ALLAN KOVALSCKI | ANDREY GUEDES OLIVEIRA

SEGURANÇA DA INFORMAÇÃO

MENTE ABERTA

RGB
DA GOVERNANÇA À ESPERANÇA

IGCP
INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO

ALLAN KOVALSCKI | ANDREY GUEDES OLIVEIRA

SEGURANÇA DA INFORMAÇÃO

MENTE ABERTA

RGB DA GOVERNANÇA À ESPERANÇA ®

IGCP INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO

CIP – Brasil. Catalogação na fonte

Oliveira, Andrey Guedes; Kowalscki, Allan -
Segurança da informação / Andrey Guedes Oliveira e Allan Kowalscki – Salvador, BA: Editora Mente Aberta, março de 2025.

102 p.
ISBN: 978-65-6023-137-5
ISBN Digital: 978-65-6023-138-2

1. Proteção de dados. 2. Segurança da informação. I. Oliveira, Andrey Guedes. II. Kowalscki, Allan. III. Título.

CDD 658

REDE GOVERNANÇA BRASIL – RGB

DIRETORIA EXECUTIVA

Presidente – Cristiane Nardes
Vice-presidente - Lucas Paglia
Diretoria Administrativo-Financeira – Cíntia Caroline
Diretoria de Relações Institucionais – Elise Brites
Diretoria de Assuntos Estratégicos – Cláudio Boros
Compliance officer –Anna Dantas
Diretoria de Governança – Sandra Vespasiano
Diretora de Comunicação e Marketing – Claudia Cataldi
Diretoria de Novos Negócios e Projetos –Flávio Feitosa
Diretoria de Relações Governamentais – Guilherme Zapponi
Diretoria Acadêmica e Científica – Elflay Miranda

CONSELHO DE ADMINISTRAÇÃO

Presidente – Paulo Renato Menzel
Conselheiro titular – Henrique Farinon
Conselheira titular – Luana Lourenço
Conselheiro suplente – José Augusto Viana

CONSELHO DE ÉTICA

Presidente – Fernando Nardes
Conselheira titular – Sheila Campos
Conselheira titular – Andréa Esper

CONSELHO FISCAL

Presidente – Alexsandro da Silva
Conselheira titular – Viviane Obadowski
Conselheiro titular – Walter Marinho
Conselheiro suplente – Guilherme Nunes

OUVIDORIA

Valdir Bianchesi

COORDENAÇÃO DA OBRA

Dinaura Tedesco
Kelly Soares Fonseca

COMITÊ RESPONSÁVEL PELO PROJETO

Comitê de Governança em LGPD e Segurança da Informação

GERENTE DE OPERAÇÕES

Cíntia Caroline da Silva e Silva Reis

AUTORES DO PROJETO

Allan Kovalscki
Andrey Guedes Oliveira

INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO – IGCP

PRESIDENTE

Ricardo Todeschini Zilio

CONSELHO FISCAL

Conselheiro – Luiz Gustavo Wiechoreki

DIRETORIA EXECUTIVA

Dinaura Tedesco
Henrique Farinon

CARTA AO LEITOR

Olá, caro leitor!

Seja muito bem-vindo a esta jornada pelo universo vital e fundamental que é a segurança da informação. Antes de iniciarmos a jornada nos capítulos que compõem este livro, quero aproveitar este espaço para destacar a importância desse tema, tão contemporâneo e estratégico a todos, organizações e cidadãos.

Encontramo-nos em um ambiente hiperconectado, com serviços e aplicações que realizam desde ações de transação bancárias, ampliações, estudos, apoio ao negócio, redes sociais, e-Gov, saúde on-line etc. Em um cenário em que todos utilizam, direta ou indiretamente, serviços na internet, as informações e ativos de tecnologia são alvos de interesse de atores maliciosos; logo, proteger esses ativos tornou-se prioridade máxima, tanto para empresas quanto para governos ou mesmo para nós, como indivíduos. A cada clique, transação e compartilhamento, colocamos em movimento uma cadeia invisível de confiança que precisa ser reforçada todos os dias. É aí que entra a segurança da informação, não como um obstáculo à inovação, mas como o alicerce que a sustenta.

Este livro foi pensado para oferecer uma visão completa, prática e estratégica dos principais pilares da segurança da informação. Seja você um profissional da área buscando atualização, um gestor que precisa tomar decisões críticas, um estudante curioso ou alguém simplesmente preocupado com a própria privacidade digital – este conteúdo foi feito para você.

O que você vai encontrar por aqui?

Dividimos este livro em capítulos cuidadosamente organizados para criar um fio condutor lógico e progressivo, indo do técnico ao estratégico, do conceito à prática. Vamos abordar:

• *tecnologias por ambiente*: entenda como diferentes contextos – nuvem, redes locais, dispositivos móveis – exigem abordagens distintas de proteção;

• *políticas de segurança e privacidade de dados*: descubra como normas, regulamentos e boas práticas estruturam a proteção desde o papel até à realidade operacional;

• *sistemas de proteção*: antivírus, *firewalls*, criptografia, autenticação multifatorial... explicamos como essas camadas se combinam para criar defesas eficazes;

• *zero trust*: conheça essa abordagem moderna que parte de um princípio simples, mas revolucionário: *nunca confie, sempre verifique*;

• *monitoramento de segurança*: explore ferramentas e processos que mantêm os olhos sempre abertos, detectando anomalias e agindo proativamente;

• *recuperação de desastres e continuidade de negócios (BCM)*: prepare-se para o inesperado com estratégias que mantêm serviços operacionais, mesmo em cenários críticos;

• *gestão de incidentes*: do planejamento à resposta, saiba como lidar com vazamentos, ataques e falhas sem perder o controle;

• *integração, interoperabilidade e inclusão digital*: porque segurança da informação também é uma questão de acesso, equidade e colaboração entre sistemas e pessoas.

Mais do que conceitos técnicos, este livro defende a ideia de que segurança da informação é também **cultura**, **comportamento** e **visão de futuro**. Em um mundo hipe conectado, proteger a informação é proteger pessoas, relações, reputações e sonhos.

Um convite à reflexão e à ação

Escrevemos cada página pensando em você. Buscamos traduzir complexidades, oferecer exemplos práticos e provocar reflexões que ultrapassem o aspecto técnico. Afinal, não se trata apenas de proteger sistemas, mas de proteger **valores, dados sensíveis e, em última instância, a confiança**.

Espero sinceramente que você encontre aqui não só respostas, mas também novas perguntas. Que cada capítulo te inspire a adotar práticas mais seguras, a repensar estratégias e, acima de tudo, a **fazer da segurança uma aliada no seu caminho pessoal e profissional**.

Boa leitura, boa reflexão e boa jornada!

Com estima,

Andrey Guedes Oliveira
Especialista em Segurança da Informação

PALAVRAS DO EMBAIXADOR

Segurança da informação

Estimados(as) leitores(as),

A transformação digital acelerou a troca de dados e a integração dos sistemas em tempo real. Se, por um lado, as tecnologias ajudam a resolver problemas e tornar os processos mais modernos e eficientes, por outro aumentou a vulnerabilidade a ataques cibernéticos e violações de dados. Com isso, a segurança da informação não é apenas mais uma alternativa, e sim uma necessidade para as empresas, fundações, cooperativas, órgãos públicos e secretarias públicas.

Em 26 de dezembro de 2023, por meio do Decreto n. 11.586, o governo federal anunciou a instituição da Política Nacional de Cibersegurança (PNCiber), cujo objetivo é enfrentar crimes e ações maliciosas em ambientes virtuais e tecnológicos.

Com isso, este material, que será atualizado com novas tecnologias e melhores práticas, segue as diretrizes do decreto, apresenta a importância da segurança da informação para a sociedade. Ela é um fator determinante para a manutenção dos serviços digitais e, por conseguinte, um instrumento protetivo contra crimes cibernéticos, fraudes, vazamento de dados e possibilidade de auditoria (governança), dentro da visão dos especialistas Allan Kovalscki e Andrey Guedes Oliveira.

A presente obra que, inclusive, traz um glossário de termos digitais para que o(a) leitor(a) entenda a linguagem de forma mais prática e eficiente, aborda assuntos relacionados às diversas tecnologias que apoiam serviços e processos que são utilizados amplamente no setor privado e público.

Tecnologias por ambiente e políticas de segurança e privacidade de dados; sistemas de proteção; monitoramento de segurança; recuperação de desastre e incidente de segurança da informação; gestão de incidentes de segurança e integração, interoperabilidade e inclusão digital ganha estão entre os temas discutidos no rico conteúdo dos autores.

Allan Kovalscki e Andrey Guedes Oliveira fazem parte da Rede Governança Brasil (RGB), com voluntários que atuam em diferentes temáticas com intuito de fomentar mecanismos de liderança, estratégia e controle na administração pública brasileira. Atualmente, a instituição conta com o trabalho de comitês, seminários, fóruns, prêmio RGB, mentoria de prefeitos, cartilhas e produtos, dentre outros.

Desejo, caro(a) leitor(a), que esta obra possa auxiliá-lo(a) a dar esse grande passo nesse tema tão relevante que é segurança da informação, e que seja um norte para orientar interessados no tema, instituições governamentais e privadas, nas ações e estratégias para proteção de informações. Abraço carinhoso do embaixador da RGB!

