MOVIMENTO
INOVAÇÃO
DIGITAL

GUIA DE CIBERSEGURANÇA

Boas práticas para o ambiente de negócios

Expediente

Presidência
Vitor Magnani

Vice-presidência
Sophia Martini Vial

Lideranças de Comitês e Conselho
Guilherme Kato
Nycholas Szucko
Samanta Oliveira

Direção Geral
Marcos Carvalho

Direção de Negócios
Adriana Próspero

Marketing e Estratégia
Ana Carolina Valente

Projetos e Inteligência
Ivan Ventura

Adm. e Operações
Beatriz Petroni

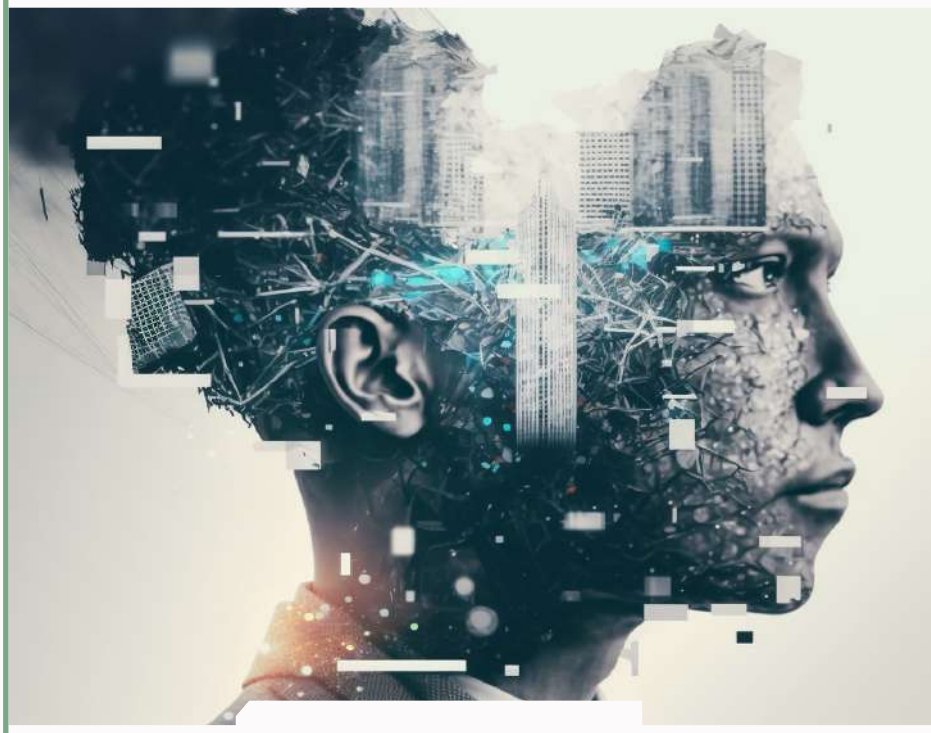
Edição:
George Leal Jamil

Produção:
André Almeida
Alexandre Finelli

Design
Rafael Lisboa

MOVIMENTO INOVAÇÃO DIGITAL

Somos o MID. Uma associação, sem fins lucrativos, de empresas inovadoras que estão promovendo a transformação digital no Brasil e no mundo, conectando o online e offline (fidigital) ou criando novos ambientes, como o metaverso. Nosso objetivo é usar a tecnologia para diminuir desigualdades, promover a competitividade e garantir soluções mais sustentáveis.



REALIZAÇÃO:

MOVIMENTO INOVAÇÃO DIGITAL

APOIO:

FIRST TECH

Microsoft

Peck+ Advogados
Direito para Inovação Digital

Tozzini Freire. ADVOGADOS

CONTEÚDO E EDIÇÃO:

INOVATIVOS

Editorial

POR UMA CULTURA CIBERNÉTICA CORPORATIVA

A segurança cibernética se transformou em um dos grandes e emergentes desafios dentro da nova economia digital.

Somente no último ano, o Brasil foi alvo de mais de 103 bilhões de tentativas de ataques cibernéticos. A conta inclui empresas, que perdem mais de uma vez: em dinheiro e na reputação, principalmente com o seu consumidor.

O Movimento Inovação Digital (MID), entidade com mais de 150 empresas do ecossistema digital, há tempos exibe preocupação com o tema e, até por esse motivo, promove discussões frequentes a respeito. O resultado dessa agenda setorial resultou neste Guia de Cibersegurança.

Ele foi produzido a partir de um Grupo de Trabalho formado por renomados especialistas em tecnologia da informação e juristas. E não paramos por aí. Nós também ouvimos dezenas de lideranças e especialistas do mercado que ajudaram em diferentes momentos para produzir esse documento.

No Guia,o objetivo é mostrar, na prática, o caminho que as empresas devem percorrer para proteger os seus dados mais críticos, as operações, os ativos digitais, assim como o que será necessário fazer, perante a Lei, quando for vítima de um ataque cibernético.

Tudo é explicado de maneira didática, em passo a passo, com todos os contextos necessários, justamente para que todos entendam a importância de uma cultura de segurança cibernética na empresa. E esperamos que esse documento seja um ponto de inflexão para um novo paradigma nacional e ganho de maturidade da cultura ciber.

Aproveite!

GRUPO DE TRABALHO

Vitor Magnani
Presidente
MID

Guilherme Kato
Líder Comitê
de TI - **MID**
CTO - **dr. consulta**

Samanta Oliveira
Líder Comitê
de Privacy - **MID**
DPO - **Mercado Livre**

Nycholas Szucko
Conselheiro de
Cibersegurança e
Tecnologia
MID

Marcos Carvalho
Diretor Geral
MID

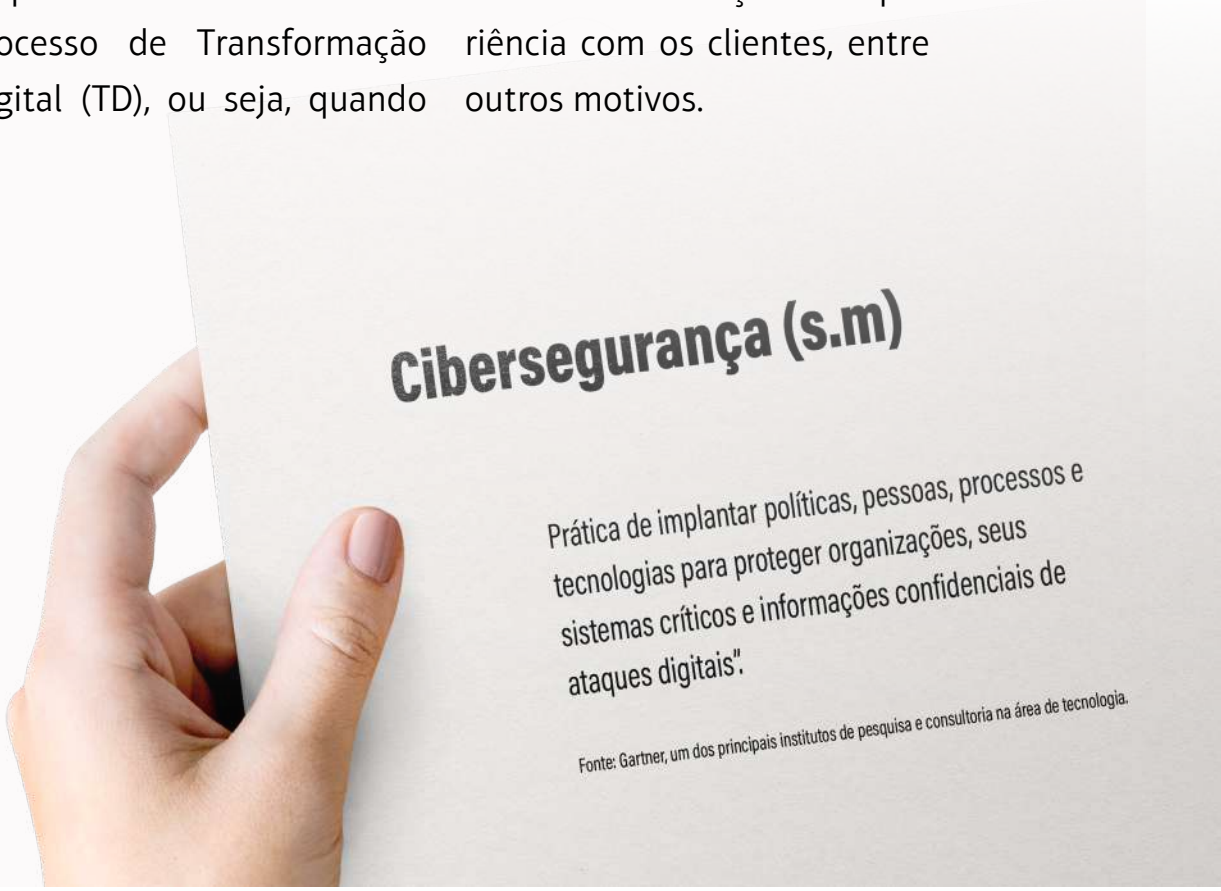
Índice

O universo da cibersegurança

O que é cibersegurança?

Um guia sobre cibersegurança não poderia começar de outra maneira senão pela pergunta mais importante: afinal, do que estamos falando?

A cibersegurança se tornou um pilar fundamental para as empresas desde o início do processo de Transformação Digital (TD), ou seja, quando as corporações passaram a incorporar processos eletrônicos em todos os seus setores progressivamente a fim de integrar departamentos, facilitar a comunicação e o compartilhamento de dados entre as equipes, além de agilizar e tornar mais eficiente e assertiva a tomada de decisões, melhorar a interação e a experiência com os clientes, entre outros motivos.



Também conhecida por segurança digital

"Também conhecida como segurança digital, ela é aplicável a todos os contextos de negócio para proteger dados, informações, dispositivos, transações financeiras, sistema operacional, segurança de rede, entre outros. Quando bem-sucedida e implementada, a cibersegurança também é eficaz para remediar e prover respostas efetivas a incidentes."

Samanta Oliveira, DPO do Mercado Livre.

O papel da cibersegurança

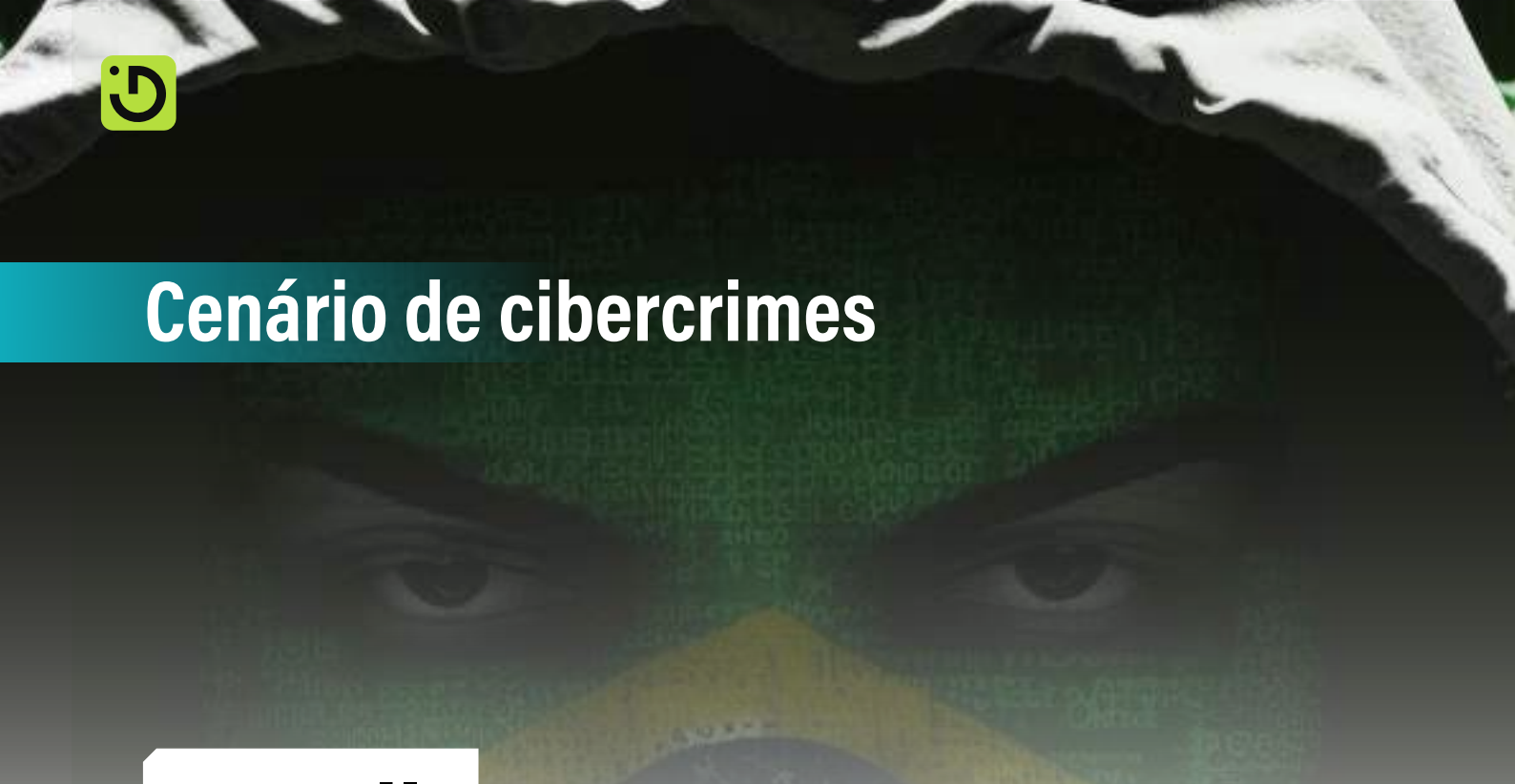
"A cibersegurança exerce um papel crítico nas organizações atualmente porque a maior parte delas entrega o seu valor através do uso de tecnologia. Dito isso, o risco do negócio frente a ciberataques é proporcional à sua digitalização e os atacantes utilizam, cada vez mais, desse fator como fonte de renda."

