GAT InfoSec

**E-BOOK**

# GERENCIAMENTO DA SUPERFÍCIE DE ATAQUE

OUTUBRO DE 2022

## INVENTÁRIO EXPOSTO E RISCO DE TERCEIROS

IDENTIFICAÇÃO E GESTÃO DE ATIVOS,
RISCOS E VULNERABILIDADES CIBERNÉTICAS

# GERENCIAMENTO DA SUPERFÍCIE DE ATAQUE

INVENTÁRIO EXPOSTO
E RISCO DE TERCEIROS

IDENTIFICAÇÃO E GESTÃO DE ATIVOS,
RISCOS E VULNERABILIDADES CIBERNÉTICAS

GAT InfoSec

OUTUBRO DE 2022

# Índice

# INTRODUÇÃO

A transformação digital trouxe grandes ganhos de produtividade, acelerou tecnologias e gerou um aumento da competitividade em diversos mercados. Essas mudanças introduziram, também, novos desafios, modelos de negócio e formas de relacionamento. Com eles, uma grande dependência de tecnologia se estabeleceu em todas as camadas, aumentando, proporcionalmente, a superfície de ataque e o risco de incidentes cibernéticos que podem trazer prejuízos à operação.

Atualmente, os cuidados com a proteção de dados expostos à Internet pública, especialmente aqueles utilizados durante a operação de negócios, são prioridade máxima, fazendo com que os mais variados setores voltem a atenção para a segurança cibernética. Diretores e executivos de empresas de todos os tamanhos estão, cada vez mais, conscientes dos impactos de um incidente cibernético, e de que é possível evitá-los ao adotar uma postura preventiva na área de Segurança da Informação.

À medida em que leis e regulações, como a LGPD e as normas ISO, impõem exigências por controles e mudança de postura em relação à Segurança da Informação, fica clara importância do envolvimentos de todos nestes processos, a fim de sanar as causas das vulnerabilidades exploradas. Do outro lado, as organizações que buscaram apoio em tecnologia, conformidade e conscientização como formas de atender a rígidos padrões de operação em um mercado cada vez mais exigente, conseguiram, ao mesmo tempo, reduzir o risco de incidentes, evitar ataques e prejuízo.

Os alvos de ataques podem ser ativos de informação pertencentes a qualquer empresa ou pessoa, em qualquer ambiente. Esses ativos fazem parte de uma enorme cadeia com empresas que podem sofrer perdas, diretas e indiretas, tais como a parada de um ambiente produtivo ou de operações críticas, violação de dados sensíveis, efeitos sobre a reputação da marca, multas e prejuízos na relação com o mercado.

Esse cenário mostra quanto é necessário adotar uma postura preventiva e o monitoramento constante para estar sempre à frente das ameaças. É possível reduzir esses riscos e, para isto, vamos mostrar os primeiros passos dessa jornada, que tem como objetivo ajudar a obter a visão dos ativos e percepção dos riscos, evitando ataques antes que eles aconteçam.

Aproveite a leitura!

**Gustavo Valdivia - Head of Marketing**

1

# SEGURANÇA CIBERNÉTICA

CAPÍTULO UM

## SEGURANÇA CIBERNÉTICA

# Superfície de ataque em constante crescimento

É preciso reduzir o nível de risco, prevenindo os possíveis ataques a softwares, computadores e redes.

Gestão de riscos e vulnerabilidades de TI é um conjunto de processos e estratégias de defesa contra ameaças existentes, que tem como objetivo final garantir a segurança de dados. Com o avanço das inovações tecnológicas e da conectividade global, os desafios na área aumentaram, pois o número de vulnerabilidades em sistemas acompanhou o crescimento da superfície de ataque, formada pelo conjunto dos dispositivos cibernéticos expostos à Internet pública.

Hoje, mais do que nunca, nossos softwares, redes e dispositivos estão superexpostos, com inúmeros riscos envolvidos e consequências negativas, que vão desde vazamentos de dados e multas até a interrupção permanente das atividades de uma organização. Já nos habituamos a ver notícias de grandes empresas que sofreram incidentes com grandes consequências, mas nunca saberemos qual será a próxima vítima de algum ataque cibernético.

Nesse cenário, não basta corrigir brechas pontuais ou apenas remediar um problema específico: é preciso reduzir o nível geral de risco, prevenindo os possíveis ataques a softwares, computadores e redes, evitando incidentes que possam ocasionar vazamentos de dados, acessos não autorizados ou outras consequências negativas que podem trazer grandes prejuízos para as organizações.

## Segurança da Informação

Prevenção e redução da probabilidade de acesso e uso não autorizados ou inapropriados de dados, além de definir ações destinadas a reduzir os impactos adversos de tais incidentes.

Não há como falar sobre segurança cibernética sem abordar o tema Segurança da Informação, base para toda a sua gestão e pilar de seus processos. Muitas vezes abreviada para S.I. ou *InfoSec* (abreviação para *Information Security*), trata-se de práticas que têm como principal objetivo proteger um conjunto de informações mitigando os riscos, no sentido de evitar acessos indevidos a fim de preservar o valor que possuem para um indivíduo ou uma organização.

Parte indispensável da gestão de risco, a Segurança da Informação envolve a prevenção e redução da probabilidade de acesso e uso não autorizados ou inapropriados de dados, além de definir ações destinadas a reduzir os impactos adversos de tais incidentes. As informações protegidas podem ter qualquer forma (eletrônica ou física), seja ela tangível (documentos em papel) ou intangível (propriedade intelectual).

Seu foco é a proteção equilibrada da confidencialidade, integridade e disponibilidade dos dados, normalmente operando dentro de um modelo conhecido como a "Tríade CIA" (*Confidentiality, Integrity and Availability*), muito conhecido e utilizado na área de Segurança da Informação para o desenvolvimento de políticas de segurança focadas na identificação de problemas e definição de soluções.


(Figura 1 - Tríade CIA)

O sistema estabelecido deve ser seguido por todos que se relacionam, direta ou indiretamente, com a infraestrutura de TI da organização.

Normalmente, isso é alcançado por meio de um processo estruturado de gerenciamento de riscos que envolve identificar as informações e ativos (além de ameaças, vulnerabilidades e impactos relacionados), decidir como tratar os riscos, implementar controles de segurança e monitorar as atividades, fazendo os ajustes necessários para resolver problemas e aproveitar oportunidades de melhoria.

