SEBRAE

DE OLHO NO LANCE

Recomendações Importantes de Segurança para o seu Negócio

SEUS DADOS SÃO VALIOSOS E PRECISAM SER PROTEGIDOS

VOCÊ JÁ CONSULTOU O NOSSO EBOOK DE DICAS DE SEGURANÇA DA INFORMAÇÃO?

No nosso Ebook de Dicas de Segurança da Informação para empresas, você aprendeu que os dados têm um enorme valor para a sua empresa, e que eles precisam ser protegidos contra criminosos, ameaças e riscos, certo?

O QUE SÃO ESSES TAIS DADOS?

São todas as informações que fazem a empresa funcionar, e sem elas, nem mesmo a melhor das ideias pode se tornar um bom negócio. São os dados de clientes e funcionários, informações administrativas, dados financeiros e bancários, contratos, notas, recibos, planilhas, documentos, acessos, estratégias, projetos e muito mais.

O QUE É DE VALOR PRECISA SER DEVIDAMENTE PROTEGIDO!

Seja gerando novos dados, tratando e usando os dados, guardando e até descartando esses dados após o uso, todos esses passos precisam ser feitos com muita segurança, protegendo os dados contra o uso incorreto, além de riscos, ameaças e criminosos.

SEBRAE

VOCÊ NÃO PRECISA SER UM ESPECIALISTA PARA SABER SE PROTEGER

Como aprendemos no Ebook de Dicas de Segurança da Informação, cuidar da proteção dos dados é uma responsabilidade de todo mundo que tem acesso à eles, e você não precisa ser um técnico e nem um especialista para isso. É preciso apenas ter práticas seguras, com dedicação, e seguir as nossas recomendações de Segurança, usando ferramentas seguras para proteger a sua empresa.

SE PROTEGER É MAIS FÁCIL DO QUE PARECE!

Lutar contra os criminosos e ameaças que colocam os dados e a sua empresa em risco não é impossível, e nem precisa ser complicado. Os criminosos preferem atacar alvos fáceis, que caem em golpes sem prestar atenção ou sem pensar, pois não sabem se defender e não obedecem às recomendações de Segurança.

ATENÇÃO:
SIGA AS RECOMENDAÇÕES DE SEGURANÇA

TENHA SENHAS SEGURAS

No topo das recomendações está o cuidado com as senhas do seu negócio! Elas precisam ser diferentes para cada conta, aleatórias, com 10 caracteres ou mais, incluindo letras maiúsculas, minúsculas, caracteres especiais e números. Infelizmente, senhas simples e fáceis de adivinhar são as primeiras tentativas dos criminosos, que também usam listas de senhas vazadas. Se as suas forem fortes e diferentes, mesmo que uma vaze, as outras estarão seguras!