Guilherme Kato, CTO do dr. consulta.

O custo da violação de dados

- **6,54 mi** de reais é o custo médio de uma violação de dados - é o valor mais alto
- **10%** foi o aumento do custo da violação em 2 anos
- **60%** das empresas globais aumentaram os custos de bens e serviços por causa do vazamento de dados
- **83%** das organizações afirma que sofreram mais de uma violação de dados
- **747 mil** de reais é a média de gasto anual das empresas com cibersegurança
- **1,8 mi** de reais é a média de gasto com cibersegurança no setor financeiro

Fonte Cost of Data Breach report e Tempest



Cenário de cibercrimes

Brasil

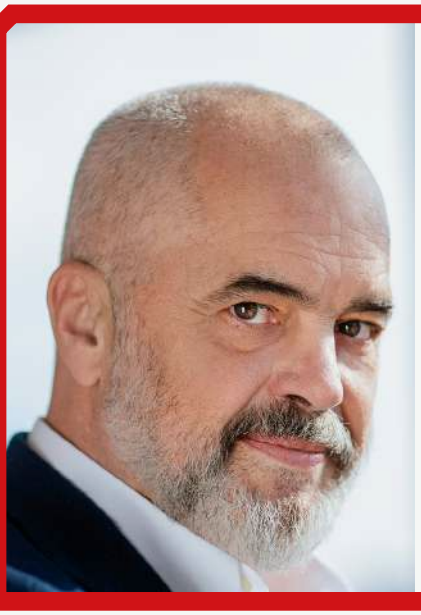
103 bilhões é o número de tentativas de ataques cibernético a empresas brasileiras em 2022

16% é o crescimento de ataques na comparação com 2021

2ª posição. É a posição do Brasil entre os países mais atacados na América Latina. México é o líder com 187 bilhões de tentativas

5ª posição. É a colocação do Brasil no ranking global

1ª posição. É a colocação do País entre as nações mais visadas para golpes a partir de links falsos no WhatsApp



> “Se o cibercrime fosse um estado seria a terceira maior economia do mundo, depois dos Estados Unidos e China, com um PIB de US$ 10 trilhões.”

Edi Rama, primeiro-ministro da Albânia. O estudo desenvolvido pela Cybersecurity Ventures aponta que o cibercrime poderá faturar US$ 10 trilhões em 2025.

Mundo

360 bilhões é o número de tentativas de ataques somente na América Latina e Caribe em 2022

86% é o percentual de empresas em todo o mundo que sofreram algum tipo de ataque em 2022

10% é o crescimento de empresas de todo mundo atacadas entre 2021 e 2022

Fonte: Fortinet, Roland Berger, Kaspersky e Índice Global de Proteção de Dados (GDPI), da Dell Technologies

Por que o cibercrime cresce no mundo?

"Trata-se de um ecossistema audacioso, que onera bem seus participantes, e atrai cada vez mais voluntários para a execução dessas atividades ilícitas. Para compreender a magnitude dessa crescente indústria, é importante destacar a ramificação desses ataques entre os diversos setores e suas consequências que desfavorecem a economia, a reputação e a operação de setores críticos das indústrias e governos."

Vanessa Pádua, diretora de cybersecurity América Latina e Caribe na Microsoft

O propósito do ransomware

"No caso do ransomware, por exemplo, o propósito é a ciber extorsão, ou seja, o sequestro de dados de uma empresa e a exigência de um valor em dinheiro (resgate) para evitar o vazamento de informações críticas."

Pedro Nuno, CISO do BMG

Como os cibercriminosos são convocados?

Uma das formas de contratar criminosos é, pasmem, por meio de anúncios na internet. A Kaspersky, empresa de segurança cibernética, monitorou fóruns da dark web e identificou mais de 200 mil anúncios ao longo de 30 meses. Em suma, os classificados do cibercrimes tinham os seguintes pré-requisitos: profissionais com habilidades em desenvolvimento de software, manutenção de infraestrutura de TI, criação de sites fraudulentos e campanhas de e-mail de phishing. Na pandemia, houve um aumento por esses profissionais.

A maior parte (83%) dos anúncios de empregos eram de grupos que procuravam "trabalhadores" altamente qualificados, incluindo desenvolvedores (61%), especialistas em ataques (16%) e designers de sites fraudulentos (10%). Muitos deles oferecem condições semelhantes aos de um emprego comum em período integral, folga remunerada e até promoção, com salários entre US$ 1,3 mil e US$ 4 mil. No entanto, também foram encontradas oportunidades para profissionais mais qualificados, com salários mensais entre US$ 15 mil e US$ 20 mil.

Crime lucrativo

"A indústria de crimes cibernéticos representa uma das mais importantes e lucrativas áreas de tecnologia dos dias atuais. O nosso último Relatório de Defesa 2022 da Microsoft aponta como as organizações criminosas evoluem e profissionalizam o desenvolvimento e distribuição de atividades maliciosas, como ransomware, phishing kits, roubo de credencias de acesso e a comercialização de ataques incluindo serviços como Phishing-as-a-Service (PhaaS) e Ransomware-as-a-Service (RaaS).

Liliane Scarpari e Davi Cruz, especialistas em segurança da Microsoft

Impactos do backdoor

"Os impactos, além de operacionais, podem acarretar uma sequência de vazamentos de dados, roubos de identidade, entre outros crimes cibernéticos, podendo causar grandes prejuízos financeiros. Além de riscos com multas e valores para resgate de dados, um ataque cibernético pode redirecionar o seu site oficial, prejudicando as vendas da companhia."

Fabiana Tanaka, CISO da Leroy Merlin

Os ciberataques mais comuns

Ransomware

Ransomware é um software malicioso que bloqueia os computadores de uma empresa por meio da criptografia dos dados. O acesso é devolvido ao dono ou a máquina é desbloqueada após o pagamento de resgate. Geralmente, os cibercriminosos exigem o pagamento por meio de criptomoedas para dificultar o rastreamento da operação e a identificação dos atacantes. Na maioria das vezes, os atacantes exploram as limitações dos controles de segurança e o despreparo das pessoas para infectar os sistemas das organizações.

Phishing

É literalmente pescar os dados da vítima. É um dos ataques mais conhecidos e com elevada incidência. Geralmente, ele consiste em enviar uma mensagem por meios eletrônicos (e-mail, rede social e outros) com mecanismos de engenharia social para enganar a vítima a tomar uma determinada ação, como visitar uma página na Internet infectada e configurada para executar ações maliciosas através de técnicas como Man-in-the-middle (MITM ou método de interceptar uma comunicação sem ser percebido acarretando em fraudes ou ataques cibernéticos). É considerado altamente eficaz e de baixa complexidade de implementação.

BEC (Business E-mail Compromise)

Uma vez que as credenciais (login e senha, por exemplo) de acesso da vítima estejam comprometidas, o cibercriminoso pode usar técnicas como BEC (Business E-mail Compromise). O Comprometimento do e-mail comercial explora a cadeia de confiança entre parceiros de negócios. O conceito é simples: o ataque é direcionado ao parceiro com menor estrutura comercial e potencialmente com recursos limitados de proteção de dados. Uma vez comprometido, o parceiro transmite ao alvo final o código malicioso, que passa despercebido, já que a relação de confiança entre ambos já existe.

Comprometimento da Cadeia de Suprimentos

Um cenário que tem recebido cada vez mais atenção entre especialistas é o comprometimento da cadeia de suprimentos. Nesse tipo de ataque, softwares legítimos são alterados por uma programação maliciosa durante as etapas de desenvolvimento ou de atualização. Feito isso, essas vulnerabilidades são exploradas e podem resultar em consequências desastrosas. Esse tipo de ataque pode ter origem tanto dentro quanto fora de uma empresa. A detecção é mais difícil, pois a sua origem pode ter ocorrido a partir de um usuário legítimo, seja de forma acidental ou não.

Fonte: com informações da Microsoft

Como funciona a estratégia do cibercriminoso

Sou especialista em cibersegurança: Posso agir em grupo ou sou um lobo solitário

“Os cibercriminosos, geralmente, são grupos de pessoas com alto conhecimento de tecnologia e que utilizam todo esse conhecimento para praticar crimes contra organizações, governos e pessoas. Porém, existem muitos ‘lobos solitários’, que atuam sozinhos em descobertas e análises de vulnerabilidades de sistemas para conseguirem explorar e ter algum ganho financeiro.”

Douglas Brancaglion, Head Cyber Security da Memed

Eu engano pessoas com mensagens e textos

De uma maneira geral, cibercriminosos se aproveitam de uma ou mais falhas e oportunidades. Atualmente, eles enganam pessoas com mensagens e textos sobre assuntos do momento (técnica de engenharia social) ou literalmente pescam suas vítimas (phishing).

Utilizo indicadores

“O cibercrime se provou um negócio muito rentável e com uma baixa chance de ser pego, de ir para a cadeia ou sofrer alguma penalidade mais severa. É muito importante entender que o cibercrime é um negócio, possui TCO (Total Cost of Ownership), ROI (Return of Investment), dentre outros indicadores.”

Nycholas Szucko, especialista em cibersegurança e conselheiro do MID

Quanto tempo dura o meu ataque?

“Esses ataques geralmente são de longa duração, pois o cibercriminoso consegue permanecer com esse acesso por muito tempo, inclusive criando novos atalhos caso ocorra a perda do acesso principal.”

Douglas Brancaglion, Head Cyber Security da Memed, destacando que o ataque pode durar, em média, 280 dias

Eu analiso a sua empresa antes de atacar

"Como as empresas são grandes, passaram por processos de fusão e aquisição, tem muitos sistemas legados, silos entre as aplicações ou, às vezes, não investiram nas ferramentas para ter visibilidade do ambiente como um todo. Assim se torna possível achar o atacante, mapear a rede, entender a localização dos dados sensíveis, os usuários com acesso às informações mais críticas, entre outras coisas."

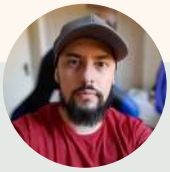
Nycholas Szucko, especialista em cibersegurança e conselheiro do MID

Uso ransomware

"Em 2022, as empresas e organizações sofreram mais ataques de ransomware, porém não pediram resgate de um servidor ou estações criptografadas. No fim, eles queriam que as bases de dados extraídas ou roubadas não fossem divulgadas ou vendidas. Esse tipo de ataque tem-se mostrado mais lucrativo."