Ministro Augusto Nardes

GLOSSÁRIO DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

AIN – Análise de Impacto nos Negócios

AN – Análise de Negócios

ANPD – Autoridade Nacional de Privacidade de Dados

ANS – Acordo de Nível de Serviços

API – Application Program Interface (Interface de Programação de Aplicações)

AV – Antivírus

BA – Business Analytics (Análise de Negócios)

BCI – Business Continuity Institute (Instituto de Continuidade de Negócios)

BCM – Business Continuity Management (Gerenciamento da Continuidade de Negócios)

BDGC – Banco de Dados de Gerenciamento de Configuração

BIA – Business Impact Analysis (Análise do Impacto ao Negócio)

Carta – Continuous Adaptive Risk and Trust Assessment (Avaliação Contínua e Adaptavel de Risco e Confiança)

CM – Crise Management (Gerenciamento de Crises)

CMDB – Configuration Management Database (Banco de Dados de Gerenciamento de Configuração)

CMS – Configuration Management System (Sistema de Gerenciamento de Configuçõe)

CP – Contrato de Apoio

CX – Customer eXperience

DLP – Data Loss Prevention

DRP – Disaster Recovery Plan (Plano de Recuperação de Desastres)

EDR – Endpoint Detection andResponse (Reposta e Detecção de Ameaças e Computadores)

Gati – Gerenciamento de Ativos de TI

GCN – gerenciamento de continuidade de negócios

Gerenciamento de Ativos de Software (GAS)

GNS – Gerenciamento de Nível de Serviço

GSTI – Gerenciamento de Serviços de TI

IaaS – Infrastructure as a Service (Infraestrutura como um serviço)

IC – Item de Configuração

IC – Item de configuração

ICN – Instituto de Continuidade de Negócios

ICS – Incident Command System (Sistema de Comando de Incidentes)

IDPS – Sistemas de Detecção e Prevenção de Intrusões;

IDS – Intrusion Detection System (Sistemas de Detecção de Intrusões)

IDS – Intrusion Detection System (Sistema de Detecção Intrução)

IEEE – Instituto de Engenheiros Elétricos e Eletrônicos

IM – Incident Management (Gerenciamento de Incidentes)

IMT – Incident Management Team (Equipe de Gerenciamento de Incidentes)

IPS – Intrusion Prevention System (Sistemas de Prevenção de Intrusões)

IPS – Intrusion Prevention System (Sistema de Prevenção Intrução)

IRT Incident Response Team (Equipe de Resposta a Incidentes)

ISIM – Incidentes de Segurança da Informação

ISO – International Organization for Standardization (Organização Intercional de Padrões)

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission.

Itam – Information Technology Asset Management (Gerenciamento de Ativos de Tecnologia da Informação)

ITSM – Information Technology Service Management (Gerenciamento de Serviços de Tecnologia da Informação)

LGPD – Lei Geral Lei Geral de Proteção de Dados Pessoais

MFA – Multi Factor Authentication

MTBF – Mean Time Between Failures (Tempo Médio entre Falhas)

MTRS – Mean Time to Restore Service (Tempo Médio para Restauração de Serviço)

NBR – Norma Brasileira

NIST – National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos)

OTR – Objetivo de Tempo de Recuperação

PaaS – Plataform as a Service (Plataforma como um Serviço)

PDP – Policy Decision Point (Política de Ponto de Decisão)

PEP – Policy Enforcement Points (Política de Ponto Mandatório)

Peste – Política, Económica, Social e Tecnológica

Pestle Política (P), Economia (E), Social (S) e Tecnologia (T)

PoC – Proof of Concept (Prova de Conceito)

RaaS – Ransomware as a Service (Ransomware como Serviço)

RDI –Retorno do Investimento

RTO – Recovery Time Objetive (Tempo de Restauração de um Objeto)

S.O – Sistema Operacional

SaaS – Software as a Service (Software como Serviços)

SAM – Software Asset Management (Gerenciamento de Ativos de Software)

SGC – Sistema de Gerenciamento de Configuração

Siem – Security Information Event Management (Sistema de Gerenciamento de Eventos e Informações de Segurança)

SLA – Service Level Agreement (Nível de Serviço Aceito)

SLM – Service Level Management (Gerenciamento do Nível de Serviço)

Soar – Security Orchestration Automation and Response (Sistema de Automação, Orquestração e Resposta)

SVS – Sistema de Valor do Serviço

SVS – The Service Value System (Sistema de Valor de Serviços)

TI – Tecnologia da Informação

TMEF Tempo Médio entre Falhas

TMRS – Tempo Médio para Restaurar o Serviço

UX – User eXperience (Experiência de Usuários)

UX – User eXperience

VBFS – Features of Virtual Business Services

VPN – Virtual Private Network (Redes Privadas Virtuais)

VRI – Valor do Retorno de Investimento

WAF – Web Application Firewall (Firewall de Proteção a Aplicações na Web)

XC – eXperiência do Cliente

XU – eXperiência do Usuário

ZTNA – Zero Trust Network Access (Acesso a Rede via Confiança Zero)

ZTNS – Zero Trust Network Security (Segurança de Rede via Confiança Zero)

GLOSSÁRIO DESCRITIVO

API (Application Program Interface): caracteriza–se por uma camada de software e protocolos de comunicação que proporcionam integração entre sistemas, com a terceirização de tarefas por meio dessa integração. Exemplo: um comercio eletrônico utiliza a chamada de uma API do cartão de crédito ou débito para pagamentos em seu comercio virtual, sem ter a necessidade de realizar um sistema de pagamentos próprio.

Bluetooth: Padrão para tecnologia de comunicação de dados e voz, baseado em radiofrequência e destinado à conexão de dispositivos em curtas distâncias.

Cloud Computing: Sistemas de Processamento remoto via Internet, com categorias de Infraestrutura como Serviços IaaS (*infrastructure as a service*), PaaS – *plataform as a service* (plataforma como serviço) e SaaS – *software as a service* (software como serviço).

Criptografia: Trata–se da utilização de técnica para embaralhar as informações, a fim de torná–la incompreensível;

Dados Pessoais: Informações que identifiquem um titular (CPF, CNPJ, RG, CNH, e–mail etc.)

Dispositivos Computacionais Móveis: Dispositivo computacional pessoal de mão capaz de armazenar informações e de comunicar–se a partir de redes sem fio (incluindo celular e/ou Wi–Fi), tais como, smartphones, tablets e PDAs.

Dispositivos de Rede: Sistemas e ferramentas que sejam parte da infraestrutura de rede, tais como, roteadores, switches, firewalls, servidores de cache e de proxy, e balanceadores de carga.

Dispositivos Removíveis de Armazenamento: Qualquer dispositivo portátil ou removível que armazena informação eletrônica e que pode ser facilmente removido e transportado (por exemplo, disco rígido portátil, pen drive, cartão de memória, CD, DVD, fita ou dispositivo de back–up etc.).

Estação de trabalho: Computador de uso profissional não portável.

Hardware: Todo e qualquer equipamento físico;

ISO/IEC 27002/2013: É uma norma internacional contendo controles para a Segurança da Informação;

MITRE ATT&CK: o acrônimo de Adversarial Tactics, Techniques, and Common Knowledge que é uma base global de comportamentos, diretrizes e classificação de ataques cibernéticos.

Notebook ou Laptop: Computador móvel de uso profissional;

***On premises*:** a expressão é relaciona a sistemas locais e não em nuvem, exemplo: adquira–se um software por aluguel ou licenciamento no servidor local, na escolha do licenciamento local a indústria relaciona como um sistema *on premises*.

P2P: Rede para compartilhamento de arquivos;
RaaS (Ransomware as a Service): grupos criminosos que vendem códigos como serviço para fins ilícitos como parte de um modelo de serviço.

SFTP: Protocolo de transferência segura de arquivos;

Sistemas: Sistemas de Usuários e Sistemas de Servidores.

Sistemas de Servidores: Sistemas computacionais compartilhados, incluindo servidores que fornecem arquivo e impressão, colaboração, grupos de trabalho, mensagem instantânea, transferência de arquivos, aplicações, ou serviços de e–mail.

Sistemas de Usuários: Dispositivo computacional pessoal utilizado por um usuário final, incluindo desktops, laptops, estações de trabalho, e Dispositivos Computacionais Móveis.

Software: Todo e qualquer programa de computador, utilizado dentro ou fora da empresa;

Site2Site: quando uma rede local possui uma conexão virtual, criptografada / segura, com outra rede via Internet.

VPN (Virtual Private Network): são redes virtuais com sistemas de criptográficas que proporcionam acesso remoto seguro de uma estação de trabalho para uma rede autônoma ou uma relação direta entre uma rede e outra.

Wi–Fi: Sistema de rede sem fio baseada no protocolo do IEEE 802.11 amplamente utilizado em redes locais.

Unidade de disco externa: Qualquer dispositivo eletrônico móvel que seja capaz de armazenar, exibir e transferir informações. (*Pendrives*, Disco externo, Smartphones etc.)

TOR: Software que proporciona o anonimato na internet.

AUTORES E COLABORADOR

Andrey Guedes Oliveira – Autor dos capítulos Tecnologias por Ambiente e Políticas de Segurança e Privacidade de Dados, Sistemas de Proteção, Monitoramento de Segurança e Recuperação de Desastre e Incidente de Segurança da Informação.