A fim de definir modelos de operação, muitos acadêmicos e profissionais colaboram para oferecer orientações, políticas e padrões sobre senhas, softwares, antivírus, firewall, criptografia, responsabilidade legal, conscientização e treinamento. Essa padronização é impulsionada pela ampla variedade de leis e regulamentos que afetam como os dados são acessados, processados, armazenados, transferidos e destruídos. A questão é que, mesmo com a implementação de quaisquer normas e orientações dentro de uma organização, seu efeito pode ser limitado caso uma cultura de segurança com melhoria contínua não seja adotada.

## Sistema de Gestão de Segurança da Informação

Atualmente, o melhor caminho para proteger uma organização é implementar uma gestão de riscos e vulnerabilidades eficaz, com controles, processos e ferramentas adequados. Mas antes de qualquer ação, é necessário fomentar uma cultura de segurança dentro da organização, introduzindo conceitos fundamentais de Segurança da Informação e cibersegurança ao treinar e conscientizar a equipe.

O Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de normas que define uma abordagem organizacional para que os dados e informações de uma organização estejam protegidos. Ele define os instrumentos utilizados para estabelecer, implementar, monitorar e analisar controles e padrões de Segurança da Informação, utilizando diversas tecnologias, estratégias, políticas e planos.

O SGSI usa como base os controles da família de normas ISO 27000 para estabelecer os processos e procedimentos que irão prover segurança no uso dos ativos tecnológicos de uma organização, devendo ser seguido por todos que se relacionam, direta ou indiretamente, com a infraestrutura de TI da organização.

Desde os funcionários até os fornecedores e parceiros, todos devem estar incluídos em um processo contínuo, que implica na implementação, manutenção e constante aprimoramento de uma série de mecanismos que permitem o gerenciamento eficiente e seguro das informações, evitando, desta forma, riscos próprios e de terceiros.

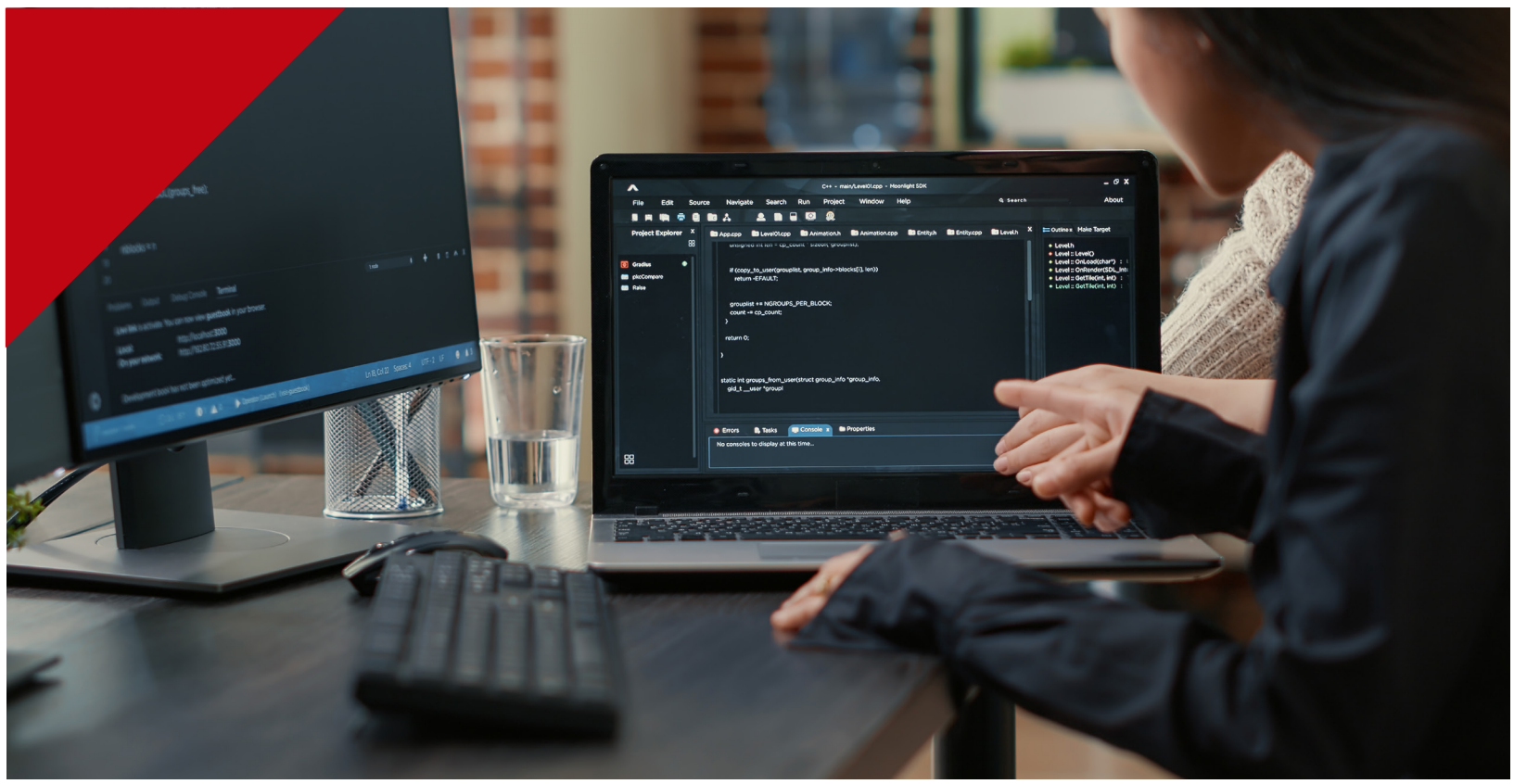
## Segurança Cibernética

Os atacantes estão sempre inovando, as tecnologias mudando e a presença digital das organizações e das pessoas crescendo.

Também conhecida como cibersegurança, consiste na prática de proteger pessoas, sistemas, redes e ativos de ataques cibernéticos que visam obter acesso a hardware e dados, alterar ou destruir informações sensíveis para obter ganho próprio, realizar extorsão financeira e, em casos extremos, afetar ou causar a paralisação da operação dos alvos.

Implementar uma política de segurança cibernética é mais desafiador a cada dia, pois os criminosos estão sempre inovando, as tecnologias mudando e a pegada digital de organizações e indivíduos crescendo, aumentando a superfície de ataque. Para garantir a segurança das operações nesse cenário, é papel da área de Segurança da Informação definir processos e procedimentos voltados para a cibersegurança, implementando controles e monitorando as atividades continuamente para proteger ativos tais como:

- Banco de dados;
- Infraestrutura de rede e ativos conectados;
- Servidores e estações de trabalho;
- Máquinas virtuais, aplicações, e sistemas;
- Identidades e credenciais de acesso dos usuários;
- Dispositivos móveis;
- Dispositivos IoT (Internet das Coisas);
- Infraestrutura em nuvem.



