Brasscom

Segurança da Informação e Segurança Cibernética

A Brasscom, Associação de Empresas de Tecnologia da Informação e Comunicação (TIC) e de Tecnologias Digitais, entidade sem fins lucrativos de representatividade nacional, e que congrega algumas das mais dinâmicas e inovadoras empresas de TIC alinhadas com a Era Digital, que prestam serviços de TIC, desenvolvem e licenciam software, fabricam e comercializam hardware ou que prestam serviços telecomunicações, e que tem como propósito trabalhar em prol de um Brasil Digital, Conectado e Inovador.

Temos a satisfação de compartilhar o presente relatório de Segurança da Informação e Segurança Cibernética. O trabalho, concebido e realizado pela Brasscom apresenta um compilado dos debates apresentado nas lives em nosso canal do YouTube sobre o tema. As demais informações foram retiradas de outras fontes e referências importantes no debate sobre Segurança da Informação, com a interpretação da equipe de Inteligência e Informação da Brasscom.

Brasscom Tecfórum Live-Impacto dos crimes cibernéticos e vulnerabilidades em Segurança da Informação.

Brasscom Tecfórum Live - Segurança da Informação na Era da Inteligência Artificial.

Brasscom Tecfórum Live - Governança e Gestão de Risco em Segurança da Informação.

Resumo Executivo

O Brasil e o mundo vivenciaram diversos ataques cibernéticos durante as rápidas transformações das organizações e da população como um todo em utilizar ainda mais serviços digitais. Diversas técnicas de ataques foram e estão constantemente sendo criadas e aprimoradas. Esse crítico cenário colocou em evidência o desenvolvimento da confiança em ecossistemas digitais, pela proteção dos dados pessoais e pela segurança da informação.

As definições entre Segurança Cibernética e Segurança da Informação são:

- Segurança Cibernética: Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

- Segurança da Informação: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Resumo Executivo

Segurança Cibernética e Segurança da Informação é uma jornada, que exige constante desenvolvimento. O desenvolvimento da segurança é pautado em 3 pilares.

- **Processos**

  Devem ser bem definidos, abrangendo uma política de segurança que adote as melhores práticas.

  Nesse caso os padrões de segurança ou políticas atuam como norteadores para que as organizações busquem suas próprias normatizações.

- **Tecnologia**

  O uso de tecnologias como a Nuvem e Inteligência Artificial (IA) são fortes avanços na segurança da informação

  Enquanto a Nuvem democratizou o acesso à segurança, a IA atua aumentando a capacidade de responder, dinamicamente, a incidentes de segurança.

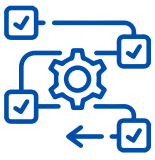
- **Pessoas**

  As vulnerabilidades são muitas vezes causadas em função de mau uso dos usuários, por isso a importância da cultura da Segurança da Informação: é necessário informação, educação, esclarecimento e de acúmulo de experiência e para empresas formações e treinamentos para funcionários.

O desenvolvimento da segurança tem avançado no Brasil:

- Brasil salta 52 posições no Ranking Global de Segurança Cibernética entre 2018 e 2020.

- Segurança da Informação deverá ter investimento de R$ 46,7 bi entre 2022 e 2025, com uma taxa de crescimento de 10% a.a.



A Relevância da Segurança da Informação e da Segurança Cibernética

A escalada dos ataques e dos prejuízos das ações criminosas ao explorar novas vulnerabilidades em ambientes digitais solapam a confiança necessária para tornar a sociedade cada vez mais conectada e digital. O Brasil e vários outros países sofreram os importantes ataques cibernéticos nos últimos dois anos e a previsão é que 2022 seja marcado pela continuidade dos ataques, especialmente de ransomware. Ressalta-se, portanto, a importância da priorização da Segurança da Informação e da Segurança Cibernética, no âmbito governamental e privado, como caminho para garantir a higidez das infraestruturas e dos serviços e a confiança no avanço da Era Digital.

Principais ataques em 2021 – Brasil e Mundo

JAN
- TRF-3 foi alvo de ataque DDoS e sequestro de dados de 223 milhões de brasileiros.
- Grupo Ultra é alvo de ransomware.

FEV
- Criminoso anunciou venda de informações da CPFL Energia.
- Hacker tenta envenenar água na Florida.

MAR
- Vulnerabilidade 0-day no Microsoft Exchange Server foi divulgada.
- Divulgada vulnerabilidades na maioria das versões BIG-IP.

ABR
- TJ:RS foi vitima de ransomware.

MAI
- Ataque de hackers a maior óleoduto dos EUA fez governo declarar estado de emergência.
- JBS é vitima de ransomware.

JUN
- O Grupo Fleury ficou com sistema fora do ar por uma semana.
- Electronic Art sofreu ataque e teve dados da FIFA e Frostbite roubados

JUL
- Sistema de trens e o governo do Irã são interrompidos após ataque.
- Kaseya VSA sofreu ataque de ransomware.

AGO
- Lojas Renner foi vitima de ransomware.
- Gigabyte Technology foi vitima de ransomware.

SET
- Hackers vazam senhas de 500 mil contas de VPN da Fortinet

OUT
- Código-fonte do sistema do Enem foi vazado.
- Invasão hacker rouba dados de toda população Argentina.

NOV
- Unicred, Atento, CVC e Porto Seguro sofreram ataques.
- Violação de segurança da GoDaddy expõe dados de usuários do WordPress

DEZ
- Grupo LAPSUS$ ataca Ministério da Saúde e outros órgãos do Governo.
- Apex Brasil foi vitima de ransomware.

Definições

O termo cibersegurança possui diversas definições que são similares entre si. Algumas dessas definições estão dispostas a seguir.

Dicionários

- Oxford Dictionaries: Online define segurança cibernética como: O estado de proteção contra o uso criminoso ou não autorizado de dados eletrônicos, ou as medidas tomadas para conseguir isso.
- Priberam Dicionário: Online define como segurança relacionada com o universo cibernético e as redes de comunicação entre computadores.

Organizações

- National Institute of Standards and Technology - NIST: capacidade de proteger ou defender o uso do ciberespaço contra ataques cibernéticos.
- ISO/IEC JTC1/SC27 IT - Security Techniques - ISO/IEC 27032:2012: preservação da confidencialidade, integridade e disponibilidade das informações no ciberespaço.
- European Network and Information Security Agency - ENISA: refere-se à segurança do ciberespaço em relação aos objetos acessíveis através de uma rede de telecomunicações generalizada, e ao conjunto de objetos próprios que permitem acesso ou participação em ações de controle dentro desse ciberespaço.
- European Network and Information Security Agency - ENISA: refere-se à segurança do ciberespaço em relação aos objetos acessíveis através de uma rede de telecomunicações generalizada, e ao conjunto de objetos próprios que permitem acesso ou participação em ações de controle dentro desse ciberespaço.

