Cibersegurança

Material Complementar

#PraTodosVerem: Fotografia da autora Déborah Tonucci.

Déborah G. Tonucci

Advogada na Gama Academy, atuante nas áreas de Direito Empresarial e Direito Digital.

Mestranda em Direito pelo Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa (IDP) e pesquisadora.

https://www.linkedin.com/in/deborahgomestonucci/

Sumário

Objetivos

Ao final da leitura, esperamos que você seja capaz de:

- Refletir sobre o que é a cibersegurança, seus fundamentos e formas;
- Identificar os pilares da segurança da informação;
- Distinguir privacidade e proteção de dados e compreender as diretrizes da Lei Geral de Proteção de Dados;
- Conceituar riscos e ataques cibernéticos, e identificar os métodos de ameaça mais comuns;
- Compreender o que é governança de dados e como funciona a sua equipe;
- Replicar boas práticas de segurança da informação na esfera individual e corporativa.

Introdução

O ato de fornecer dados faz parte do cotidiano de cada pessoa. Ao realizar uma compra *online*, por exemplo, é natural que se forneça senhas, endereços, números de cartão de crédito, e mais. E igualmente nas empresas, em que informações de negócios, investimentos e até planejamentos circulam entre áreas e pessoas.

Mas como garantir que essas informações ficarão protegidas? Como preservar os dados no **2º país que mais sofre com ataques cibernéticos**[1]?

A resposta está na **Cibersegurança**, que visa justamente garantir que tais dados só estejam acessíveis a quem possui autorização, entre outros objetivos em prol do fortalecimento da segurança da informação.

[1] **Fonte:** Relatório de inteligência de ameaças do segundo semestre de 2021 da NETSCOUT

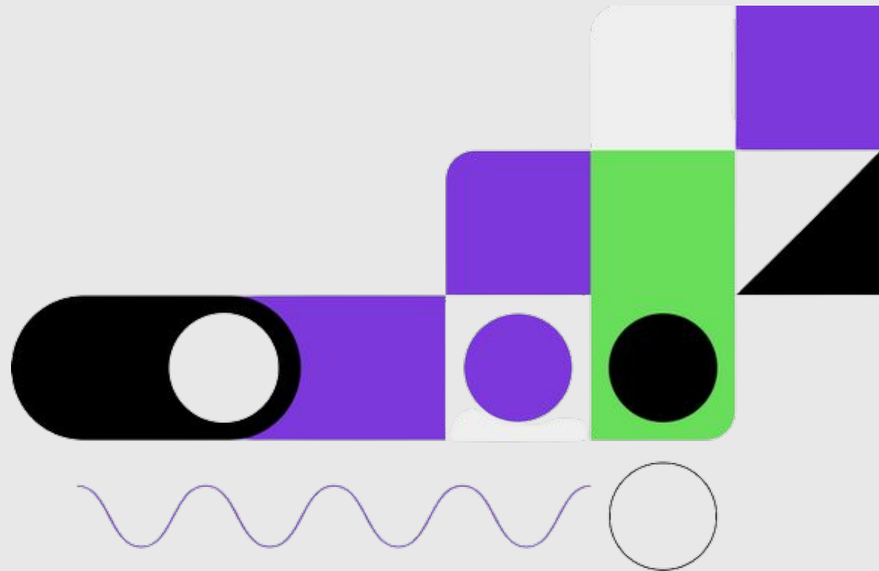
O que é cibersegurança?

Conceito:

Conjunto de ações e técnicas para proteger sistemas, programas, redes e equipamentos de invasões.

Objetivo:

Garantir que dados e informações valiosas só estejam acessíveis a quem possui autorização, assim como que não vazem ou sejam violados em ataques cibernéticos



Cenário brasileiro

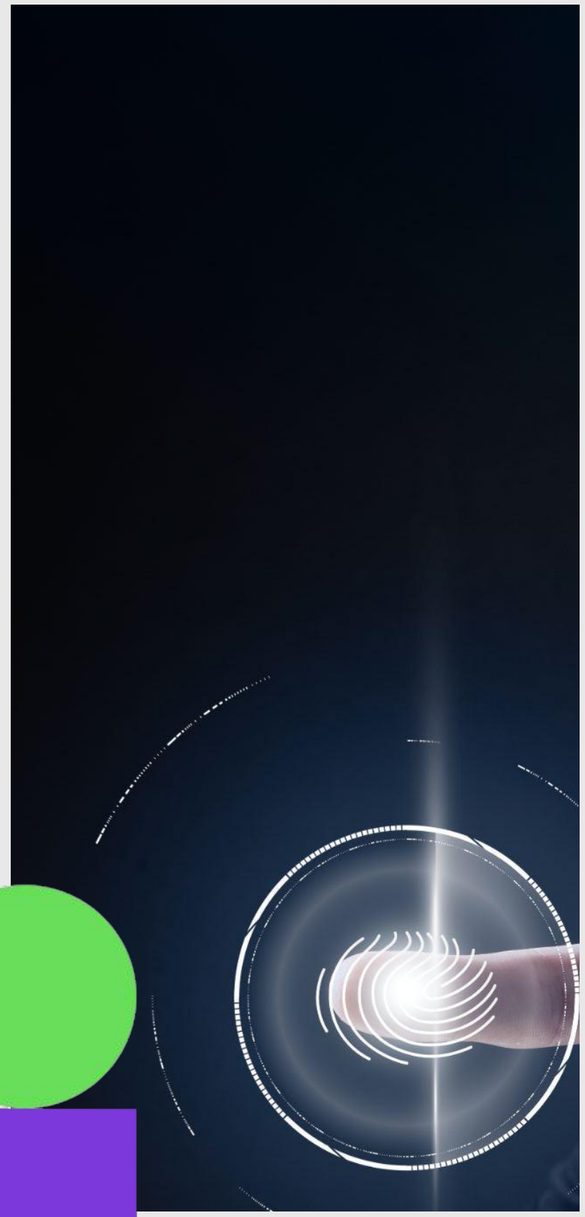
O relatório da Netscout, uma das maiores plataformas de análises e respostas avançadas a ameaças, em 2021, apresentou dados sobre ataques cibernéticos em escala mundial:

No primeiro semestre de 2021 foram lançados mais de **6,4 milhões de ataques cibernéticos no mundo**. Apenas no Brasil, em torno de 439 mil, isso dá 7,1%, nos inserindo na 2ª posição entre os países mais alvo de ataques, atrás apenas dos Estados Unidos, com 21,7%. Em terceiro lugar aparece a Coreia do Sul, com 6,3%, seguida pelo Reino Unido, com 5,7%, e pela China, com 4,2%.

O relatório ainda indica que os 6 setores mais visados por hackers foram:

1. operadoras de telecomunicações sem fio;
2. operadoras de telecomunicações com fio;
3. processamento de dados, hospedagem e serviços relacionados,
4. fábricas de computadores,
5. telecomunicações em geral
6. e-commerces.