## Quando e Como se Proteger

Não basta mais ser otimista e achar que não é um alvo. Hoje é essencial ser realista e adotar um Programa de Segurança da Informação com ações preventivas.

Muitas pessoas instalam sistemas de monitoramento ou alarmes contra invasão logo após um assalto na vizinhança ou na própria casa. Da mesma forma, a maioria só passa a cuidar da saúde de forma preventiva quando descobre um problema. Aparentemente, a situação em termos de segurança cibernética segue a mesma lógica, com a maioria das organizações tomando atitudes somente após algum incidente. Infelizmente, parece que estavam apenas esperando que os dados sensíveis de sua operação, de seus clientes ou de seus fornecedores fossem expostos para, então, adotar medidas de proteção.

O pensamento reativo é algo comum, porém inaceitável. Ao mensurar, objetivamente, a quantidade de riscos, as chances de um incidente com consequências negativas e o prejuízo associado, fica claro que, frente aos investimentos necessários em termos de cibersegurança, a opção sensata é prevenir, ao invés de remediar. Muitos ataques são executados durante meses sem serem detectados, não pela complexidade, mas pela ausência de processos de gestão de vulnerabilidade, desenvolvimento seguro e monitoramento contínuo.

Não é incomum que um incidente cibernético seja seguido de uma parada de produção, às vezes grande demais para permitir que o dano seja revertido. Além da perda causada pela paralisação das operações e do abalo na reputação da marca, muitas vezes irreversível, os gastos com a gestão da crise e processos judiciais podem comprometer a continuidade do negócio após o incidente.

Não basta mais ser otimista e achar que não é um alvo. É essencial adotar uma postura realista e iniciar um Programa de Segurança da Informação com ações preventivas. Isso significa não tratar do tema por meio de iniciativas isoladas, mas estabelecer um programa contínuo e bem planejado, de acordo com as características da operação.

## Benefícios e Vantagens

### Evitar vazamento de dados

Vazamentos de dados ocorrem frequentemente, como mostram as constantes notícias sobre grandes empresas sendo afetadas. Este tipo de ataque pode ocorrer de diversas maneiras, sendo as mais comuns aquelas executadas por meio de vulnerabilidades encontradas em códigos de aplicações, configurações de serviços, sistemas operacionais, APIs desprotegidas e ambientes de nuvem mal configurados.

Muitos ataques são executados durante meses sem serem detectados, não pela complexidade, mas pela ausência de processos.

Esses incidentes são altamente prejudiciais à reputação e à operação, com o tamanho do prejuízo variando de acordo com o tipo e do volume de dados vazados. Um bom motivo para evitar vazamentos de dados é escapar de multas e sanções regulatórias como, por exemplo, da LGPD. A Lei Brasileira de Proteção de Dados prevê multas de 2% do faturamento bruto anual, limitada a R$ 50 milhões por infração, conforme o nível de conformidade com os requisitos de proteção de dados exigidos pela lei.

## Proteger a Operação Contra *Ransomware*

Um dos tipos de ataque que mais cresce em número de ocorrências é o *ransomware*, ou sequestro de dados. O *ransomware* é um tipo de ataque que encripta os dados da vítima e torna inacessíveis as informações contidas nos dispositivos afetados, sejam eles telefones celulares, tablets, máquinas físicas (notebooks, desktops e servidores) ou máquinas virtuais (ambientes em nuvem).

A execução deste ataque se dá, principalmente, por meio de sistemas operacionais desatualizados e downloads de arquivos contaminados, muitas vezes anexados a mensagens de e-mail. Para recuperar o acesso aos dados, as vítimas têm poucas opções entre pagar o resgate (geralmente em *bitcoins*) ou quando, possível, solicitar ajuda a uma empresa ou especialista em cibersegurança.

Ataques de *ransomware* podem ser ainda mais devastadores que vazamentos de dados, chegando a causar a paralisação das operações e trazer grandes prejuízos para as organizações afetadas. Neste cenário, o Brasil ocupa uma posição de destaque entre os países mais atingidos, com um número crescente de ataques.

## Mitigar Ataques de Engenharia Social

Conjunto de técnicas que visa a manipulação de pessoas para obter acesso a locais físicos e informações confidenciais, a engenharia social é um sistema que depende da interação humana e da manipulação psicológica para induzir as vítimas a cometerem erros de segurança ou fornecerem informações sensíveis.

Um dos ataques de engenharia social mais comuns é o *phishing*, ataque em que o usuário é, geralmente, induzido a clicar em um link contido em uma mensagem, fazer o download de um anexo infectado (facilitando a instalação de software malicioso no sistema da vítima), ou fornecer dados pessoais. No caso dos links, estes podem direcionar a vítima para uma página que simula sites confiáveis ou promoções, solicitando o preenchimento de dados restritos, tais como nomes de usuário, senhas e dados bancários.

# 2

# SUPERFÍCIE DE ATAQUE

CAPÍTULO DOIS

## SUPERFÍCIE DE ATAQUE

# Pegada digital sujeita a ataques cibernéticos

Vulnerabilidades presentes em ativos e ambientes de uma organização fazem deles possíveis pontos fracos na infraestrutura.

Em ambientes de negócios modernos, diversas organizações estão enfrentando uma pressão crescente para adotar soluções digitais a fim de manterem-se competitivas. Embora tais soluções tenham benefícios incontestáveis, sua multiplicação traz níveis elevados de exposição a riscos cibernéticos que, se não forem resolvidos, podem causar brechas de segurança rotineiramente exploradas por cibercriminosos.

Neste contexto, surge o que é chamado de superfície de ataque. Ela consiste na soma de todos os dispositivos, sistemas e aplicações em uma operação que estejam expostos à Internet pública, tais como hardware de rede, tablets, computadores, máquinas virtuais, periféricos e dispositivos móveis. Isso significa que as vulnerabilidades presentes em ativos e ambientes de uma organização tornam-se possíveis pontos fracos na infraestrutura e, consequentemente, vetores de ataque.

Conhecer a superfície de ataque significa, realizar um levantamento de ativos, com o objetivo de mapear o inventário digital de uma organização que contem os ativos cibernéticos expostos à Internet pública e que fazem parte da operação. Deve-se, inclusive, levar em consideração os ativos cibernéticos de terceiros com quem são realizadas trocas de dados, sejam eles fornecedores, parceiros ou clientes, se estes também estiverem expostos à Internet pública, pois são portas de entrada em redes corporativas costumeiramente exploradas por criminosos.

