te enviar o arquivo de instalação por e-mail. Assim que receber, você baixa e executa o arquivo para mim? Para executar, basta dar um clique duplo no arquivo.

Vítima – Claro. Sem problemas.

Golpista – Muito obrigado.

Vítima – Imagina.

Figura 25 - Cibercriminoso assume a identidade de um funcionário da empresa Fortinet para obter informações de sistemas e programas da empresa.

Golpista – Bom dia, meu nome é Pedro e trabalho no comercial da empresa de tecnologia Fortinet. Eu conversei com o rapaz de segurança da informação...Qual é mesmo o nome dele?

Vítima – Ah! O Flávio!

Golpista – Isso. Exatamente. Ele me pediu um orçamento de serviço. Só que eu acabei não anotando as versões de software que ele me passou. Pode me ajudar?

Vítima – Claro.

Golpista – Que sistema operacional vocês usam nas estações? Windows, Linux, Mac? E qual a versão?

Vítima – Aqui, nós utilizamos Windows, versão X em todas as estações

Golpista – Certo, e qual a versão de antivírus?

Vítima – Nós usamos o AVG, versão Y.

Golpista – Ok. Muito obrigado!

Vítima – De nada. Disponha.

8.1.3 Como se proteger da engenharia social

- Nunca passe informações da empresa para estranhos. Exemplos: *softwares* e versões utilizadas, usuários e senhas, fabricante dos *notebooks* corporativos, políticas de senhas, políticas de controle de acesso, processos financeiros, entre outros.
- Não divulgue informações sigilosas sobre a empresa nas redes sociais.
- Mantenha o antivírus sempre atualizado. Habilite mecanismos para filtragem de *spams* e *e-mails* maliciosos.
- Utilize gerenciadores de senhas.
- Não fale sobre assuntos privados em locais públicos.
- Não entre em *sites* maliciosos e tenha cuidado com *sites* falsos.

9.0 MALWARES

9.1 Definição de *Malware*

Malware é um nome genérico utilizado para designar todo e qualquer tipo de código de computador malicioso como: *vírus*, *worm*, *ransomware*, *trojan* entre outros.

Estas ameaças digitais são programas especialmente desenvolvidos para roubar e criptografar informações, espionar o usuário, apagar arquivos e programas, modificar arquivos e programas inserindo códigos maliciosos, causar mau funcionamento e lentidão nos sistemas afetados e toda sorte de objetivos escusos pretendidos pelo cibercriminoso. A tabela 3, exibe os principais tipos de *malwares* e suas características.

9.1.2 Principais tipos de *Malware*

Tabela 3 - Principais tipos de *malwares* e suas características.

| Tipo de <i>Malware</i> | Características | Método de infecção | Meios de propagação | Tipos comuns |
|------------------------|---|---|--------------------------|---|
| Vírus | Se propaga inserindo cópias de si mesmo em outros programas e arquivos. | O programa hospedeiro deve ser executado para que o mesmo se torne ativo e dê continuidade ao processo de infecção. | <i>E-mail, pen drive</i> | Vírus disseminado por <i>e-mail</i> , vírus de script, vírus de macro, vírus de telefone celular. |

| Tipo de <i>Malware</i> | Características | Método de infecção | Meios de propagação | Tipos comuns |
|------------------------|--|---|---|---|
| <i>Trojan</i> | Programa que além de executar as funções para as quais foi projetado, também executa códigos maliciosos sem o conhecimento do usuário. | Precisa ser executado para que a instalação ocorra. Pode ser instalado pelo próprio usuário ou pelo atacante. | Após invadirem o equipamento, alteram os programas já existentes para executarem ações maliciosas. Porém, as funções originais do programa são mantidas, a fim de evitar suspeitas. | <i>Trojan backdoor, Trojan Spy, Trojan Banker</i> (Bancos), <i>Trojan Downloader</i> e <i>Trojan</i> destrutivo |

| Tipo de <i>Malware</i> | Características | Método de infecção | Meios de propagação | Tipos comuns |
|--------------------------|---|---|---|--|
| <i>Ransomware</i> | Tem como objetivo tornar inacessível os dados do equipamento comprometido. Normalmente usando chaves de criptografia e exigindo pagamento de resgate para restabelecimento do acesso. | Através do uso de técnicas de engenharia social usando <i>e-mail phishing</i> ou <i>Downloads Drive-by</i> que são ataques realizados a partir de um <i>site</i> malicioso, onde o usuário sem saber realiza o <i>download</i> e instalação do <i>ransomware</i> para o seu computador. | Se espalha buscando outros dispositivos conectados na rede para criptografá-los também. | <i>Locker</i> : que impede o acesso ao equipamento. <i>Crypto</i> : Impede acesso aos dados armazenados no equipamento. |