Definições

A definição presente no Glossário do Gabinete de Segurança Institucional (GSI) – Brasil:

Segurança Cibernética. Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Segurança da Informação. Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

> Eu costumo falar com muitos que eu entendo a segurança da informação como tendo duas abordagens: uma abordagem que eu chamaria de estática, que comporta a gestão de risco, proteção perimetral e a higidez de todo o ambiente; e outra, que eu chamo de dinâmica, que é o combate aos incidentes.

Sérgio Paulo Gallindo, Presidente da Brasscom.

Estática

Envolve a implementação de um conjunto adequado de controles que inclui políticas, processos, procedimentos, estrutura organizacional.

Política Controles Processos Estrutura

Governança

Dinâmica

Práticas de segurança de operações para garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético.

Regulamento Criptografia Software e Hardware

Tecnologias de Defesa

Rol Exemplificador de Ataques Cibernéticos

Os ataques correspondem a qualquer ação que comprometa a segurança da organização. Quando um ataque é bem-sucedido causa dano de diversas magnitude à organização.

Exemplos de técnicas que geram vulnerabilidades

Engenharia Social: Uma tentativa de induzir alguém a revelar informações (por exemplo, uma senha) que podem ser usadas para atacar sistemas ou redes.

Phishing: Uma técnica para tentar adquirir dados confidenciais, como números de contas bancárias, por meio de uma solicitação fraudulenta por e-mail ou em um site, na qual o criminoso se disfarça de empresa legítima ou pessoa respeitável.

Ataques de Força Bruta: Utiliza criptoanálise para buscar exaustivamente a descoberta de senhas nos mais variados meios tecnológicos, web, servidores, ativos de rede etc.

Fake News: O compartilhamento de fake news e os processos de desinformação são pontos chave no cenário atual de ataques digitais.

Rol Exemplificador de Ataques Cibernéticos

Exemplos de técnicas que exploram as falhas

Negação de Serviço (DoS e DDoS). Interromper um serviço, um ou mais computadores conectado à internet, com a geração de sobrecarga no processamento do computador alvo ou no tráfego de dados da rede à qual o alvo está conectado.

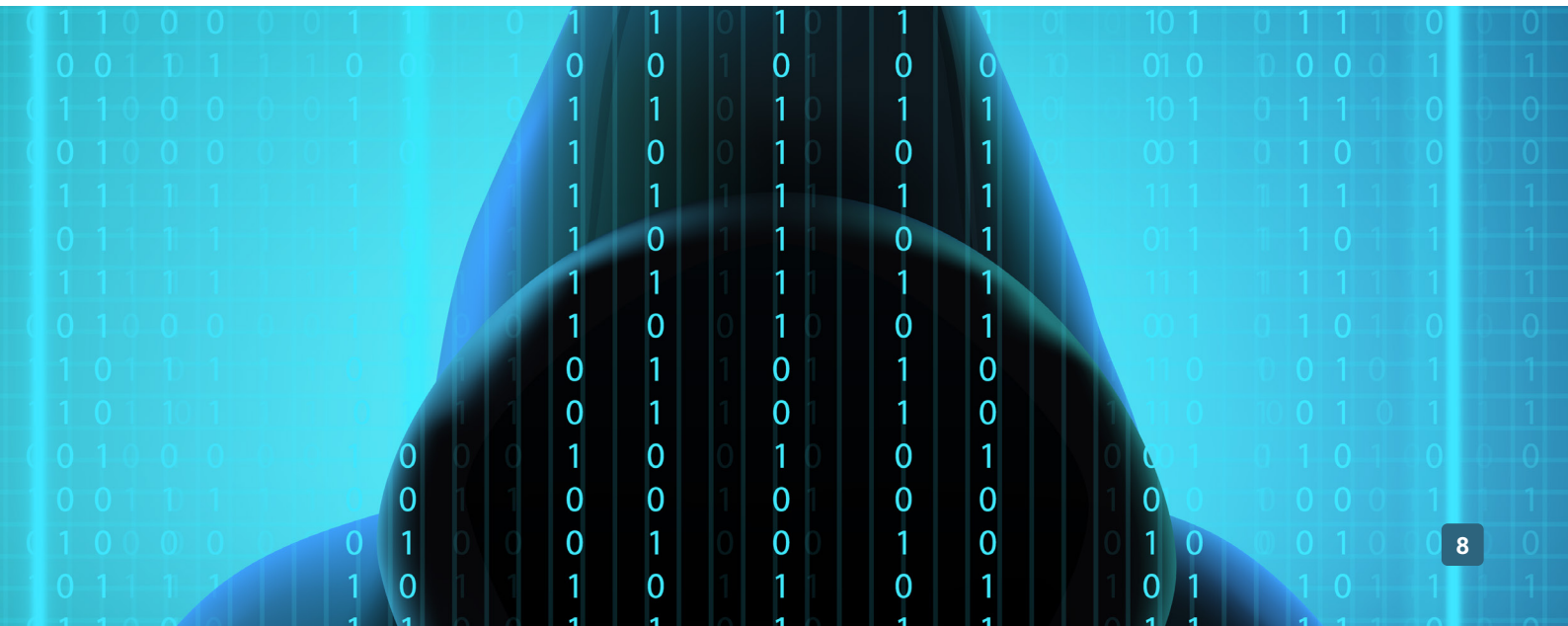
Pharming: Usar meios técnicos para redirecionar os usuários para acessar um site falso disfarçado de legítimo e divulgar informações pessoais.

IP Spoofing: Falsificar o endereço de envio de uma transmissão para obter entrada ilegal em um sistema seguro.

Malware: Programas maliciosos que se infiltra e obtém controle sobre um sistema de computador ou dispositivo móvel para roubar informações valiosas ou danificar dados, tais como: vírus, cavalos de tróia, adware, spyware, backdoors, keyloggers, worms, bots e rootkits.