Fundador da ESCS (Esyner Cyber Security) autuando como empreendedor e principal executivo (CEO, CISO e DPO) da empresa pioneira na implementação do conceito de Zero Trust no Brasil. Membro do comitê de LGPD na Rede Governança Brasil.

Mestre em Engenharia de Telecomunicações pela PUC de Campinas, MBAs em Gestão Empresarial e Projetos, especialista em Segurança da Informação e Formado em Administração com ênfase em Análise de Sistemas. Extensões acadêmicas na Universidade da California e Florida International Business School.

Executivo de tecnologia e segurança da informação por mais de 20 anos. Experiência com foco na Governança, Gestão de Serviços de TI, Sistemas e Projetos no mercado nacional e internacional. Participação em processos de startup e fusão de empresas. Gestão Orçamentária (rentabilidade e redução de custos) e de P&L – Capex e Opex.

Participante de projetos voltados ao Desenvolvimento Agil de Software, CISM, Gestão de Pessoas, Plano e Investimentos, Gestão Orçamentária, Cloud Computing, Inovação, APM, Produtos, Canais, Gerenciamento de Projetos (PMI/PRINCE2) de Implantação (ITO, TCO e Arquitetura), Contratos e Pré–Vendas. Lider de Projetos baseados em interfaces com Transformação Digital, Negócios, Business Cases e Team building. Domínios Técnicos em Tecnologia: Cloud Com-

puting (AWS, Google e Azure), Agile, Scrum, Lean, ITIL, Cobit, PMI, Six–Sigma, ERP (SAP/TOTVS), CRM, BI, B2B, B2C, HR and Tax, Infraestrutura, Desenvolvimento de Sistemas/Software e Administração de Banco de Dados. Certificações: CCISO (EC COUNCIL), CloudMicrosoft AZ–900;Cisco CCNA, CCNP; Fortinet NSE 4.0; EXIN Privacy and Data Protection Practitioner (PDPP);Data Protection Officer (RBC–CDPO);APM, ISO 20000; ITIL Foundation, COBIT, ITIL: RCV (Release, Control and Validation)/OSA (Operational Support and Analysis)/PPO (Planning, Protection and Optimization); APPGATE RANGER/COMMANDER; HCIA, HCIP, EC–Council: CND.

Allan Kovalscki – Autor do capítulo Gestão de Incidentes

Fundador da GCRC Desenvolvimento, mestrando em Administração, com ênfase em Governança Corporativa, MBA em Gestão Empresarial, MBA em Governança Corporativa, Pós–MBA em Governança Corporativa e Risco, Pós–graduando em Ciência de Dados e Big Data Analytics, Pós–graduado em Gestão de Projetos, Pós Graduando LLM em Proteção de Dados: LGPD & GDPR, MBA em Segurança da Informação, MBA em Riscos Cibernéticos. Atualmente ocupa também a função de Diretor Geral da COMPLY LGPD Solutions, Diretor Técnico – CTO na Armin GRC, coordenador técnico do Fórum de Proteção de Dados Pessoais nos municípios, é membro da RGB – Rede Governança Brasil, foi membro do Comitê de Auditoria Estatutário do Grupo CEEE, sendo ainda professor e consultor na Fundação Universidade Empresa de Tecnologia e Ciências – Fundatec e professor convidado na FADISMA. Na Companhia Riograndense de Saneamento, empresa pública de economia mista, onde trabalhou por 20 anos, foi Superintendente de Controles Internos, Gestão de Riscos e Compliance, onde criou a área e implementou a metodologia e os processos de governança corpo-

rativa, gestão de riscos e compliance, foi Chefe do Departamento de Projetos e Processos, onde implementou o PMO da área de tecnologia na companhia e foi Superintendente de Tecnologia da Informação e Comunicação, tendo sido responsável pela implantação da Governança em TI, através do COBIT. Ainda, na Corsan, fez parte do Conselho Universitário e da Comissão de Ética. Possui certificação como DPO e certificações como Auditor Líder de Sistemas Integrados de Gestão em Compliance e Antissuborno, – Lead Assessor SIG ISO 19600:2014 e ISO 37001:2016, Gestão de Riscos e Continuidade de Negócios – Lead Assessor SIG ISO 31000:2009 e ISO 22301:2019, Gestão da Segurança da Informação e Gestão de Privacidade da Informação – Lead Assessor SIG ISO 27001:2005 e ISO 27701:2019.

Paulo Emerson de Oliveira Pereira – Colaborador

Graduado em Tecnologia de Processamento de Dados com ênfase em Administração e Direito (Ciências Jurídicas como começou o curso).

Especialista em Implantação em Software Livre, Direito Digital, Mediação, Infraestrutura de Ambientes Críticos, Perícia Forense Digital e Investigação Cibernética, Negócios Internacionais e com licenciatura para o magistério superior com ensino à distância. Atuo no mercado de TI nos últimos 35 anos e no jurídico nos últimos 10 anos.

Colaborador em importantes projetos e serviços no Brasil como a Câmara de Compensação Financeira Bancária – COMPE, Câmara de Compensação Financeira da Exploração Mineral CFEM, Portal de Visão de Despesa do Governo, Portal de Integração e Inteligência em Informações do Governo – i^3GOV, dos Padrões de Interoperabilidade do Governo Eletrônico – ePing, modelo de Arquitetura Referencial de Integração – ARI, do Termo de Ajuste de Conduta da Datamec.

DATAPREV (reestatização dos sistemas do Ministério do Trabalho e Emprego), modernização da DATAPREV, e atuante em Projetos de Lei para Lei Geral de Proteção de Dados Pessoais – LGPD e melhorias para os interesses da classe dos DPOs no Brasil através da Associação Nacional dos Profissionais em Privacidade de Dados – APDados.

Colaborador na Rede Governança Brasil – RGB nos comitês de LGPD e Governança e Riscos, onde o nosso slogan é “Da Governança à Esperança.”

SUMÁRIO


intro

1
INTRODUÇÃO

A presente obra vem proporcionar um guia para entidades governamentais e privadas para conhecimentos básicos e necessários para compreensão sobre o universo de segurança da informação em tecnologia da informação. O documento será atualizado com novas tecnologias e melhores práticas, assim como seguir as diretrizes da Política Nacional de Cibersegurança (PNCiber), estabelecida no Decreto n. 11.856, de 26 de dezembro de 2024.*

Adicionalmente, aborda temas relacionados às diversas tecnologias que apoiam serviços e processos que são utilizados amplamente no setor privado e público, bem como informações e conceitos sobre equipamentos de infraestrutura, programas ou softwares, tecnologias de nuvem, plataformas e integrações, entre outros.

Destaca-se a fundamental importância da segurança da informação, que se torna um fator determinante para a manutenção dos serviços digitais e, por conseguinte, um instrumento protetivo contra crimes cibernéticos, fraudes, vazamento de dados e possibilidade de auditoria (governança).

Num cenário de transformação digital e de dependência de procedimentos, processos, rotinas, programas e métodos, notam-se as diversas camadas de relacionamento digital, com integrações em um ambiente altamente conectado. Outro ponto importante a ser analisado são os fatores de riscos na internet, com serviços em nuvem, integrações entre sistemas, redes interconectadas e sistemas voltados para a mobilidade por meio de aplicativos para celulares. Exemplos

* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2023–2026/2023/decreto/D11856.htm.

disso são: sistema interno com chamadas para uma plataforma de integração (API), com os seus arquivos e correio eletrônico na nuvem; sistema de recursos humanos em uma plataforma on-line; colaboradores em regime de teletrabalho; reuniões on-line; servidor de impressão local; redes com wi-fi e redes cabeadas etc.

À conjuntura é somada a proteção dos dados privados pessoais pela Lei Geral de Proteção de Dados Pessoais (LGPD, coma redação dada pela Lei n. 13.853/2019), que propicia diversos aspectos protetivos, com papeis definidos no tratamento desses dados, assim como as boas práticas de segurança. Então, temos uma relação direta entre segurança da informação e privacidade de dados e, em vista disso, a obra vem trazer a relação direta para melhor compreensão com o foco na proteção digital.

Nesse contexto, a segurança da informação tornou-se um dos temas mais importantes temas, assim como a privacidade de dados.

A obra está organizada nos seguintes tópicos:

i) introdução;
ii) tecnologias e políticas de segurança e privacidade de dados;
iii) sistemas de proteção;
iv) monitoramento de segurança;
v) recuperação e incidente de segurança da informação;

Passemos, então, ao exame dos demais tópicos.