| Tipo de <i>Malware</i> | Características | Método de infecção | Meios de propagação | Tipos comuns |
|------------------------|--|--|--|--|
| <i>Spyware</i> | Programa espião que monitora as atividades de um sistema, coleta e envia para terceiros. | “Clicar” em <i>links</i> ou anexos de e-mail desconhecidos. Acessar <i>sites</i> maliciosos, baixar e instalar programas <i>freeware</i> de empresas desconhecidas pois um <i>Spyware</i> pode estar infiltrado. | Se propaga pela <i>web</i> e compromete dispositivos móveis e computadores. Portanto, deve-se ter cuidado ao baixar <i>softwares</i> , navegar em <i>sites</i> e sempre evitar clicar em <i>links</i> suspeitos. | <i>Keylogger</i> , <i>Screenlogger</i> e <i>Adware</i> . |
| <i>Worm</i> | Este tipo de malware se propaga de forma automática pela rede, enviando cópias de si mesmo de um equipamento para outro. | Execução direta das cópias. Exploração automática de vulnerabilidades em programas da rede. | 1 - identifica os equipamentos alvos com aplicações vulneráveis. 2 - Envia as cópias. 3 - Ativa as cópias. | <i>E-mail worms</i> . <i>Network worms</i> . |

9.2 Contramedidas para proteção contra *Malwares*

1. Instale e mantenha um antivírus sempre atualizado. Configure o mesmo para que verifique periodicamente arquivos anexados ao *e-mail* e obtidos pela Internet e também os *Hds* da estação.
2. Sempre verifique arquivos de unidades removíveis (*pen drives*, unidades USB) com o antivírus antes de utilizá-los.
3. Mantenha o *firewall* pessoal habilitado.
4. Mantenha o sistema e aplicativos sempre atualizados. Sempre baixe e instale todas as atualizações de segurança.
5. Remova programas que não são mais utilizados.
6. Mantenha várias cópias de *backup* dos seus arquivos. Sendo que, uma delas deve estar desconectada da rede e da Internet.

