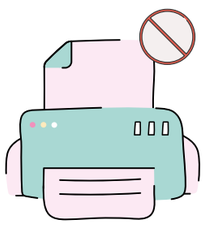
CARTILHA DE SEGURANÇA DA INFORMAÇÃO

Segurança da Informação

Esteja Seguro

Politica de mesa e tela limpa

São praticas de segurança recomendadas para que você evite a exposição desnecessária de informações sensíveis e confidenciais. Abaixo segue alguns exemplos do que fazer em seu ambiente de trabalho



Não imprimir documentos apenas para lê-los. Leia-os na tela do computador sempre que possível

Nunca anotar senhas em lembretes e tentar esconde-las no local de trabalho

No computador sempre utilizar o bloqueador de tela quando sair de seu ambiente de trabalho

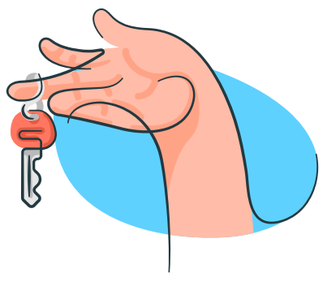
Nunca deixar crachá de identificação ou chaves em qualquer lugar; Mantenha-as junto a você

Armazenamento de Dados

Todos os arquivos e informações de trabalho ainda que armazenados nas estações de trabalho, notebooks e dispositivos móveis, devem ser transferidos para os servidores da rede de modo a assegurar sua atualização e a devida salvaguarda por meio do backup corporativo

Você Sabia?

O compartilhamento de credenciais com outros funcionários ou terceiros é um dos comportamentos mais destrutivos para uma empresa, por isso nunca compartilhe seu usuário e senha



A segurança consiste na responsabilidade de saber e agir de maneira correta

PENSE

Segurança da Informação

O que é Phishing?

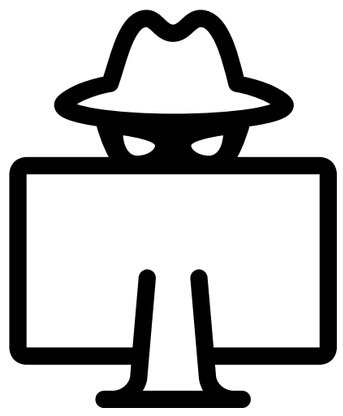
É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social

Como funciona o ataque?

Geralmente é utilizado e-mail, redes sociais, SMS e telefone. O golpista envia um texto com objetivo de convencer a vitima a clicar em um link e realizar o download de um anexo ou envio de informações

Quais são os impactos?

Este tipo de ataque pode levar a roubo de credenciais, roubo de informações sigilosas, ocasionar indisponibilidade em toda rede da empresa dentre outros



Como me protejo contra Phishing?

Observe sempre as características da mensagem como erros ortográficos e argumentos persuasivos

Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens

Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos

Em caso de dúvidas sobre a legitimidade de uma mensagem, entre em contato com o setor de TI pelos canais de atendimento

Você Sabia?

Suas credencias de acesso a sistemas e aplicações são somente suas e não deverão ser cedidas para ninguém, nem mesmo para a equipe de TI. Caso desconfie que sua senha não esteja mais segura, redefina imediatamente e procure a TI

Antes de tudo, desconfie sempre!

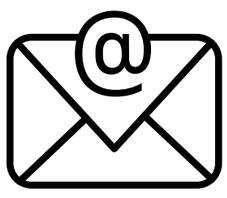
Esteja sempre desconfiado de toda comunicação não desejada que você receba. Não considere uma mensagem confiável utilizando apenas como base o remetente

Segurança da Informação

Privacidade

Nada impede que você abdique de sua privacidade e, de livre e espontânea vontade, divulgue informações sobre você. Entretanto, há situações em que, mesmo que você queira manter a sua privacidade, ela pode ser exposta independente da sua vontade, por exemplo quando:

outras pessoas divulgam informações sobre você ou imagens onde você está presente, sem a sua autorização prévia



um atacante invade a sua conta de e-mail ou de sua rede social e acessa informações restritas;

seus hábitos e suas preferências de navegação são coletadas pelos sites que você acessa e repassadas para terceiros

Proteja sua privacidade

Procure divulgar a menor quantidade possível de informações, tanto sobre você como sobre seus amigos e familiares, e tente orientá-los a fazer o mesmo

fique atento a ligações telefônicas e e-mails pelos quais alguém, geralmente falando em nome de alguma instituição, solicita informações pessoais sobre você, inclusive senhas

seja cuidadoso ao divulgar informações em redes sociais, principalmente aquelas envolvendo a sua localização geográfica pois, com base nela, é possível descobrir a sua rotina, deduzir informações

LGPD

A Lei Geral de Proteção de Dados (LGPD - 13.709/2018) vem para proteger os direitos fundamentais de privacidade de cada indivíduo. A LGPD estabelecera uma série de regras que empresas e outros organizações atuantes no Brasil terão de seguir para permitir que o cidadão tenha mais controle sobre o tratamento que é dado as suas informações pessoais.