Celso Hummel, head comercial e especialista em cybersecurity da First Tech

A principal tática é a engenharia social



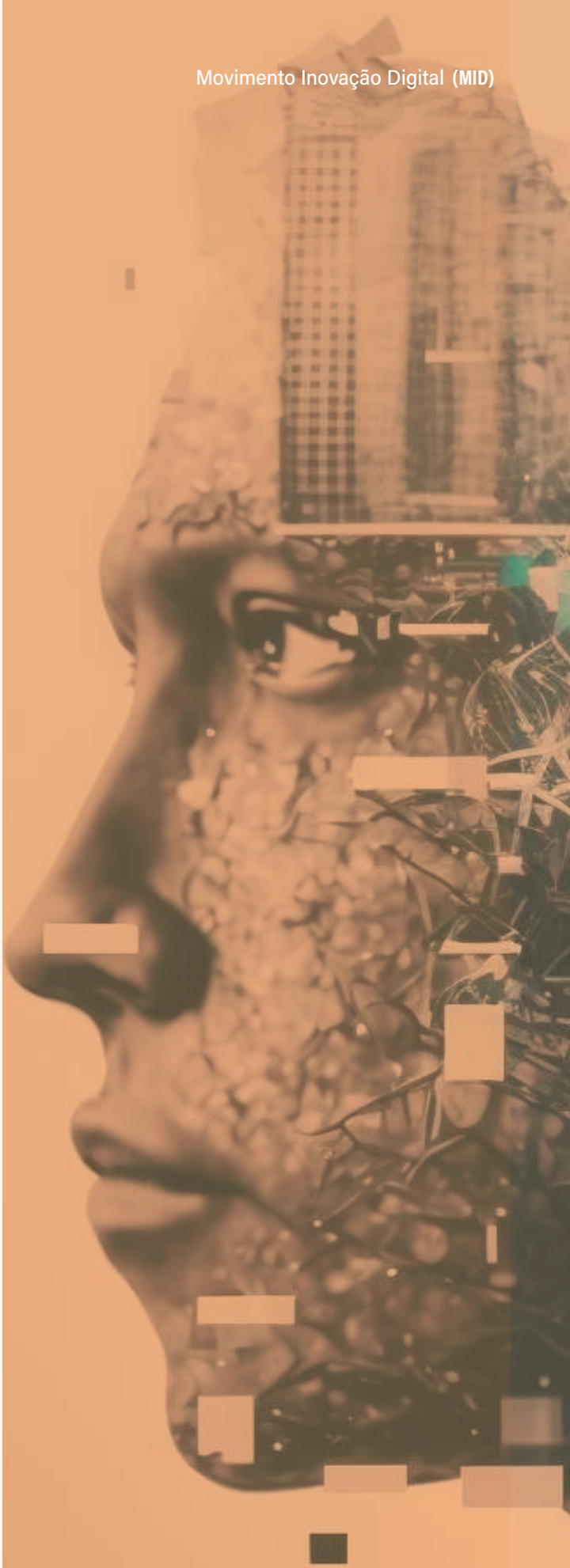
"Existem vários métodos de ataques, porém o mais impactante nos dias de hoje, responsável pela maioria das perdas financeiras, é o chamado de Engenharia Social. Por meio dele, os atacantes simulam outras identidades e fazem os funcionários da empresa ou organização confiar no e-mail, telefonema ou até mesmo em alguém, levando, na maioria das vezes, a acessos privilegiados por meios físicos ou digitais."

Douglas Brancaglion, Head Cyber Security da Memed

Corrupção

"Alguns cibercriminosos podem corromper financeiramente alguns funcionários.
"Conhecido como insider, este é um dos grandes pesadelos dos CISOs, pois coloca o atacante dentro da empresa e já de posse de usuário e senha válidos."

Nycholas Szucko, especialista em cibersegurança e conselheiro do MID



Quem é quem no cibercrime?

Estado-nação

Tem motivações geopolíticas e atacam países inimigos para defender os interesses da sua própria nação. Geralmente, buscam o roubo de informações confidenciais e defendem que a prática de ciberespionagem são atividades legítimas para defender o Estado.

Mercenários

O dinheiro é a principal motivação de um cibercriminoso e os meios para chegar a esse objetivo são inúmeros, seja através da aplicação de golpes via engenharia social até por ataques cibernéticos mais complexos, como o ransomware (sequestro de dados).

Caçadores de fama

Tende a ser praticado por pessoas que desejam provar o seu conhecimento no ambiente digital para um grupo, mostrando que é capaz de derrubar uma operação, tirar um site do ar ou apenas furar a estratégia de segurança de uma organização.

Agentes internos - Insiders

Colaboradores ou parceiros com acesso a informações críticas, cooptado por um grupo mal-intencionado, que fornece credenciais válidas para cibercriminosos adentrar uma organização. Importante lembrar que nem todo agente interno age propositalmente, podendo também comprometer a empresa por descuido ou negligência.

Hacktivistas

Alguns cibercriminosos usam das suas habilidades para atacar empresas que vão contra seus ideais. Geralmente, são motivados por alguma causa, promovem o boicote contra uma companhia e aplica ações que tiram um site do ar ou pichações.

Espiões corporativos

Tem como principal objetivo a obtenção de informações estratégicas de uma organização a fim de ganhar vantagem sobre ela. Envolve atividades de suborno, vigilância constante e chantagem.

Os 5 setores mais visados

Finanças

Os ciberataques relacionados a serviços financeiros aumentaram 419% na América Latina, entre os anos de 2021 e 2022. Os dados são do estudo "Enemy at the Gates – Analyzing Attacks on Financial Services", publicado pela Akamai.

Saúde

As instituições de saúde e suas plataformas tiveram um aumento de 64% dos ataques no Brasil, entre 2020 a 2021, de acordo com estudo realizado pela Check Point Research.

Governo

Levantamento da CloudSek apontou que o número de ataques direcionados ao setor de governo aumentou 95% no segundo semestre de 2022, em comparação com o mesmo período de 2021.

Varejo

Dos 422 líderes de TI do setor de varejo pesquisados no mundo todo, inclusive no Brasil, 77% admitiram que suas organizações foram atingidas por ataques de ransomware em 2021. O aumento foi de 75% em relação a 2020, segundo o relatório da Sophos.

Indústria

Estudo da Capgemini Research Institute revelou que 51% das empresas do setor industrial acreditam que o número de ciberataques às fábricas inteligentes aumentará nos próximos meses.

Ciberataques e o ecossistema digital

Especialistas em cibersegurança garantem que as empresas nativas digitais estão tão ou até mais expostas aos ataques cibernéticos em comparação às companhias tradicionais. Quanto às ameaças mais comuns, eles destacam ataques contra Apps, APIs, portais web e mobile, além de falhas no controle de acesso do uso da cloud e da gestão de comunicação de rede.

Vulnerabilidade

"As nativas digitais não necessariamente são menos vulneráveis. Isso depende do estágio de vida dessas empresas e de qual a prioridade que o board define para esse tema. O fato de geralmente não terem processos de segurança bem definidos e times dedicados, fazem das startups mais vulneráveis a ataques."

Norman Sabino, CTO do Provu

Gestão centralizada

"As empresas tradicionais são menos suscetíveis pois estão menos expostas do ponto de vista da infraestrutura. Elas possuem uma gestão centralizada, o que reduz a superfície de ataque."

Bruno Guerreiro, Security Operations Advisor da Datasec

Ameaças contra Apps e portais Web

"As nativas digitais estão mais suscetíveis às ameaças relativas ao mundo digital, como ataques aos Apps e portais web, assim como ataques sobre vulnerabilidades de desenvolvimento em mobile e web."

Celso Hummel, head comercial e especialista em cybersecurity da First Tech

MOVIMENTO
INOVAÇÃO DIGITAL

Somos o MID. Uma associação, sem fins lucrativos, de empresas inovadoras que estão promovendo a transformação digital no Brasil e no mundo, conectando o online e offline (fidigital) ou criando novos ambientes, como o metaverso. Nosso objetivo é usar a tecnologia para diminuir desigualdades, promover a competitividade e garantir soluções mais sustentáveis.

JORNADA IMERSIVA

Nessa Revolução Digital não basta usarmos as tecnologias disponíveis, precisamos adotar novos métodos de gestão, processos e cultura. Por isso, nos reunimos nas sedes das empresas mais inovadoras para gerar conhecimento entre executivos que realmente conquistam resultados positivos.

REPRESENTAÇÃO

Estamos comprometidos em dialogar e posicionar as pautas do Ecossistema Digital junto ao Poder Público, academia e sociedade civil para avançarmos na transformação digital, competitividade e sustentabilidade do Brasil e do mundo.

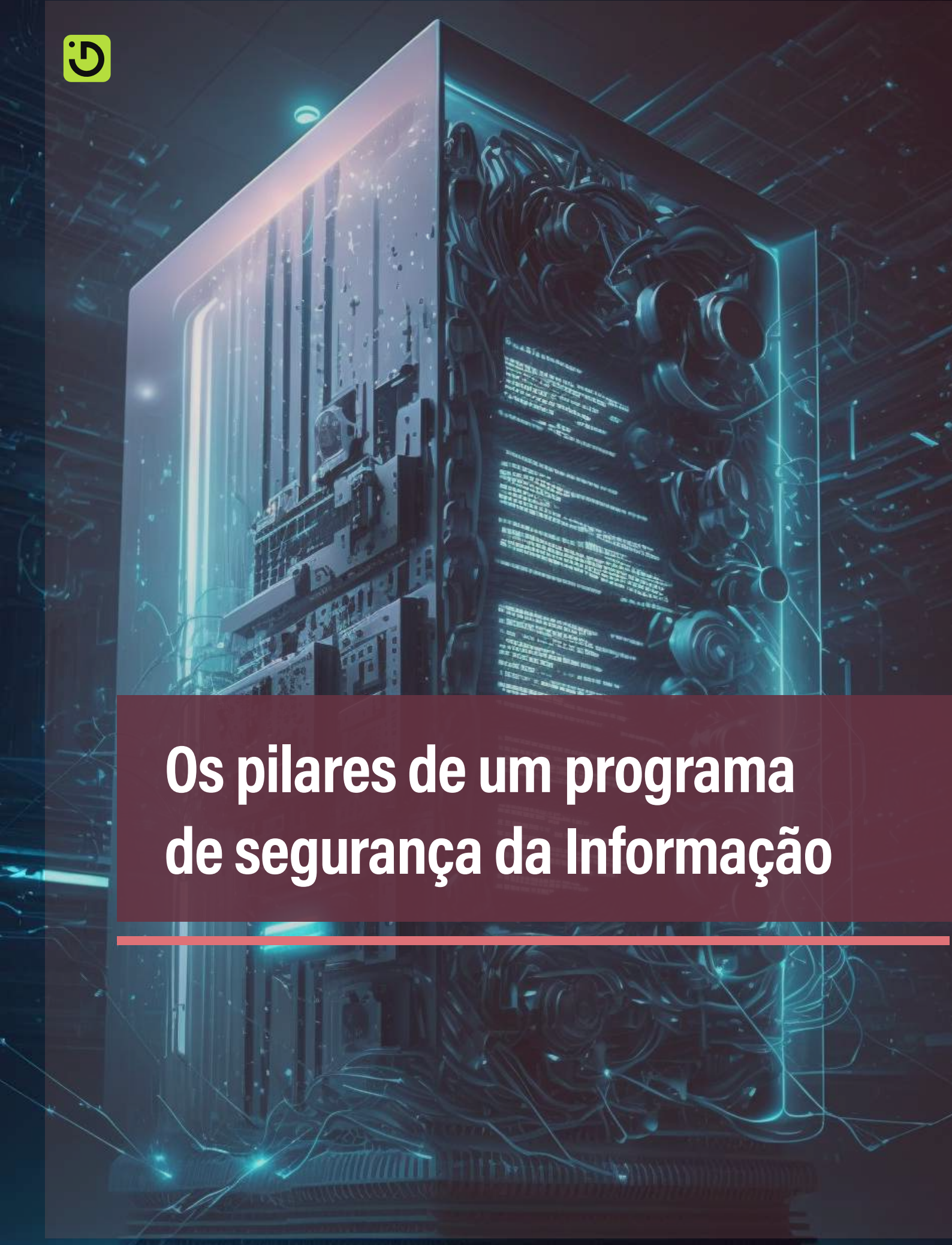
MAIS DE 150 EMPRESAS ASSOCIADAS

Conheça nossos Planos

Entre em contato:

contato@movimentoinova.com.br/

movimentoinova.org.br



Os pilares de um programa de segurança da Informação

Um dos alvos frequentes de ataques cibernéticos contra empresas é o conjunto de dados armazenados na companhia. Até por esse motivo, companhias de todos os tamanhos e segmentos precisam construir uma gestão sólida no uso das informações de terceiros.