SEBRAE

USE UM GERENCIADOR DE SENHAS

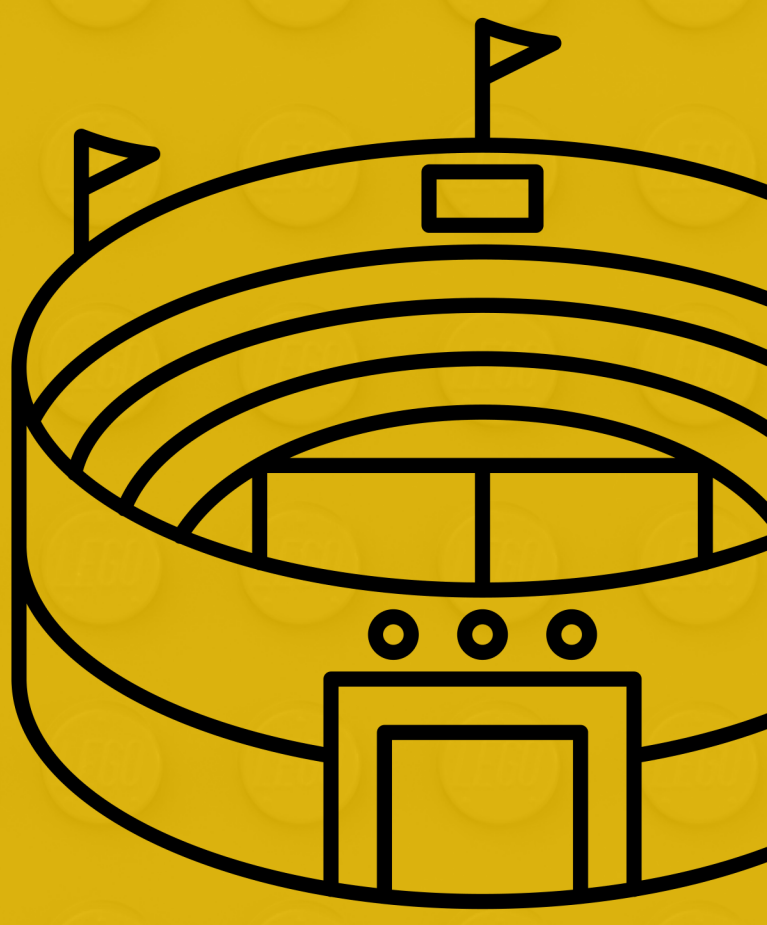
Nunca, jamais anote as suas senhas em cadernos, post-its ou mesmo planilhas. É também uma péssima ideia salvar suas senhas no navegador, mesmo que ele ofereça. A **forma mais segura de proteger a sua senha é usando um aplicativo confiável de gerenciador de senhas**, recomendado por especialistas. Além de armazenar suas senhas de forma segura, o aplicativo também pode gerar senhas fortes e até mesmo alertar sobre reuso de senhas ou vazamento de dados.

ATIVE O DUPLO OU MÚLTIPLO FATOR DE AUTENTICAÇÃO

Em todas as suas contas, serviços e aplicativos, ative o MFA, conhecido como Múltiplo Fator de Autenticação, ou Duplo Fator de Autenticação (2FA). **Você pode ativar o MFA nas configurações de Segurança e Privacidade das suas contas!** Ele serve como uma camada extra de segurança, podendo ser um pin numérico, um sms, uma confirmação extra ou até mesmo um token - sendo este o método mais seguro. Assim, se a sua senha for roubada ou vazada, a conta permanece protegida por este fator extra de segurança.

EXPLORE AS CONFIGURAÇÕES DE SEGURANÇA E PRIVACIDADE

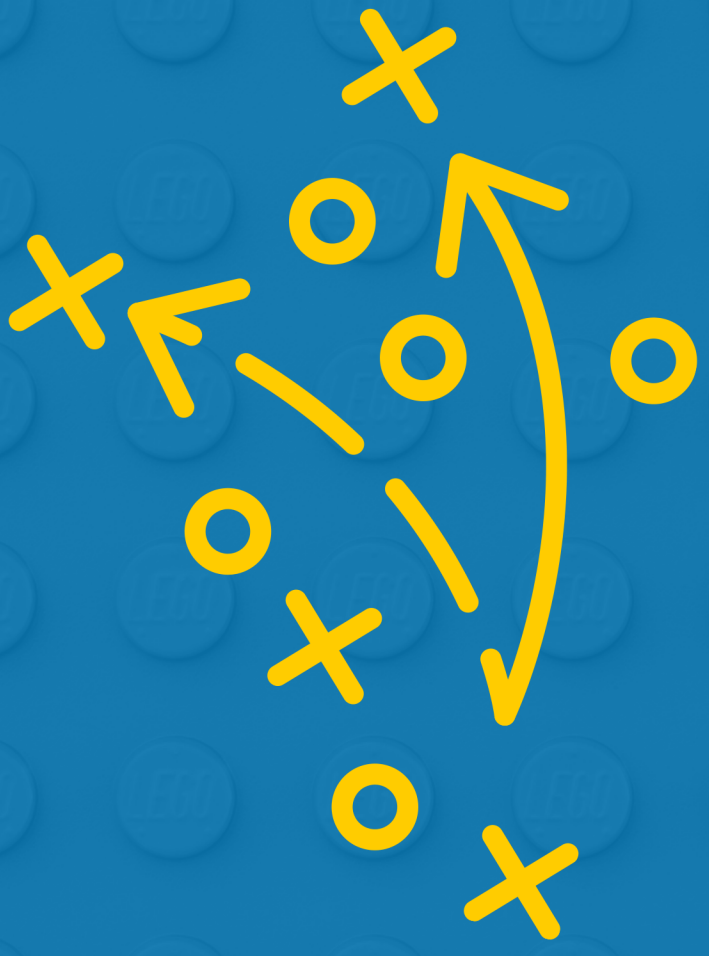
Não deixe de navegar pelas configurações de segurança e privacidade das suas contas, aplicativos e serviços, se certificando de que as melhores opções de segurança estão ativadas e atualizando essas configurações periodicamente. Você também pode ter acesso aos códigos de acesso de backup das contas, salvando em lugar seguro, que servem como uma garantia, mesmo que você perca acesso à conta.