Segurança da Informação

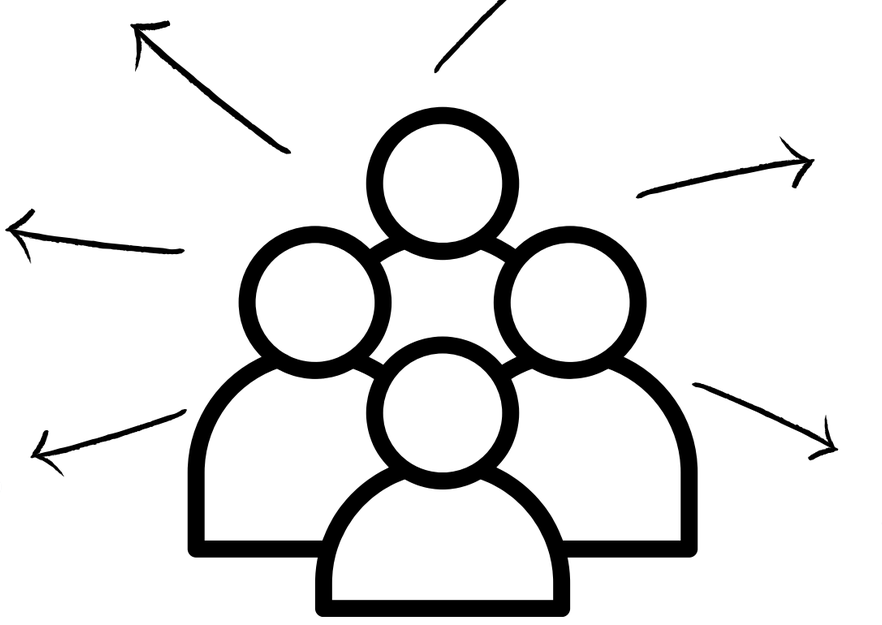
Lei Geral de Proteção (LGPD – 13.709/2018)

Quais direitos os usuários tem ?

Ser informado o motivo que a empresa está utilizando e tratando seus dados

Solicitar autorização para utilização de seus dados para uma causa diferente da que foi aceitado

Solicitar anonimização, bloquei ou eliminação de dados a qualquer tempo



Soliticar a portabilidade de seus dados para outra empresa.

Corrigir dados incorretos, ou não atualizados

Saber quais dados a empresa tem sobre você

A Lei Geral de Proteção de Dados Pessoais (LGPD - 13.709/2018) em breve será uma realidade para toda empresa e com isso mudanças substanciais em processos e na cultura organizacional irão acontecer. Além disso há alguns motivos para que as empresas estejam em conformidade são eles, sanções de até 2% do faturamento da empresa limitado em até 50 milhões de reais por infração, quebra da confiança na marca da instituição, processos iniciados pelos titulares dos dados.

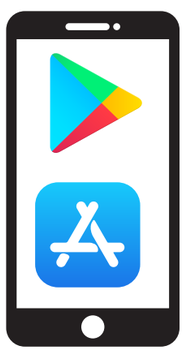
Por isso, tudo pode mudar. Esteja preparado!

Segurança da Informação

Mais dicas de segurança!

A internet nos oferece inúmeras possibilidades de uso, mas para aproveitar cada uma delas de forma mais segura é importante que alguns cuidados sejam tomados

Não utilize sites de busca para acessar e-mail ou site de instituições bancarias (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas)



Ao usar seu dispositivo móvel mantenha o sistema e aplicativos instalados com a versão mais recente e sempre instale os mesmos de fontes confiáveis (Play Store App Store) e que sejam bem avaliadas pelos usuários

Seja cuidadoso ao usar redes Wi-Fi públicas, atacantes podem utilizar deste meio para captura de informações. Caso tenha opção de não utilizar faça isso

Cuidados na criação de senha

É bastante comum o vazamento de dados de usuários por sites invadidos por hackers. O exemplo mais recente é o site "vakinha" responsável por arrecadar dinheiro para diversas causas , nele foram vazados 4,8 milhões de registro de usuários e nestes dados consta as credencias de acesso. Uma pratica comum utilizada por hackers é utilizar destas credenciais vazadas para acessar outros sistemas, tendo em vista que muitos usuários utilizam a mesma senha para todos os sistemas. Por isso **nunca use a mesma senha** para acessar diferentes sistemas

Diretrizes

O Principal objetivo da gestão de Segurança da Informação da Grande Moinho Cearense S.A. é orientar por meio de diretrizes as ações de segurança para reduzir os riscos e prover suporte as operações do negócio, garantindo a confidencialidade, disponibilidade e integridade das informações