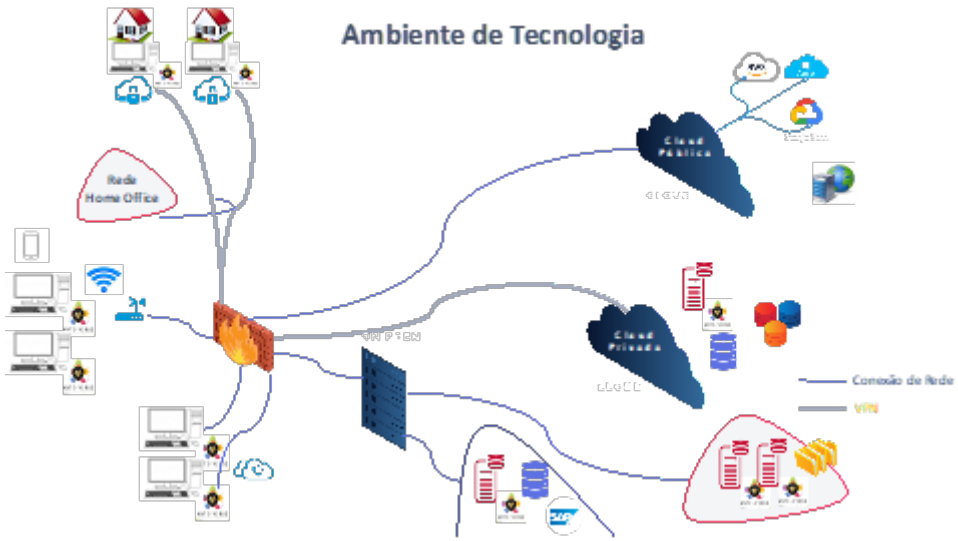

7
home
4
1
end

2
TECNOLOGIAS POR AMBIENTE E POLÍTICAS DE SEGURANÇA E PRIVACIDADE DE DADOS

Os ambientes tecnológicos, ilustrados na figura 1, representam os diversos ambientes com sistemas locais, remotos e em nuvem.

As políticas de segurança da informação e privacidade de dados são ações formais que ratificam as regras, controles, direitos e deveres. As políticas são amplamente utilizadas, assim como referenciadas no conjunto de normas da ISO, LGPD, NIST etc.

Figura 1 – Topologia computacional.



Fonte: elaborada por Andrey Oliveira.

2.1 TECNOLOGIAS DA INFORMAÇÃO (AMBIENTES)

As redes deixaram de possuir ambientes locais, com servidores de arquivos, impressão, correio eletrônico, entre outros, para adoção de tecnologias em nuvem, migração para *datacenters*, utilização de virtualização híbrida, com redes públicas, locais e privadas, sendo interconectadas por VPN.

A virtualização foi outro fenômeno que aumentou o ambiente computacional de empresas e governos. A barreira era a aquisição de hardwares específicos para projetos computacionais, no entanto, após a virtualização, com apenas um servidor, pode-se ter diversos servidores pessoais para atendimento a demandas tecnológicas, por óbvio, aumentando o risco devido à quantidade de servidores na rede.

Esse novo horizonte, alterado pelo advento das tecnologias em nuvem ou por serviços (Ciasullo; Lim, 2022) gerou novas oportunidades de negócios, automação de serviços, relacionamos com vantagem, desafios e novas oportunidades.

A nova conjuntura interligada por sistemas on–line, com ambientes híbridos que vão desde as redes tradicionais (locais) à interligação com nuvens privadas e públicas, criou um contexto, transformando os sistemas que outrora eram centralizados e com poucas variáveis em um modelo complexo, inter-relacionado e heterogêneo, ou seja, uma nova arquitetura tecnológica que, por conseguinte, gera novas oportunidades e ameaças que são traduzidas, atualmente, por ataques digitais e vazamento de dados.

Os ambientes de ação computacional são ambientes locais (*on premises*)* e seus servidores como ERP, AD, arquivos e impressão. As *clouds* privadas ou ambientes virtualizados estão em *datacenter*, com conectividade direta por meio

* A expressão é relaciona a sistemas locais, e não em nuvem. Exemplo: adquira-se um software por aluguel ou licenciamento no servidor local; na escolha do licenciamento local, a indústria relaciona como um sistema *on premises*.

de links diretos ou VPN Site2Site.* Já os serviços em nuvem pública, com sistemas por serviços SaaS (software como um serviço), PaaS (plataforma como um serviço) e IaaS (infraestrutura como um serviço), são elementos que interagem com usuários e sistemas via API, por consumo ou integração para que as empresas possam automatizar e realizar ações conforme o seu negócio. O interessante é que cada elemento possui registros (logs) que geram dados de segurança, podendo ser utilizados como um controle de segurança e auditoria.

As redes possuem ambientes e tecnologias. A seguir, temos a explicação deles, para melhor compreensão sobre tecnologias e como realizar a proteção de cada variável. Os ambientes estão divididos por função, conforme abaixo apresentado:

• *ambiente computacional interno*: rede destinada a servidores para atendimento a usuários, com serviços como arquivos compartilhados, controle de acesso, senhas dos usuários e impressão. Há também possibilidade de outras tecnologias internas para atendimento da rede local, a vantagem é a velocidade e a utilização da infraestrutura interna;

• *rede de usuários*: rede destinada a usuários para acesso cabeado ou por meio de ambiente sem fio. A boa prática é que os usuários possuem uma rede diferente do ambiente computacional interno (destinado a servidores);

• *rede wi–fi de visitantes*: empresas e órgãos governamentais podem proporcionar acesso à internet de visitantes, mas tal condição deve possuir controles de segurança para atendimento das políticas internas e da garantia de um uso adequado do serviço;

---

* *Site to site*: quando uma rede local possui uma conexão virtual, criptografada/segura, com outra rede via internet.

• *rede de teletrabalho (home office)*: rede local de cada funcionário ou colaborador que acessa remotamente, via VPN,* ambientes sistêmicos das empresas e entidades governamentais;

• *datacenter*: ambiente computacional com infraestruturas redundantes (energia, ar-condicionado, segurança física/computacional, sistemas de backup, armazenamento etc.) que garantem condições seguras para sistemas informativos;

• *cloud pública*: sistema computacional de infraestrutura, plataforma e serviços em ambiente público, compartilhado e orquestrado por um painel de controle;

• *cloud privada*: sistema computacional de infraestrutura, plataforma e serviços em ambiente dedicado e privado, orquestração por um painel de controle.

O sistema denominado *Security Observability* é um conceito aplicado ao monitoramento de ameaças atrelado aos ambientes de TI, interconectado aos sistemas distribuídos, microsserviços e nuvem. A reunião de *logs* de segurança, atrelada à inteligência de vulnerabilidade, realiza a avaliação preventiva e preditiva de ameaças digitais.

2.2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

As políticas são instrumentos formais que proporcionam regras, direitos e deveres para usuários, prestadores de serviços e atores internos e externos.

---

* *Virtual private network* ou rede privada pessoal é provida por tecnologia de criptografia para comunicação entre um computador e/ou uma rede com outra por meio da internet. A expressão foi utilizada para o teletrabalho, que é uma conexão entre um computador (*endpoint*) e um *firewall* via IPSec.

As políticas são organizadas em um programa, isto é, documento que é dividido por assunto e especialidades.

A Política de Geral Segurança da Informação Cibernética e Privacidade de Dados constitui as diretrizes formais com a definição sobre seu compromisso com a proteção das suas próprias informações ou daquelas que estão sob sua custódia, devendo ser seguida e respeitada por todos os funcionários, colaboradores, prestadores de serviços ou qualquer indivíduo que faça uso de algum dos elementos aqui citados, além de servir como um guia para qualquer espécie de dados ligados a segurança institucional

Cada política deverá conter os princípios destacados na norma ISO/IEC 27001/27002/27701. A segurança da informação é alcançada pela implementação de um conjunto de controles que quando estabelecidos, implementados, monitorados, analisados de forma crítica e melhorados, asseguram que os objetivos da organização.

A política de segurança da informação e privacidade de dados deve obedecer aos seguintes princípios:

• *integridade*: garantia de que a informação seja mantida em seu estado original, de modo a protegê–la, na guarda ou transmissão contra alterações indevidas, intencionais ou acidentais;

• *confidencialidade*: garantia de que apenas pessoas autorizadas tenham acesso à informação;

• *disponibilidade*: garantia de que o acesso à informação, às pessoas autorizadas, estará disponível sempre que necessário;

• *privacidade por desenho e/ou padrão (privacy by design and default)*: a privacidade é dada como algo padronizado no processo de construção de produtos e serviços, não obstante o seu uso como algo inerente à cultura corporativa,

tendo-a como elemento cultural para comportamento acerca da privacidade de dados;

• *segurança como padrão (security by default)*: concepção comportamental de cunho social e cultura, a qual se caracteriza pelo pensamento em segurança da informação como padrão nos serviços e produtos empresariais;

• *conscientização e treinamento constante*: o modelo de treinamento e conscientização contribuem para que haja entendimento dos aspectos de segurança da informação e privacidade de dados, em que os funcionários são envolvidos e parte do programa de treinamentos.

3
SISTEMAS DE PROTEÇÃO

Os sistemas protetivos são tecnologias que auxiliam as corporações e entidades governamentais na mitigação de riscos de ataques cibernéticos.

3.1 FIREWALL

Os firewalls são sistemas baseados em hardwares e softwares que geram uma proteção ativa, que possui a capacidade de filtrar pacotes da rede e restringir o acesso às páginas indesejadas ou indevidas para os serviços das redes da prefeitura e dos municípios.

Isso pode ser um equipamento (ativo de rede) ou um software (programa) instalado em outros ativos. Dependendo de sua configuração, ainda faz o registro das atividades e dos acessos que foram solicitados, arquivos que foram baixados, compartilhados.

Os firewalls possuem uma nova geração com funções estendidas de IPS,* WAF**, filtro de conteúdos etc.

---

* IPS são sistemas que analisam o tráfego de rede para identificação de anomalias (assinaturas de ataques) provenientes de ataques escondidos (tráfego legítimo), por conseguinte realizando um bloqueio ativo. O IDS *Intrusion Detection System* ou Sistema de Detecção Intrusão apenas detecta e não possui bloqueio, com a função de monitoramento apenas.