SIM Jacking: O criminoso usa várias técnicas que geram vulnerabilidade, geralmente engenharia social, para transferir o número de telefone da vítima para o seu próprio cartão SIM com objetivo de redefinir as senhas ou receber códigos de verificação e acessar contas protegidas

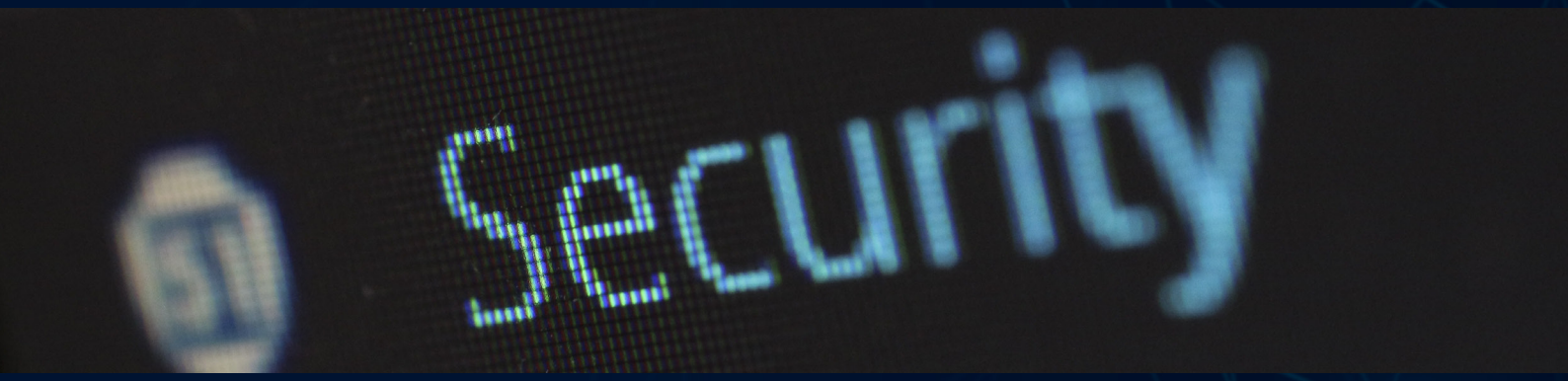
Nota: Existem outros tipos de técnicas de ataques e que estão constantemente se sofisticando e sofrendo modificações. Fonte: Brasscom, NIST (https://csrc.nist.gov/glossary) ; Europol, 2020; Mascarenha Neto e Junqueira. Segurança da Informação: Uma visão sistêmica para implantação em organizações 2019;



Importância da Segurança da Informação e da Segurança Cibernética

A Segurança da Informação e a Segurança Cibernética impactam todas as instâncias e níveis dentro de uma organização e por isso é essencial que as instituições, tanto pública quanto privadas, façam o gerenciamento de riscos no âmbito da segurança da informação, que consiste no processo de identificar, quantificar e gerenciar os riscos para estabelecer meios de minimizar as vulnerabilidades e mitigar os danos dentro da organização.

Muito embora, o gerenciamento de risco não seja uma prática obrigatória, é extremamente indicada, principalmente com o acelerado avanço da transformação digital das empresas. Essa prática é um importante elemento da boa governança, pois aumenta a transparência e a capacidade das organizações em lidarem com incertezas para que os objetivos sejam alcançados.



> ...a segurança cibernética não é apenas uma questão tecnológica. Todo mundo que trabalha em segurança sabe que é um tripé de processos, tecnologia e pessoas.

Alexis Aguirre, Diretor de Cybersecurity para América Latina da Unisys

Gestão de Risco

A **Gestão de Risco** visa **conter e prevenir a possibilidade de impactos negativos** sobre objetivos pretendidos, caso alguns dos riscos avaliados venham a se concretizar. Portanto, o g**erenciamento de riscos** objetiva **reduzir ao mínimo possível os impactos dos riscos sobre a própria organização e terceiros**, com a adoção de melhores práticas de infraestrutura, políticas e metodologias, tendo em mente a tecnologia disponível; o custo de implementação; a natureza, escopo, contexto e finalidade das atividades de processamento do controlador de dados; e a probabilidade e magnitude dos riscos envolvidos.

Considerando a ampla variedade de tratamento de dados realizados por diferentes tipos de organizações, é importante manter uma flexibilidade em torno da metodologia de análise de risco de modo que as especificidades de cada organização e da natureza dos dados que ela trata possam ser ponderados como parte desse processo de avaliação. Nesse sentido, **as organizações podem se basear nas diversas metodologias de avaliação e gerenciamento de risco existentes e que melhor respondem aos seus modelos de negócios**.

> (...) Entenda tudo aquilo que pode interferir no processo de geração de valor e comece sabendo quem são as ameaças do seu negócio, se a sua ameaça é um funcionário interno descontente, se a sua ameaça é um hacker, se a sua ameaça é um país; entenda quem pode ameaçar a prosperidade do seu negócio, se é um fraudador de sistema financeiro, se ele está interessado no dinheiro ou na informação e o que ele pode fazer com isso.
>
> **Daniel Aviz - Gerente de Segurança da Informação TOTVS**

Fonte: Brasscom, 2017; CPIL, 2014 ; CPIL, 2016.