O primeiro passo é entender as leis e como identificar o programa de gestão de dados mais apropriado para cada negócio. Feito isso, entram as ações operacionais para a proteção de dados que devem ser adotadas nas empresas.

Os pilares de um programa de segurança da Informação

A primeira etapa é uma espécie de autoconhecimento sobre o negócio de uma maneira ampla. Entre ou- tras coisas, é preciso fazer uma avaliação crítica sobre as ameaças, vulnerabilidades e os dados tratados em seu negócio. O passo seguinte é construir um programa de segurança da informação, que deverá atender três pilares:

Governança

Estrutura de liderança e responsabilidade estabelecida para garantir que as políticas, contratos e práticas de segurança da informação sejam implementadas e gerenciadas. Isso inclui estabelecer responsabilidades claras, monitorar o desempenho e garantir que as políticas sejam revisadas e atualizadas regularmente. Atualmente, técnicas de visual design podem auxiliar na leitura e compreensão do tema de segurança da informação.

Tecnologia

Conjunto de ferramentas e sistemas utilizados para proteger a informação, como firewalls, sistemas de detecção de intrusão, criptografia, e outras

Cultura

Conjunto de valores, crenças e comportamentos que promovem a segurança da informação em toda a empresa e são disseminados por meio de treinamentos, palestras, materiais visuais e demais ações de conscientização.

INOVATIVOS

Plataforma Multicanal de Conteúdo

NOTÍCIAS

TV DIGITAL

PODCAST

Sua fonte de conhecimento e conexão com a nova economia

WWW.INOVATIVOS.COM.BR

Por dentro da LGPD

O que é a LGPD?

A LGPD (Lei Geral de Proteção de Dados) regulamenta as atividades de tratamento de dados pessoais bem como a governança e seus controles de segurança. A lei ainda obriga empresas a implementarem medidas de segurança técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito.

Penalidades

Advertência - Emite uma advertência e determina um prazo para que a infratora possa regularizar a situação.

Multas - Multa simples que pode chegar a 2% sobre o faturamento do negócio, tendo o limite de 50 milhões de reais. Há, ainda, a multa diária.

Publicização da infração - Após apurada e confirmada a infração, a ANPD pode dar publicidade a infração. Esta sanção pode manchar a reputação da empresa no mercado.

Bloqueio de dados pessoais - Confirmada a infração, os dados pessoais do sistema da empresa podem ficam blo- queados até a regularização. Ou seja, as atividades que necessitam dessas informações para serem executa- das terão que ser paralisadas temporariamente.

Eliminação de dados pessoais - Nos casos mais graves, a empresa será obrigada a eliminar os dados pessoais armazenados. Essa medida pode praticamente inviabilizar a continuidade da empresa.

Atenção: *existe ainda a possibilidade sanções na esfera cível e criminal*

Regras para a aplicação das multas

Existem dois tipos de infratores:

Primários que não incidiram em violação prévia à LGPD: multa simples; multa diária; publicização da infração; bloqueio de dados pessoais; e eliminação de dados pessoais;

Reincidentes: suspensão do acesso e uso do Banco de dados; suspensão do exercício de atividades de tratamento; e proibição do exercício de atividades de tratamento;

A multa cresce quando há:

- Reincidência específica: de **10% a 40%**;
- Reincidência genérica: de **5% a 20%**;
- Descumprimento de medida orientativa ou preventiva: **20% a 80%**;
- Descumprimento de medida corretiva: **30% a 90%**.

A multa diminui em:

- **75%**, caso o agente de tratamento consiga encerrar a infração antes da ANPD instaurar procedimento preparatório, ou seja, averiguar se a conduta efetivamente ocorreu;
- **50%**, se a o encerramento da infração ocorrer após instauração de procedimento preparatório e até a instauração de procedimento administrativo sancionador;
- **30%**, se a infração for cessada após a instauração de processo administrativo sancionador (análise do caso na ANPD), até a prolação de decisão de primeira instância.

Controle de segurança e direitos fundamentais

"Implementar controles de segurança é proteger os direitos fundamentais dos titulares dos dados e garantir a confiança na empresa. Também é uma forma de garantir a confidencialidade, integridade e disponibilidade dos dados pessoais."

Leandro Bissoli, sócio do Peck Advogados

Houve vazamento de dados. O que faço?

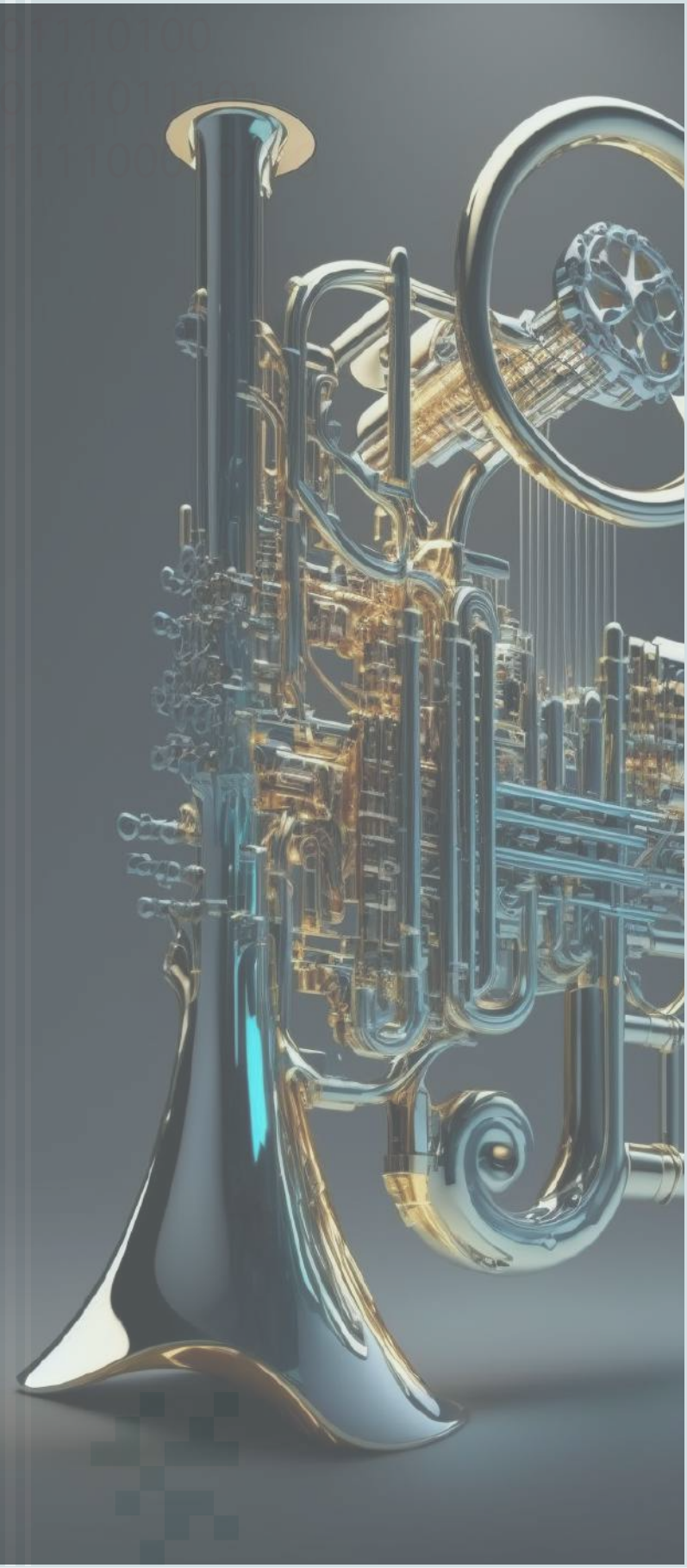
A Lei Geral de Proteção de Dados define os procedimentos que as empresas devem seguir no caso de incidentes. Além disso, existem normas para setores específicos da economia.

Pilares para a aplicação da LGPD

- Tratamento de dados precisa ser realizado em território brasileiro
- Operações de tratamento que tenham por objetivo ofertar ou fornecer bens ou serviços em território brasileiro, ou que envolvam o tratamento de dados de titulares localizados em território brasileiro
- Qualquer operação que envolva dados coletados em território brasileiro

Em caso de incidente, a empresa deverá:

Coletar dados, organizar e manter atualizadas todas as informações relacionadas ao incidente, além de atualizar as medidas adotadas após o início da investigação.



Comunicação de incidentes

A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados
- As informações sobre os titulares envolvidos
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial
- Os riscos relacionados ao incidente
- Os motivos da demora, no caso de a comunicação não ter sido imediata
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo

Atenção: Sobre a comunicação aos titulares de dados pessoais, até o momento, não há procedimento específico sobre o tema.

Incidentes de segurança em setores regulados

Alguns setores regulados da economia possuem regras próprias para incidentes de segurança.

Exemplos de regras de ciber em alguns setores da economia

Financeiro

A Resolução CMN nº 4.893/2021 determina que as instituições autorizadas a funcionar pelo Banco Central (Bacen) devem:

- Implementar e manter políticas de segurança cibernética para assegurar a confidencialidade, integridade e disponibilidade dos sistemas de informação;
- Desenvolver um plano de ação e de resposta a incidentes com: iniciativas que serão desenvolvidas para adequar as estruturas aos princípios e diretrizes da política de segurança cibernética; as rotinas, os procedimentos, os controles e as tecnologias utilizados na prevenção e na resposta a incidentes; e a área responsável pelo registro e controle dos efeitos de incidentes;
- Todos estes documentos deverão ser aprovados pelo conselho de administração ou pela diretoria da instituição, além da necessidade de elaboração de relatórios e revisão das políticas anualmente; dentre outros pontos.

Seguros

A Circular SUSEP nº 638/2021, entre outras medidas, exige:

- Criar políticas de segurança cibernéticas (compatíveis com o porte, natureza, complexidade de operações e grau de exposição ao risco)
- A política de segurança cibernética deve conter objetivos, além dos compromissos da alta direção com os temas propostos no documento, incluindo melhoria contínua, e muito mais
- Possuir e manter atualizados procedimentos e controles efetivos para identificar e reduzir vulnerabilidades de forma proativa e detectar, responder e recuperar-se de incidente
- Comunicar incidentes relevantes no prazo máximo de cinco dias úteis a partir do conhecimento do evento e detalhando a extensão do dano causado e as ações adotadas para regularizar a situação, além dos respectivos responsáveis e prazos

Energia

O destaque é a Resolução ANEEL nº 964/2021, que também tem por objetivo estabelecer diretrizes e conteúdo mínimo das políticas de segurança cibernética. Ela define, por exemplo:

- A empresa deve notificar a coordenação setorial de incidentes cibernéticos do tema sobre o incidente de maior impacto
- Em caso de ataque, é preciso incluir a análise da causa e do impacto, bem como a indicação das ações de mitigação dos danos adotadas,
- A notificação ainda deverá prever procedimentos de compartilhamento de informações sobre ameaças e outras informações relativas à segurança cibernética de forma sigilosa e não discriminatória.

Telecomunicações

Entre as normas, o destaque é a Resolução ANATEL nº 740/2020, responsável por estabelecer condutas e procedimentos para a promoção da segurança nas redes e serviços de telecomunicações, incluindo segurança cibernética e proteção de infraestruturas críticas de telecomunicações. Ela determina:

- A adoção de normas e padrões nacionais ou internacionais, e referências de boas práticas no tema;
- A disseminação de uma cultura de segurança cibernética;
- A identificação, proteção, diagnóstico, resposta e recuperação de incidentes de segurança cibernética;
- A cooperação entre diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos;
- A adoção de conceitos de security by design e privacy by design no desenvolvimento e aquisição de produtos e serviços no setor de telecomunicações; dentre outros.

Leis específicas aplicáveis

"Em caso de incidente com informações não pessoais em setores não regulados (e-commerce, por exemplo), existem leis específicas aplicáveis, e a análise seria exclusivamente técnica sobre eventuais danos e suas respectivas reparações."