** Os *Web Application Firewall* ou Firewall de Proteção a Aplicações na Web são sistemas preparados para atuarem como portais contra tentativas de invasão e proteção mediante análise de ameaças.

3.2 ANTIVÍRUS

Os antivírus (AV) são o conjunto de programas que protegem o sistema operacional contra ameaças virtuais. As ameaças primárias são os vírus de computador caracterizados por um software que utiliza meios para ação de controle nesses sistemas, gerando impacto ao usuário.

Esses programas buscam assinaturas, como vírus, Worms,* programas maliciosos e comportamentos já catalogados e, dessa forma, conseguem remover ou colocar em quarentena os programas e arquivos identificados com as assinaturas. Alguns verificam os downloads, os arquivos baixados da internet, a fim de melhor promover a proteção do usuário.

As portas de entrada de códigos maliciosos são várias e podem aparecer via e-mails, arquivos, *pen drives*, sites de conteúdo, sites proibidos e, além desses acessos, ainda possuem a capacidade de se multiplicar e contaminar diversas partes do seu equipamento, dos ativos disponíveis na rede utilizada.

Os malwares possuem finalidades diferentes, com as suas variantes apresentadas a seguir:

3.2.1 Vírus

O vírus tem, como característica, a execução do programa/arquivo a partir do computador ou dispositivo computacional, efetuando estas etapas:

- tornar-se ativo ou validação do sistema desprotegido;
- execução e infeção.

* Vide explicação no mesmo capítulo

Seus principais meios de propagação são por via email, *script*, macro e telefone celular.

3.2.2 Cavalo de Tróia/trojan

Cavalo de Tróia ou trojan é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Ação de infeção depende de uma execução.

Os principais meios de propagação são: pelo próprio usuário; por atacantes.

Após invadir o equipamento, alteram programas já existentes para executar ações maliciosas, além das funções originais;

3.2.3 Backdoor

Bacdoor é um programa instalado que possibilita o acesso remoto ao sistema operacional ou a aplicativos.

Ação de infeção depende de uma execução.

Os principais meios de propagação são: pelo próprio usuário; por atacantes; por rede comprometida.

3.2.4 Worm (Verme)

Worm é um programa que possui a característica de se autorreplicar na rede e com cópias na máquina infectada.

A ação de infeção depende de uma execução (USB, e-mail etc.) e de vulnerabilidades.

Os principais meios de propagação são: identificação dos equipamentos-alvos; envio das cópias; ativação das cópias; reinício do processo.

3.2.5 Bot (robô) / Botnet

Bot ou botnet é um programa que possui a característica de controle remoto ou comunicação.

Possui um modo de propagação similar ao Worm, com execução direta das cópias e exploração automática de vulnerabilidades em programas. No Botnet, a máquina é controlada remotamente pelo atacante.

Os principais meios de propagação são: canais de mensageria; servidores web; redes ponto a ponto;

3.2.6 Root Kit

Root kit é um conjunto de programas e técnicas que possam esconder suas atividades nos sistemas.

Suas ações no sistema operacional são estas:

- remover evidências em arquivos de logs;
- instalar outros códigos maliciosos;
- esconder atividades e informações;
- capturar informações da rede;
- mapear potenciais vulnerabilidades em outros equipamentos.

Os principais meios de propagação são: vírus; malwares em geral.

3.2.7 Spyware

Spyware é um programa projetado para funcionar como um espião e que tem, como objetivo, coletar informações e enviar para o atacante.

Estes são alguns tipos de spyware:

• *keylogger*: capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento;

• *screenlogger*: capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado;

• *adware*: projetado para apresentar propagandas

Seu modo de propagação é por navegação web.

3.2.8 Ransomware

Ransomware é um programa que explora vulnerabilidade ou é instalado no sistema operacional, com o uso de criptografia e exigência de pagamento de resgate para restabelecer o acesso aos arquivos sequestrados.

Existe dois tipos principais:

• *locker*: impede o acesso ao equipamento;

• *crypto*: impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia.

Quando presente, o ransomware executo as seguintes ações diretas:

• infecta backups;
• utiliza criptografia forte;
• invade a rede e explora sistemas vizinhos e vulneráveis;
• facilita a extorsão por meio pagamento do resgate (geralmente feito via *bitcoins*).

* * *

Posteriormente à descrição dos tipos de Malware, torna-se imprescindível o entendimento das soluções de antivírus (AV), que são agentes instalados nos sistemas operacionais aos quais se conecta uma console que atualiza a base de dados de ameaças conhecidas. Assim, quando há identificação de uma ameaça, o agente realiza o bloqueio ou envia o arquivo para quarentena. Outro método é o modelo heurístico, que realiza análise de comportamentos que possam ser ameaças escondidas para uma ação ativa na eliminação de um ataque diretor ao sistema operacional.

Os agentes evoluíram para novas funcionalidades, aumentando a proteção dos sistemas operacionais, tais como: firewalls, bloqueios de conteúdos/software/hardware, proteção à caixa postal etc.

Vale lembrar que os antivírus protegem as estações de trabalho, servidores e redes de ameaças conhecidas, no entanto há falhas de vulnerabilidades nos sistemas operacionais que podem ser exploradas, assim como novos vírus (sem vacina como os Zero Day),* vulnerabilidades de sistemas, brechas de segurança e indústria do RaaS (*ransomware as a service*)

* *Zero day* é a expressão para uma ameaça (malware) não identificada e sem proteção pelos sistemas tracionais de segurança da informação.

3.2.9 EDR (*endpoint detection and response*)

Os fabricantes de AV ajustaram a proteção para o uso de um modelo de detecção e resposta, mais inteligentes e eficazes, melhorando o processo heurístico para uma análise consistente de comportamento, ajustados às novas ameaças.

Abaixo, segue a lista de funcionalidades dos EDR:*

• realiza o monitoramento e a detecção em tempo real de ameaças, incluindo aquelas que podem não ser facilmente reconhecidas ou definidas pelo antivírus padrão;

• utiliza análise de comportamento, portanto, pode detectar ameaças desconhecidas com base em um comportamento anômalo do tradicional do S.O;

• coleta e analisa os dados que determinam os padrões de ameaças e alertam as empresas sobre ameaças;

• utiliza recursos forenses que podem ajudar a determinar o que aconteceu durante um evento de segurança;

• as soluções isolam e/ou direcionam ataques ou comportamentos suspeitos para uma quarentena, utilizando métodos como *sandboxing*;**

• o EDR pode incluir correção ou remoção automatizada de certas ameaças, interagindo com *security information event management* (Siem)*** e *security orchestration automation and response* (Soar).

---

* *Endpoint detection and response* (reposta e detecção de ameaças e computadores) são sistemas AV estendidos para proteção aos novos tipos de ameaças.

** *Sandbox* é uma área ou mecanismo de isolamento de ameaças, com sistemas analíticos para bloqueio e verificação forense.

*** Vide explicação no capítulo 4.

3.2.10 O que um EDR não protege

As soluções de EDR não realizam a proteção completa de ameaças. Logo abaixo indicamos alguns exemplos de não mitigação por parte destas soluções:

- correlacionamento de eventos;
- zero day, novos vírus;
- movimento alteração proveniente de um ransomware;
- comando e controle de uma máquina invadida;
- ações de vazamento de dados;
- espionagem industrial;
- aplicação da não confiança para quaisquer conexões;
- controle de conexões;
- validação de conexões;
- microssegmentação para servidores e usuários, evitando o movimento de exploração dos ransomware;
- auditoria e validação via contexto de conexão;
- proteção contra bugs e vulnerabilidades (apenas as conhecidas).

3.3 ZERO TRUST

A expressão Zero Trust ou Confiança Zero é a nova perspectiva na segurança da informação. Os seus princípios e a aplicação de sua filosofia vão em todas as camadas tecnológicas, tornando-a a próxima fronteira na proteção tecnológica.

Atualmente a expressão é amplamente divulgada e utilizada, com alguns críticos indicando que há uma certa perda de propósito ou significado, todavia existe ainda uma grande jornada para aplicação do modelo e que haja incremen-

to de elementos, para que a expressão se torne um método de proteção multicamada.

A ideia nasceu da publicação do artigo "*No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*",* do analista da Forrester** John Kindervag, em 2010, que introduziu a expressão "Zero Trust".

Em 2014, a Google iniciou a aplicação prática em suas operações/redes, tendo como base a restrição de acesso ou remoção de acessos à rede de produção. Tal ação influenciou fortemente o setor com uma série de artigos documentando sua implementação interna e inovadora.

No mesmo ano, 2014, a Cloud Security Alliance apresentou a arquitetura de perímetro definido por software (*software defined perimeter* – SDP), *cloud security alliance* (CSA) e da BeyondCorp, que fornecia uma especificação concreta para um sistema de segurança compatível com Zero Princípios de confiança.

Já em 2017, empresas de segurança começaram utilizar o modelo, e este foi ratificado pelo Gartner, que o revisou, incluindo-o no *Continuous Adaptive Risk and Trust Assessment* (Carta), avaliação de confiança e risco adaptável contínuo, com que possui princípios em comum. O conceito era substituir a aceitação implícita de confiança incorporada nas origens da internet por um requisito de confiança comprovada explícita.