SEBRAE

CONFIRA AS SESSÕES ATIVAS E PERMISSÕES DE APPS

Nas configurações de segurança e privacidade você também pode **checar quais as sessões estão ativas** (ou seja, onde a conta ou o aplicativo está logado), para **confirmar se não há nenhum acesso indevido**, e até mesmo desligar aparelhos conectados na conta. Você também pode ver quais aplicativos de terceiros têm acesso à conta, gerenciando o que é realmente importante ficar conectado e o que não é.

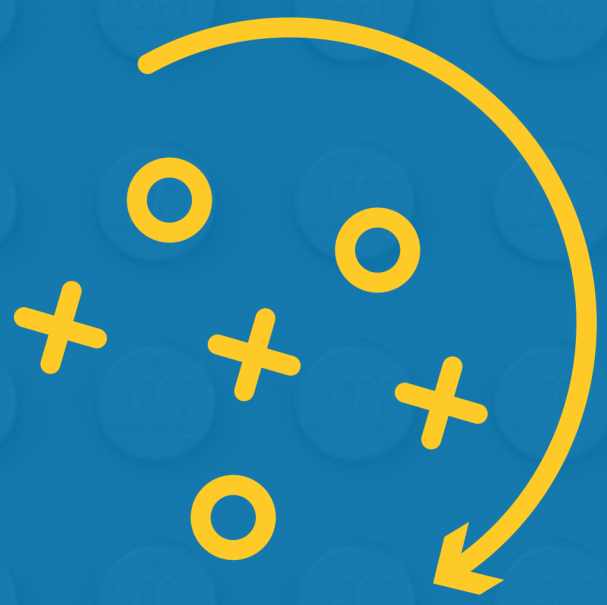


SEMPRE ATUALIZE OS SEUS APLICATIVOS, SISTEMAS E DISPOSITIVOS

Sempre **mantenha os seus dispositivos, sistemas e aplicativos atualizados!** Isso é extremamente importante e não pode ser ignorado. Só assim é que atualizações de Segurança podem consertar falhas e portas de entradas para atacantes, protegendo as suas contas e dados. **Um dispositivo e aplicativo desatualizado é um prato cheio para criminosos.**

USE UM ANTIVÍRUS CONFIÁVEL E RECONHECIDO

Para proteger o seu dispositivo contra ataques conhecidos e populares, você pode instalar um antivírus, desde que seja confiável, reconhecido e recomendado, hein! **Os antivírus não protegem contra os golpistas que atacam as pessoas, mas eles bloqueiam uma grande variedade de programas maliciosos, que possam parecer inofensivos.**



SEBRAE

CUIDE DOS SEUS DISPOSITIVOS CORPORATIVOS E PESSOAIS

Se possível, prefira usar dispositivos separados para o seu trabalho e para o seu uso pessoal. Isso evita que um dispositivo infecte o outro, caso um deles seja atacado. Se isso não for possível, tenha cuidado redobrado com a forma que você navega, no que você clica, baixa ou acessa. Tenha um usuário no seu computador separado para o seu trabalho, e um separado para o seu uso pessoal, e nenhum deles pode ser o usuário administrador do computador, okay?

MANTENHA UM AMBIENTE DE TRABALHO SEGURO

Tome muito cuidado com o seu ambiente de trabalho, tanto o digital quanto o físico! Principalmente se for um ambiente compartilhado com outras pessoas. **Sempre bloqueie o seu computador e dispositivos com senhas seguras ao se distanciar, e desligue tudo ao final do seu expediente.** Não deixe documentos ou arquivos expostos, guarde tudo com chave.