Identificar quais ativos têm riscos e vulnerabilidades exploráveis associados a eles permite realizar a gestão dos riscos de forma preventiva, utilizando estes dados para evitar incidentes causados pela exploração de falhas existentes nos ativos expostos.

Os atacantes estão sempre inovando, as tecnologias mudando e a presença digital das organizações e das pessoas crescendo.

Para ajudar na proteção contra incidentes em que a superfície de ataque é explorada por meio de diferentes técnicas de intrusão, muitas organizações estão adotando programas de gerenciamento da superfície de ataque com o objetivo de, continuamente, avaliar seu inventário exposto em busca de potenciais riscos. Com um programa de gerenciamento de superfície de ataque implementado, é possível avaliar os riscos de forma proativa e reduzir a superfície de ataque em tempo real, limitando o impacto das ameaças cibernéticas.

## Análise da Superfície de Ataque

A análise da superfície de ataque é uma etapa essencial que permite o seu gerenciamento. Trata-se de um conjunto de atividades que têm como foco mapear os ativos digitais expostos que contêm ou enviam dados entre si, ajudando organizações de todos os portes a tratar as vulnerabilidades associadas e reduzir os riscos. Seus objetivos são:

- Realizar o levantamento do inventário digital exposto;
- Identificar, detalhar, e classificar os ativos encontrados;
- Avaliar o estado de cada ativo e seu risco para a operação;
- Apontar correções para as vulnerabilidades identificadas.

As organizações que empregam tais métodos melhoram sua postura geral de segurança cibernética, além de tornarem-se aptas a reduzir sua superfície de ataque ativamente, enquanto demonstram maior transparência, fortalecendo o relacionamento com clientes e parceiros.

Utilizando somente dados públicos, é possível mapear a superfície de ataque externa de cada fornecedor no *supply-chain*.

Deve-se levar em consideração que, após realizar a análise, esta servirá de subsídio para a criação de um programa de gerenciamento da superfície de ataque. O uso de automação e a integração de ferramentas e processos, desde o início, traz a inteligência de riscos com contexto de negócio, pois isso ajudará a melhorar a eficiência do programa.

## Identificação e Priorização de Ativos

A primeira etapa na análise da superfície de ataque consiste em identificar e priorizar os ativos voltados para a Internet pública. Depois de obter um registro dos ativos, é preciso classificá-los com base em sua criticidade e no nível de risco que representam para a operação, comparando aos níveis de risco de ativos individuais e considerando a tolerância ao risco organizacional.

## *Rating* de Segurança

Com avaliações de segurança baseadas na superfície de ataque, é possível classificar e atribuir uma nota em relação aos diferentes níveis de risco de segurança cibernética encontrados. Por exemplo, utilizando somente dados públicos, é possível mapear a superfície de ataque de cada fornecedor no *supply-chain*, permitindo o monitoramento contínuo de ecossistemas compostos por terceiros.

As classificações de segurança também ajudam as organizações a gerenciar o risco de terceiros, fornecendo percepção de risco de forma clara e centralizada. Isso permite que identifiquem, priorizem e resolvam problemas de maneira rápida e fácil em seu portfólio de fornecedores, evitando que sua operação seja prejudicada por falhas externas. Afinal, ao trabalhar com terceiros, você corre os mesmos riscos que eles, o que significa que a visão eficaz de riscos de terceiros é essencial para a segurança da operação de organizações com diversos fornecedores.

## Avaliações Contínuas de Segurança

Avaliações contínuas de segurança permitem que as organizações monitorem o nível de integridade cibernética em seus ambientes e nos ambientes de terceiros, o que é vital para o sucesso dos programas de gerenciamento da superfície de ataque. Com uma visão contínua dos ambientes e dos ativos de rede, é possível otimizar a identificação de vulnerabilidades, reduzindo, gradualmente, a superfície de ataque.

Um monitoramento eficaz de ambientes expostos à Internet pública, tanto internos quanto externos, permite uma visão mais clara dos riscos a que uma operação está sujeita. Com tais dados, é possível tomar decisões estratégicas e reduzir o nível de exposição ao priorizar o aumento do nível de maturidade em Segurança da Informação.

# 3

# GERENCIAMENTO DA SUPERFÍCIE DE ATAQUE

CAPÍTULO TRÊS

## GERENCIAMENTO DA SUPERFÍCIE DE ATAQUE

# Visão e controle dos riscos em ativos expostos

Garantir que as ações de Segurança da Informação cubram todos os ativos de TI expostos.

O gerenciamento da superfície de ataque olha para a segurança do ponto de vista de um invasor, ajudando a proteger os ativos cibernéticos e os recursos de uma organização. Seu objetivo principal é garantir que as ações de Segurança da Informação envolvam todos os ativos de TI expostos à Internet pública, tanto próprios quanto presentes nas infraestruturas de fornecedores, parceiros e terceiros.

Os processos envolvidos no gerenciamento da superfície de ataque vão muito além da descoberta e monitoramento do inventário cibernético exposto, utilizando os dados obtidos no levantamento, classificação e monitoramento dos ativos expostos contidos na infraestrutura de TI de uma organização. Tais dados são essenciais para a segurança dos ativos e colaboram com a garantia da continuidade da operação.

# O Que é Gerenciamento da Superfície de Ataque

Com o nível de digitalização dos negócios aumentando a cada dia, o gerenciamento da superfície de ataque é uma prática necessária para qualquer organização que tenha ativos expostos à Internet pública.

Mais do que nunca, com o nível de digitalização dos negócios aumentando a cada dia, o gerenciamento da superfície de ataque é uma prática necessária para qualquer organização que tenha ativos expostos à Internet pública. Aborda diversos processos em Segurança da Informação, mas sempre a partir da perspectiva de um agente malicioso externo, fornecendo a visibilidade dos riscos associados aos ativos expostos com vulnerabilidades exploráveis.

Com a virtualização dos ambientes de trabalho, acelerada pela pandemia de COVID-19, o número de ativos expostos, possíveis alvos que as equipes de segurança devem proteger, cresceu muito rápido. Além disso, criminosos cibernéticos estão, frequentemente, automatizando suas ferramentas de varredura e descoberta, com o objetivo de sondar e analisar as superfícies de ataque externas, uma avaliação que muitas equipes de segurança nunca executam totalmente.