Gestão de Risco

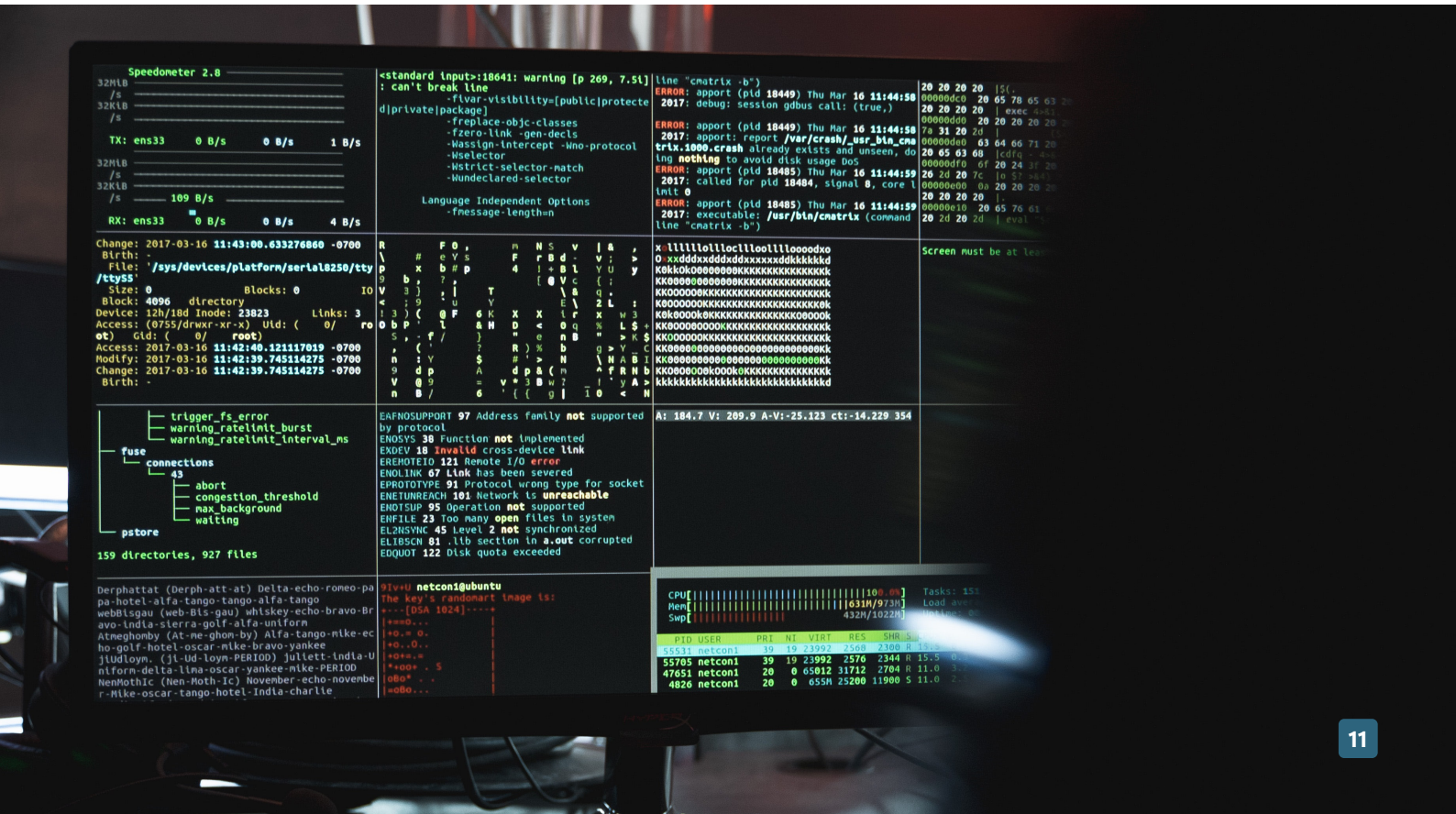
Avaliação de risco

A **ENISA** define a avaliação de risco como um processo científico e tecnológico composto por três etapas: identificação de riscos, análise de risco e avaliação de risco . O escopo da avaliação é coordenar o uso de recursos e monitorar, controlar e minimizar a probabilidade e/ou o impacto de eventos infelizes que possam colocar em risco a informação de interesse para a segurança da sociedade e do Estado.

Gerenciamento de risco

O **NIST** diz que o gerenciamento de riscos é o processo contínuo de identificação, avaliação e resposta ao risco. Para gerenciar riscos, as organizações, públicas ou privadas, devem entender a probabilidade de um evento ocorrer e o impacto resultante. Com esta informação, podem determinar o nível aceitável de risco para a entrega de serviços e sua tolerância ao risco. Com uma compreensão da tolerância ao risco, pode haver priorização das atividades de segurança da informação e segurança cibernética, permitindo que decisões conscientes sobre os gastos com segurança da informação e/ou segurança cibernética sejam tomadas.

Fonte: Brasscom, 2017; CPIL, 2014 ; CPIL, 2016.



Padrões de Segurança

Para orientar as organizações sobre as melhores práticas de segurança da informação, diversos órgãos, nacionais e internacionais, consolidaram normas e boas práticas para alcance efetivo da segurança em seu ambiente.

NIST *Privacy framework*

Desenvolvido pelo US National Institute of Standards and Technology's, elaborado em colaboração com uma série de organizações, oferece um **conjunto de ferramentas para viabilizar uma estratégia de privacidade para as organizações** que desejam aprimorar sua forma de utilizar a proteger os dados pessoais; também oferece detalhadamente explicações sobre conceitos de gerenciamento de risco. O NIST não se trata necessariamente de uma lei ou regulação do setor, mas sim uma ferramenta de uso voluntário que pode ajudar as organizações a melhor gerenciarem seus produtos e serviços em função da segurança.

Metodologia ENISA

Contribui para a Gestão de Risco através da análise e classificação de informação na área dos riscos emergentes das ameaças digitais e fornece um Inventário de Gestão de Riscos e Métodos e Ferramentas de Avaliação de Riscos. Além disso, disponibiliza direcionamentos para melhorar a sua postura de cibersegurança de pequenas e médias empresas e para estruturas críticas.

"A gente se baseia nessas normas de segurança. Porém, colocamos "um molho" de percepção do especialista. Agora, quando a gente fala da percepção de risco, de ter essa visão um pouco mais holística, de ter esse sentimento, esse feeling, aí você precisa ter um especialista, precisa ser o especialista, por exemplo, do processo de manufatura, aquele especialista que está efetivamente no dia a dia; de repente, não é nem o diretor e nem o operador da máquina, mas é uma pessoa que tem a visão de todos os processos, que sabe como funciona, sabe onde o calo aperta, onde está pegando efetivamente, onde podemos melhorar, ele já tem essa noção e visões muito claras de risco."

Sergio Ribeiro - Consultor e Pesquisador de Segurança da Informação no CPqD

Padrões de Segurança

Normas ISO

Em 2001, a Associação Brasileira de Normas Técnicas (ABNT), traduziu a norma britânica **BS 7799:1999**, e publicou a **NBR/ISO 17799** – Código de Práticas para a Gestão da Segurança da Informação e, a partir de 2010 a ABNT publicou outras versões da série de normas conhecidas como família **NBR ISO/IEC 27000**.

Com destaques para:

- **ISO 27001:2013**, integra um conjunto de políticas, procedimentos e processos que formam o Sistema de Gestão da Segurança e Informação, uma estrutura central que permite às organizações adotar uma consistência para os seus exercícios de gestão de risco e segurança da informação.

- **ISO 27005:2018** sustenta os conceitos aplicados da ISO 27001 e delineia como as organizações podem identificar os perigos de segurança da informação, priorizar suas maiores ameaças e selecionar um curso de ação apropriado. Esta norma também contém passos que as organizações podem tomar para atingir a resiliência cibernética para proteger processos comerciais críticos.

- **ISO 31000:2018** apresenta um conjunto de diretrizes para a gestão de riscos enfrentados por quaisquer organizações.

Fonte: Brasscom, 2021; Mascarenha Neto e Junqueira: Segurança da Informação: Uma visão sistêmica para implantação em organizações, 2019

Governança da Segurança da Informação

Marcos Semola (2014) entende que,

> [...] um dos principais desafios da implementação da segurança da informação é a falta de planejamento sistêmico das ações e processos a serem colocados em prática.