FAÇA O REGISTRO E GERENCIAMENTO DE CONTAS CORPORATIVAS COM SEGURANÇA

Ao criar contas para o trabalho, faça uso apenas de emails corporativos e designados apenas para aquele propósito. Assim, se uma conta for invadida, ela não prejudica as outras. Além disso, **os seus dados pessoais não podem se misturar com os dados do negócio.**

SEBRAE

NAVEGUE DE FORMA SEGURA

Muito cuidado com a rede de internet e o navegador que você usa! **As redes públicas são como praças, e por isso não podem ser usadas para fazer nada sensível ao negócio, como transações bancárias ou troca de dados sensíveis da empresa.** Prefira usar um serviço de VPN* ou uma rede de internet confiável, em um local de trabalho seguro, com uma senha forte e controlada. E use sempre um navegador de internet que seja confiável e reconhecido.

***VPN: A Virtual Private Network (Rede Virtual Privada)** é um serviço de conexão segura, que cria uma camada de proteção entre o seu dispositivo e a rede que ele está acessando

USE UM CARTÃO VIRTUAL

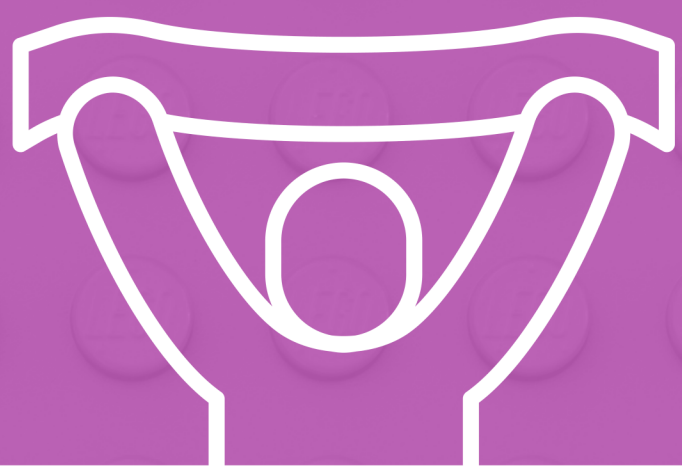
Ao usar um cartão de crédito ou débito para compras online, prefira sempre usar um cartão virtual, que pode ser gerado pelo aplicativo do banco. Assim, **se os dados do cartão forem vazados ou usados sem permissão, não afetará o cartão original**, além de ser mais fácil encontrar a fonte do vazamento e se recuperar do golpe.

CUIDE DA SEGURANÇA DOS SEUS DOCUMENTOS

Ao criar, salvar ou compartilhar documentos em plataformas online, **certifique-se que o acesso é restrito apenas para quem é realmente relevante.** Você pode até mesmo configurar um tempo limite de acesso à documentos. Além disso, prefira sempre fazer a troca de documentos por meios seguros, como email, serviços de cloud ou de comunicação criptografada.

SEBRAE

COMUNIQUE-SE DE FORMA SEGURA



Ao compartilhar dados importantes do negócio, **tenha certeza de que você tem um canal de comunicação seguro e confiável com a outra parte**, evitando que esses dados sejam acessados de forma indevida ou até mesmo interceptados. Por isso, use apenas aplicativos e serviços já conhecidos, usados por outras empresas e recomendados por especialistas.

FAÇA O BACKUP (A CÓPIA DE SEGURANÇA) DOS SEUS DADOS

Sempre que possível, salve uma cópia dos seus dados importantes, como documentos e contratos, em um serviço de nuvem/cloud (como o Google Drive), além de um drive físico (como um HD*). Não se esqueça de configurar as suas contas de backup e recuperação de acesso em todas as suas contas e aplicativos, nas configurações de segurança e privacidade. Assim, se você perder acesso aos seus dados ou às suas contas, você ainda terá acesso ao seu backup, para recuperação!

HD: O Hard Drive é um dispositivo físico que funciona como um grande pendrive. Ou seja, você pode usar esse equipamento para salvar uma grande quantidade de dados e informações, que ficam seguras e desconectadas da internet.