Em 2019, criou-se o entendimento do Zero Trust Network Access (ZTNA) como um modelo facilmente reconhecido para acesso às redes e aderente à Cloud Computing.

---

* Em tradução livre para português, pode ser lido como "Não há mais centros rígidos: confiança zero um modelo de segurança da informação" (o autor utilizou a expressão borracha, que foi expressa pela palavra "rígido").

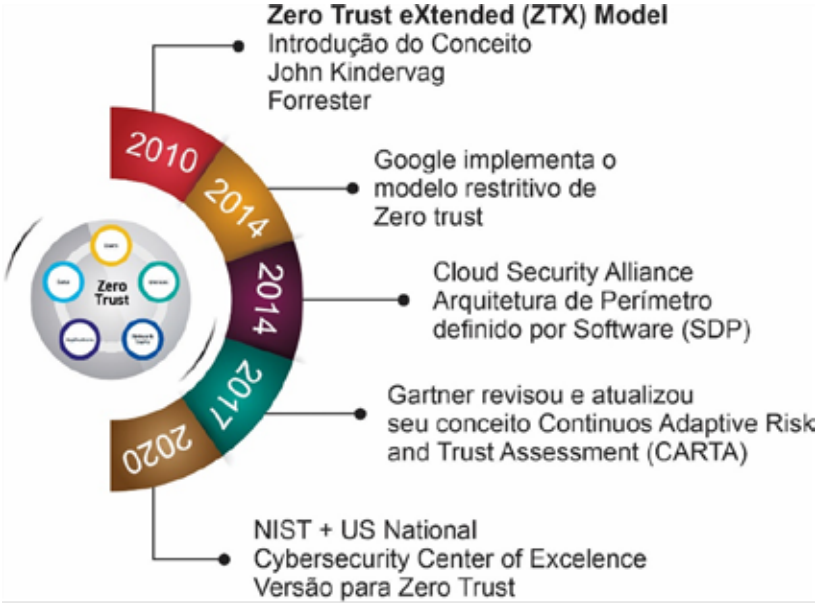
** A Forrester é uma empresa norte-americana de pesquisa de mercado que presta assessoria sobre o impacto existente e potencial da tecnologia e a segurança da informação.

Em 2020, a ênfase de toda a indústria em Zero Trust continuou, com o National Institute of Standards and Technology (Nist) associado com a US National Cybersecurity Center of Excellence dos EUA, que lançaram uma publicação dedicada à arquitetura Zero Trust.

A ideia foi iniciada por perímetros para as comunicações de rede, independentemente de onde estivessem (como em tese redes confiáveis), mas se garantindo que as sessões de comunicações fossem de certa maneira válidas e controladas. Isto é, o perímetro inicial deveria ser protegido para que não houvesse movimento lateral, que são os ataques internos de exploração de vulnerabilidades e uso de credenciais.

O conceito inclui a ideia de risco adaptativo contínuo e avaliação de confiança como um compromisso utilizável para fornecer a máxima segurança possível, sem afetar a usabilidade.

Figura 2 – Histórico da adoção do Conceito Zero Trust.



Elaboração: Andrey G Oliveira e Allan Kovalscki.

3.3.1 Conceitos–chave

Um conceito-chave na ZTNA é o papel de um validador de confiança. O agente (software instalado nas máquinas) de confiança, residente fora da rede, fornece o nível certo de confiança a um usuário autenticado para acessar um aplicativo específico, incluída criptografia.

A abordagem de controle impede toda e qualquer comunicação recebida de qualquer pessoa que não seja um usuário confiável autenticado. Já o aplicativo informa ao *broker* quem pode ser autenticado para acessar quais aplicativos.

O validador ou controlador impede que invasores possam se conectar sem uma espécie de autenticação.

Esse modelo altera ou cria um paradigma de conexão de rede, autenticação e com o emprego de softwares.

O controlador pode verificar a integridade do dispositivo, sua geolocalização e outras biometrias comportamentais do usuário.

As condições são algo que gera um instrumento de políticas de acesso, e qualquer usuário que queira acessar um aplicativo diferente precisa se autenticar novamente para esse aplicativo, e a autenticação de requisitos pode ser diferente.

3.3.2 Princípios Básicos

Os princípios básicos do Zero Trust que são geralmente aceitos foram inicialmente definidos no “No More Chewy Centers”:

• **Princípio 1: Acesso seguro** – “Garantia de que todos os recursos sejam acessados com segurança, independentemente da localização”. O modelo de

acesso seguro exige que todos os recursos sejam incluídos no escopo de um Zero Trust solução. Implicitamente, isso exige que as organizações adotem uma abordagem holística com Zero Trust e que devem eliminar barreiras que historicamente existiram entre ferramentas de segurança e equipes, com proteção ao acesso, identificação de sistemas e comportamento humano no acesso a sistemas;

• **Princípio 2: Acesso identificado** – "Garantia de que todos os recursos sejam identificados com segurança, independentemente da localização". A adoção dessa filosofia protege o acesso de todas as identidades (humanos e máquinas), a todos os recursos (dados, aplicativos, servidores), independentemente da localização, da identidade e da tecnologia do recurso que está sendo acessado. Esse princípio efetivamente determina a dissolução da sociedade tradicional de perímetro e sua substituição por um paradigma de segurança alternativo. Significa também que não apenas o tráfego de rede deve ser criptografado à medida que transita em áreas de rede não confiáveis, mas que todo acesso deve estar sujeito uma política;

• **Princípio 3: Privilégio mínimo** – "Garantia de que os acessos a quaisquer sistemas tenham o mínimo de privilégio". O conceito de acesso menos privilegiado aos recursos não é novo, mas vem sendo difícil de aplicar amplamente antes do Zero Trust. O privilégio mínimo deve ser consistentemente gerenciado em locais e tipos de recursos, e tanto na rede quanto no aplicativo camada, usando o contexto de segurança e identidade;

• **Princípio 4: Inspecione e registre todo o tráfego** – "Garantia de que os dados sejam inspecionados para manutenção da integridade". As redes são os ambientes. Via de regra, são exploradas para ataques, uma vez que são os meios pelos quais os componentes distribuídos se conectam e se comunicam uns com os outros. É por essa razão que o princípio central final requer inspeção e regis-

tro de tráfego de rede. A inspeção não é a quebra de integridade e confidencialidade, mas um mecanismo tecnológico que propicia a identificação de dados comprometidos.

As informações de tráfego de rede devem ser enriquecidas pelo sistema Zero Trust adicionando identidade, contexto de dispositivo e alimentado em firewalls de última geração, IPS, ferramentas de monitoramento, para melhorar sua capacidade de tomar decisões para detectar, alertar e responder a um incidente.

3.4 SENHAS E CREDENCIAIS

A abundância de sistemas e serviços sempre requer um login (nome do usuário) e uma senha. Se antes tínhamos poucos sistemas, hoje a quantidade de portais/aplicativos gerou uma enorme quantidade de credenciais, criando um problema bem "comum": lembrar de tudo isso!

Outro desconforto é a complexidade, incluindo o duplo fator de autenticação,* o que gera descontentamento pela dificuldade de uso com caracteres especiais, letra maiúscula e quantidade mínima caractere. Não obstante, as ações dos usuários para recordação dessas informações tornaram-se um novo risco. Afinal, a "lembrança de todas as senhas" criou uma grande barreira, levando-os a utilizar o que há disponível: as chaves "gravadas" em planilhas e/ou documentos no Microsoft Word ou mesmo senhas e logins repetidos em todos os sistemas, e alguns chegam até a anotar em cadernos ou *post-id*.

Um dos maiores fatores de riscos, de fato, são relacionadas às senhas; essa "porta" gera a oportunidade ou mesmo a "certeza" de que o crime cibernético "vale a pena". No fim das contas, o atacante sabe que é "fácil" descobrir ou tentar

* Os duplos fatores de autenticação, via de regra, são os mecanismos de confirmação via celular ou e-mail, justamente para "evitar" que alguém utilize o sistema no lugar do usuário.

(via software) saber a senha de outrem, facilitando as invasões aos sistemas, fraudes, roubo de identidades, entre outros crimes digitais.

A utilização de cofres de senha atrelados à conscientização dos riscos torna-se um excelente sistema de proteção contra os acessos indevidos.

A utilização de *multi factor authentication* (MFA) ou múltiplo fato de autenticação auxilia e protege contra furto de identidades. Em resumo, é uma forma de proporcionar mais uma camada de checagem sobre o acesso a um sistema, como contrassenha por e-mail ou utilização de sistemas de *token** para validação do acesso.

* Tokens são softwares que geram códigos dinâmicos e sincronizados para autenticação, comumente usados por aplicativos bancários.

4
MONITORAMENTO DE SEGURANÇA

O monitoramento de TI atualmente descrito como *observability* (Pourmajid *et al*., 2023) procura simplificar e dar uma visão de negócios em ambientes sistêmicos localizados em *cloud* (pública e/ou híbrida), *on premises*, fornecedores, integrações etc.