Embora a opinião do autor são seja recente, o fato é que o nível de maturidade das empresas e órgãos públicos no que tange a Governança da Segurança da Informação é ainda bastante dispare, variando deste organizações altamente preparadas até organizações que ainda não estão sequer conscientizadas.

É fundamental estabelecer uma **Governança** organize a contínua identificação dos riscos e as ações preventivas e corretivas necessárias para garantir a segurança da informação e a defesa de ataques. Neste contexto, o desenvolvimento de uma **Política de Segurança** da Informação, internas ou públicas, poder atuar como norteadores no seio das nas organizações.

O **Macrossetor de TIC** tem empresas altamente maduras e especializadas de que podem prestam serviços a para outras organizações, em particular que têm como modelos negócio diverso ao de tecnologia, propondo governança, desenvolvendo de estratégia tecnológica e até mesmo ofertando o outsourcing completo do arcabouço de segurança da informação e de segurança cibernética.

Fonte: Brasscom, Semola, Marcos. Gestão da segurança da informação: uma visão executiva. 2 ed. Rio de Janeiro: Elsevier, 2014.

Política de segurança da informação

Iniciativa em âmbito governamental

Política Nacional de Segurança da Informação - PNSI

Estabelecimento de estrutura e modelo de governança para a integração e a coordenação nacional das atividades de segurança da informação, em um cenário de crescentes ataques cibernéticos e elevada interdependência das tecnologias da informação, bem como evitar superposições, concorrências e redundâncias de ações e tarefas que afetam o cidadão e o Estado brasileiro. O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) coordena uma série de ações voltadas para a implementação da PNSI no âmbito da administração pública federal, com desdobramentos nas administrações subnacionais. A PNSI foi instituída pelo Decreto nº 9.637/2018.

GSI - Órgão do governo brasileiro responsável pela assistência direta e imediata ao Presidente da República no assessoramento pessoal em assuntos militares e de segurança

> PNSI conta com dois grandes instrumentos, que são: a Estratégia Nacional de Segurança da Informação e o Plano Nacional de Segurança da Informação. No âmbito da Estratégia Nacional, nós temos publicada a ***E-Ciber***, que é a ***Estratégia Nacional de Segurança Cibernética***, e a ***Estratégia Nacional de Segurança de Infraestruturas Críticas***. E está em andamento, no âmbito dos Planos, a elaboração do Plano Nacional de Gestão de Incidentes Cibernéticos e o Plano Nacional de Segurança das Infraestruturas Críticas.
>
> Nós temos um papel de coordenação, que é diferente de controle(...) Temos o papel de normatizar e de ser aquele ponto inicial para que as próprias organizações busquem aprimorar as suas normatizações, para que elas não fiquem sem ter um norte.

Marcelo Fontenele - Diretor do Departamento de Segurança de Informação do Gabinete de Segurança Institucional da Presidência da República

Fonte: Brasscom; GSI, 2020

Segurança da Informação é um requisito da Lei Geral de Proteção de Dados (LGPD)

A **Segurança da Informação** é fundamental para que as instituições se adequem à **LGPD**. Afinal, a segurança é um dos 10 princípios que estruturam como requisito básico de conformidade.

A **LGPD** estabelece diversas responsabilidades e controles que devem ser implementados por entidades públicas e privadas que efetuam o tratamento de dados pessoais.

1. Finalidade
2. Adequação
3. Necessidade
4. Livre acesso
5. Qualidade dos dados
6. Transparência
7. Segurança
8. Prevenção
9. Não discriminação
10. Responsabilidade de prestação de contas

Portanto, não há proteção de dados sem Segurança da Informação

> A LGPD veio para ajudar as empresas a melhorarem os seus processos. O foco da LGPD são as pessoas e os dados das pessoas, sejam elas do mundo digital ou do físico. Essa disciplina que existe para a captação de dados, para a utilização dos dados das pessoas, para a comunicação com as pessoas, é muito importante. A segurança é parte do negócio hoje em dia, ela não pode ser mais tratada como simplesmente: "eu estou com um antivírus mais potente, eu resolvo todos os meus problemas

Adriano Frare - Especialista de Segurança Sênior da Cast Group

Fonte: Brasscom, Ministério da Cidadania, 2021

A Segurança da Informação denota diligência na Proteção de Dados

Joacil Rael - Membro do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD).

A evolução tecnológica se refere principalmente à tecnologia da informação e comunicação. Os crimes cibernéticos são cada vez mais sofisticados e exploram as vulnerabilidades dos sistemas (...) Se alguém pensa que consegue eliminar todas as vulnerabilidades, certamente está errado. As vulnerabilidades são encontradas em softwares, em hardwares, em recursos humanos - até poderia dizer que é principalmente em softwares.

Deve-se minimizar as vulnerabilidades com **medidas administrativas e medidas técnicas disponíveis.**

Após estabelecidos, implantados e monitorados, estas medidas devem ser periodicamente revisadas buscando melhorias com vista de assegurar que os objetivos específicos de segurança e do negócio sejam atendidos.

Medidas Administrativas

- Desenvolvimento de estudos
- Política de segurança da informação
- Conscientização e treinamento de recursos humanos em TIC
- Gerenciamento de contratos

Medidas Técnicas

- Controle de acesso
- Segurança dos dados pessoais armazenados
- Segurança das comunicações
- Manutenção de programa de gerenciamento de vulnerabilidades
- Medidas relacionadas ao uso de dispositivos móveis
- Medidas relacionadas ao serviço em nuvem
- Versões atualizadas dos sistemas e adequadamente configuradas
- Senha forte - dupla autenticação quando possível
- Não instalar produtos sem saber o que está instalando
- Usar criptografia sempre que possível

Fonte: Brasscom; ANPD, 2021

Segurança da Informação nas empresas

Boas práticas para o desenvolvimento da Segurança da Informação nas empresas:

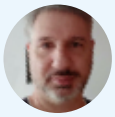
- **Identificar e mensurar as vulnerabilidades**
- **Criar Métricas** para verificar a resiliência do negócio, exemplo: "quanto tempo o site pode ficar fora do ar?"
- **Armazenamento da Informação** para avaliar qual informação deverá ser mantida
- **Escolha da Segurança** deve-se pautar na confiança, daquele parceiro que vai ser o melhor nos momentos de crise.
- **Maturidade**, os responsáveis pela empresa devem trabalhar para conscientizar até o menor nível, e para isso deve haver,
- **Comunicação** entre todos os funcionários, para que qualquer problema possa ser relatado e tratado.