Formas de Cibersegurança



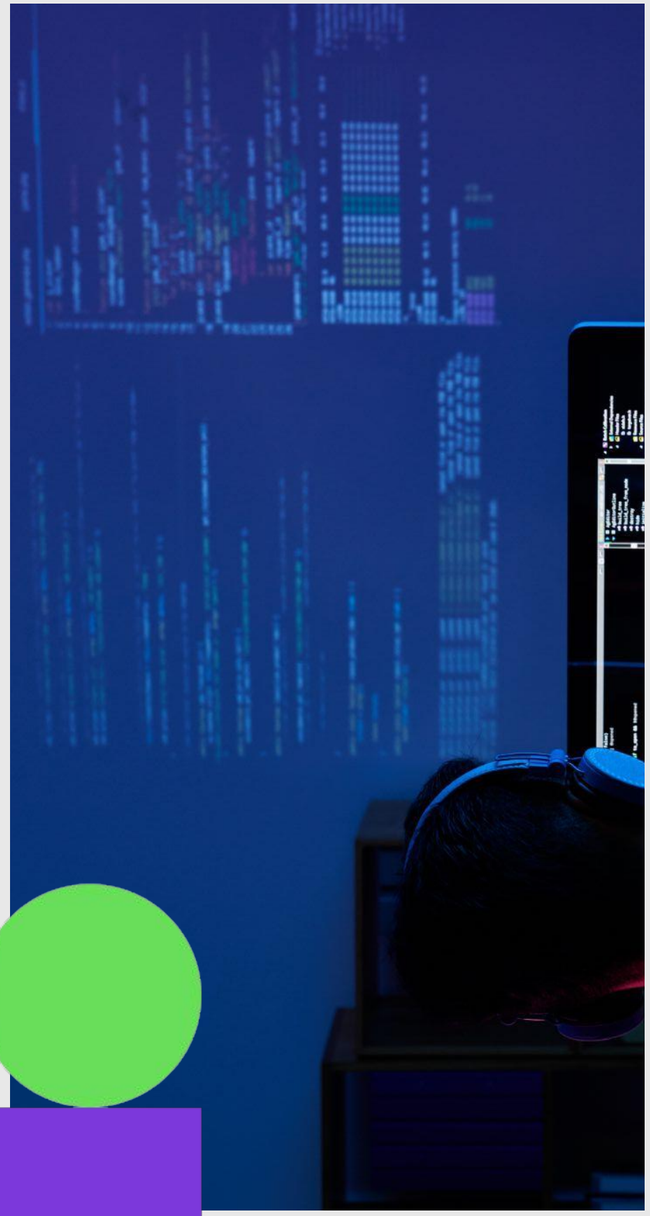
Cibersegurança Física

Restrição do acesso a informações que funcionários de determinado setor não precisam para realizar suas demandas diárias.

Objetivo de garantir a segurança de informações relevantes e confidenciais.

Exemplos:

Sistema de identificação de funcionários por crachás, catracas e portas de acesso com senha ou biometria e até mesmo câmeras de segurança.



Cibersegurança Lógica

Programas que impedem o acesso de softwares mal-intencionados, que representam ameaça.

Necessita de estrutura sólida para funcionar de forma eficaz. Tendo softwares de segurança atualizados para produzirem relatórios frequentes, e profissionais da cibersegurança capazes de entender esses programas e os relatórios que vão ser utilizados para garantir a segurança da empresa.

Exemplos:

Firewalls, antivírus e softwares de segurança atualizados, gerando relatórios periódicos, e equipe de cibersegurança preparada para usá-los.

Programa de Cibersegurança

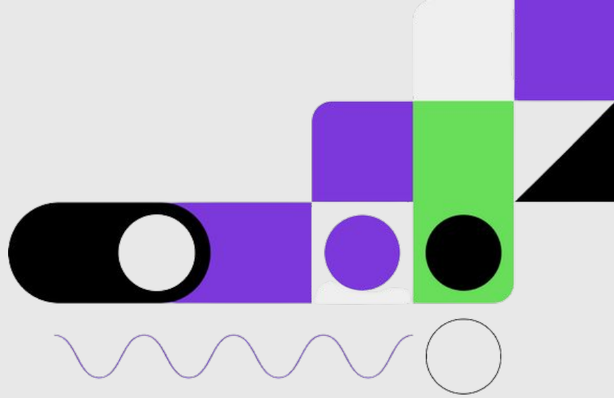
Um programa de cibersegurança eficaz deve ser capaz de prevenir ameaças e ataques cibernéticos.

Para garantir sua efetividade, algumas funções são consideradas imprescindíveis.

São algumas:

- Identificação e avaliação de riscos;
- Ações de prevenção e proteção;
- Monitoramento e testes;
- Criação do plano de resposta e
- Governança.

Funções



01. Identificação e avaliação de riscos

Identificar os riscos internos e externos, ativos de hardware, software e processos que precisam ser protegidos.

02. Ações de prevenção e proteção

Estabelecer um conjunto de medidas em busca de prevenir e diminuir o acontecimento dos riscos identificados.

03. Monitoramento e testes

Encontrar ameaças rapidamente, a fim de reforçar os controles e detectar irregularidades que possam ser sanadas.

04. Criação do plano de resposta

Ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação.

05. Governança

Conservar o programa de segurança atualizado, de forma contínua, nos termos das estratégias e diretrizes.

Segurança da Informação e Cibersegurança

Segurança da Informação

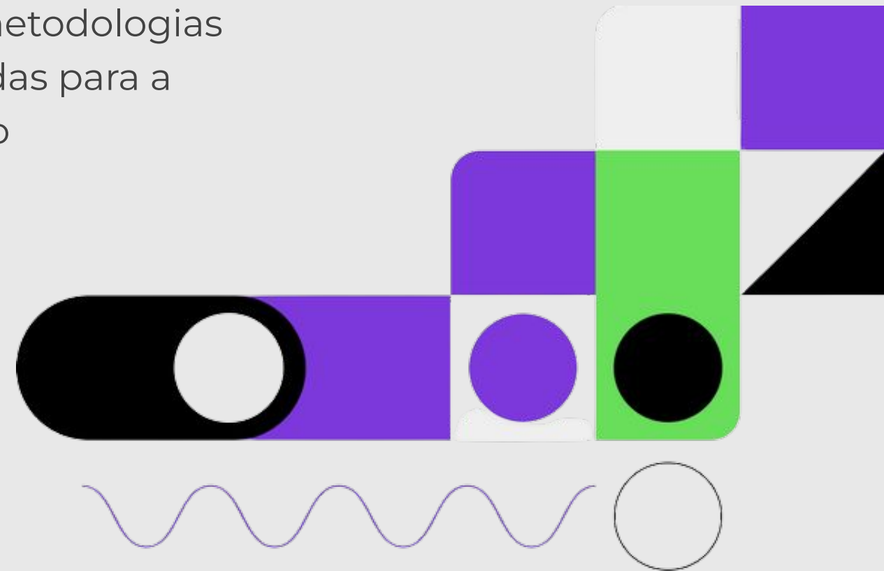
Tem um significado mais amplo, pois trata da proteção de todos os dados sigilosos de uma empresa.

Conjunto de normas, técnicas e práticas necessárias para que as informações sensíveis ao negócio estejam sempre protegidas de uma divulgação indevida.

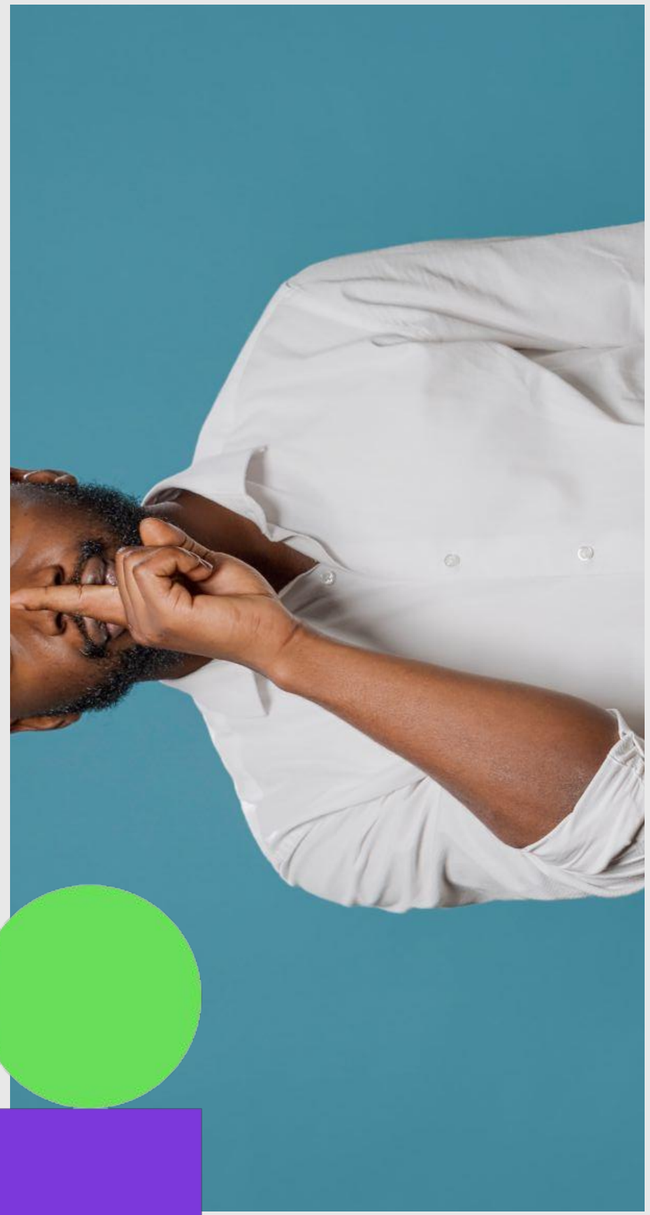
Cibersegurança

Segmentação específica dentro do campo da Segurança da Informação.