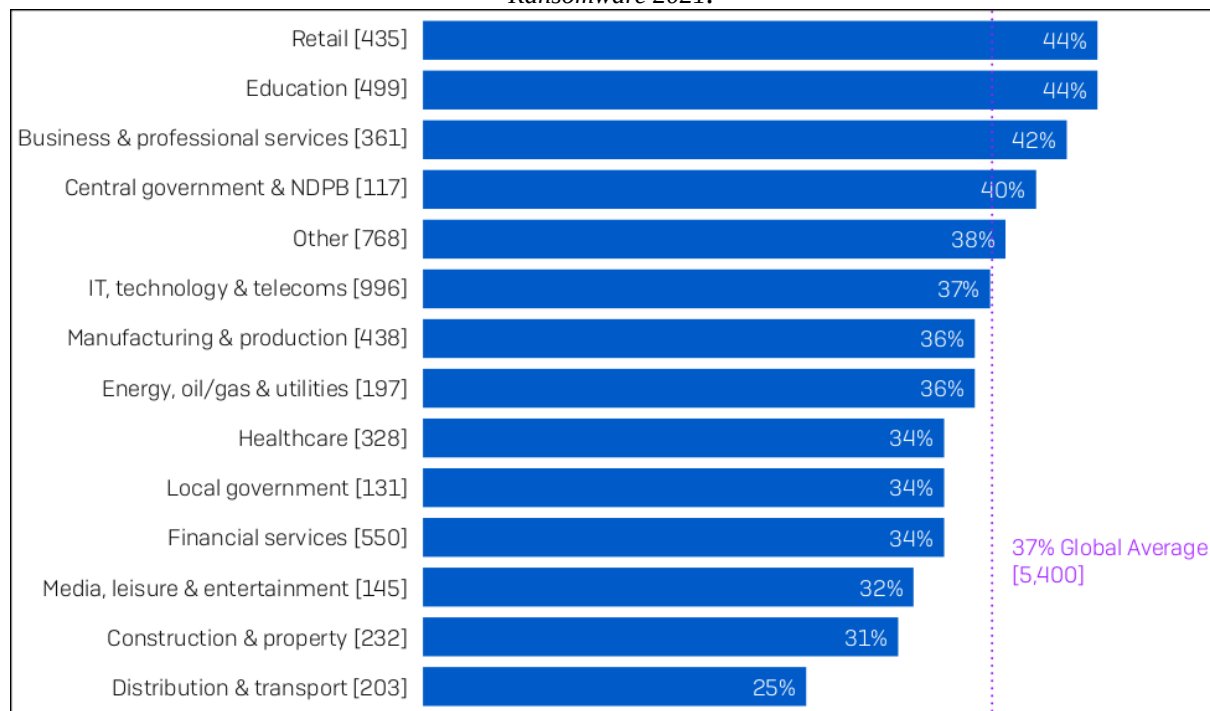
10 RANSOMWARE

Atualmente, o *Ransomware* tem se destacado como uma das principais ameaças de *malware* para as empresas. Após comprometer um sistema alvo e criptografar seus arquivos (tornando-os incompreensíveis) os invasores pedem uma certa quantia financeira em troca de uma chave de descriptografia para recuperação dos dados, ou seja, um resgate. Este valor pode variar de centenas de reais, para uma pequena empresa ou até mesmo milhões de reais, para organizações de grande porte.

10.1 Estatísticas do *Ransomware* pelo mundo

De acordo com o relatório da empresa de *cybersecurity* Sophos “*The State of Ransomware 2021*”, 37% das organizações entrevistadas foram atingidas por ataques *Ransomware* em 2021. A Sophos contratou a companhia de pesquisa independente Vanson Bourne para entrevistar 5400 líderes de TI em 30 países diferentes e a pesquisa foi realizada nos meses de Janeiro e Fevereiro de 2021. A figura 26, mostra que os setores de varejo e educação foram os mais atingidos. Portanto, devemos ter medidas eficazes de segurança para mitigar esta ameaça.

Figura 26 - Setores mais atingidos pela ameaça Ransomware de acordo com o relatório Sophos “The State of Ransomware 2021.