Fonte: Brasscom; ANPD, 2021

Segurança da Informação nas empresas

Daniel Aviz - Gerente de Segurança da Informação TOTVS

Cada ambiente que a gente coloca no ar tem um risco de exposição, tem um nível de vulnerabilidade, e você nunca vai conseguir zerar isso. O que você tem que fazer é manter isso num nível de controle mínimo para garantir que o negócio continue funcionando. Quando você identificar essas vulnerabilidades ou essas suas fragilidades, você vai ter que priorizar, porque são muitas. A gente, que está do lado que defende, tem que defender todas as fronteiras, mas quem está atacando só precisa de uma para fazer um estrago.



Adriano Frare - Especialista de Segurança Sênior da Cast Group

Eu sempre digo: não compre segurança, adquira confiança de que ele vai ser seu parceiro, de que ele vai te atender nas suas necessidades, nos seus momentos de crise, na sua cadeia de suprimento, é a confiança de que você está fazendo o melhor junto com o seu parceiro, junto com o seu fornecedor. Tem muita empresa que fala: "eu vou adquirir uma solução de segurança", mas não é a ferramenta que dá segurança, é escolher a melhor ferramenta, o melhor parceiro para estar junto com você nesses momentos.

Não existem só ferramentas, existem as pessoas por trás disso. A ferramenta, a tecnologia não vai resolver isso. Então, esse conhecimento que você estava compartilhando com os seus demais e, também, com a sua cadeia de fornecedores é muito importante. Você não está sozinho no mundo, você depende dos outros.

A importância da Cultura de Segurança da Informação

Guilherme Aquino - Coordenador do laboratório de segurança cibernética do Inatel

(...) o ponto principal é a questão da cultura da segurança. Eu vou puxar um pouco para o meu lado, que é a academia. A academia tem uma função principal nesse ponto. A gente precisa acordar e acordar rápido para começar a colocar na cabeça dos nossos alunos, até antes da academia, ainda no Ensino Médio, a questão da cultura, do aculturamento com relação à segurança.

Joacil Rael - Membro do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD)

Para se criar uma cultura, a gente precisa de muitas coisas: informação, educação, esclarecimento e de acúmulo de experiência. No meio empresarial, podemos acrescentar formações e treinamentos como agregadores na construção dessa cultura.

- **41%** das empresas possuem algum tipo de política de segurança da informação.
- **63%** entre as médias empresas adotaram políticas de segurança digital
- **74%** entre grandes empresas implantaram políticas de segurança da informação.
- **37%** entre as pequenas empresas possuem políticas de segurança da informação.
- **65%** das empresas do setor de TIC possuem algum tipo de política de segurança da informação.

Fonte: Nic.Br, 2020;

José Gontijo - Diretor do Departamento de Ciência, Tecnologia e Inovação Digital do Ministério das Ciências, Tecnologias, Inovações e Comunicações

Existe um trabalho muito grande sendo feito na Secretaria de Governo Digital, pelo GSI na Estratégia de Cyber segurança Nacional, no âmbito da Estratégia Brasileira de Transformação Digital. É um trabalho de vários atores, em que o Governo é uma pequena parcela. Aqui no Governo, a gente pensa muito na defesa das informações governamentais, mas talvez a maior fragilidade seja na ponta, nas pequenas e médias empresas que, quiçá, sabem o que é cyber segurança. Quando muito, elas colocam firewall ou um antivírus AVG gratuito para proteger as suas redes e muitas vezes não faz o efeito que poderia fazer.

Fonte: Brasscom, 2021

A Importância dos Usuários na Prevenção das Ameaças

No Brasil, segundo Núcleo de Informação e Coordenação do Ponto BR (NIC.BR), **poucas empresas implantaram iniciativas que envolvem os funcionários com pautas de segurança digital**:

21% das empresas aplicam treinamento sobre segurança digital.
33% das empresas tem a segurança digital como pauta em suas reuniões.
22% das empresas mencionam segurança digital em seus contratos.
18% das empresas têm incentivos de desempenho para redução de risco de digital.

- Brasil sofreu mais de **16,2 bilhões** de tentativas de **ataques cibernéticos** na primeira metade de 2021
- Brasil foi o **5º maior alvo** de crimes digitais no mundo em 2021
- Pico do **ransomware e phishing** em plena covid-19

Fonte: Brasscom; Fortinet, 2021; Instituto Igarapé; RNP, 2020, NIC.BR, 2020;

Grande parte das vulnerabilidades são causadas em função de mau uso dos usuários, que não estão devidamente treinados, então o treinamento e a conscientização do usuário é importante.

Marcelo Copati - Diretor de Cybersegurança da TIVIT

Aculturamento dos Usuários nas Empresas

Os dados reportados pelo NIC.BR apontam para um **cenário desafiador** dentro das empresas em relação ao treinamento dos funcionários e a implementação e iniciativas que os envolvam na atuação da segurança digital.

O **aculturamento dos usuários** diminui as exposições das vulnerabilidades, pois um dos responsáveis pela segurança cibernética é o próprio usuário de um dado sistema.

Os **funcionários devem receber orientações e treinamentos** para evitar atitudes que possam expor falhas a serem exploradas.

A garantia da s**egurança da informação depende de todos os atores**. Todos desempenham uma importante função no aperfeiçoamento, manutenção e construção de uma sociedade resiliente e preparada para combater os desafios de segurança.

Marcelo Zillo - Diretor de sucesso do cliente para segurança cibernética Microsoft

"Eu costumo dizer que a Segurança da Informação deveria ser um assunto de domingo da mesa de família. Eu fazia isso antes da pandemia, quando eu estava em família: "como você protege o seu Zap Zap?", "como eu projeto o meu Zap Zap?", "é, deixa eu te mostrar um negócio". "Tio, como você protege rede social? Você sabe que tem um negócio chamado MFA?"

Guilherme Aquino - Coordenador do laboratório de segurança cibernética do Inatel

"Eu vi uma frase esses dias, infelizmente não vou lembrar o autor, que disse o seguinte: "se você acha que todos os seus problemas de segurança vão ser solucionados com tecnologia, você não entende nem de tecnologia nem dos seus problemas". Ou seja, o ponto principal é a questão da cultura da segurança."

Fonte: Brasscom; Fortinet, 2021; Instituto Igarapé; NIC.BR, 2020.

O Papel da Tecnologia na Segurança da Informação

Dentro das dinâmicas sociais e corporativas o papel da tecnologia desempenha e assume obrigatoriamente uma abordagem de **segurança da informação** para proteção os dados pessoais e corporativos e minimizar os riscos dos ataques cibernéticos.

A **tecnologia pode facilitar e democratizar** a implementação de soluções de segurança da informação, tornando-as possíveis para pequenas e médias empresas que não poderiam arcar com custos elevados como as grandes organizações.