Maria Eugênia Geve de Moraes Lacerda, advogada da área de Cybersecurity e Data Privacy de TozziniFreire Advogados

Exemplos de frameworks de segurança cibernética

Para todos os setores

- **Família ISO / IEC 27001 -** traz os controles / requisitos de sistemas de gestão da segurança da informação, além dos temas segurança cibernética e privacidade
- **Framework de cybersecurity do NIST -** fornece um conjunto de práticas, diretrizes e padrões de segurança cibernética para organizações de todos os tamanhos e setores que pretendem começar ou aprimorar o seu programa de cibersegurança. Estruturado em cinco funções: identificar, proteger, detectar, responder e recuperar
- **Framework de cybersecurity do CIS Controls -** traz em sua última versão (v8) um conjunto de 18 controles de segurança cibernética para apoiar as organizações na proteção de seus sistemas e dados contra ameaças cibernéticas. Os controles estão organizados em três camadas: básica, intermediária e avançada

Para setores específicos

- **PCI DS -** consiste em requisitos de segurança para as organizações que tratam dados de cartões de crédito. O padrão foi criado pelas principais empresas de cartões de crédito para estabelecer segurança no tratamento de dados dos cartões e reduzir o risco de fraudes e violações de segurança
- **Cloud Controls Matrix (CCM) -** apresenta um conjunto de controles de segurança cibernética que visam proteger os dados e sistemas em ambientes em nuvem

Atualização de estrutura

"A segurança da informação é um tema estratégico que requer atualização constante e deve ser acompanhado pela alta gestão e conselhos das empresas. Por isso, alguns frameworks de segurança da informação são atualizados regularmente. As empresas devem criar um programa avaliando os principais estruturas em uso no mercado e, por fim, comparar os controles com às suas necessidades."

Patricia Peck, sócia fundadora do Peck Advogados

Uso de dados no ambiente corporativo

Principais regras para o uso de dados

- Os dados precisam estar sempre disponíveis
- A disponibilidade deve se mantida mesmo em caso de falha no hardware (computador), no software, problema na rede, entre outros motivos
- A disponibilidade 24 x 7 pode ocorrer por meio de controles de redundância, backups regulares e planejamento de continuidade dos negócios
- É preciso criar diferentes níveis de acessos a informação. Para assegurar a confidencialidade é necessário implementar controles de segurança de acesso a informação
- É preciso ter controle de acesso aos dados em suporte físico também
- Os dados e as informações também devem ser protegidos contra alterações acidentais ou maliciosas, assegurando sua integridade
- É necessário monitorar e auditar modificações nas informações para identificar atividades suspeitas.
- Todas as atividades de tratamento das dados (sejam dados pessoais ou não) devem estar em conformidade com as leis e regulamentos aplicáveis
- Algumas práticas comuns para assegurar a legalidade incluem a realização de auditorias regulares, a implementação de políticas e procedimentos internos e a capacitação dos colaboradores sobre leis e regras aplicáveis

Outras normas que tratam de segurança cibernética

ANEEL	Resolução Normativa **964** de 14 de dezembro de 2021
ANATEL	Resolução **740** de 21 de dezembro de 2020
CVM	Resolução **35/2021** com as alterações introduzidas pela Resolução **Nº 134/22**
BANCO CENTRAL DO BRASIL	• Resolução **4.893** de 26 de fevereiro de 2021 • Resolução **85** de 8 de abril de 2021
SUSEP Superintendência de Seguros Privados	Circular **638** de 27 de julho de 2021

Como construir uma gestão de segurança cibernética

Segurança é um tema que guarda uma relação estreita com fatores culturais. Hábitos, o respeito às determinações coletivas e às leis, as definições de organização e outros aspectos formam itens de uma cultura organizacional que irá fundamentar a avaliação e o alinhamento à cibersegurança.

O caminho é o da conscientização e o da exposição à realidade. Nesse sentido, treinamento, discussões, exemplo de conduta e postura, políticas bem descritas e acessíveis são essenciais para a construção da cultura corporativa de cibersegurança

Cultura corporativa da cibersegurança

A importância da cultura de cibersegurança

"Na medida em que pessoas e empresas avançam digitalmente, elas transformam nossos modos de viver e de se relacionar, formando organizações que coletam, armazenam e tratam digitalmente dados e informações. Com isso vem a preocupação com a proteção, à privacidade e com a segurança no ambiente cibernético, absolutamente indispensável no mundo moderno",

George Leal Jamil, professor, escritor e consultor de gestão e tecnologia

Fique de olho: Nos Estados Unidos, pelo menos um dos conselheiros de administração de companhias precisam saber sobre cibersegurança.

O papel do CEO

A cibersegurança é um tema que interessa a alta gestão por diversos motivos. Sob a sua responsabilidade, vão existir tarefas, procedimentos, designações de planejamentos estratégico e tático, o processamento com os bens "dados", que precisam ser protegidos, securitizados e tratados de acordo com princípios legais. E o custo, como todos sabem, é um assunto que sempre interessa aos CEOs.

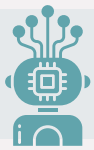
"Junto com todas as preocupações e perspectivas de seus cargos e trabalhos, os dirigentes, líderes e CEOs devem ter total atenção a esses bens intangíveis, pois também administram esforços nas empresas que irão gerar dados e informações"

George Leal Jamil, professor, escritor e consultor de gestão e tecnologia

Mapeando o negócio e os riscos

Entender o contexto do negócio e o cenário de cibersegurança da companhia - incluindo as fragilidades - é essencial para um correto mapeamento de riscos.

Os cenários que os executivos precisam considerar na macro gestão em cibersegurança:



O aumento da abrangência de acessos com o 5G

Crescimento de máquinas autônomas conectadas na rede

Elevação de análises em tempo real feitas a partir da inteligência artificial

E que precisamos ter respostas mais rápidas conforme evolui o aprendizado de máquinas

A cibersegurança se tornou um risco operacional, que pode impactar até a continuidade do negócio

É preciso refletir se o negócio sobreviveria a um ataque e/ou quantos dias a empresa poderá ficar sem operar aplicações e serviços

Maturidade cibernética

"A primeira medida é identificar a maturidade de segurança da empresa utilizando um dos vários frameworks de mercado"

Rodrigo Veiga, diretor de Cibersegurança da OLX Brasil

Finalidade do modelo de mapeamento de risco

"(O uso de modelos de estruturas para mapeamento de risco) Serve também para identificar os riscos atrelados a cada um dos controles. Usar o mesmo framework para calcular também o risco ajuda a definir prioridades sobre quais controles implementar primeiro"

Douglas Rocha, gerente executivo de Segurança da Informação do Banco Inter

Documentar tudo

"Não é possível identificar os riscos daquilo que não se conhece. Isso pode ser feito por meio de uma rotina de atualização contínua entre as áreas de negócio. A documentação também é importante para atualizar o conhecimento dos processos entre os colaboradores, evitando depender de pessoas específicas."

Eduardo Tamaki, Information Security Manager da Mevo

Definindo o que é risco

"Para implementar um bom mapeamento é necessário, antes de tudo, ter uma definição clara do que é considerado risco, saber identificá-lo, além de implementar um comitê na empresa sobre o tema. Assim fica mais fácil classificá-los de acordo com a probabilidade, ocorrência e impacto. Da mesma forma, permite desenvolver uma matriz de priorização para identificar riscos a serem abordados imediatamente."

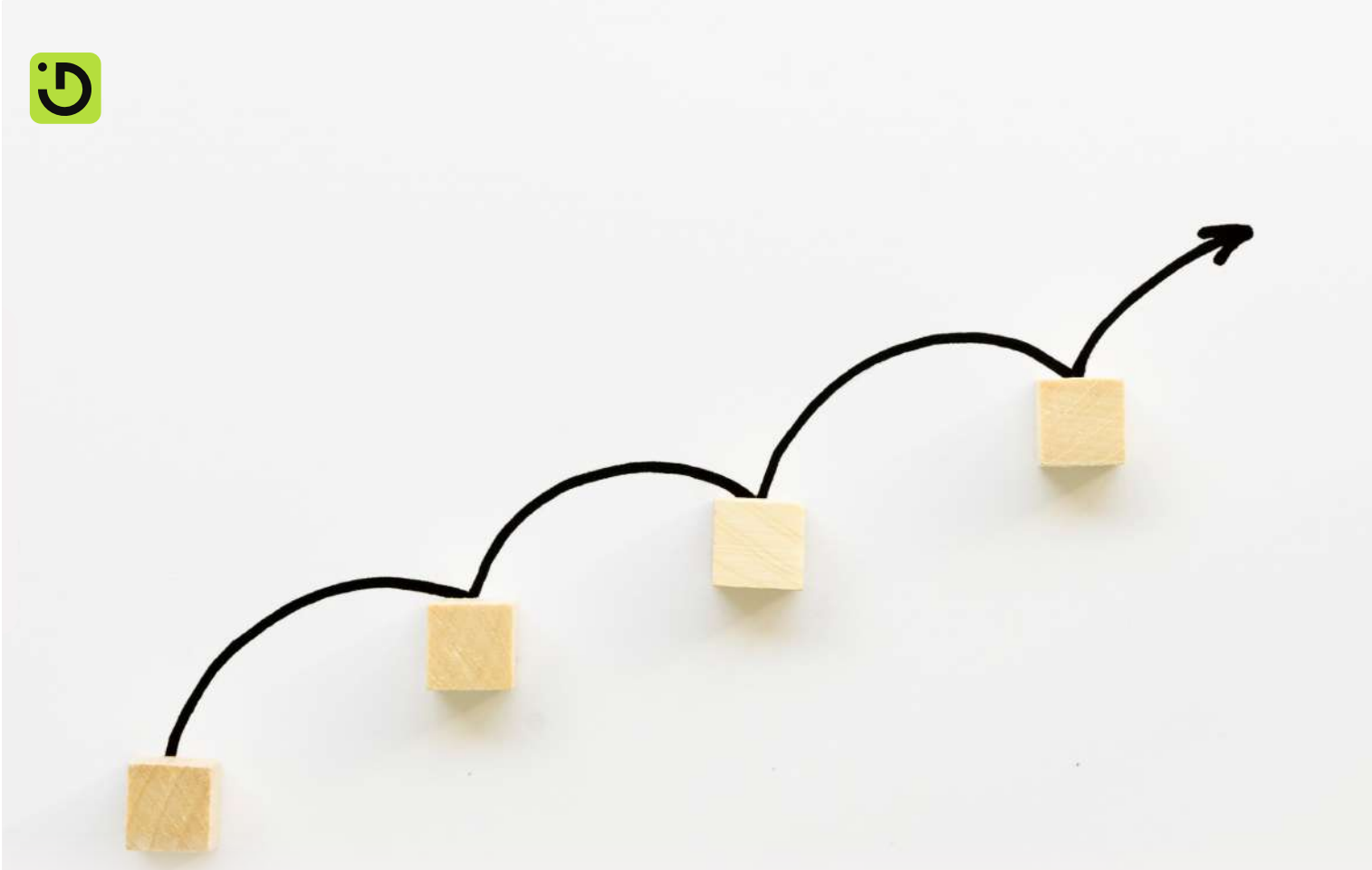
Vasco Pineda, Brazil Launcher da Yuno

A importância da política da gestão de risco

"É importante construir uma política de gestão de riscos cibernéticos e segurança da informação com objetivos claros, uma estrutura de identificação, prevenção, detecção, resposta e recuperação bem estabelecida. Da mesma forma, é fundamental ter uma governança com bons indicadores, utilizar o modelo de três linhas de defesa e ter um gerenciamento de crises envolvendo as principais áreas da empresa."

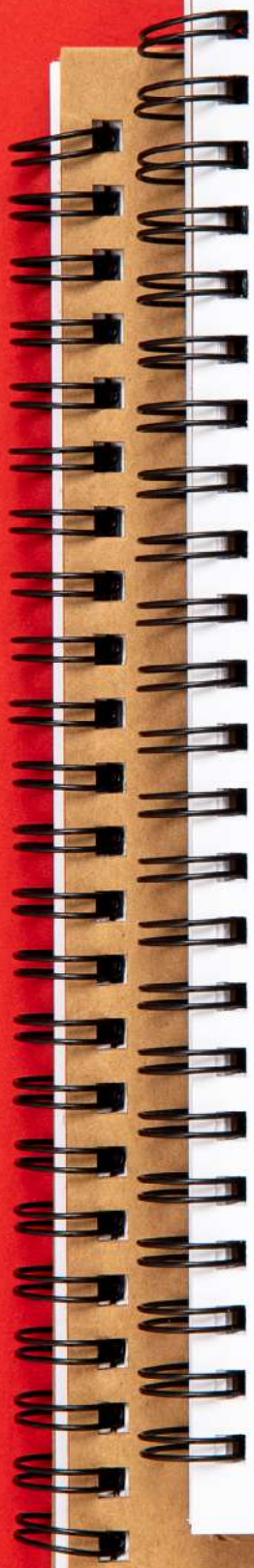
Vinicius Fiel, superintendente de Segurança da Informação da Porto

Passo a passo do plano de gestão de segurança cibernética



Existem diferentes modelos de gestão de segurança cibernética disponíveis no mercado. Alguns deles são conhecidos dos profissionais de segurança. No entanto, a ideia é montar um plano a partir de alguns pilares fundamentais, tais como prevenção, defesa, implementação de um plano de segurança em nível e outros fatores, resposta contra incidentes, arquitetura e outros.