Diversos termos são utilizados para definir o gerenciamento da superfície de ataque, sendo os mais comuns:

- ASM (*Attack Surface Management*)
- CAASM (*Cyber Asset Attack Surface Management*)
- EASM (*External Attack Surface Management*)

Estes termos podem parecer semelhantes e, a grosso modo, se referem à descoberta e gerenciamento de ativos vulneráveis, abordando práticas e processos ligeiramente diferentes. Como também estamos levando em consideração ambientes externos e de terceiros, vamos falar da superfície de ataque de maneira ampla, dentro do conceito mais abrangente de ASM (*Attack Surface Management*). Nesse cenário, o gerenciamento da superfície de ataque inclui riscos e vulnerabilidades associados a dados, *hardware* e *software* tais como:

- Ativos inseguros;
- Ativos desconhecidos;
- Ativos de terceiros expostos publicamente;
- Ativos e recursos em ambientes *cloud*;
- Credenciais de usuários;
- Vazamentos de dados;
- Bases públicas.

A superfície de ataque é um assunto extenso e serve como subsídio para longas discussões, mesmo para organizações menores. Garantir sua segurança é primordial mas, com sua extensão mudando constantemente (especialmente com ativos em ambientes *cloud*), o desafio é continuamente crescente.

## Por Que é Necessário

O gerenciamento da superfície de ataque coloca as equipes de Segurança da Informação em uma posição melhor para priorizar as áreas da superfície de ataque que mais precisam de atenção.

O baixo nível de maturidade em Segurança da Informação, a falta de orçamento dedicado para a área e a dificuldade nas contratações continuam sendo os principais desafios na maioria das organizações, representando fontes de riscos e vulnerabilidades, normalmente desconhecidos ou, até, negligenciados pelas equipes de Tecnologia da Informação e Segurança da Informação. Tal postura pode transformar a superfície de ataque de tais organizações na maior ameaça à continuidade de suas operações.

A natureza mutável e expansiva de muitos ambientes de trabalho permite que inúmeras vulnerabilidades passem despercebidas, fazendo com que ativos vulneráveis permaneçam não testados. Com o regime de home-office, por exemplo, muitas pessoas passaram a levar para suas residências os equipamentos da empresa. Inúmeros dispositivos foram conectados a redes domésticas que não tinham os mesmos protocolos de segurança que o ambiente de trabalho, visto que não são semelhantes às redes presentes nas infraestruturas corporativas.

Para combater estes desafios, é importante garantir uma visibilidade completa e um monitoramento contínuo, com o objetivo de gerenciar e mitigar os riscos e vulnerabilidades identificados antes que criminosos os encontrem e utilizem como vetores de ataque. Com as ferramentas corretas e o treinamento adequado, o gerenciamento da superfície de ataque é algo que pode ajudar as organizações a fazer exatamente isso.

Ao realinhar o pensamento de segurança, de um defensor para um invasor, o gerenciamento da superfície de ataque coloca as equipes de Segurança da Informação em uma posição melhor para priorizar as áreas da superfície de ataque que mais precisam de atenção, a partir do momento em que passam a olhar para a própria infraestrutura com os olhos de um agente malicioso externo.

## Como Ajuda a Impedir Invasões

O baixo nível de maturidade em Segurança da Informação, a falta de orçamento dedicado para as áreas e a dificuldade nas contratações continuam sendo os principais desafios.

As equipes de Segurança da Informação foram obrigadas a agir mais rápido que os invasores quando vulnerabilidades e possíveis explorações passaram a ser divulgadas regularmente, algo que só é possível quando a superfície de ataque é mapeada continuamente. Com o gerenciamento da superfície de ataque, é possível identificar, rapidamente, ativos expostos que contenham vulnerabilidades associadas, entre outros fatores de risco e vetores de ataque em potencial, a fim de mitigar riscos e diminuir as chances de quaisquer incidentes que possam surgir como consequência.

As estratégias de segurança clássicas sempre se concentraram na identificação, classificação e proteção de ativos cibernéticos de uma operação, mas o gerenciamento da superfície de ataque, quando aplicado corretamente, automatiza parte dessas atividades e cobre ativos fora do escopo dos controles tradicionais de mapeamento, tais como antivírus, VPN, *firewall* e proteção de *endpoint*.

As ferramentas utilizadas nesses processos fornecem uma análise mais abrangente da superfície de ataque e permitem o gerenciamento de vulnerabilidades a fim de evitar falhas em controles de segurança e reduzir o risco de incidentes. Com isso, é possível identificar ativos com vulnerabilidades exploráveis, falhas de configuração e outros possíveis vetores de ataque, incluindo:

- Software desatualizado ou não corrigido;
- Problemas de criptografia;
- Configurações incorretas de hardware e software;
- Vazamentos de credenciais;
- Riscos à imagem da marca.

## Estratégia e Resposta

Ferramentas fornecem uma análise de superfície de ataque e permitem o gerenciamento de vulnerabilidades a fim de evitar falhas em controles de segurança.

Muitas organizações têm investido em tecnologia e treinamento como formas de proteção contra ataques voltados à sua superfície de ataque. Com inúmeros processos envolvidos, o uso de automação passou a ser algo obrigatório para garantir o bom desempenho e a otimização dos investimentos em Segurança da Informação.

Com o tempo, soluções integradas focadas exclusivamente no gerenciamento da superfície de ataque passaram a ser ofertadas no formato de plataformas SaaS (*Software as a Service*). São sistemas gerenciados baseados em ambientes *cloud*, tais como o **GAT Security Score**, que descobre, automaticamente, os ativos expostos que os invasores podem enxergar, além de realizar avaliações em relação a feeds de inteligência de ameaças, de código aberto e proprietários, gerando ratings (classificações de segurança em forma de nota) para a postura geral de segurança cibernética de uma organização e dos terceiros com quem se relaciona, com base na superfície de ataque.

Tais resultados são obtidos por meio do levantamento de ativos visíveis, expostos à Internet pública (endereços IP, domínios, subdomínios e aplicações *web* e contas de e-mail) e de eventuais falhas de configuração em hardware e software, além de fatores de risco como presença em listas de envio de SPAM, credenciais encontradas em vazamentos de dados e outros. Os resultados são úteis para diversas partes não técnicas interessadas, dentro e fora da organização, tais como o conselho consultivo, executivos, gerência, parceiros e clientes.

Atualmente, os recursos de monitoramento contínuo produzem informações sobre o perfil de risco cibernético das organizações avaliadas, e os riscos individuais dentro das infraestruturas, buscando até mesmo na *deep web* por credenciais expostas em violações de dados de terceiros que podem ser utilizadas em tentativas de ataque.

## Automação como Solução

À medida em que mais organizações passam pela transformação digital, o gerenciamento da superfície de ataque se tornará uma necessidade cada vez mais evidente.