Responsável por definir as metodologias e tecnologias que serão usadas para a proteção de dados dentro do ciberespaço



Pilares da Segurança da Informação



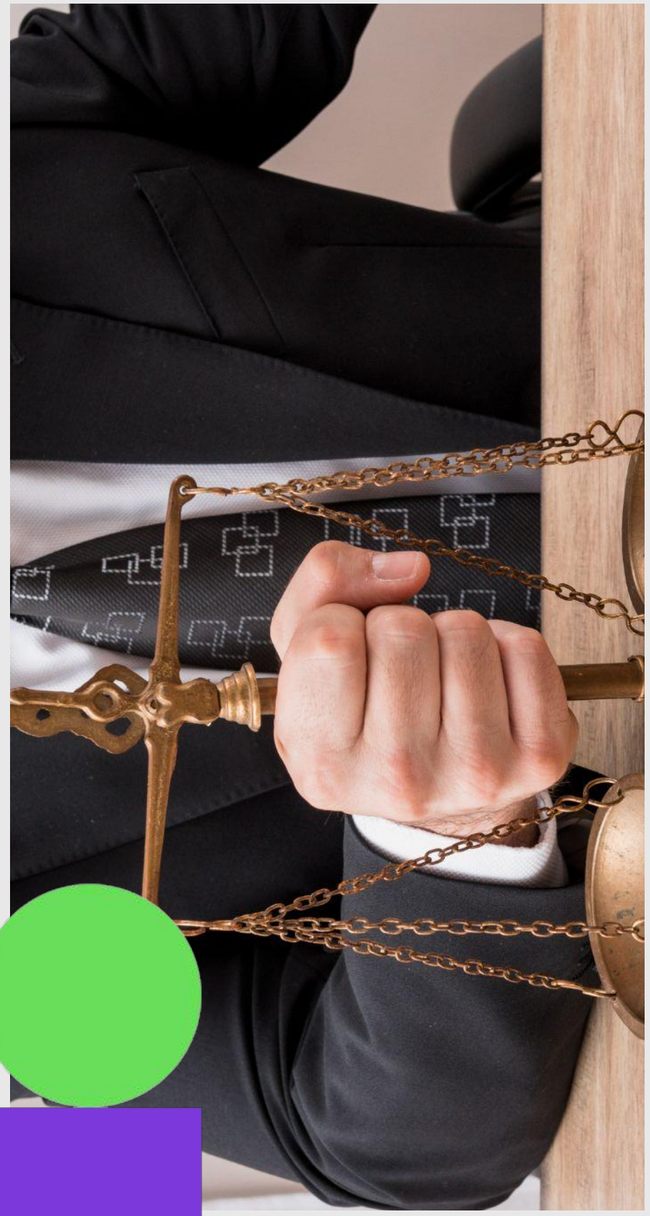
1 confidencialidade

A confidencialidade garante que os dados estejam acessíveis a determinados usuários e protegidos contra pessoas não autorizadas.

É um componente essencial da privacidade, que se aplica especialmente a dados pessoais, sensíveis, financeiros, psicográficos e outras informações sigilosas.

Exemplos:

Criptografia de dados, autenticação de dois fatores, verificação biométrica e uso de token.



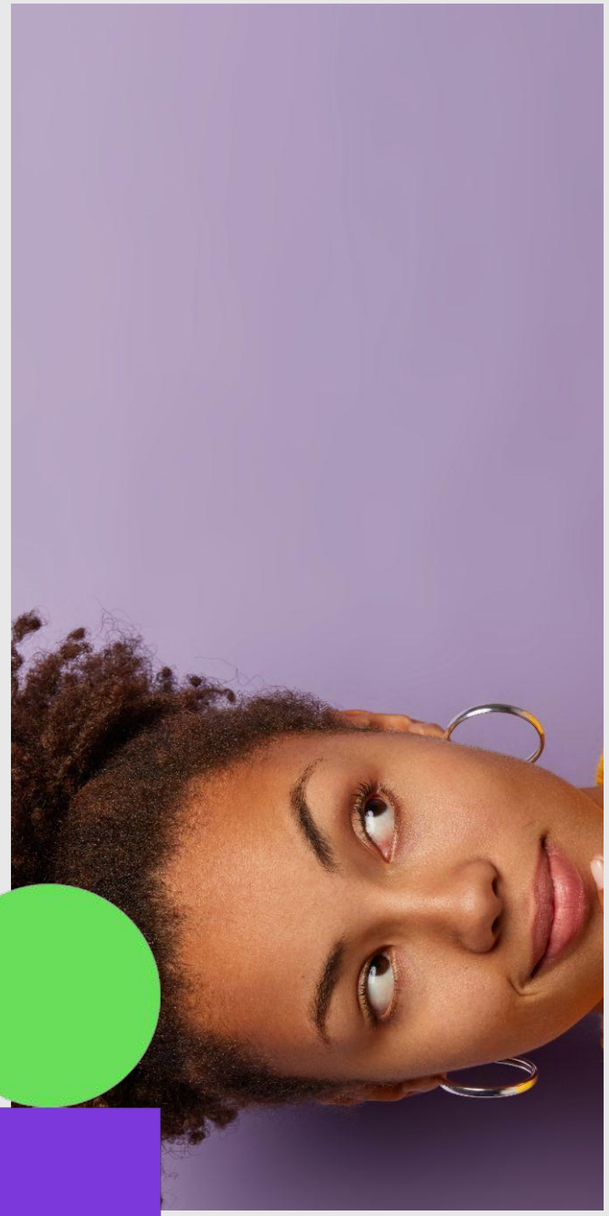
2 legalidade

Manter a Política de Segurança em conformidade com a legislação, assegurando que todos os procedimentos relacionados à informação dentro da empresa sejam feitos dentro dos termos legais.

Evita que ocorram impedimentos operacionais, averiguações e auditorias de órgãos fiscalizadores.

Exemplos:

Conformidade com a Lei Geral de Proteção de Dados (LGPD)



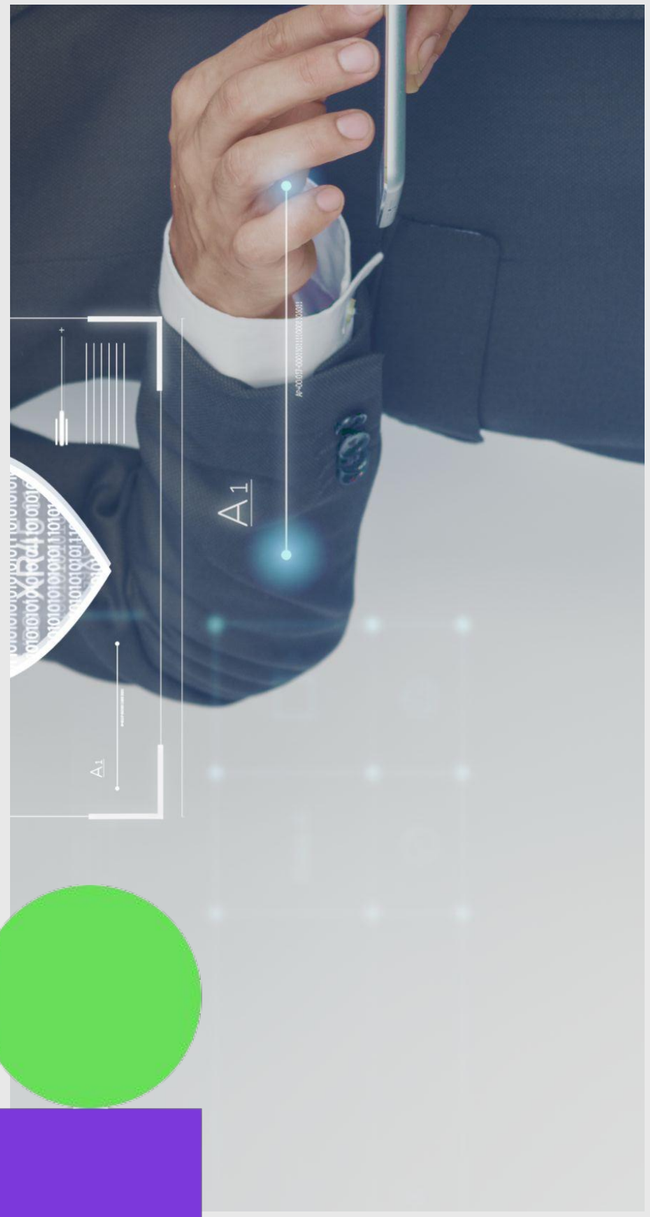
3 integridade

Garantia de que a informação estará completa, exata e preservada contra alterações indevidas, fraudes ou até mesmo contra a sua destruição.