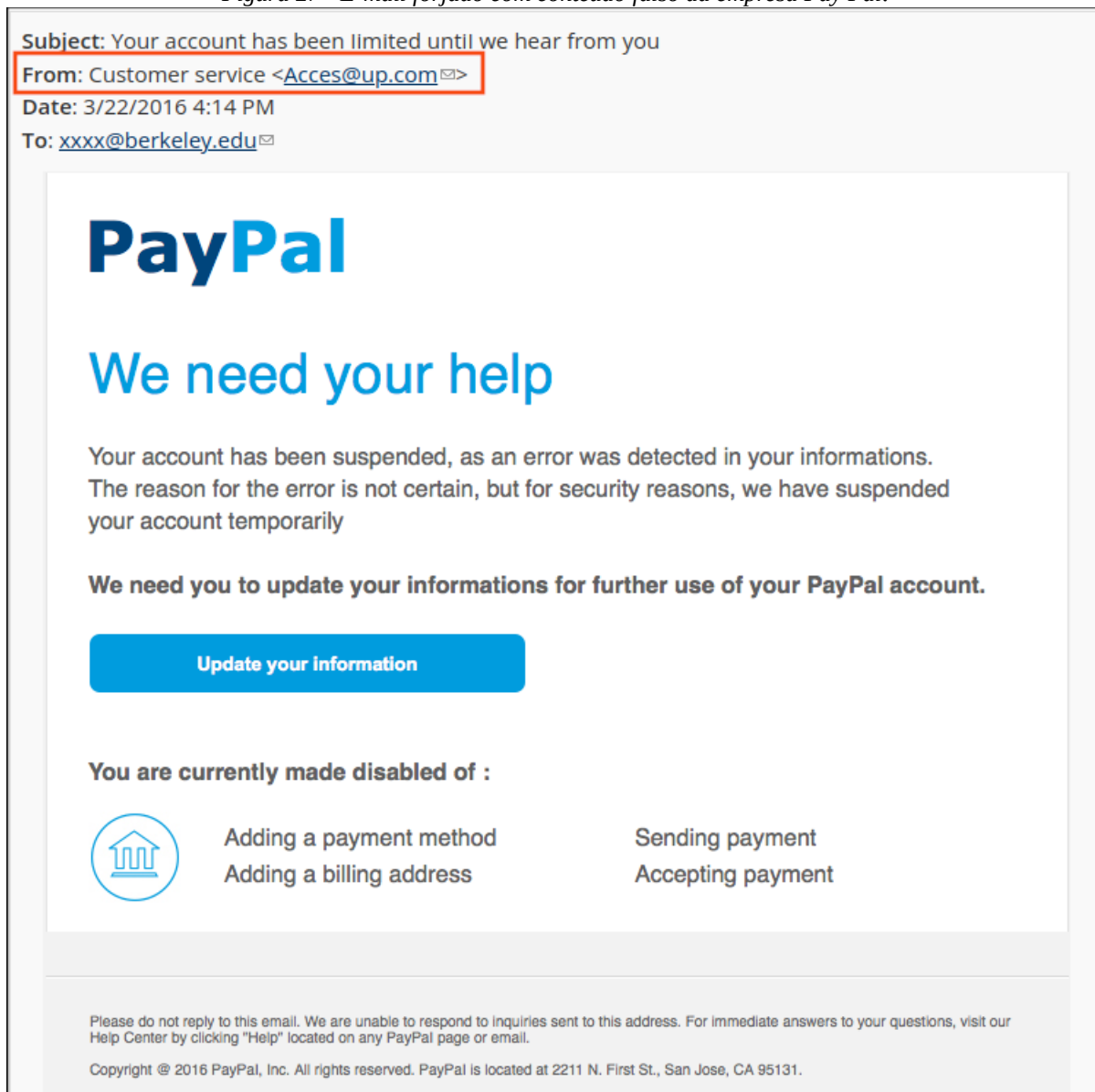


10.2 Métodos de infecção

Os cibercriminosos utilizam uma grande variedade de técnicas para comprometer uma organização com *Ransomware*. Entretanto, algumas se destacam pela sua eficiência e estão entre os métodos mais comuns de infecção, são elas:

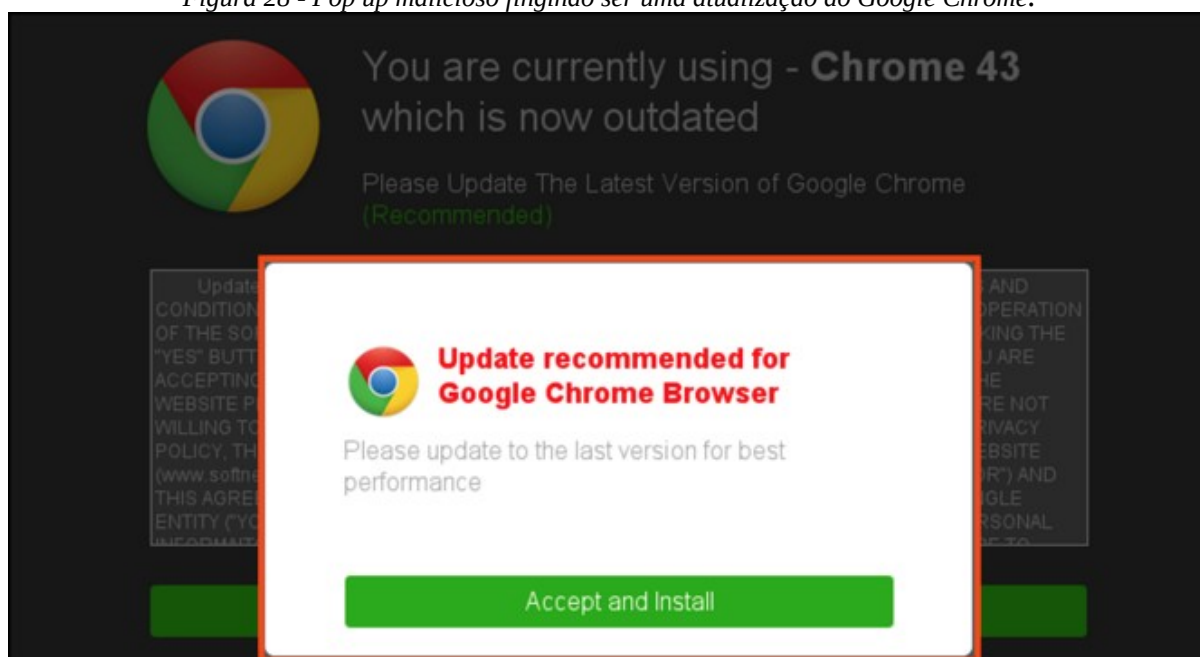
Campanhas de e-mail phishing: Os cibercriminosos enviam *e-mails* contendo arquivos ou *links* maliciosos. Ao clicar no *link* ou fazer o *download* do arquivo e posterior execução, a máquina é infectada. A figura 27, exibe um *e-mail* forjado pelos criminosos que assumem a identidade da empresa de pagamentos *Paypal*. Neste exemplo, é usada uma estratégia de intimidação que diz ao usuário que sua conta será suspensa, se o mesmo não clicar no *link* para *update* de suas informações. Pode-se observar que no campo **From:** (que indica o remetente da mensagem) têm-se o endereço: Acces@up.com. Esta informação também serve como indicativo da fraude, pois um *e-mail* da empresa *Paypal* deveria estar associado ao domínio *paypal.com*.