Frequentemente, o custo das soluções e a dificuldade nas contratações são relatados como as principais barreiras que atrapalham na gestão de cibersegurança e Segurança da Informação. Nesse cenário, a automação e a priorização inteligente podem ser a saída para as dificuldades com a falta de mão de obra e o orçamento restrito. Provavelmente, são as maiores aliadas para aprimorar a gestão da superfície de ataque em qualquer operação, otimizando custos e reduzindo o risco de incidentes, tais como: ciberataques, *ransomware*, indisponibilidade, vazamentos de dados e não-conformidades, entre outros.

Ferramentas, como o **GAT Security Score**, combinam classificações de ameaças com valor e impacto, para avaliar a eficácia dos controles de segurança existentes e ajudar na priorização, oferecendo recursos adicionais que permitem às equipes monitorar as alterações na superfície de ataque e observar as melhorias ao corrigir riscos.

A chave para gerenciar, com eficácia, a superfície de ataque é garantir a visibilidade dos ambientes expostos, próprios e de terceiros. As organizações que utilizam plataformas integradas com alto nível de automação, como as soluções da **GAT InfoSec**, garantem uma visão de fora para dentro da infraestrutura de TI de forma contínua, priorizando a correção de vulnerabilidades e diminuindo a janela de exposição.

À medida que mais organizações passam pela transformação digital, o gerenciamento da superfície de ataque se tornará uma necessidade cada vez mais evidente. É essencial garantir o acesso às ferramentas e recursos de que as equipes de Segurança da Informação precisam para desenvolver e manter programas abrangentes de gerenciamento da superfície de ataque pois, apenas com os insights obtidos com base nas análises das ameaças, é possível otimizar o gerenciamento de riscos, reduzindo a superfície de ataque e as chances de um incidente.

# 4

# INVENTÁRIO E FATORES DE RISCO

CAPÍTULO QUATRO

## INVENTÁRIO DIGITAL

# Identificação de riscos em ativos cibernéticos

O risco é o resultado obtido quando uma potencial ameaça passa a explorar vulnerabilidades presentes em um ou mais ativos de informação, podendo trazer impactos nas atividades e nos negócios da organização.

Com a transformação digital, a quantidade de vulnerabilidades que podem ser exploradas por diversas ameaças e, assim, comprometer informações é cada vez maior. Nesse cenário, mensurar e gerenciar riscos é uma prática fundamental para garantir que as informações relevantes, estratégicas e confidenciais estejam protegidas, assegurando a imagem, reputação e valor de mercado da organização.

## Riscos em Ativos Cibernéticos

A norma ISO 31000 define risco como sendo o "efeito da incerteza no alcance dos objetivos da organização". Em termos de Segurança da Informação, essas incertezas estão relacionadas a vulnerabilidades presentes em ativos (informação digital ou física, hardware, software, pessoas ou ambientes físicos). O risco é o resultado obtido quando uma potencial ameaça passa a explorar vulnerabilidades presentes em um ou mais ativos, podendo trazer impactos nas atividades da organização.

Para identificar a quais riscos uma operação está exposta, é preciso construir o bom hábito de executar, rotineiramente, uma análise de riscos de Segurança da Informação. Com isso é possível identificar ameaças e avaliar os possíveis impactos aos ativos e à operação de uma organização, facilitando a adoção dos melhores controles e processos para protegê-los.

A partir dessa perspectiva, fica claro o quanto um programa de segurança cibernética é essencial para a redução de riscos operacionais e como a gestão da superfície de ataque pode contribuir para isso.

# Gestão de Ativos no Inventário Digital

O processo de gestão de riscos de segurança da informação é cíclico, devendo ser revisado, e atualizado dentro de períodos regularmente definidos.

Um ativo é todo elemento que agrega valor ao negócio, podendo ser uma informação digital ou física, hardware, software, pessoa ou ambiente físico, cuja a quebra da confidencialidade, integridade ou disponibilidade trará prejuízo. E justamente por ser fundamental ao negócio, deve ser adequadamente protegido. Para isso, é preciso:

## Identificar

Antes de tudo, é preciso mapear quais ativos são essenciais para a operação e estratégicos para o negócio. Quais destes ativos de informação, se impactados, podem chegar a parar a operação? Este mapeamento é de suma importância, pois garante que controles adequados sejam aplicados nos recursos relevantes à operação.

## Classificar

Após a etapa de levantamento e identificação dos ativos, é preciso consolidar uma base de dados, definir a relação entre eles e com a operação da organização, sua criticidade em relação à continuidade das operações e o nível de vulnerabilidade encontrado.

## Entender o Impacto

É necessário entender o nível de impacto no caso do comprometimento de um ativo. Se a informação contida estiver indisponível por um período de tempo, qual é o grau de risco? Com estas respostas é possível entender o grau de risco em caso de indisponibilidade, perda, roubo ou alteração das informações. Quais destes ativos de informação, se impactados, podem causar efeitos negativos à marca ou à operação?

## Testar

Os testes vão demonstrar se existe risco real das informações serem perdidas ou não, e os possíveis impactos causados, na eventualidade de um incidente real. A partir disso, é possível levantar as opções para proteger as informações críticas.

## Monitorar Continuamente

O processo de gestão de riscos é cíclico, devendo ser revisado, e atualizado dentro de períodos regulares. É necessário saber, o quanto antes, se alguma brecha surgiu ou se ocorreu algum tipo de alteração ou problema, por meio de um ciclo de análise das informações, verificação das vulnerabilidade e busca contínua das soluções.

# Avaliação de Fatores de Risco

Após a identificação do inventário digital da empresa, é essencial realizar uma busca por possíveis problemas de segurança relacionados a cada um dos ativos. Os apontamentos identificados representam fatores de risco que podem estar associados a diversas origens, tais como:

## Risco de Imagem da Marca

Problemas que podem acarretar na perda de credibilidade da marca. Por exemplo, domínio encontrado em alguma lista de envio de SPAM, má configuração de servidores, entre outros.

## Vazamento de Dados

Vazamentos de credenciais de acesso pertencentes a contas corporativas, que podem representar riscos à operação.

## Problemas de Websites

Questões relacionadas a certificados digitais, má configuração de serviços, tecnologias web inseguras e vulnerabilidades conhecidas.

## Problemas de Rede

Questões relacionadas a endereços IPs, tais como portas abertas, serviços expostos e tecnologias inseguras sendo utilizadas.