FIQUE DE OLHO NA SUA SEGURANÇA FÍSICA

Para qualquer tamanho de empresa, **é muito importante prestar atenção na segurança do ambiente ao seu redor.** Desconfie de estranhos e desconhecidos circulando no seu ambiente de trabalho, preste atenção nos pontos de acesso, entradas e saídas, e sempre guarde os seus documentos, dispositivos e pertences com o **máximo de cuidado e segurança**, mesmo durante o horário de almoço e intervalos.

SEBRAE

OS CUIDADOS COM A INTELIGÊNCIA ARTIFICIAL

CUIDADO COM O QUE VOCÊ COMPARTILHA COM A INTELIGÊNCIA ARTIFICIAL

Além de ser recomendado usar apenas programas já reconhecidos, confiáveis, oficiais e bem recomendados, por questões de Segurança (afinal, isso significa que eles já passaram por vários testes), é muito importante tomar cuidado com o que você compartilha com a IA. **Nada de compartilhar suas senhas, dados confidenciais, códigos e acessos únicos e secretos, okay?** Assim, você evita que seus dados sejam salvos por um programa que não precisa deles, ou até mesmo de serem vazados em algum acidente.

É SEMPRE BOM CONFERIR AS INFORMAÇÕES, MESMO QUANDO NÃO É GOLPE

Você já sabe que precisa pesquisar algo antes de acreditar naquilo cegamente, certo? Pois é, essa prática é recomendada para muitas outras atividades, mesmo que elas não sejam golpes. As ferramentas baseadas em dados e de inteligência artificial estão sempre sendo atualizadas, mas isso não significa que elas estejam 100% corretas o tempo todo. **Sempre pesquise e compare os resultados que você obtiver com as ferramentas, em fontes confiáveis, como portais de notícias e pesquisas de mercado.**

USE A IA COMO UM SUPORTE, MAS NÃO COMO UM SUBSTITUTO

As ferramentas de inteligência artificial nos ajudam muito nas tarefas do dia a dia, mas elas ainda estão em evolução, e não são perfeitas. Não se preocupe, ela não vai roubar o nosso emprego, como tanta gente diz por aí, mas ela vai sim **ajudar com as nossas tarefas, economizando nosso esforço, tempo e dinheiro! Use a IA como uma base, uma ferramenta para dar suporte ao que você precisa fazer**, mas sempre confira as informações com cuidado e complemente com a sua própria experiência e conhecimento.

SEBRAE

FERRAMENTAS SEGURAS PARA O SEU NEGÓCIO

CUIDADO COM FERRAMENTAS FALSAS OU DESPROTEGIDAS!

Ao usar serviços, ferramentas ou aplicativos, sempre escolha os que forem amplamente reconhecidos, testados e recomendados por especialistas. **Muito cuidado ao baixar aplicativos ou programas que não são oficiais** ou que não possuem recomendações - por isso, sempre pesquise antes de usar!

MENSAGEIROS:

- **Slack:** O serviço é usado mundialmente por grandes empresas para comunicação interna e imediata, com diversos usuários, e possui versão gratuita.

- **Telegram Business:** Substitutivo ao Whatsapp, é um aplicativo de mensagens, com grupos e chats privados/secretos, sem compartilhar o número de telefone e com a destruição de histórico. App é gratuito.

- **Signal:** Substitutivo ao Whatsapp, é um aplicativo de mensagens, com grupos e chats privados/secretos, sem compartilhar o número de telefone e com a destruição de histórico, amplamente conhecido por seus princípios de privacidade. App é gratuito.

- **Whatsapp Business:** O mais comum serviço de mensagens, com integração de serviços de atendimento ao cliente, canal de vendas, canais comerciais, chats para grupos, mensagens privadas e mais. App é gratuito, com opcionais pagos.

SEBRAE

SERVIÇOS DE EMAIL:

- **Gmail:** O mais comum e reconhecido serviço de email, produto do Google. Possui versão gratuita, mas para uso de domínio corporativo é pago. Possui amplas opções de segurança, além de filtro contra phishing e spam. Dá acesso à serviços laterais do Google, como o Google Drive (para armazenamento cloud), Google Calendar (para calendário) e Google Meets (para reuniões).