Mecanismos de controle para evitar que as informações sejam alteradas ou deletadas por pessoas não autorizadas.

Exemplos:

Uso de assinatura eletrônica, controles de versões e sistemas de verificação para detectar alterações nos dados.



4 disponibilidade

Certeza de que a informação estará acessível e disponível sempre que necessário, garantindo o acesso em tempo integral.

Deve garantir que as informações estejam disponíveis a todos que têm autorização de acesso.

Exemplos:

Processos de manutenção rápidos, eliminação de falhas de software, atualizações constantes e Plano de Recuperação de Desastres.

5 autenticidade

Busca saber, por meio de registro apropriado, quem realizou acessos, atualizações e exclusões de informações, de modo que haja confirmação da sua autoria e originalidade.

E ainda, que quem envia certas comunicações, é de fato a pessoa autorizada para tanto.

Exemplos:

Para o acesso, logins e senhas, autenticação biométrica. Para a comunicação, assinatura digital, que garante a autenticidade.

Privacidade e Proteção de Dados

Privacidade

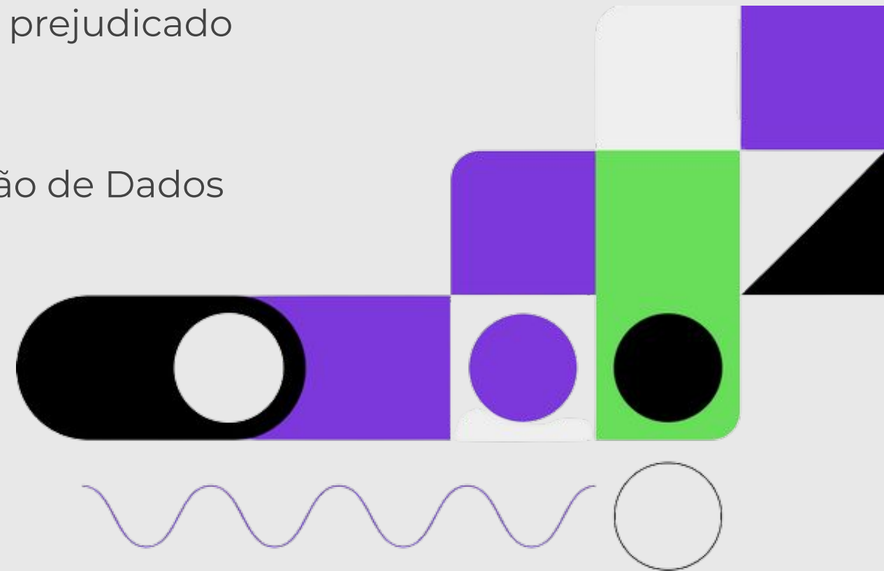
Direito à vida íntima sem que sejam expostas de forma arbitrária, e viver sem intervenções ilegais.

Previsão: artigo 5º, inciso X, da Constituição Federal (inviolabilidade da vida privada)

Proteção de Dados

Fornecimento de dados, desde que com consentimento do titular e conhecimento científico de sua finalidade, para que não seja prejudicado direta ou indiretamente.

Previsão: Lei Geral de Proteção de Dados



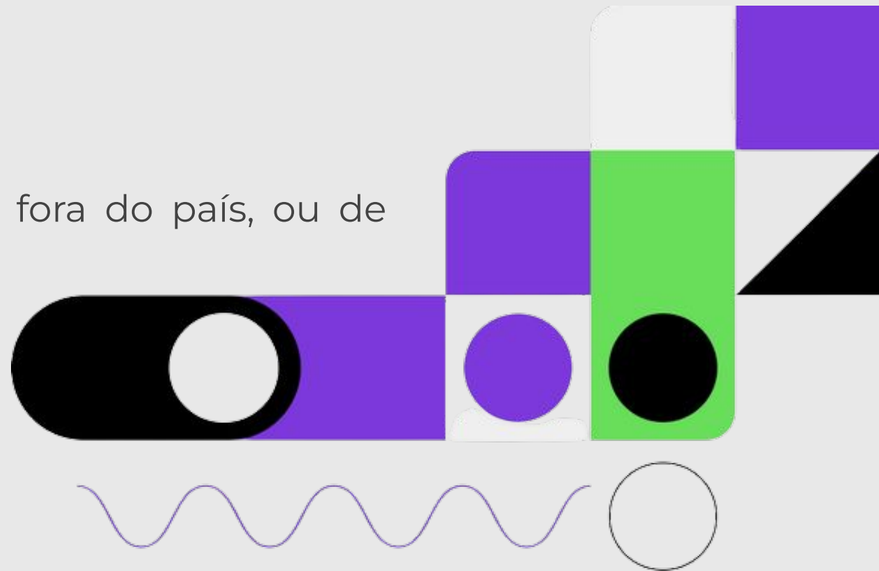
Lei Geral de Proteção de Dados

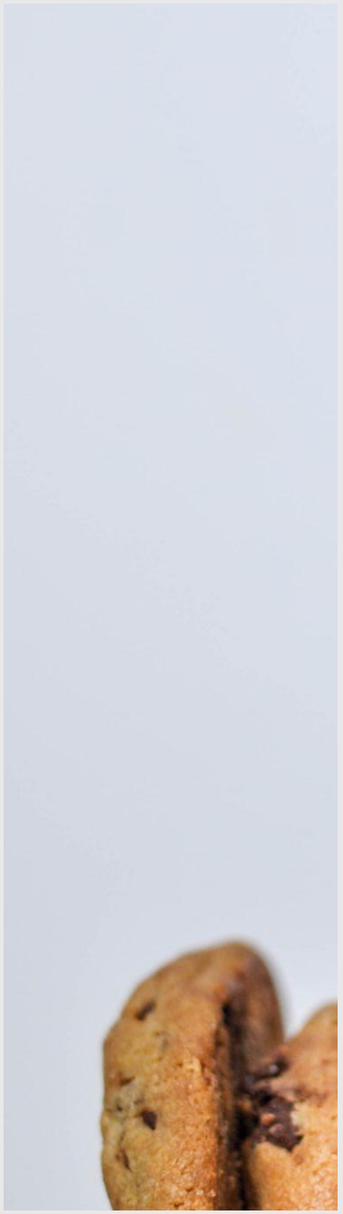
Objetivo:

Adoção de medidas técnicas e administrativas, estabelecendo padrões de segurança aptos a proteger os dados pessoais coletados interna e externamente, de acessos não autorizados, entre outras situações.

Aplicação:

Todo processamento de informações, ainda que seja de pessoas brasileiras fora do país, ou de estrangeiros que estão em território nacional.