Não obstante, a verificação de SLA, que abrange componentes, aplicações, chamadas de serviços, API, infraestrutura, é um elemento do monitoramento de negócio e, por conseguinte, um monitor de funcionamento corporativo e de seus clientes. No entanto, os itens de segurança da informação que fazem parte do ecossistema de tecnologia e possuem métricas próprias acabaram se tornando um desafio ou mesmo um item pouco explorado pelas operações de tecnologia e negócio. Em suma, como os temas de segurança da informação são distintos de tecnologia da informação, estes são transformados na nova fronteira de *observability*, isto é, uma nova visão que possibilita a verificação de ameaças e riscos que podem gerar prejuízos financeiros e de imagem, além de multas provenientes de vazamentos de dados (LGPD).

A seguir, abordam-se os riscos com vazamento de dados e controle de segurança, com a descrição do modelo *Information Security Observability* e suas nuances.

4.1 SIEM

As soluções de Siem possuem, como característica principal, a centralização de registros (*logs*). Isso significa que os sistemas de tecnologia enviam os seus

logs para a solução e a tecnologia consolida-os via correlação, dando-lhes uma visão de segurança por níveis de criticidade e risco. Cabe salientar que a correlação é o elo entre eventos distintos em elementos tecnológicos diferentes, mas que apresentam uma combinação ou comportamento a partir dos quais se possa identificar ameaças digitais.

A figura 3 destaca o fluxo de funcionamento com a coleta de dados por origem (*data sources*), a consolidação desses eventos correlacionados por métodos como Mitre ATT&CK* para uma marcação analítica que possa gerar informações de ataques para que o SOC possa agir.

As origens dos dados são diversas, como firewalls, antivírus, gerenciamento de vulnerabilidades, servidores, Syslog**, estações de trabalho e demais ferramentas de segurança.

Figura 3 – Funcionamento do Siem.

Fonte: elaborado por Andrey G. Oliveira.

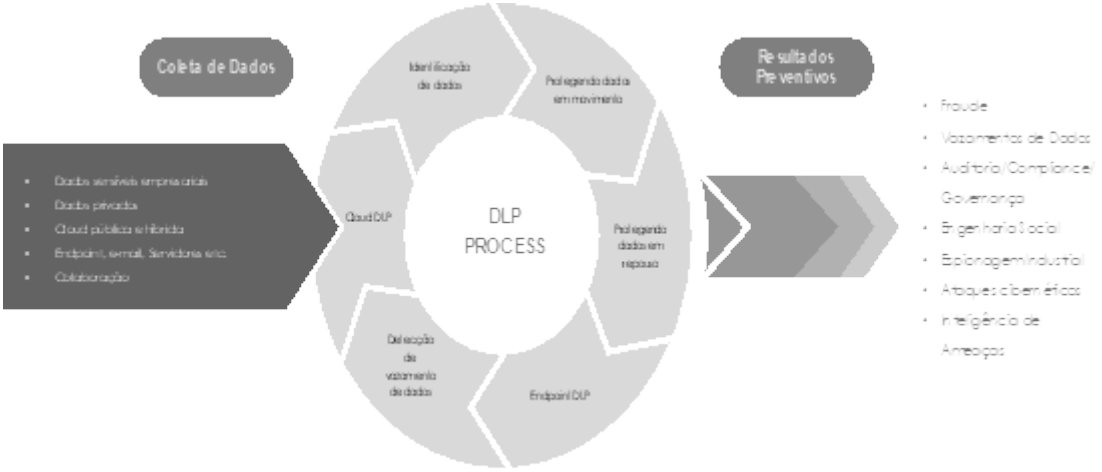
* Mitre ATT&CK é o acrônimo de *adversarial tactics, techniques, and common knowledge*, que é uma base global de comportamentos, diretrizes e classificação de ataques cibernéticos.
** Syslog é um sistema que recebe os registros de equipamentos, com marcadores de horário, tipo de evento, descrição etc.

4.2 DLP – DATA LOSS PREVENTION

A prevenção de vazamento/perda de dados (DLP) tem o propósito de monitorar, gerenciar, identificar e bloquear comportamento da utilização de dados em sistemas locais, remotos e em *cloud computing*.

O processo de utilização de uma solução de DLP parte da classificação dos dados com a aplicação de políticas; consequentemente, tais passos realizam as verificações ativas ou bloqueios, não obstante aos avisos sobre violações que não atendam às regras destacadas na sua implementação. Os resultados esperados da solução são: prevenção a fraudes, vazamentos de dados, atendimento a leis e regulamentos, sabotagem, diminuição de exposição a engenharia social, contrainteligência e eliminação de espionagem industrial.

Figura 4 – Processo de funcionamento do DLP.



Fonte: elaborado por Andrey G. Oliveira.

O DLP só é útil se for dito o que é e não for sensível. As empresas e organizações em geral devem usar uma ferramenta automatizada de descoberta e

classificação de dados para garantir identificação e categorização confiáveis e precisas dos dados, em vez de deixar para os humanos decidirem. A seguir, seguem alguns casos de uso:

• protegendo dados em movimento (*protecting data in motion*): análise dos dados que são movidos internamente, e as violações externas geralmente dependem disso para redirecionarem os dados. O software DLP pode ajudar a garantir que os dados em movimento não sejam roteados em algum lugar em que não devem ir;

protegendo dados em repouso (*protecting data at rest*): essa técnica protege os dados quando não estão se movendo, como residir em bancos de dados, outros aplicativos, repositórios em nuvem, computadores, dispositivos móveis e outros meios de armazenamento;

endpoint (DLP): tipo de funcionalidade de DLP que protege os dados no nível do dispositivo final – não apenas computadores, mas também telefones celulares e tablets. Ele pode impedir que os dados sejam copiados ou criptografam todos os dados à medida que são transferidos;

• detecção de vazamento de dados (*data leak detection*): a técnica envolve a definição de uma linha de base da atividade normal e, em seguida, procura um comportamento incomum;

• *cloud* DLP: as soluções DLP evoluíram para gerenciar e proteger dados críticos em aplicativos de software como serviço e infraestrutura como serviço.

4.3 VAZAMENTOS DE DADOS E CONTROLE DE SEGURANÇA

O vazamento de dados significa, na prática, que dados saíram da organização sem autorização, sendo divulgados na rede pública de computadores e, em consequência, afetando a confidencialidade e acarretando infortúnios e prejuízos.

As informações podem ser classificadas ou etiquetadas de acordo com a sua importância. Baseando-se no provável impacto, cada organização adota um determinado critério para proteção desses dados (Calder; Matkins, 2015).

Os tipos de vazamento podem ser caracterizados como:

• *social intencional*: ação de pessoas interessadas no vazamento;
• *social por acidente ou desleixo*: envio de forma não dolosa ou por descuido;
• *engenharia social*: indução de indivíduos internos que são levados ao erro por meio de manipulação;
• *furto tecnológico de informações*: extração direta ou indireta por meio de tecnologia que utiliza software para extração e envio aos interessados;
• *espionagem industrial*: tipo de furto de informação para fins específicos que possui, como alvo, indivíduos, empresas e governos com o intuito de utilização de informações confidenciais para seus próprios interesses;
• *sequestro de dados*: utilização da extração (furto) com a utilização de tecnologia que realiza a criptografia dos dados e promove a extorsão mediante pagamento para liberação do acesso a eles.

O ciclo modelo, destacado na figura 5, ilustra um processo de treinamentos, palestras e conscientização que dão suporte para avaliação continuada e testes de conhecimento, ou temas que são expostos a maior risco no comportamento dos usuários.

A seguir serão exploradas as etapas do ciclo.

Figura 5 – Programa de conscientização aos usuários.

Fonte: elaborado por Andrey G. Oliveira e Allan Kovalscki.

4.4 PLANO DE CONSCIENTIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

O plano de conscientização passa pelas etapas de trilhas que funcionam como um guia de treinamento e divulgação.

Conforme destacado na figura 6, o primeiro passo, ou mesmo sendo uma premissa para o início do plano, é a avaliação das políticas de segurança e privacidade de dados (LGPD) à qual todos os usuários deverão ter acesso, estando conscientes de seus deveres e direitos.

As políticas geram uma formalidade necessária, diminuindo o risco de comportamentos indevidos. Não obstante, em caso de má-fé, é preciso que os postulantes saibam das consequências de seus atos. Sem contar o entendimento de ferramentas de monitoramento de segurança da informação, como Siem e DLP, que possam proporcionar a detecção ativa de um vazamento de dados. A

conformidade com leis e regulamentos internos é algo fundamental, que que ser demostrado a e ratificado por todos os usuários.

Os treinamentos e palestras proporcionam a visão básica dos conceitos e, de acordo com a trilha, as informações relevantes para proteção dos usuários.

A continuidade de serviços é parte do modelo e possui o intuito de preparar as equipes em caso de indisponibilidade, assim como aplicar os planos de continuidade de negócios.

Figura 6 – Plano de Conscientização da Segurança.

Fonte: elaborado por Andrey G. Oliveira e Allan Kovalscki.

5
RECUPERAÇÃO DE DESASTRE E INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Nesta seção, são abordados os temas para recuperação de incidentes de segurança da informação com os planos de recuperação, continuidade de negócios, contingência de TI e recuperação de desastre

5.1 PLANO DE RECUPERAÇÃO

Ameaças como *ransomware* crescem devido ao modelo industrializado do *ransomware as a services* (RaaS), isto é, novos malwares ou Zero Day estão se espalhando exponencialmente, tendo assim grande possibilidade de sucesso em ataques cibernéticos.

O impacto do comportamento do *ransomware* traduz-se no mecanismo de *comando e controle*, junto ao qual o atacante instala um Zero Day e compromete os sistemas operativos, assim como também os sistemas de recuperação.