# 5

# RISCO DE TERCEIROS

CAPÍTULO CINCO

## RISCO DE TERCEIROS

# Maioria das violações causada por terceiros

O gerenciamento de riscos de terceiros consiste em uma série de processos que têm como objetivo a análise e a minimização dos riscos associados à terceirização, independente da posição ou função dos terceirizados.

Inúmeras organizações estão buscando otimizar suas operações para focar nas competências essenciais, terceirizando tarefas rotineiras para obter vantagens competitivas. Nesses casos, quando tais terceiros não conseguem manter suas políticas de Segurança da Informação operando, minimamente, dentro dos níveis esperados, falhas na segurança podem trazer impactos devastadores e duradouros para todos os integrantes da cadeia.

O fato é que, nos últimos dois anos, a maioria das violações relacionadas à Segurança da Informação foram causadas por terceiros, e a tendência é que este ritmo não diminua. Nesse cenário, destaca-se a importância do gerenciamento de riscos de terceiros, identificado pela sigla TPRM (*Third-Party Risk Management*). Trata-se de um tipo de gerenciamento de risco com foco na identificação e redução de riscos relacionados a integrantes externos de uma cadeia de suprimentos, sejam estes clientes, fornecedores, parceiros ou prestadores de serviços temporários.

O gerenciamento de riscos de terceiros consiste em uma série de processos que têm como objetivo a análise e a minimização dos riscos associados à terceirização, independente da posição ou função dos terceirizados. Uma vez que os relacionamentos com terceiros são vitais para as operações de uma infinidade de negócios, é um componente essencial a todos os programas de Segurança da Informação.

Embora as definições exatas possam variar, o gerenciamento de risco de terceiros é uma prática que costuma ser utilizada de forma abrangente, isoladamente ou junto a outros conceitos comuns ao setor, dando origem a diversas nomenclaturas relacionadas, tais como:

O relacionamento com terceiros, direta ou indiretamente, afeta o nível de segurança de uma organização, a partir do momento em que os dois lados trocam dados entre si, aumentando a complexidade da relação e as exigências em relação à Segurança da Informação.

- TPRM (*Third-Party Risk Management*);
- SRM (*Supplier Risk Management*);
- VRM (*Vendor Relationship Management*);
- SCRM (*Supply Chain Risk Management*).

No entanto, TPRM (*Third-Party Risk Management*), cuja tradução direta é "gerenciamento de risco de terceiros" é, frequentemente, considerada como a disciplina mais abrangente, que engloba diversos tipos de terceiros e riscos associados. Foi projetada para dar às organizações melhor compreensão sobre os terceiros com quem se relacionam, como se relacionam, quais proteções estes terceiros têm em vigor e, na ausência destas, quais riscos eles representam à operação.

O escopo e os requisitos de um programa de gerenciamento de risco de terceiros dependem muito da organização, podendo variar muito de acordo com o setor, orientação regulatória e outros fatores. Ainda assim, muitas práticas recomendadas são universais e aplicáveis a todos os tipos de organizações.

## Quais Riscos um Terceiro Oferece?

A terceirização é um componente necessário na administração de um negócio moderno. Mais que economizar o dinheiro de uma empresa, é uma maneira simples de aproveitar a experiência de terceiros que uma organização pode não ter internamente. A desvantagem é que, se não houver um programa adequado de gerenciamento de risco de terceiros, depender destes terceiros pode deixar uma empresa vulnerável.

O gerenciamento de riscos em terceiros é extremamente importante porque o relacionamento com terceiros, direta ou indiretamente, afeta o nível de segurança de uma organização, a partir do momento em que os dois lados trocam dados entre si, aumentando a complexidade da relação e as exigências em termos de Segurança da Informação. Um dos aspectos mais relevantes é a gestão de riscos decorrente de ativos cibernéticos de terceiros, que possam impactar a operação de uma organização. No cenário atual, o número de vulnerabilidades e o tamanho das superfícies de ataque crescem proporcionalmente ao número de dispositivos e parceiros de negócios, criando situações onde o potencial para danos se estende muito além do prejuízo financeiro.

Existem muitos riscos em potencial que as organizações enfrentam ao trabalhar com terceiros, que podem incluir riscos financeiros, ambientais, de reputação e de Segurança da Informação, entre outros. Em geral, estes riscos existem porque os fornecedores têm acesso a propriedade intelectual, dados confidenciais e credenciais de acesso.

Dependendo da criticidade do fornecedor, uma organização pode optar por um fornecedor alternativo, o que é uma prática comum nos setores de serviços.

Muitos riscos cibernéticos presentes na operação de terceiros costumam causar problemas que vão desde afetar a reputação até graves prejuízos financeiros. Alguns são mais comuns que outros, mas os principais exemplos incluem, mas não se limitam a:

## Risco à Privacidade

Risco de exposição de dados ou perda destes, como resultado de um ataque cibernético, violação de Segurança da Informação (física ou digital) ou outros incidentes de segurança.

Geralmente é adereçado e mitigado por meio de um processo de *due-diligence* antes da integração de um fornecedor, ou por meio do monitoramento contínuo durante todo o ciclo de vida do fornecedor.

## Risco Operacional

Risco de um terceiro causar interrupção nas operações, normalmente gerenciado por acordos de nível de serviço (SLAs) contratualmente vinculados, bem como de planos de continuidade de negócios e resposta a incidentes. Dependendo da criticidade do fornecedor, uma organização pode optar por um fornecedor alternativo, o que é uma prática comum nos setores de serviços financeiros e saúde, por exemplo.

## Risco Legal, Regulatório e de Conformidade

Risco de um terceiro afetar o nível de conformidade de uma organização frente à legislação, regulamentação ou acordos locais. Muito relevante no caso de serviços financeiros, da área de saúde, organizações governamentais e seus parceiros de negócios.

## Risco Reputacional

Risco de opinião pública negativa devido a um terceiro. Clientes insatisfeitos, interações inadequadas e recomendações ruins são apenas a ponta do iceberg. Os eventos mais prejudiciais são as violações de dados de terceiros resultantes de uma falha na segurança de dados.

## Risco Financeiro

Risco que um terceiro tem de causar um impacto negativo no sucesso financeiro de uma organização, seja por mau gerenciamento ou causando prejuízos.

# 6

# CONCLUSÃO

CAPÍTULO SEIS

**CONCLUSÃO**

# Automação como palavra de ordem

Dependendo da criticidade do fornecedor, uma organização pode optar por um fornecedor alternativo, o que é uma prática comum nos setores de serviços.

Neste cenário desafiador, as equipes de segurança atuais dedicam atenção constante para evitar incidentes e garantir que tenham as habilidades e os recursos para prevenir e reduzir os riscos. Assim, o gerenciamento da superfície de ataque está se tornando popular entre CIOs, CTOs, CISOs e equipes de segurança, pois permite que monitorem e reduzam sua superfície de ataque.