Consentimento

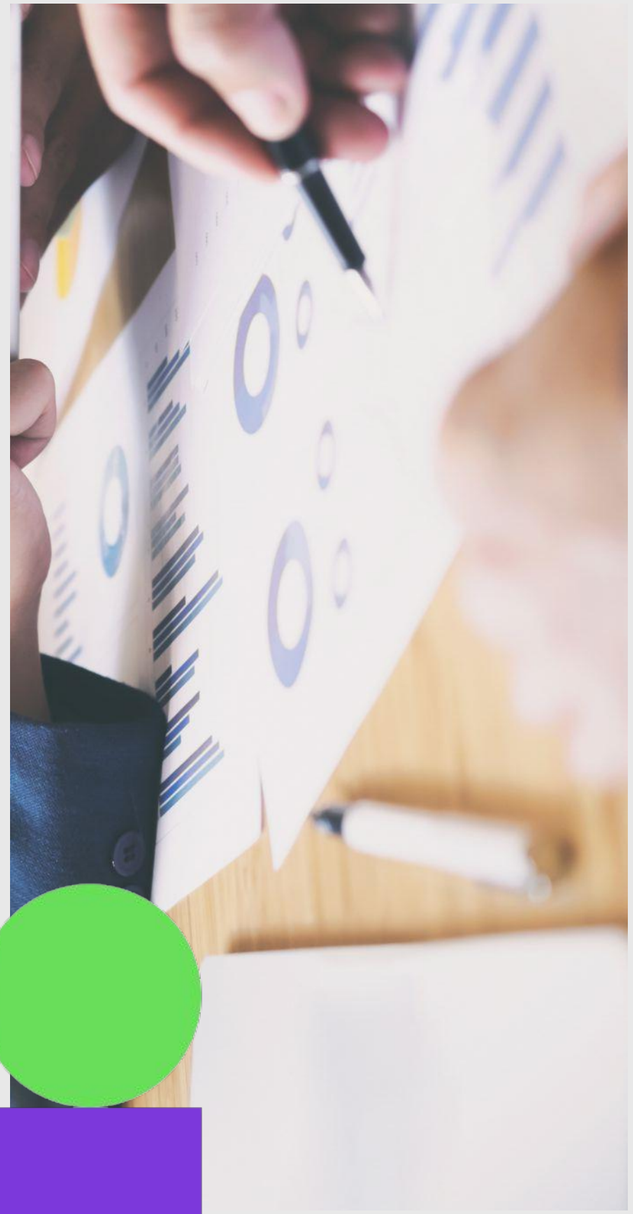
Elemento essencial para o tratamento de dados.

Deve apresentar a finalidade necessidade, e garantir:

1) a exclusão dos dados pessoais;
2) revogação do consentimento;
3) transferência dos dados para outro fornecedor de serviços, entre outras ações

Exemplos:

Aviso de cookies: explicitar a prática (utilização de cookies), a finalidade (melhorar a navegação) e solicitar o consentimento.



Quem fiscaliza?

- **Autoridade Nacional de Proteção de Dados Pessoais (ANPD)**

- **Agentes de tratamento de dados:**

  - **Controlador**, que toma as decisões sobre o tratamento;
  - **Operador**, que realiza o tratamento, em nome do controlador;
  - **Encarregado**, que interage com os titulares dos dados pessoais e ANPD.

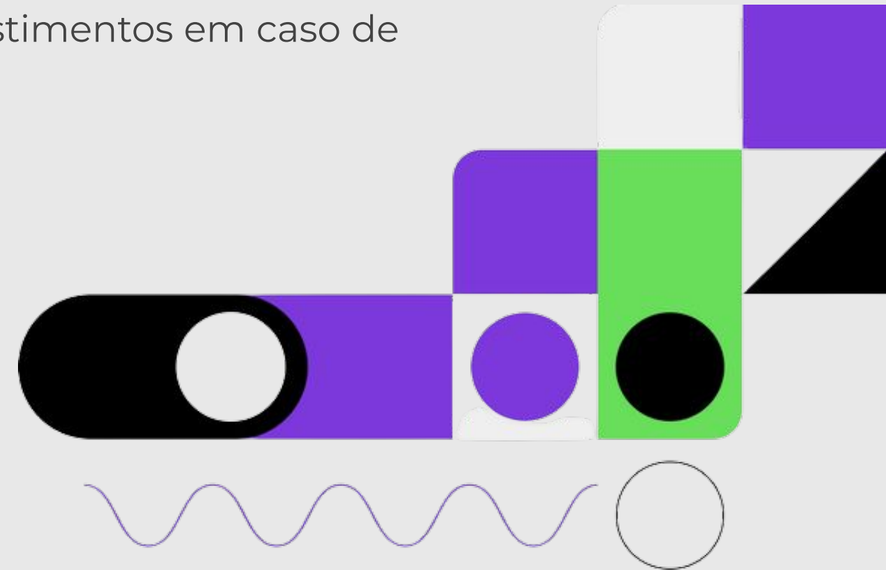
Ataques cibernéticos

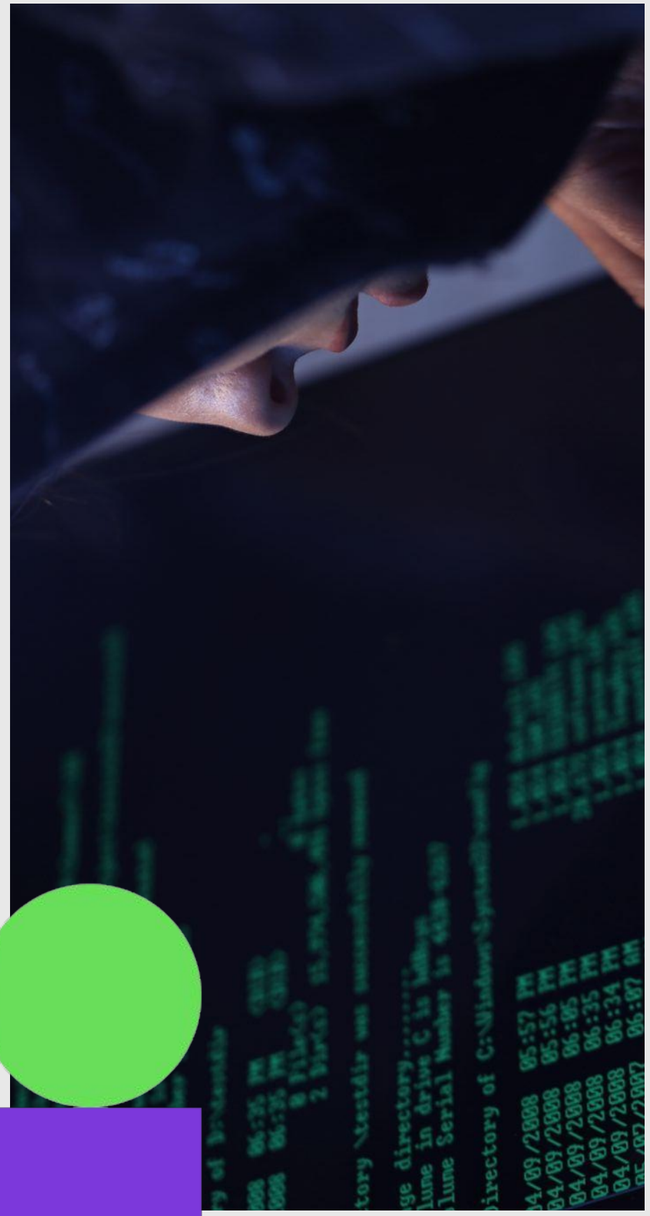
Conceito:

Atividades criminosas que, prioritariamente, tem como alvo organizações empresariais ou governamentais, buscando danificar uma rede ou sistema, por meio de fraquezas operacionais deixadas pelos usuários.

Objetivo:

Na maioria dos casos, lucra com pedidos de resgate para devolução dos dados, provocando à vítima prejuízos financeiros e de credibilidade, danos à imagem e até queda de investimentos em caso de empresas.





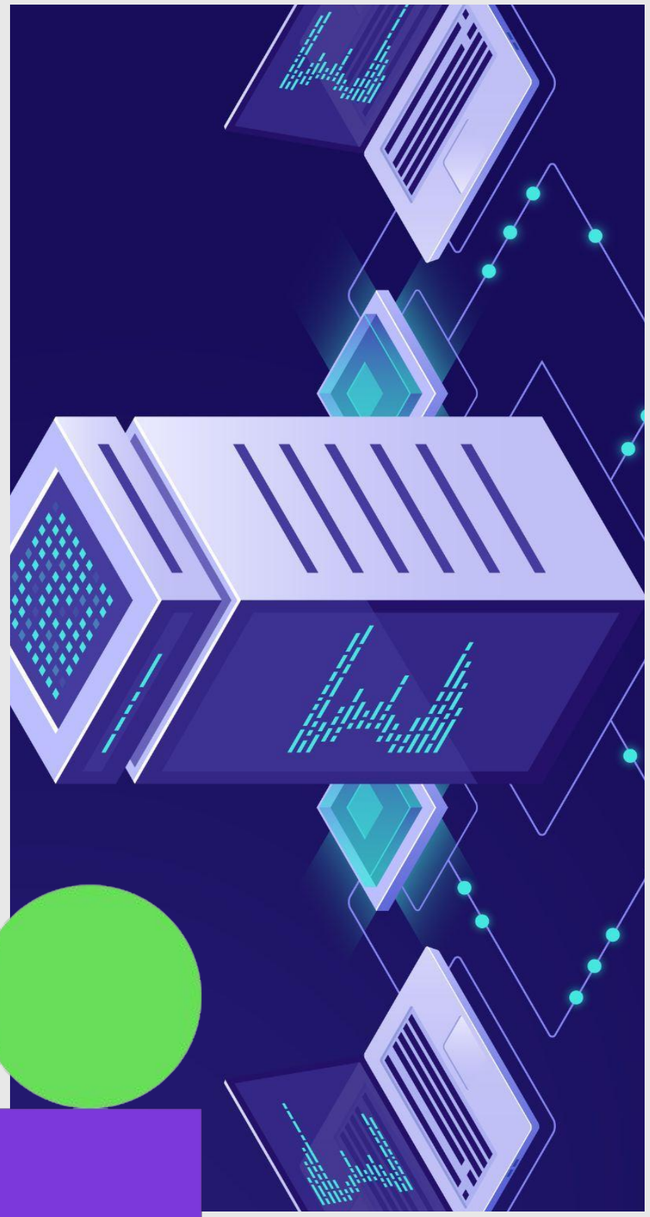
DoS (Denial Of Service)

Sobrecarregamento de servidor ou computador com um alto volume de pedidos de pacotes, que por não conseguir lidar com as requisições, fica indisponível.