Principais ações para prevenir um ciberataque



- Melhorar a infraestrutura da segurança por meio de visibilidade e inventário (ou anotações)
- Sempre validar as configurações para manter as melhores práticas de mercado e também ativar as funcionalidades de segurança
- Oferecer programas de conscientização em cibersegurança para funcionários
- Usar ferramentas que protejam credenciais de acesso, além de (sempre) ativar o duplo fator de autenticação
- Implementar soluções que monitorem o comportamento e acessos do usuário, além de incluir alertas para ações "anormais" de uma pessoa
- Implementar gestão de usuários privilegiados (ou administradores de sistemas)
- Implementar soluções de criptografia para banco de dados, informações sigilosas e dispositivos móveis
- Manter uma rotina diária de backup de sistemas e dados, com testes contínuos para garantir a recuperação segura e íntegra das informações
- E muito mais

Boas práticas de Segurança da Informação

"É preciso ter minimamente o básico das boas práticas de segurança da informação corretamente aplicado em todos os ambientes da empresa, como duplo fator de autenticação para acesso a sistemas e dispositivos, senhas com expiração, comprimento e complexidade adequados, bloqueio automático de sistemas por inatividade, uma boa gestão de acesso, entre outras medidas. Um ponto relevante para se preparar para as ameaças de ataque é pensar não 'se' a empresa será atacada, mas sim 'quando'."

Cleverson Arashiro, VP Infosec e IT da Loft

Definindo o framework

"É preciso escolher um framework de ciber que irá guiá-lo sobre os controles necessários em cada um dos domínios de segurança. Este plano de ação se transformará no plano operacional a ser implementado em cada uma das frentes de segurança, seja defesa, ataque, arquitetura, resposta a incidentes, etc."

Douglas Rocha, gerente executivo de Segurança da Informação do Banco Inter

Estratégia para pontos mais críticos

"Dependendo da quantidade de problemas, eles acabam interferindo na companhia como um todo, impactando no ambiente de negócios e no core (business). O ideal seria montar um plano de dois anos. Após esse período, após o plano cobrir os pontos mais críticos, é possível analisar onde a empresa chegou, qual o próximo plano que você vai ter que montar e onde vai ter que reinvestir. É o que chamamos de PDCA (método gerencial aplicado para gerenciamento de processos)."

Willians Santos, CISO no Banco Carrefour

"Ciber 360 graus" e investimento em tecnologia

"Não podemos ver o assunto como um tema técnico isolado, por isso devemos trazê-lo para deliberações dos times da empresa como um todo e não apenas do departamento de engenharia e tecnologia. Por fim, deve haver o investimento em tecnologias que permitam garantir a segurança dos processos e ativos da empresa, bem como auxiliar o time na condução das atividades diárias."

Eduardo Tamaki, Information Security Manager da Mevo

Etapas do plano de segurança cibernética

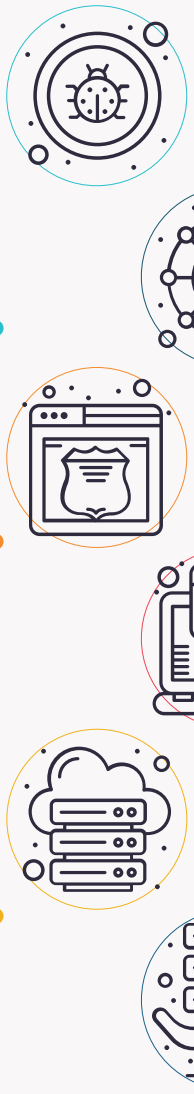
O plano a seguir é uma sugestão a partir das ferramentas disponíveis atualmente. Elas podem mudar com o tempo

Inicial:

Teste de invasão para análise de maturidade inicial e também estabelecer recorrência de segurança (conhecido por Pen Test ou teste de invasão)

Incluir proteção de dispositivos eletrônicos e de servidores

Realizar backup (cópia de documento) e restore (ação de recuperar dados durante a rotina de backup) já implementados e validados



Instalar uma proteção de Identidade: MFA (um método de autenticação eletrônica), uma rede privada VPN e acesso administrativo seguro, PIM (privileged identity management) e PAM (privileged access management)

Validação da exposição da marca e sistemas frente aos adversários (Threat Intelligence)

Treinamento colaboradores, usuários e terceiros: palestras educativas e teste de phishing

Investimento:
3% a 5% do orçamento de TI

Essencial

Proteger as aplicações, tais como Pen Test e outros

Plano de resposta a incidentes e comunicação ANPD (Agência Nacional de Proteção de Dados)

Ter um monitoramento inicial, que inclua: "log de evento" (ou registro de tudo em sistemas operacionais e equipamentos), auditoria por empresa habilitada, gestão de alertaas (ou seja, realiza o monitoramento, recepção e emissão de documentos eletrônicos), NOC (Network Operations Center) ou SOC (Security Operations Center) básico, interno ou externo

Evolução do processo de IAM (Verifica a identidade e faz o controle do acesso a determinadas informações)

Criptografia para dados em repouso (ou todos as informações armazenadas) e também para dispositivos móveis (celulares)

Treinamento do plano de resposta que prevejam tabletop exercise (simulação de um ataque), além de ações para casos de vazamento de dados e ataque ransomware

Investimento:
6% a 10% do orçamento de TI

Fonte: Especialistas em cibersegurança do Movimento Inovação Digital (MID)

Maduro

Estrutura organizacional do time de segurança, governança e processos bem definidos

Educação executivos e cyber range (ambientes virtuais utilizados para cibersegurança, treinamento em ciberguerra, simulação ou emulação e desenvolvimento de tecnologias relacionadas à cibersegurança) para equipe técnica

Avaliação de parceiros e fornecedores

Monitoramento de ambiente avançado SIEM (realiza análise de comportamento de usuários e entidades e orquestração, automação e resposta de segurança) com apoio de parceiro ou interno

Incrementar maturidade do processo de IAM

Investimento:
10% a 15% do orçamento de TI

Fonte: Especialistas em cibersegurança do Movimento Inovação Digital (MID)

Monitoramento de riscos e indicadores

Gestão de monitoramento

É um processo contínuo de identificação, análise e planejamento de novos riscos, acompanhamento de ameaças já identificadas, reavaliação de riscos existentes, entre outras ações. Ele também envolve os monitoramentos das condições que acionam os planos de contingência e dos riscos residuais e a revisão da implementação das respostas aos riscos enquanto se avalia sua eficácia.

010 00001010 101100 01000000111

Endpoints

"Deve-se iniciar o monitoramento pelos pontos chaves do seu produto, priorizando os endpoints (nó de rede de comunicação). Outro ponto importante, baseado no comportamento dos usuários, é criar um padrão de acesso e monitorar os desvios desse padrão."

Rodrigo Veiga, diretor de Cibersegurança da OLX Brasil

Atualização de processos

"O processo de monitoramento e controle de risco também inclui a atualização dos ativos do processo da organização. Isto inclui bancos de dados de lições aprendidas do projeto e modelos de gerenciamento de risco para o benefício de projetos futuros."

Vasco Pineda, Brazil Launcher da Yuno.

Registros em um único repositório

“Existem ferramentas que você pode gerar alertas a partir delas próprias. Porém, o ideal é concentrar todos estes logs (registros) em um único repositório. Dessa forma, é possível criar regras de correlacionamento e identificar mais facilmente comportamentos suspeitos. Sem os logs estamos cegos sobre o que acontece em nosso ambiente corporativo.”

Douglas Rocha, gerente-executivo de Segurança da Informação do Banco Inter

Gestão de monitoramento: contexto e características

“A gestão de monitoramento deve ser baseada, primeiramente, no contexto do ambiente e suas características. Por exemplo, um ambiente Cloud tem necessidades diferentes de um ambiente On Premise (servidores locais). Além disso, é fundamental que todas as superfícies de ataque sejam consideradas, no qual processos bem definidos, documentações estruturadas, mapeamento de riscos, ferramentas adequadas e a construção de times capacitados são fundamentais para um monitoramento de segurança efetivo.”

Eduardo Tamaki, Information Security Manager da Mevo

Indicadores

A construção de indicadores de monitoramento surgem por meio dos resultados dos próprios processos de monitoramento, como dados gerados pelas tecnologias utilizadas por cada companhia para esse fim, como alertas e notificações.

Use os pontos-chaves

"A primeira medida é identificar a maturidade de segurança da empresa utilizando um dos vários frameworks de mercado. Assim como em uma multidão que entra em um estádio, em que é difícil observar individualmente cada pessoa, monitorar ativos de tecnologia contra ataques também pode ser um desafio. Por isso, deve-se iniciar o monitoramento pelos pontos-chaves do seu produto, priorizando os endpoints."

Rodrigo Veiga, diretor de Cibersegurança da OLX Brasil

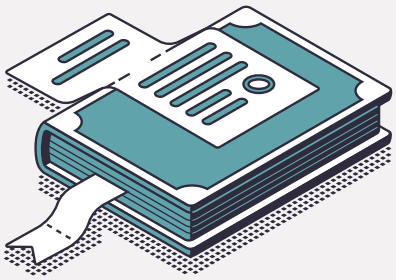
Eficiência e tomada de decisão

"Esses indicadores são fundamentais para criar uma gestão mais eficiente, além de permitir que as tomadas de decisão estratégica ocorram de forma mais assertiva. Por último, também servem como base de melhoria do próprio processo de monitoramento, minimizando a ocorrência de falsos positivos e fortalecendo a importância da gestão baseada em dados."

Eduardo Tamaki, Information Security Manager da Mevo

Fui atacada. E agora?

Estrutura de uma gestão de segurança cibernética



Fique atento às normas sobre o tema

Leis e regulamentos gerais:

- Lei Geral de Proteção de Dados (Lei nº 13.709/2018)
- Marco Civil da Internet (Lei nº 12.965/2014) e
- Decreto Regulamentador do Marco Civil da Internet (Decreto nº 8.771/2016).

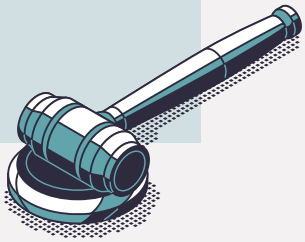
Leis e regulamentos setoriais:

- (i) Resolução BCB nº 4.893/2021 para o Setor Financeiro);
- (ii) Circular SUSEP nº 638/2021 para o Setor de Seguros;
- (iii) Resolução ANATEL nº 740/2020 para o Setor de Telecomunicações; e (iv) Resolução ANEEL nº 964/2021 para o Setor de Energia.

Defina abordagem e esteja em dia com a documentação

É sempre bom colocar no papel a abordagem sobre o tema. Cada empresa adota um modelo, mas todos precisam conter os seguinte tópicos

- Prevenção e Preparação
- Identificação e Avaliação
- Mitigação e Notificação
- Impactos Diversos de Incidentes de Segurança Envolvendo Dados



Prevenção e Preparação

A continuidade dos negócios depende da interrupção da violação de dados e evitar sua reincidência. Para isso, é necessário:

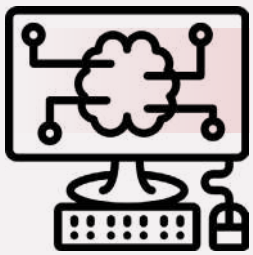
- Fomentar a cultura de governança de dados técnica e administrativamente;
- Adotar tecnologias de segurança e realizar programas de adequação da empresa à LGPD (e demais normas setoriais, conforme aplicável); e
- Realizar a capacitação contínua de funcionários sobre cibersegurança e a adoção de políticas que tratem sobre o tema.