Uma **tecnologia** que tem esse perfil é **nuvem**, que apresenta um ambiente muito parecido com a segurança aplicada em datacenters locais, só que sem os custos de manutenção das instalações e do hardware. Na nuvem, utiliza-se f**erramentas de segurança** baseadas em software de proteção e monitoramento do fluxo de informações dentro e fora deste ambiente sem a necessidade de gerenciar servidores físicos ou armazenar em dispositivos.

Além da democratização, com a finalidade de reforçar a segurança de ambientes em nuvem tem sido aplicado o **princípio de confiança zero** que entende que todas as etapas estão susceptíveis a ataques e por isso a solução é criação de protocolos de autenticação e validação de cada etapa.

Marcelo Zillo - Diretor de sucesso do cliente para segurança cibernética Microsoft

A nuvem democratizou a segurança. Se você olhar para o passado, só empresas com muito investimento conseguiam implementar bons controles de segurança: tinha que comprar muita tecnologia, comprar hardware, configurar, ter equipes, etc.. Com a nuvem, você consegue comprar recursos de segurança como serviço e não precisa fazer grandes investimentos, então isso democratiza, significa que: uma empresa pequena, média e grande podem ter o mesmo nível de segurança, com custos muito próximos.

Marcelo Copati - Diretor de Cybersegurança da TIVIT

A nuvem facilita de forma absurda, porque você coloca os controles nos seus endpoints, independentemente de eles estarem conectados, ou não, à sua rede. Isso facilita muito, isso democratiza muito a segurança, isso facilita, em todo tamanho de empresa, colocar controles de segurança nos endpoints, para que os funcionários acessem de forma mais segura os seus ambientes.

Fonte: Brasscom; Grupo Redes, 2022; AWS Amazon – informações retiradas do site: https://aws.amazon.com/

O Papel da Tecnologia na Segurança da Informação

Outra tecnologia que tem sido aplicada para dinamizar e aprimorar a segurança são as soluções de ferramentas baseadas em **Inteligência Artificial (IA)**.

Essas soluções podem **detectar a invasão e diminuir o tempo de permanência** - período de tempo que um invasor cibernético tem domínio livre em um ambiente desde o momento em que entra até ser erradicado. Em Dezembro de 2019, na Europa, o tempo de permanência era de cerca de 177 dias, e invasores foram descobertos em apenas 44% dos casos devido a violação de dados ou outros problemas. Utilizando técnicas de IA, o tempo de permanência foi drasticamente reduzido.

As soluções de IA ainda sofrem certa resistência de adesão por parte das organizações. Pensando nisso, o NIST tem trabalhado junto da comunidade de Inteligência Artificial para identificar os requisitos técnicos necessários para cultivar a confiança de que os sistemas de IA são precisos e confiáveis, seguros e protegidos, explicáveis e livres de preconceitos.

No entanto, a falta de profissionais com qualificações em IA tem se apresentado com uma barreira no avanço da adesão dessa tecnologia.

Alexis Aguirre - Diretor de cybersecurity para América Latina da Unisys

> A capacidade de responder, dinamicamente, a incidentes de segurança, ou seja: se há algum comportamento anômalo, a inteligência artificial ajuda bastante as tecnologias de UEBA, User and Entity Behavior Analytics, ou seja, numa análise de comportamentos estranhos/anômalos de usuários, a inteligência artificial ajuda muito.

Rodrigo Jorge - CISO da Neoway Business Solutions

> Um grande problema da indústria é a falta de profissionais de segurança da informação qualificados. Por que se fala tanto em inteligência artificial nesse mercado? É para tentar suprir falhas humanas.

Fonte: Brasscom; Optiv – Dicionário; Matt Walmsley: Intervenção na live no YouTube Cybersecurity@CEPS Summit 2019, [3:05:40]); NIST – informações do site: www.nist.gov.

O Papel da Tecnologia na Segurança da Informação

Além de Nuvem e Inteligência Artificial, o uso de **criptografia** é que cada vez mais importante para **garantir segurança** para transações de comércio eletrônico, uso de dispositivos móveis e demais trocas de dados.

Para Australian Cyber Security Centre - **ACSC** - a **criptografia** objetiva a **confidencialidade, integridade, autenticação e irretratabilidade dos dados**. Ao aplicar criptografia, se protege os dados tornando-os ilegíveis para todas as entidades, exceto as autorizadas, protegendo contra manipulação acidental ou deliberada.

O **Estudo Global sobre Tendências em Criptografia** do ***Ponemom Institute*** (2021), realizado com **6.610 indivíduos** de diversos setores em **17 países**, revelou que **50%** dos participantes relataram que a empresa tem um plano ou estratégia geral de **criptografia implementado de forma consistente**, e **37%** relataram que a empresa tem um **plano ou estratégia** limitado aplicado a **determinados aplicativos e tipos dados**.

A **ENISA** entende a **criptografia** como elemento chave da **privacidade** e da **proteção aos dados confidenciais** e indica que sempre que possível as pequenas e médias empresas também devem utilizar criptografia para proteger seus dados, principalmente ao utilizar redes públicas. Além disso, possui recomendações dos requisitos de medidas de **proteção criptográficas** aplicáveis no contexto de **dados pessoais** e dos algoritmos, comprimentos de chave, parâmetros e protocolos com distinção para **aplicação em sistemas implementados e projetos futuros**.

O **NIST** tem **padrões criptográficos** aplicáveis à dispositivos móveis, caixas eletrônicos e dados federais ultrassecretos. Além disso, corrobora com governos, indústrias e academias em todo o mundo para desenvolver padrões e diretrizes de criptografia mais fortes e confiáveis.

Fonte: Ponemom Institute, 2021; ACSC - https://www.cyber.gov.au/; ENISA - https://www.enisa.europa.eu; NIST-https://www.nist.gov/

O Papel da Tecnologia na Segurança da Informação

Use criptografia sempre que possível. Eu costumo dizer que a segurança não depende só da criptografia, depende de muitos fatores, mas onde não tem a criptografia não tem, por exemplo, o sigilo de uma informação ou de um dado.

O desenvolvedor de um sistema já deve prever, em um projeto, a proteção dos arquivos que precisam ser protegidos. Ele vai desenvolver criptografia para isso? Tipicamente, não. As pessoas não estão nem preparadas para isso. Mas tem esses recursos criptográficos disponíveis em bibliotecas criptográficas abertas e basta o desenvolver ir lá, pegar, puxar o código, adequar ao seu sistema e dar proteção àquilo a que precisa dar proteção.