Objetivo é tirar um sistema servidor do ar e fazer com que deixe de oferecer o seu serviço.

Exemplos:

uma página fora do ar, inacessível porque algum hacker diretamente realizou ataques no sistema servidor.



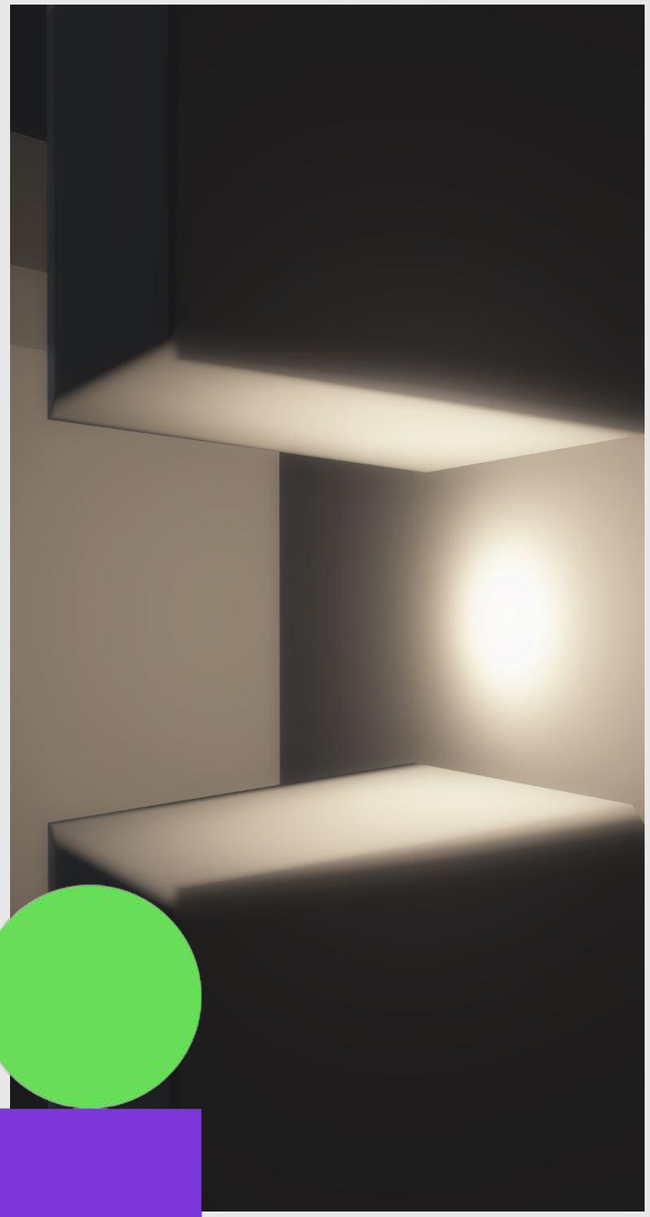
DDoS (Distributed Denial of Service)

Sobrecarregamento de servidor por meio de um ataque simultâneo de diversos computadores.

O hacker acessa diversas máquinas e as direciona ao servidor, para acessá-lo, e por não conseguir lidar com diversas requisições, fica indisponível.

Exemplos:

O hacker instala vários programas (bots), em vários computadores, e por “acesso remoto” acessa simultaneamente um site, tirando-o do ar.



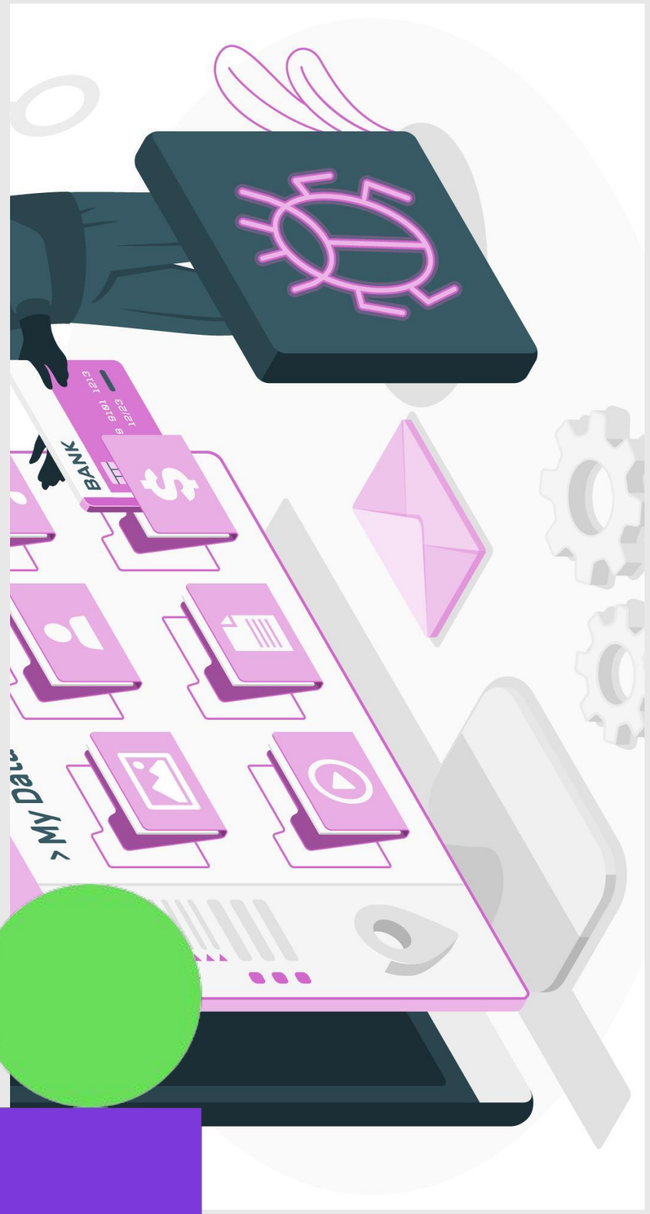
MITM (Man In The Middle)

Roubo de dados confidenciais por um invasor que intercepta uma comunicação.

Usualmente visa o roubo de dados bancários, mas podem ser direcionados para qualquer tipo de transação online.

Exemplos:

envio de faturas e documentos financeiros falsos e criação de redes falsas nas quais as pessoas se conectam



Malware

Softwares que contém instruções maliciosas visando ao roubo de informações, entre outros objetivos fraudulentos.

Nesse tipo de ameaça o hacker mal-intencionado envia um link ou documento que, acessado, instala o programa.

Exemplos:

envio de malware na forma de anexos que, por sua vez, levam a aplicações do tipo .exe (executável).