## Eficiência, Desempenho e Automação

Nas organizações que investem em Segurança da Informação, há uma tendência maior em relação ao uso de tecnologia por parte das equipes de alto desempenho, que utilizam melhores práticas, com as quais outras organizações podem aprender. Algumas das características e abordagens de tais equipes de alta performance são:

- Automação;
- Orquestração;
- Visibilidade;
- Investimento em novas tecnologias;
- Planos de contingência e resposta a incidentes;
- Testes periódicos recorrentes; e
- *Machine Learning*.

De acordo com a pesquisa *Cyber Resilient Organization Report* publicada pela IBM, a maioria entre tais equipes relataram um uso significativo de automação. Entre as equipes do grupo pesquisado:

- 70% utilizaram para melhorar a eficiência operacional;
- 64% utilizaram para dar suporte às equipes de segurança de TI.

## Plataformas Integradas Como Solução

Resultados podem ser utilizados para a análise do nível de exposição cibernética, análise de risco em terceiros, benchmark e levantamentos para utilização em processos de Due Diligence, Cyber Underwriting e Seguro Cyber, entre outros.

O **GAT Security Score** coleta dados disponíveis publicamente na Internet (de forma não intrusiva) para dar uma perspectiva externa da postura de Segurança da Informação nas operações. Os dados são divididos em 4 diferentes fatores de risco que, juntos, formam a base para o cálculo do seu *score* (Pontuação de Segurança).

Nosso algoritmo atribui, automaticamente, uma nota em formato de uma nota de Segurança Cibernética com base na análise da superfície de exposição dos ativos da empresa à Internet pública e, como consequência, a ataques cibernéticos. O sistema entrega uma avaliação do nível de segurança em forma de *rating*, contendo apontamentos de riscos da empresa, de seus fornecedores e terceiros.

Os resultados podem ser utilizados para a análise do nível de exposição cibernética, análise de risco em terceiros, *benchmark* e levantamentos para utilização em processos de *Due Diligence*, *Cyber Underwriting* e Seguro *Cyber*, entre outros.

### Inventário Digital

Por meio do domínio do endereço de e-mail informado no momento do cadastro (por exemplo, pessoa@dominio.com), nosso algoritmo inicia uma busca por diversos tipos de ativos vinculados a esse domínio e seus subdomínios, atualmente expostos à Internet pública.

Em geral, as ferramentas de Security Rating limitam suas buscas somente aos IPs relacionados ao domínio. O **GAT Security Score** busca:

- IPs;
- Subdomínios;
- Aplicações *Web*;
- E-Mails.

## Fatores de Risco

Após a identificação do inventário digital do domínio, o sistema realiza uma busca por possíveis problemas de segurança relacionados a cada um desses ativos. Os apontamentos identificados são divididos em quatro tipos diferentes de fatores de risco:

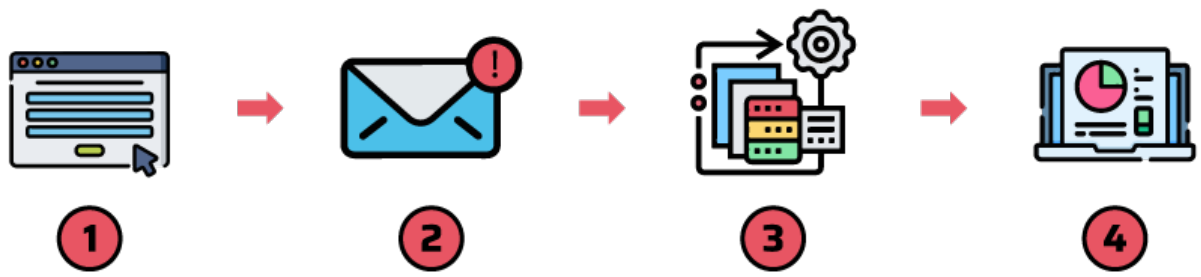
- Risco de Imagem à Marca
- Vazamento de Dados
- Problemas de *Websites*
- Problemas de Rede

## Score de Risco

Com base nos resultados encontrados, o sistema utiliza um algoritmo que realiza o cálculo do score de segurança do domínio. Nosso algoritmo se adapta ao longo do tempo, de acordo com os avanços na área da Segurança da Informação, a fim de se adaptar e refletir as mudanças.

## Como Começar Gratuitamente

Para ter acesso gratuito ao score de risco cibernético do seu domínio e aprimorar o nível de segurança cibernética de sua operação, basta utilizar o QR Code abaixo, ou acessar a página de cadastro do GAT Security Score (**https://www.securityscore.com.br/cadastro**).




1. Preencha o formulário com seus dados;
2. Confira seu e-mail e confirme o cadastro no sistema;
3. Aguarde enquanto nossos algoritmos calculam o score;
4. Verifique os apontamentos identificados no domínio.

A **GAT InfoSec** está reinventando a forma sobre como estabelecer a governança de riscos cibernéticos. Acreditamos que Privacidade e Segurança Digital são bens tangíveis e fundamentais, por isso promovemos esta cultura de forma acessível para toda sociedade, com inovação e compartilhamento do conhecimento.

Otimizamos os processos relacionados à gestão de Segurança da Informação, governança e conformidade, para evitar riscos e ameaças por meio de uma visão integrada do ecossistema de negócios digitais, de parceiros e colaboradores a tecnologias e processos.

Por meio do uso intensivo de automação, integrações com as principais ferramentas do mercado, regras de automação e workflows, nossas soluções já ajudaram a melhorar a postura cibernética e a eficiência da equipe de segurança em diversas organizações.

Entre em contato e saiba o que podemos fazer por sua operação.

**DISCLAIMER**

Os indicadores, conceitos e exemplos apresentados neste material são divulgados com a finalidade de prover informações ao mercado em geral, não representando recomendações para e/ou solicitações de compra e venda de qualquer produto ou serviço. Eles são baseados unicamente em conceitos amplamente difundidos, informações públicas e dados empíricos, provenientes de estudos e da operação da própria empresa, bem como aqueles advindos de seus profissionais do mercado de Segurança da Informação, ao longo de mais de 20 anos de atuação prestando serviços para os mais diversos setores.

Quaisquer decisões estratégicas relacionadas a Segurança da Informação devem ser tomadas com base nas necessidades particulares de cada empresa, após extensa discussão entre os profissionais da área dentro de sua própria equipe e com o parecer de um responsável técnico.