Fique de olho também

A Recomendação 34/2022 do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) indica algumas boas práticas sobre o tema. São elas:

- Elaborar e revisar periodicamente da política de segurança da informação, de segurança cibernética ou equivalente;
- Elaborar e revisar periodicamente o plano estratégico de segurança dos ativos críticos da organização, além de manter atualizado o inventário desses ativos críticos;
- Ter um plano de gestão de backup que contemple o armazenamento seguro dos dados copiados em lugar isolado, offline, redundante e que seja submetido a testes periódicos de recuperação de dados;
- Possuir ambiente com virtualização de servidores, onde se considere a utilização de snapshots (preservando o estado e os dados de uma máquina virtual em um determinado momento), atualizados regularmente, de forma a viabilizar o rápido retorno de sistemas críticos quando necessário;

Plano de atualização de sistemas computacionais



Sistemas computacionais representam um conjunto de dispositivos eletrônicos (hardware) que processam diversos programas (softwares).

O que o plano deve conter:

- Implementar e revisar periodicamente a política de senhas da organização. Elas precisam ser fortes, não repetidas quando trocadas e devem expirar após um determinado período.
- Mapear e rever os privilégios de usuários, implementando a política de privilégio mínimo, na qual cada usuário deverá ter apenas os privilégios de acesso a pastas e informações estritamente necessários para o desempenho de suas funções.
- Implementar um plano de segurança de acesso remoto da organização. Ele deve incluir a utilização de VPN (rede particular) e duplo/múltiplo fator de autenticação, além da revisão periódica sobre a necessidade de acesso remoto para cada caso.
- Implementar um plano de autenticação de sistemas que contemple a utilização de múltiplo fator de autenticação, além de gestão de acesso a usuários internos e externos, ativos ou afastados;
- Implementar plano de bloquear credenciais de colaboradores que estejam afastados (férias, licenças e outros);
- Manter os sistemas de gerenciamento contra malwares (antivírus, firewall, dentre outros) sempre atualizados, avaliando possíveis recomendações de melhoria que o produto ou fabricante possa oferecer

Conscientização e Educação

Algumas das mais importantes medidas em segurança cibernética não dependem de uma tecnologia específica. Existem ações que estão relacionadas a conscientização e educação em cibersegurança.

Educação = atenção à segurança

"A partir disso, a empresa aumenta sua segurança ao ter seus funcionários mais atentos ao tema (inclusive em relação a tentativas de ataques, como e-mails de phishing, atualmente a maior razão de ataques externos) e diminui seu tempo de resposta ao garantir uma rápida identificação da ocorrência a partir da colaboração de todos."

Carla do Couto Hellu Battilana, sócia da área de cybersecurity e data privacy de TozziniFreire Advogados.

Pilares da educação em cibersegurança

- É preciso saber identificar incidentes (por exemplo, indicando exemplos de phishing, práticas suspeitas e "DOs e DONT's" em termos de segurança da informação), atividades suspeitas ou riscos potenciais ou efetivos à segurança da informação, seja por atuação humana, seja por códigos ou programas maliciosos.

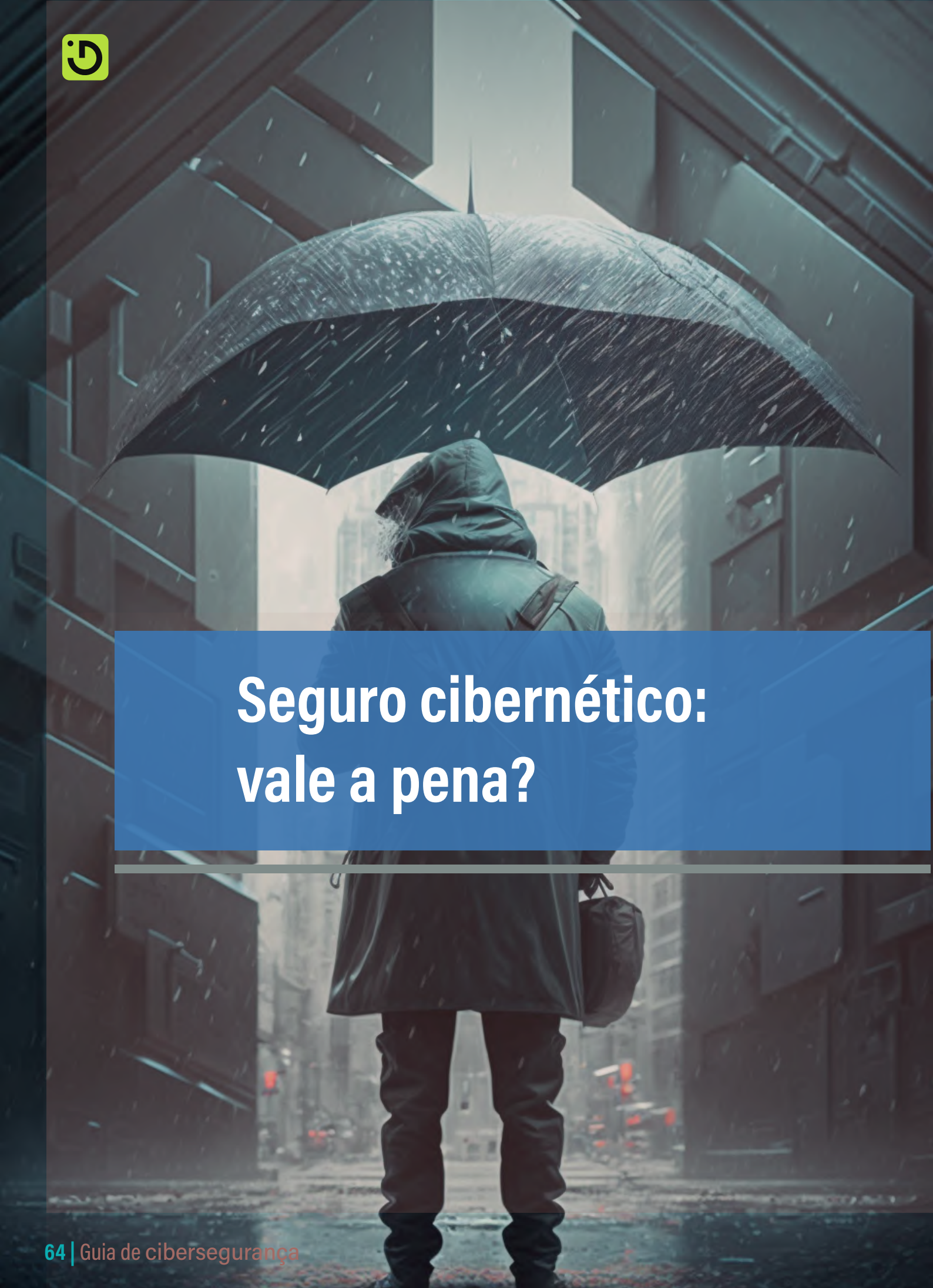
- Devem aprender como entrar em contato com um especialista dentro da empresa. É recomendável que ao menos os responsáveis pela gestão da segurança da informação da empresa, jurídico e o encarregado de dados (quando o incidente envolver dados pessoais) – ou um comitê de segurança da informação, quando houver – sejam contatados;

- Uma introdução ao tema, destacando a importância todos os colaboradores zelar pela segurança e integridade das informações em posse da empresa, de forma a conter riscos relacionados a informações (pessoais ou não), assegurando a confidencialidade e integridade dos dados e minimizando a possibilidade de ocorrência de incidentes desta natureza, ou minimizando seus efeito.

- Orientações com relação à documentação do incidente, quando verificada a ocorrência ou suspeita de ocorrência da situação.

- Orientações sobre contenção, resolução e recuperação de informações, por exemplo, sobre a alocação de pessoal para a investigação e gestão do incidente e/ou contratação de empresas especializadas, bem como os ritos de aprovação de tais decisões, conforme prática da empresa. Este ponto também pode trazer orientações sobre a reativação dos sistemas e bancos de dados envolvidos, bem como à revisão e reestruturação de procedimentos que tenham contribuído ou possam ter contribuído com a ocorrência do Incidente, inclusive em meios físicos, tomando todas as medidas pertinentes e necessárias; e

- Orientações sobre comunicações e/ou notificações do incidente, de acordo com a natureza dos dados e do setor da empresa, se o caso.



Seguro cibernético: vale a pena?

O seguro cibernético garante a indenização de danos decorrentes de ataques cibernéticos, como sequestro ou vazamento de dados, e inclui cobertura para casos de extorsão, multas aplicadas por autoridades e até mesmo lucros cessantes.

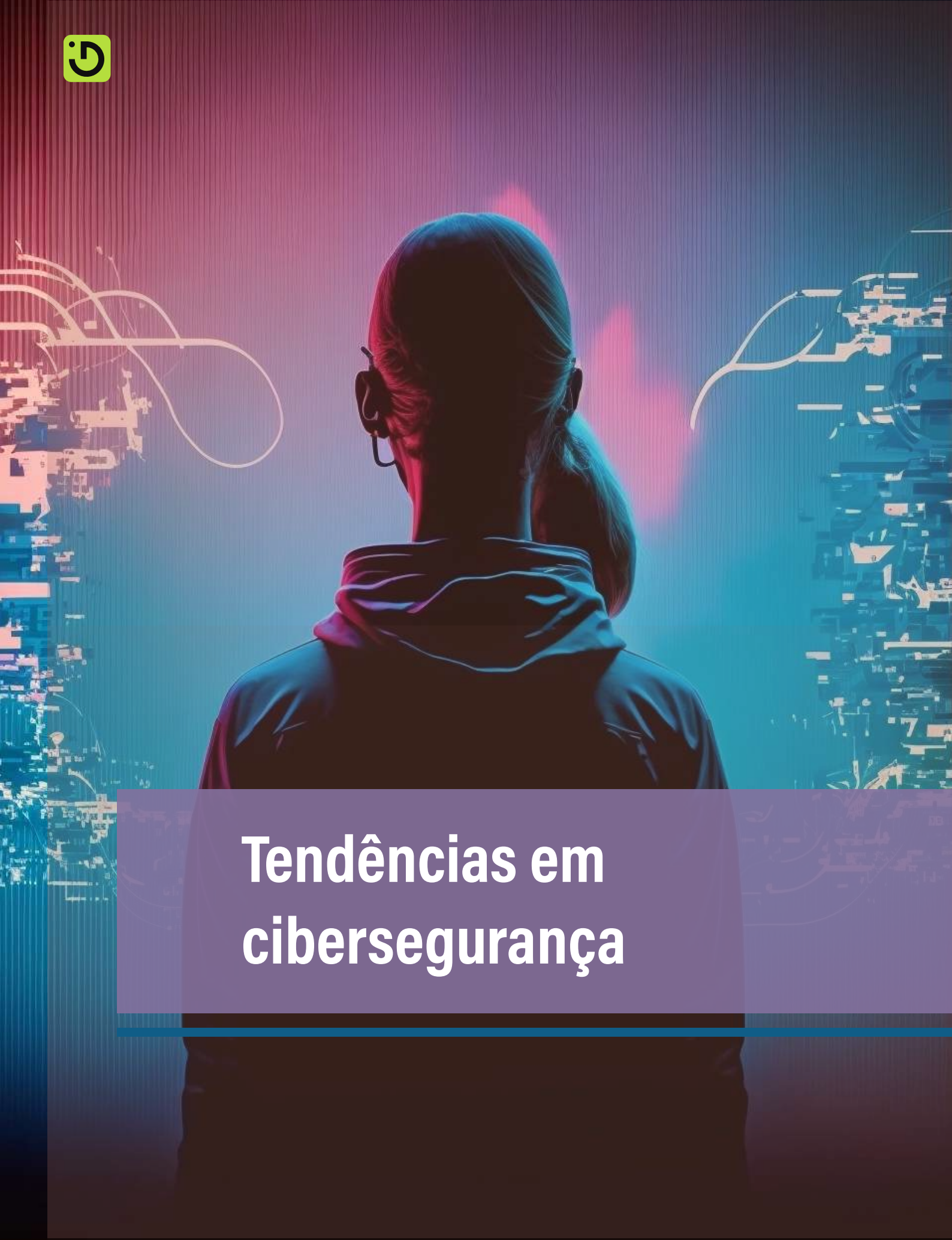
Seguro em alta

"Essa modalidade de seguro se popularizou com o aumento dos incidentes de segurança e são importantes para mitigar as consequências de qualquer ocorrência nesse sentido – ainda que um plano de resposta a incidentes tenha sido elaborado e seja prontamente cumprido."

Carla do Couto Hellu Battilana, sócia da área de cybersecurity e data privacy de TozziniFreire Advogados.