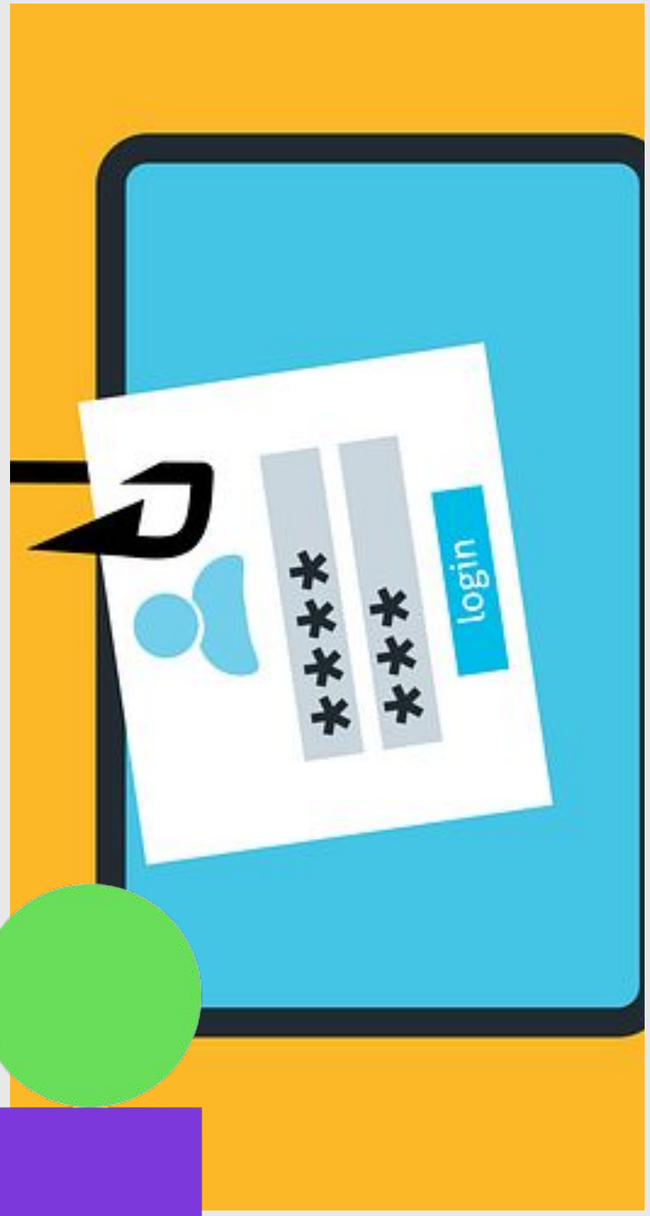
Ransomware

Software que tem por objetivo bloquear o acesso a arquivos de um dispositivo.

Buscam cobrar uma espécie de “resgate” para devolver o acesso a esses dados, configurando assim um crime de extorsão, previsto no artigo 154-A do Código Penal brasileiro.

Exemplos:

O hacker “sequestra” arquivos de um computador e cobra um pagamento de resgate, que geralmente é feito com moeda virtual.



Phishing

Comunicações falsificadas que parecem vir de uma fonte confiável, como empresas e corporações sérias, solicitando dados financeiros, pessoais, etc, via e-mail e mensagens.

Exemplos:

Emails com solicitações de recadastramento de senhas, intimações ou citações judiciais, que levam o destinatário a abrir algum link.

Mas também, um site completo parecido com o verdadeiro, com a intenção de capturar informações de identificação pessoal do usuário.

Governança de Dados

Governança

Conjunto de decisões e responsabilidades explícitas e implícitas de uma instituição para com seus clientes, parceiros e a sociedade.

Como as decisões tomadas por uma organização e suas consequências se relacionam com seus objetivos e as partes envolvidas?

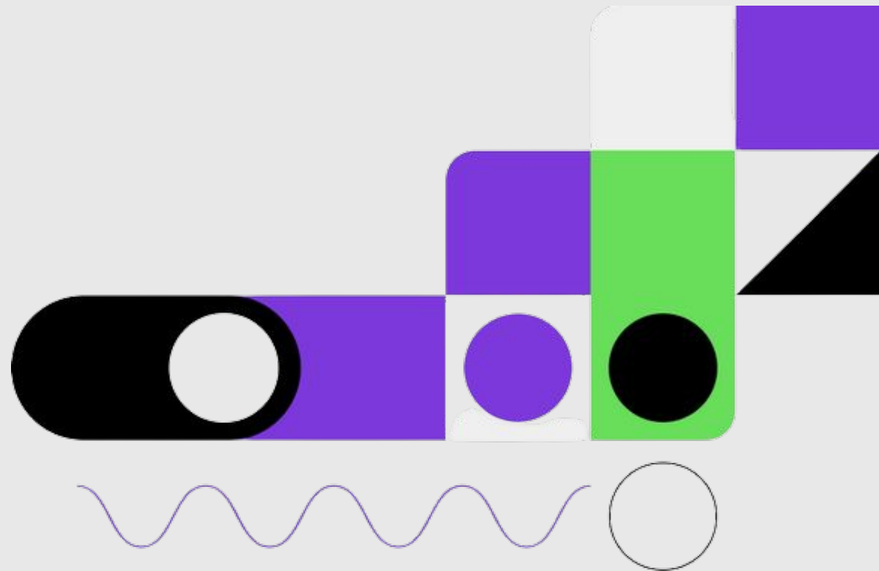
Exemplo:

A empresa deixa de utilizar embalagens plásticas em excesso, pois seus clientes e parceiros também reprovam esta conduta.

Governança de Dados

Engloba processos, políticas, e métricas que garantem o uso das informações com eficiência e integridade, facilitando o alcance das metas corporativas, uma vez que as empresas podem ter mais segurança de que estão protegidas contra uma gestão ruim de dados.

Facilita a tomada de decisões certas ou assunção de riscos estratégicos. Mas para tanto, necessita de profissionais especializados.



Time de governança de dados

Proprietários de dados

Direcionam as necessidades por dados e a qualidade dos dados da corporação.

Devem saber exatamente quem em sua organização deve ter acesso aos dados, e fornecer a eles as ferramentas de que precisam para gerenciar e auditar o acesso.

Organizadores de dados

Conferem se políticas e padrões estão sendo colocadas em prática e propõem melhorias.

Realizam a gestão de estruturas de dados, definição de modelos e padrões lógicos de dados e desenvolvem estratégias de arquitetura de banco de dados.

Operadores de dados

Crie e mantenha os dados de acordo com as políticas e padrões da empresa.

Desempenham uma organização e técnica, garantindo atualizações e manutenção dos dados.

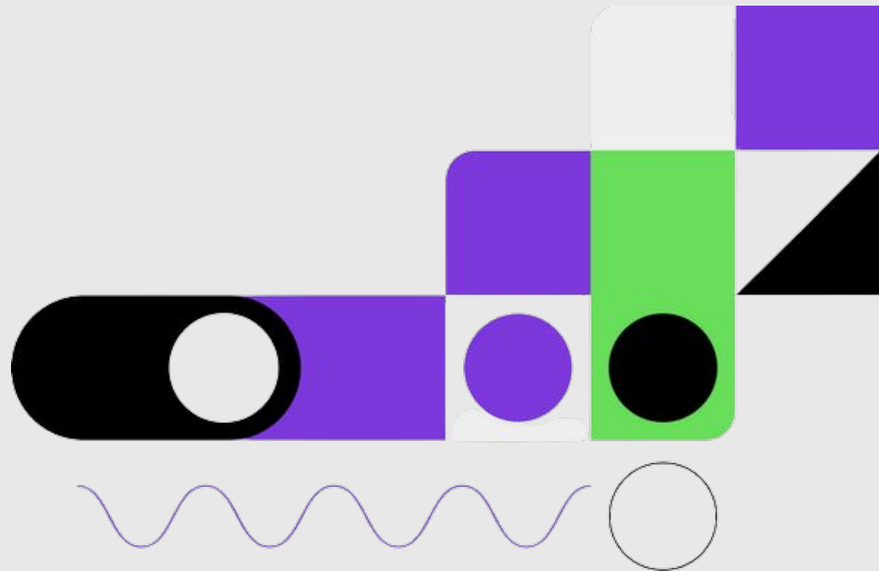
Comitê de Dados

Dão a última palavra sobre as políticas e normas e se responsabilizam pela resolução de problemas escalonados.

Estabelecem quem, o quê, quando, onde e por quê da governança de dados.

Pode criar subcomitês, para tratar de assuntos mais singulares.

É recomendável que a equipe de governança de dados possua cada um desses perfis, de forma a potencializar a expertise do setor e garantir ainda mais segurança à empresa.