Figura 27 - E-mail forjado com conteúdo falso da empresa Pay Pal.



Drive-by download: Neste cenário, os cibercriminosos utilizam *sites* maliciosos ou comprometem *sites* com falhas de segurança para inserir códigos nocivos que contém *ransomware* e *malwares* em geral . Ao navegar neste tipo de *site*, os usuários geralmente são surpreendidos com um *Pop-up* (janela) pedindo para atualizar algum programa do computador. No entanto, trata-se de uma atualização falsa, pois ao clicar no botão *install* o *ransomware* ou *malware* é instalado no computador da vítima. É importante ressaltar, que uma falha de segurança no navegador do usuário, também pode instalar o programa malicioso em seu computador sem que seja preciso que o mesmo clique ou interaja com algum *Pop-up* do *site*. A figura 28, mostra um *Pop-up* malicioso assumindo a identidade do *Google* e pedindo para que uma atualização seja feita no navegador *Chrome*.

Figura 28 - Pop up malicioso fingindo ser uma atualização do Google Chrome.



Vulnerabilidades no protocolo RDP (*Remote Desktop Protocol*): O RDP é um protocolo de rede proprietário da *Microsoft*. Os cibercriminosos costumam usar ataques de *força bruta* neste serviço para descobrir as credenciais de um usuário e realizar um acesso não autorizado. Vulnerabilidades no protocolo RDP também podem ser exploradas para obtenção de um acesso arbitrário. Uma vez dentro do sistema alvo, o invasor instala o *ransomware*.

Programas vulneráveis: Falhas nos programas, juntamente com definições e configurações inseguras são exploradas pelos invasores para conseguir um acesso não autorizado e em seguida instalar o *ransomware*.

10.3 Mecanismos de defesa e contramedidas contra *ransomwares* e *malwares* em geral

1. Realizar periodicamente *backup* de seus dados, imagens de sistemas e configurações. Testar regularmente a integridade de seus *backups* e sempre manter cópias de *backup offline* (sem acesso a Internet).
2. Manter programas e sistemas sempre atualizados.
3. Sempre utilizar MFA (*Multi factor authentication*).
4. Sempre verificar se as soluções de segurança da informação estão atualizadas.
5. Nunca habilite o serviço *remote desktop services* também conhecido como área de trabalho remota do *Windows* sem a permissão do departamento de TI. Pois ao habilitar este recurso o seu equipamento ficará com o serviço RDP ativado e portanto, mais vulnerável.
6. Remova os programas que não são mais utilizados, pois eles ficam desatualizados e são potencialmente vulneráveis a falhas de segurança.

7. Instale e mantenha um programa antivírus (*antimalware*) sempre atualizado, incluindo o arquivo de assinaturas. Configure o antivírus para verificar automaticamente toda e qualquer extensão de arquivo, arquivos anexados aos *e-mails* e obtidos pela Internet, discos rígidos e unidades removíveis.
8. Verifique sempre os arquivos recebidos antes de abri-los ou executá-los.
9. Seja cuidadoso ao clicar em *links* no corpo do *e-mail*. Mensagens de conhecidos nem sempre são confiáveis. O campo remetente do *e-mail* (From) pode ter sido falsificado ou o mesmo foi enviado a partir de contas falsas ou invadidas.
10. Habilite ou instale um *firewall* pessoal no seu sistema. Sempre habilite o *firewall* do *Windows*.

11 CONSIDERAÇÕES FINAIS

As ameaças digitais estão presentes no nosso cotidiano e podem comprometer de forma total ou parcial as operações de uma empresa. Os prejuízos relacionados a roubo e exclusão de informações são imensos. Perdas financeiras, danos a reputação e a imagem da companhia, processos litigiosos, entre outros. Contudo, acreditamos que colaboradores bem informados e mais capacitados nas questões relacionadas à segurança da informação constituem uma importante camada de defesa para frustrar as investidas dos cibercriminosos.

Nossa meta é criar e manter uma cultura de segurança da informação no grupo. E a cartilha de segurança da informação é um primeiro passo para que possamos atingir este objetivo.