Como contratar um seguro de cibersegurança:

- Verificar a reputação da seguradora no mercado;
- Avaliar a cobertura para responsabilidade civil, administrativa e penal, à empresa e aos terceiros afetados
- É necessário ter o apoio de gestão de crise para mitigação dos impactos reputacionais causados pelo incidente
- Ter o suporte técnico de empresa especializada em gestão de riscos.



Tendências em cibersegurança

Na avaliação de especialistas, teremos um aumento de ataques promovidos por ciberterroristas, com foco nas espionagens militar e industrial, além de ameaças contra determinadas infraestruturas. Esses grupos podem ser profissionais ou até funcionários (caso de militares) de um determinado estado-nação. A seguir, veja alguns cenários apontados pela Microsoft.

Internet das Coisas

Será preciso redobrar a atenção na segurança de controles industriais e Internet das Coisas (IoT). Malware ou códigos maliciosos exploram a ineficiência de práticas de segurança de sistemas, em muitos casos, sistemas legados ou desenvolvidos desconsiderando análises prévias de vulnerabilidades. Exemplos: automóveis e dispositivos de ingestão de insulina para pacientes diabéticos.

Aumento de ataques de ransomware

Haverá aumento nos ataques de ransomware, de ataques cibernéticos coordenados contra infraestruturas críticas e de ataques de phishing (que pesca dados a partir de engenharias sociais) massivos e personalizados com o uso de Inteligência Artificial (IA) e bots voltados a fraude bancária, roubo de senhas e lavagem de dinheiro. Os bots de IA estão sofrendo reengenharia e sendo transformados em “evils” (bots do mal).

Ameaça interna

Haverá um aumento do chamado Insider Threat (ou ameaça interna). Em breve, certos ataques comuns terão mais dificuldade para serem bem-sucedidos, logo o método consiste em cooptar o funcionário de uma empresa que “abrirá as portas” da organização para o cibercriminoso entrar. É possível ainda que o ataque ocorra a partir de um funcionário do parceiro de negócios ou fornecedor.

Quanto mais complexo, mais potencial de ataque

“Teremos cada vez mais abrangência de acessos com o 5G. Além disso, haverá mais máquinas autônomas conectadas na rede, um número maior de análises em tempo real com a inteligência artificial e respostas mais rápidas com o aprendizado de máquinas. Com toda essa complexidade, quase tudo será uma potencial porta de entrada para atacantes entrarem nos sistemas de empresas, expor dados, causar fraudes e consequentes prejuízos financeiros.”

Cleverson Arashiro, VP Infosec e IT Infra na Loft

Insider Threat

“Gradativamente, a segurança cibernética e a maturidade das empresas estão aumentando. Certos ataques comuns terão mais dificuldade para serem bem-sucedidos. Por isso, a chamada Insider Threat (ameaça interna) vai aumentar. O método consiste em cooptar o funcionário de uma empresa e usá-lo para ‘abrir as portas’ da organização para o cibercriminoso entrar.”

José Luiz Santana, Head of Cibersecurity do C6 Bank

Ciberterrorismo

"Outra tendência preocupante é o aumento de ataques como os de ciberterrorismo, espionagem militar e industrial e ameaças contra infraestruturas críticas, desenvolvidos por grupos criminosos profissionais e estado-nações. Esses ataques afetam diretamente a estratégia de segurança de economias e sociedades e são considerados armas digitais de elevada complexidade técnica, com objetivos e alvos pré-definidos, paralisar e destruir seus alvos."

Marcelo Camara, Chief Security Advisor da Microsoft

Suply Chain Attack

"A busca por um fornecedor, que tem uma segurança mais fraca, também será um caminho mais recorrente para se chegar ao alvo (no futuro). Primeiramente atacam o parceiro para depois invadir o alvo. É o que chamam de Suply Chain Attack, ataque à cadeia de suprimentos. Tende a crescer mais devido ao aumento da maturidade das empresas."

José Luiz Santana, Head of Cibersecurity do C6 Bank

O objetivo será o mesmo no futuro?

"O objetivo e o dano nunca mudam. Os atacantes continuam buscando a indisponibilização ou roubo de informações confidenciais, com o intuito de varrer uma empresa do mapa ou colocá-la em descrédito por meio do dano em sua imagem."

José Luiz Santana, Head of Cibersecurity do C6 Bank

Glossário da cibersegurança

Assessment - Procedimento de auditoria interna, que avalia controles, processos e procedimentos, compondo um relatório que descreve a situação atual da segurança de informação organizacional.

Board - órgão corporativo que faz a supervisão dos trabalhos de uma organização, com a responsabilidade de guiar as estratégias

Backup - cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso de perda dos dados originais

CISO - É o diretor de segurança da informação. Ele é responsável por estabelecer e manter a visão, a estratégia e o programa da empresa para garantir que os ativos e tecnologias de informação sejam adequadamente protegidos

Criptografia - conjunto de técnicas computacionais que visa tornar informações indecifráveis para quem as acessa indevidamente

Criptomoedas - dinheiro virtual que utiliza códigos criptografados para realizar as transações

Cloud - ou computação na nuvem, permite acesso remoto a softwares, armazenamento de arquivos e processamento de dados

Cyber Range - ambiente que simula um ambiente digital totalmente comprometido a fim de treinar os profissionais para estarem preparados quando um acontecer um ataque cibernético

Dark Web – área da internet menos regulamentada construída em redes de sobreposição que só podem ser acessadas por meio de um software especial

Deep Web – área da internet que, por razões técnicas, não é considerada pelos principais mecanismos de pesquisa

Endpoints - qualquer dispositivo que seja, fisicamente, um "ponto final" em uma rede

Engenharia Social – técnica usada por cibercriminosos para explorar as pessoas, induzindo-as a enviar dados críticos

Ethical Hacking – processo em que um profissional de Segurança da Informação trabalha para encontrar vulnerabilidades de segurança

Fábrica inteligente - termo usado para designar fábricas que mapear, analisar e utilizar dados gerados na produção de forma automatizada . Também é conhecido como indústria 4.0

Firewall - sistema de segurança de rede de computadores que restringe o tráfego da Internet para, de ou em uma rede privada

Framework - conjunto de códigos prontos com diversas funções que podem ser utilizados no desenvolvimento de sites

Gap - brecha, lacuna. Interrupção de algo ou do seu prosseguimento

IAM - Gerenciamento de Acesso e Identidade, é uma tecnologia que gerencia quem pode acessar o que em um ambiente digital

Insider Threat – colaboradores corrompidos que fornecem acesso a dados estratégicos aos cibercriminosos

Logs - registros das ações realizadas nos sistemas

MFA - Autenticação Multifator. É quando é adicionada uma camada a mais de segurança, ou seja, quando os usuários precisam fornecer mais dados para provar a sua identidade, como as próprias digitais ou um código recebido no dispositivo

MSSP - do inglês Managed Security Services Providers. São empresas que proveem serviços gerenciados de segurança para outras empresas, através de um SOC – Security Operations Center.

Nativas Digitais - empresas que já surgiram em um modelo de negócio totalmente digital, operam e comercializam os seus produtos e serviços nesse mesmo ambiente

On-premise - ambientes on-premise são aqueles estruturados dentro do espaço físico de uma empresa ou instituição

Pentest - também conhecido como método de intrusão, é um exercício que testa a segurança de uma empresa de várias formas

Phishing – ações enviadas por cibercriminosos para enganar usuários a fim de roubar informações estratégicas

Playbooks - conjunto de ferramentas, condições, lógica de negócios, fluxos e tarefas usadas para responder a eventos de segurança e ameaças em um ambiente

Privacy by design - implementação de medidas de segurança que garantem a privacidade dos dados desde a fase de concepção do produto ou serviço

Quick wins - forma de encontrar soluções eficientes, de baixo custo e alto impacto em resultados empresariais em curto prazo

Repositórios - sistemas que servem para armazenar, preservar e organizar informações

Restore - ação de recuperar os dados armazenados em determinado dispositivo durante a rotina de backup, garantindo que todas as informações gravadas estejam intactas

Security by Design – prática que considera a segurança desde o início no processo de desenvolvimento de um produto ou serviço

SIEM - Gerenciamento de Informações e Eventos de Segurança é uma solução que permite análise de ameaças em tempo real, gerenciar logs, ter uma visão ampla dos registros e das atividades no ambiente de TI

Sistemas de detecção de intrusão - sistema que monitora uma rede em busca de eventos que possam violar as regras de segurança dessa rede

SOC - Centro de Operações de Segurança, instalação que comporta profissionais especializados em segurança da informação para monitorar e analisar o ambiente continuamente e agir sempre que houver um comportamento suspeito

Sistema Legado – tecnologias mais antigas que ainda estão em uso nas organizações

Superfície de ataque - são as inúmeras possibilidades que um atacante possui para tentar invadir um dispositivo ou sistema

Token - dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador

Visual design - segmento do design que contribui para uma melhor composição visual de produtos, serviços e da identidade das empresas

VPN - Rede Privada Virtual, serviço que cria uma rede privada entre os dispositivos, levando mais privacidade ao usuário e proteção às informações que trafegam pela rede

Galeria de lideranças

Conheça os executivos que ajudaram a produzir o guia de cibersegurança

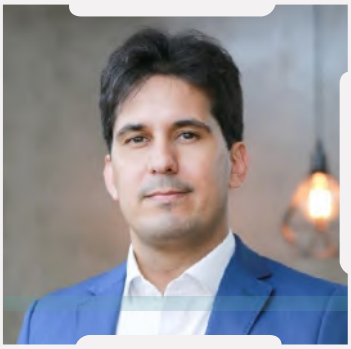
Bruno Guerreiro
Security Operations Advisor
Datasec

Carla do Couto
da área de cybersecurity e Data Privacy
TozziniFreire Advogados

Celso Hummel
head comercial e especialista em cybersecurity
First Tech

Cleverson Arashiro
VP Infosec e IT
Loft

Douglas Brancaglion
Head CyberSecurity
Memed



Douglas Rocha
gerente executivo de Segurança da Informação
Banco Inter

Eduardo Tamaki
Information Security Manager
Mevo

Fabiana Tanaka
CISO
Leroy Merlin

George Leal Jamil
professor, escritor e consultor de gestão e tecnologia

Guilherme Kato
CTO
dr. consulta

José Luiz Santana
Head of Cibersecurity
C6 Bank

Leandro Bissoli
sócio
Peck Advogados

Marcelo Camara
Chief Security Advisor
Microsoft

Maria Eugênia Lacerda
advogada de Cybersecurity e Data Privacy
TozziniFreire Advogados

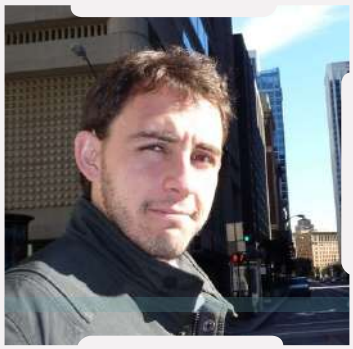
Norman Sabino
CTO
Provu

Nycholas Szucko
especialista em cibersegu-
rança e conselheiro
MID

Patricia Peck
sócia fundadora
Peck Advogados

Pedro Nuno
CISO
BMG

Samanta Oliveira
DPO
Mercado Livre



Rodrigo Veiga
diretor de Cibersegurança
OLX Brasil

Vanessa Pádua
Diretora, Cybersecurity
América Latinca e Caribe
Microsoft

Vinicius Fiel
superintendente de
Segurança da Informação
Porto

Vasco Pineda
Brazil Launcher
Yuno

Willians Santos
CISO
Banco Carrefour

MOVIMENTO
INOVAÇÃO
DIGITAL

A mais relevante comunidade de Líderes de Tecnologia, Cibersegurança e Proteção de Dados

Mais de **150 empresas inovadoras** associadas, dentre nativas digitais e grandes corporações em transformação.

Uma agenda setorial totalmente dedicada à:

- TROCA DE EXPERIÊNCIAS
- NETWORKING
- CONSTRUÇÃO DE CONHECIMENTO COLABORATIVO
- MELHORES PRÁTICAS
- GERAÇÃO DE NEGÓCIOS
- PROPÓSITO DE DESENVOLVIMENTO MERCADOLÓGICO

REALIZAÇÃO: MOVIMENTO INOVAÇÃO DIGITAL

APOIO: FIRST TECH, Microsoft, Peck Advogados, Tozzini Freire Advogados

CONTEÚDO E EDIÇÃO: INOVATIVOS

www.movimentoinova.com.br