Boas práticas de segurança na web

Proteção na esfera corporativa

1. Gerenciar permissões:

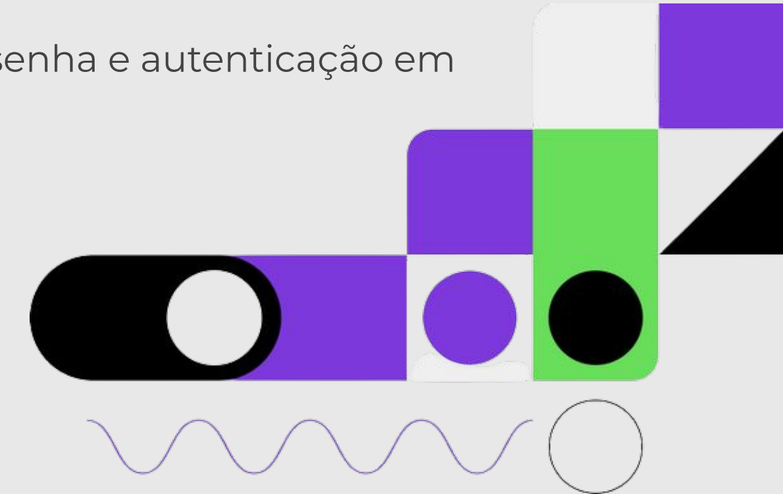
A política de gerenciar o acesso às informações por funções, acompanhada pela administração adequada de permissões e senhas, é uma forma de defesa.

2. Utilizar arquivos criptografados

Pode ser instalado um software ou hardware específico para garantir que os dados ou as informações sejam transferidos com segurança. Esses processos são conhecidos como criptografia em segurança de rede.

3. Evitar o uso de dispositivos externos:

É recomendado o compartilhamento de arquivos por meio da nuvem, em que há uma senha e autenticação em duas etapas, ou seja, respeita o princípio da autenticação.



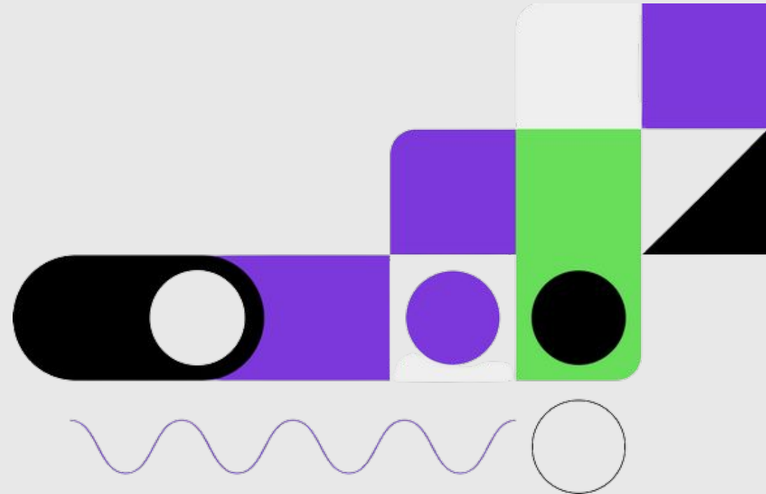
Proteção na esfera corporativa

4. Manter um histórico de incidentes

Para mitigar os incidentes futuros, é necessário conhecer a fundo aqueles que aconteceram no passado. É natural que existam categorias de incidentes mais suscetíveis a ocorrer na empresa, portanto, para evitar os danos que podem ser causados pelos incidentes, deve se perguntar quais deles são mais prováveis de acontecer dentro da sua gestão, observando o histórico.

5. Identificar ameaças por e-mail

É fundamental difundir as boas práticas de segurança e conscientizar os funcionários da empresa a fim de não acessarem ou baixarem arquivos suspeitos, que possam ser de alguma forma ataque cibernético.



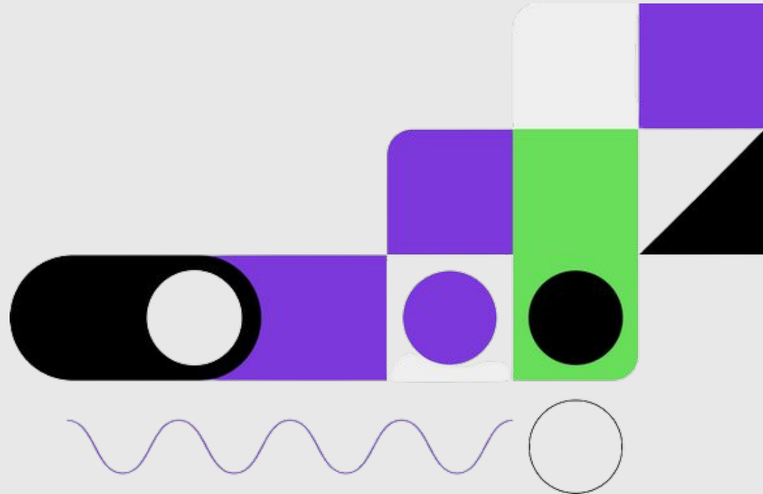
Proteção na esfera individual

1. Gerir senhas para acesso seguro

Criar senhas diferentes para as diversas contas e aplicações, incluir letras, números e caracteres especiais, apostar em ferramentas de gestão de senhas, e investir em autenticação multifator, sempre que possível.

2. Navegar de forma segura pela web

Identificar domínios falsos e ilegais, distinção entre redes seguras e redes inseguras de navegação, conscientização acerca da não divulgação de informações em websites e e-mails suspeitos e identificação de ataques comuns na navegação online, tais como phishing .



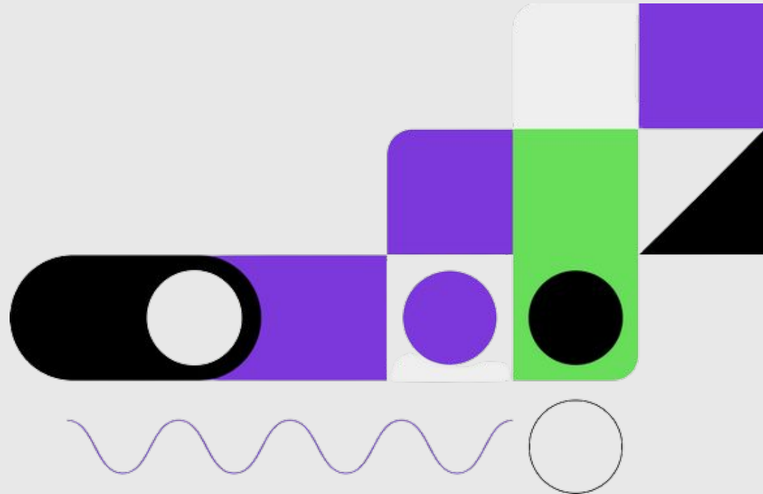
Proteção na esfera individual

3. Usar de forma consciente as redes sociais

Adotar uma conduta consciente para o uso das redes, especialmente ao tratar de redes sociais de companhias renomadas, uma vez que cibercriminosos podem se disfarçar para passar confiabilidade, e ponderar o conteúdo postado nas redes sociais, pois as informações compartilhadas podem ser utilizadas contra outros usuários em ataques de phishing.

4. Usar de forma segura dispositivos removíveis e USB

É indicado evitar o uso de mídias removíveis consideradas inseguras e jamais executar mídias removíveis automaticamente, sem antes escanear possíveis ameaças.



Conclusão

Este material objetivou-se a apresentar uma reflexão sobre a importância da cibersegurança e do correto tratamento de dados.

Espero que você tenha conseguido visualizar o impacto tanto no âmbito corporativo, quanto individual, e as diversas oportunidades que existem para atuar nessa área.

Nos vemos em breve!

Abraços da professora Déborah :)

Ah, uma listinha de conteúdos que te ajudarão ainda mais:

- **Relatório:** Privacidade e Proteção de Dados, de Danilo Doneda
- **Livro:** Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques, de Vinny Troia
- **Série:** Mr. Robot (2015)-

Referência Bibliográfica

ROTHROCK, Ray A.. **Digital Resilience: Is Your Company Ready for the Next Cyber Threat?**. Nova Iorque: HarperCollins Leadership, 2018.

DONDE, Danilo. **Da Privacidade À Proteção De Dados** São Paulo: Revista dos Tribunais, 2019.

GOODMAN, Marc **Future Crimes:** Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso São Paulo: HSM, 2019.

NETSCOUT. Netscout **Threat Intelligence Report**, 2021. Disponível em: https://www.netscout.com/threatreport/