- **Outlook:** Outro serviço de email amplamente reconhecido, produto da Microsoft. Possui versão gratuita, mas para uso de domínio corporativo é pago. Possui amplas opções de segurança, além de filtro contra phishing e spam. Dá acesso à serviços laterais, como o OneDrive (para armazenamento cloud), Calendar (para calendário) e Microsoft Teams (para reuniões).

- **Protonmail:** Serviço de email reconhecido por seu compromisso elevado com a privacidade dos usuários, serviço da Proton. Possui versão gratuita, mas para domínio corporativo é pago. Possui extensas opções de segurança e privacidade, além de filtro contra phishing e spam. Dá acesso à serviços laterais como ProtonDrive (armazenamento cloud), ProtonCalendar (para calendário), ProtonPass (gerenciador de senhas) e ProtonVPN (navegação segura).

SERVIÇOS DE ARMAZENAMENTO EM NUVEM/CLOUD:

- **Google Drive:** O serviço de armazenamento do Google tem versão gratuita e é amplamente usado ao redor do mundo para criar, armazenar e compartilhar arquivos.

- **OneDrive:** O serviço de armazenamento da Microsoft tem versão gratuita e também é amplamente usado ao redor do mundo para criar, armazenar e compartilhar arquivos.

- **Dropbox:** O serviço de armazenamento da empresa Dropbox tem versão gratuita, é globalmente reconhecido para criar, armazenar e compartilhar arquivos, além de ter acesso à serviços laterais, como o Sign (para assinatura de documentos digitais).

SEBRAE

NAVEGADORES:

- **Chrome:** O mais famoso navegador web é um serviço gratuito do Google, com proteções básicas de segurança e compatível com um enorme número de extensões.

- **Brave:** É um dos navegadores mais indicados para os aficionados por privacidade e segurança, extremamente similar ao Google Chrome, gratuito e intuitivo.

- **Firefox:** Um dos mais famosos navegadores, amplamente usado no mundo todo, com consideráveis opções de segurança e privacidade.

- **Safari:** Para usuários de iOS, o Safari é um dos navegadores mais indicados, produto da Apple, com proteções básicas de segurança.

- **VirusTotal.com:** Não é um navegador, mas sim um site indicado para checar a confiabilidade de um link, de acordo com relatórios de empresas confiáveis.

GERENCIADORES DE SENHAS:

- **Bitwarden:** É um dos gerenciadores de senhas gratuitos mais bem recomendados do mercado. Possui versão paga corporativa.

- **ProtonPass:** O gerenciador de senhas gratuito da Proton é um dos mais recomendados por especialistas de Segurança da Informação, com versão corporativa paga.

- **1Password:** Um dos líderes em gerenciamento de senhas, o 1Password não tem versão gratuita, mas os planos possuem preços acessíveis.

SEBRAE

MÚLTIPLO FATOR DE AUTENTICAÇÃO (APPS DE TOKEN):

- **Google Authenticator:** É um app gratuito do Google, amplamente recomendado para autenticação de múltiplo fator.
- **Microsoft Authenticator:** Também gratuito, é o app de autenticação em token da Microsoft, também reconhecido.
- **Authy:** O app autenticador da Twilio também é gratuito, e um dos preferidos dos especialistas de Segurança da Informação.
- **Yubikey:** É um token físico de autenticação, um dispositivo pago, mas que representa a mais segura forma de autenticação entre todas as apresentadas.

VPN (VIRTUAL PRIVATE NETWORK – NAVEGAÇÃO SEGURA):

- **ProtonVPN:** A Proton oferece alguns dos melhores serviços de privacidade gratuitos, como a sua VPN, altamente recomendada para conexões mais seguras.
- **PIA VPN:** Serviço pago de VPN, com preço acessível e ampla recomendação de mercado.
- **NordVPN:** Serviço pago de VPN, com preço acessível e bem recomendado.

SEBRAE

ANTIVÍRUS:

- **Avast:** Um dos mais populares antivírus gratuitos, confiável e de fácil uso.
- **Kaspersky:** Possui versão gratuita, sendo um dos antivírus mais recomendados por profissionais de Segurança da Informação.
- **AVG:** Outro antivírus gratuito globalmente reconhecido e de fácil uso.

SEBRAE