Joacil Rael - Membro do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD)

O Papel do Indivíduo na Segurança da Informação

O uso corriqueiro de sistemas informatizados integrados por meio de redes é uma característica da sociedade atual. Essa característica também implica na necessidade de condutas que evitem exposição das vulnerabilidades dos sistemas utilizados.

Muito embora as tecnologias de segurança sejam importantes, elas por si só não são capazes de resolver os problemas de SI integralmente e aqui entra o papel do indivíduo na segurança da informação.

A conscientização de que todos possuem papéis sejam da tecnologia, da indústria e dos indivíduos, é o primeiro passo rumo à confiança no ecossistema digital.

Boas práticas para dia-a-dia dos indivíduos:

- Escolha de senhas fortes;
- Nunca divulgue ou compartilhe senhas pessoais;
- Alteração periódicas de suas senhas;
- Preferencialmente não utilizar senhas iguais para serviços diferentes;
- Utilize a autenticação de dois fatores;
- Leia as políticas de privacidade e uso do aplicativo;
- Mantenha antivírus sempre atualizado e pleno funcionamento;
- Não ignore notificações sobre detecção de ameaça;
- Mantenha opção de backup ativada;
- Cuidado com redes de wi-fi não seguras;
- Não abrir e-mail de remetentes desconhecidos;
- Sempre verifique a URL dos sites que irá acessar;
- Não insira seus dados pessoais em sites duvidosos;
- Mantenha-se atualizado sobre boas práticas de segurança da informação.

Fonte: Brasscom; Legal Grunds Institute – Guia de boas práticas de segurança da informação, 2021

O Papel do Indivíduo na Segurança da Informação

Alexis Aguirre - Diretor de cybersecurity para América Latina da Unisys

Então, realmente a conscientização de qual é o papel de cada um como usuário, ou como público, ou como usuário corporativo, é fundamental para segurança da informação.

Rodrigo Jorge - CISO da Neoway Business Solutions

É bem importante a conscientização de todos que estão nesse ecossistema: tecnologia, usuários, indústria. Nunca vai existir uma bala-de-prata que vá resolver um problema. A bala-de-prata seria a conscientização, conscientizar que a segurança e a responsabilidade é compartilhada, seja com quem consome a informação (o sistema, a tecnologia) ou seja com quem produz, que faz um setup.

Brasil Salta 52 Posições no Ranking Global de Segurança Cibernética

Índice Global de Segurança Cibernética (GCI)

Ranking Mundial

70ª
2018

18ª
2020

O Brasil tem avançado no tocante a segurança cibernética

Índice Global de Segurança Cibernética (GCI)

Ranking da América

6ª
2018

3ª
2020

Fonte: Brasscom; UIT, 2018; UIT 2020;

Autoavaliação, não euxariente, da maturidade em Segurança da Informação

Conhece-se as pessoas que têm acessos administrativos ao ambiente? Elas realmente precisam desse nível de acesso?

O acesso remoto a ambientes críticos e de usuários administradores requerem múltiplo fator de autenticação (senha + token, por exemplo)?

Os protocolos de acesso remoto são rotineiramente atualizados e criptografados?

O comprimento mínimo das senhas é superior a 14 caracteres para ambientes incompatíveis com múltiplos fatores de autenticação?

Você pessoalmente e a sua corporação possuem backup dos dados críticos? São efetuados testes contínuos de recuperação dos dados?

Os dados críticos estão criptografados, tanto em trânsito quanto em repouso?

A varredura de vulnerabilidades é realizada mensalmente, pelo menos? Em quanto tempo é realizada a correção das vulnerabilidades a partir da respectiva identificação?

Testes de invasão são realizados pelo menos uma vez por ano para sistemas críticos?

Adota-se algum tipo de filtragem de e-mails maliciosos?

Adota-se controles para monitorar a segurança das estações de trabalho, além dos antivírus?

Os logs dos ambientes críticos são coletados e armazenados por tempo adequado à necessidade?

Há conscientização e treinamento sobre o uso adequado de tecnologia e sobre segurança da informação e segurança cibernética?

Existe clareza quanto aos riscos causados por uma falha de segurança ou por um ataque cibernético?

Perspectivas de Investimentos 2022–2025 (R$ bilhões)

Segurança da Informação - R$ 46,7 bi (10% a.a)

Inteligência Artificial - R$ 49,7 bi (18% a.a)

Nuvem e Datacenter - R$ 181,8 bi (24% a.a)

Perspectivas de mercado para a Segurança da Informação em 2022

Ajustes nas práticas de Segurança Cibernética em ambientes de nuvem será um dos principais **desafios** dos gestores de TI.

57% das empresas afirmam que contarão com **apoio externo** focado em gerenciar e operar ambientes com soluções de segurança mais modernas. Os serviços de segurança totalizarão quase **US$ 1B** no Brasil, enquanto que as **soluções de segurança, em hardware ou software**, superarão **US$ 860M**.

A **otimização** das práticas de **segurança de gestão e proteção dos dados** receberá maior atenção das lideranças.

O **5G** no Brasil movimentará **US$ 25,5B** até **2025** e impulsionará diversas tecnologias, inclusive tecnologias de segurança.

Melhoria da segurança compõem os **principais KPIs de avaliação** de sucesso nas implementações de IoT pelas organizações.

Fonte: Brasscom; IDC (Black Book 3ª Plataforma, 2021 H1); IDC- Predictions, 2022

Outros documentos da Brasscom sobre o tema

1. Contribuições à minuta da política nacional de Segurança da Informação. Clique aqui para acessar os anexos.

2. Contribuições à consulta pública referente à estratégia nacional de Segurança Cibernética (E-Ciber) Clique aqui para acessar os anexos.

Inteligência e Informação

Liderança

Sergio Paulo Gallindo
Presidente Executivo

Mariana Oliveira
Diretora Executiva

Coordenação

Helena Loiola Persona
Especialista em Inteligência

Equipe

Stephanie Felix Sieber
Analista de Inteligência

Tainá Ferreira de Melo
Analista de Inteligência

Kyem Araújo dos Santos
Analista de Inteligência

Identidade Visual

Luély Vaz Barbosa
Analista de Comunicação

Sara Mendes do Nascimento
Diagramação e arte

Brasscom

A Brasscom – Associação das Empresas de Tecnologia da Informação e Comunicação (TIC) e de Tecnologias Digitais – promove o setor de TIC junto atores públicos e privados e entidades representativas, de forma fundamentada, propagando tendências e inovações, intensificando relações, propondo políticas públicas e promovendo a Era Digital, competitividade, educação e segurança jurídica.