Um plano de continuidade de negócios (*business continuity plan*), figura 7, gera mais um elemento de proteção, levando em consideração o backup tradicional, o plano de recuperação e de continuidade de negócios.

Figura 7 – Tipos de Recuperação.

Fonte: elaborado por Andrey G. Oliveira & Allan Kovalscki.

5.2 PLANO DE CONTINGÊNCIA DE TI

O plano de contingência de tecnologia da informação é um recurso com os seguintes elementos:

• *arquitetura*: infraestrutura, banco de dados, sistemas que proporcionem capacidade de contingência e retorno rápido de um ambiente comprometido;
• *cloud pública e privada*: utilização do ambiente de *cloudcComputing* como meio de continuidade em caso de um evento grave;
• *alta disponibilidade*: ambientes com redundâncias ou capacidade de retorno rápido, no prisma que vai desde hardware, software e serviços de *cloud*;
• *backup e restauração*: ambientes que proporcionem cópias de segurança e com possiblidade de restauração rápida para reparação, parcial ou total, de sistemas;
política de contingência de TI: documento que descreve o plano, com pilares e fundamentos como base a ser seguida pelas equipes técnicas;

• *procedimentos e instruções de trabalho*: documentos que suportam as equipes e realizam os preceitos descritos na política;

• *business impact analysis (BIA)*: documento (análise de impacto nos negócios) que ratifica o impacto ao negócio em caso de ausência de serviços ou da produção, assim dizendo, a inatividade das operações corporativas ou de instituições que levam em conta o plano de execução em caso de indisponibilidade.

5.3 PLANO DE CONTINUIDADE DO NEGÓCIO OU BCP (*BUSINESS CONTINUITY PLAN*)

O plano consiste em ações técnicas, administrativas e estratégicas para que o negócio não seja impactado por ameaças ou mesmo inviabilize a sua continuidade. Já os planos tradicionais tratavam de ameaças como desastres naturais ou atreladas a riscos físicos, não obstante elementos como terrorismo e sabotagens.

O plano é uma ferramenta importante e estratégica, não apenas para contingência, emergência ou desastre, tornando-se um diferencial competitivo, sendo reconhecido por investidores e clientes.

São partes dessa proposta:

• *plano de recuperação de desastres (disaster recovery plan –DRP)*: ações associadas ao plano de recuperação de tecnologia, somadas com as áreas de negócios, para que a empresa possa continuar suas operações;

• *classificação de ativos*: identificação de ativos críticos para priorização, tanto para proteção quanto para recuperação;

• *uso de recursos durante a indisponibilidade*: mitigação das perdas no uso da contingência;

• *processo empresarial*: mapeamento dos processos que estejam no *plano de contingência e recuperação*.

5.4 BUSINESS CONTINUITY MANAGEMENT (BCM)

A disponibilidade de ambientes sistêmicos na atual conjuntura tornou-se imprescindível, tanto pelo contexto operacional quanto pelos sistemas de *backoffice* com aos ambientes de apoio direto ao negócio. As ameaças cibernéticas tornaram-se um elemento de risco considerável, em especial de ataques de *ransomware* que podem levar à indisponibilidade total de ambientes por longos períodos.

Não obstante, há eventos adicionais que levam ao risco, tais como desastres, incidentes físicos, incêndios, catástrofes naturais, distúrbios sociais, entre outros. Sugere-se que empresas tenham modelos de mitigação de riscos ou que proporcionem ações que diminuam o impacto, garantindo a continuidade dos negócios e acelerando o processo de recuperação. Outro fator importante é o capital humano para que as ações de recuperação ou planos de contingência funcionem adequadamente.

A lista abaixo relaciona modelos, conceitos, planos e processos que gerem capacidade administrativa, tecnologia e corporativa para continuidade de negócios, assim como detalhes de cada um, destacados em suas respectivas seções:

i) continuidade de negócios – *business continuity* (BC);
ii) plano de continuidade de negócios – *business continuity plan* (BCP);
iii) análise de impacto nos negócios – *business impact analisys* (BIA);
iv) recuperação de desastres – *disaster recovery* (DR);
v) plano de recuperação de desastres – *disaster recovery plan* (DRP).

5.4.1 Continuidade de negócios – *business continuity* (BC)

A continuidade de negócios é baseada em processos, procedimentos, decisões e atividades que garantem a continuidade da função de negócios da organização, independentemente do risco potencial, da ameaça ou da causa de uma interrupção.

Conforme é corroborado pela norma ISO 22301:2019, o "BC é a capacidade da organização de continuar a entrega de serviços ou produtos em níveis predefinidos aceitáveis após um desastre"; logo, as estratégias de BC visam reduzir o tempo de inatividade após um evento que gere uma interrupção.

A continuidade de negócios é uma estratégia centrada nos negócios que enfatiza mais a manutenção das operações de negócios, em face da dependência de qualquer organização no tocante aos sistemas modernos de produção, baseados em tecnologia da informação. Dentro desse contexto, é necessário prever os custos do tempo de inatividade determinados pelo hiato excessivo de "queda", gerando um impacto significativo na condução dos negócios ou mesmo levando a perdas irreparáveis as operações de negócios. Tal condição foi acelerada pelos ataques de *ransomware* (Fezzey *et al*., 2023), em especial após a pandemia de Covid-19, que levou as empresas a entenderam o aumento de risco no uso de ambientes virtuais e a transformação digital. Dado que há risco acentuado às empresas e aos governos, torna-se imperativa a adoção de plano de BC em ambientes redundantes e resilientes.

Destacam-se, na figura 8, benefícios e objetivos de um BC continuado e testado.

Figura 8 – Benefícios e objetivo do *business continuity*.

Fonte: elaborado por Andrey G. Oliveira e Allan Kovalscki.

• *manutenção do negócio*: significa que a continuidade das operações empresariais auxilia na condução póstuma a um evento que leve a falhas ou à impossibilidade de uso de ambientes instalados;

• *proteção à reputação*: suporta as empresas e governos a gerenciar desastres e garante uma recuperação de desastres com baixo impacto ou percepção de seus clientes/cidadãos, proporcionando que produtos e serviços críticos estejam preservados e, por conseguinte, protegendo a reputação e sua marca, respectivamente;

• *preparação e treinamento*: à medida que os planos são realizados para que haja treinamentos e simulações, as organizações podem promover melhorias e ajustar a eficiência;

• *validação de padrões/lei*: as organizações que estão em conformidade com os padrões BC são consideradas confiáveis pelas partes interessadas. Conformidade à privacidade de dados (LGPD);

• *redução de riscos e perdas financeiras*: o último item é a diminuição do risco de violação de dados, que pode ser obtida com a configuração de uma rede resiliente e com recursos robustos de backup, por exemplo.

5.4.2 Plano de continuidade de negócios - *business continuity plan* (BCP)

O plano de continuidade de negócios (BCP) é um processo que garante a continuidade das operações de negócios após incidentes disruptivos. A estrutura do BCP permite que as entidades antecipem riscos e ameaças internas e externas. Os itens do BCP (figura 9) são:

• *gerenciamento de crises*: gerenciamento de crises (*crise management* – CM) é a capacidade de uma organização responder a crises e, assim, minimizar os danos à sua marca, operação comercial e receita. Um atraso na expedição do plano CM pela alta administração causa uma sobreposição entre os planos e as responsabilidades dos processos CM e BC;

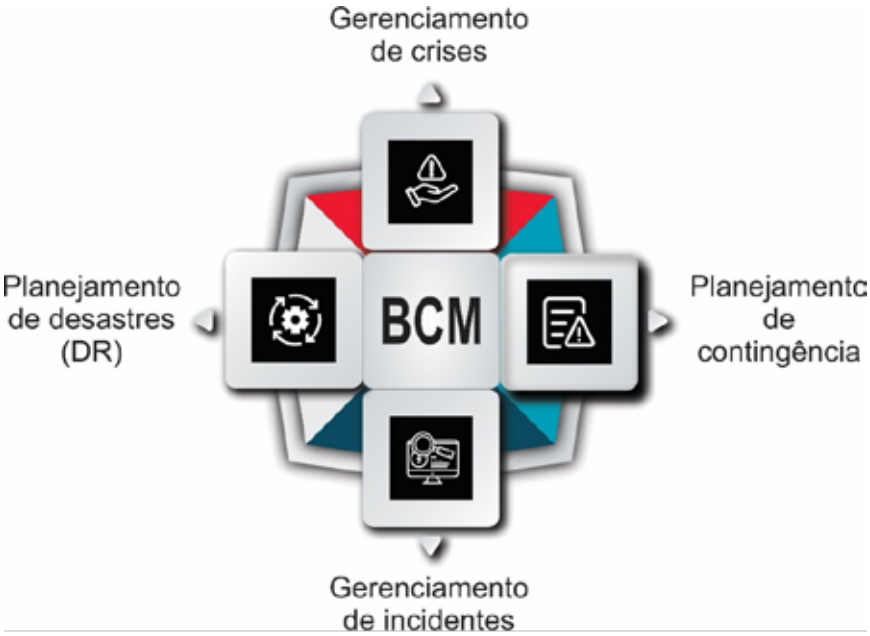
• *gerenciamento de incidentes*: o gerenciamento de incidentes (*incident management* – IM) permite que exista análise, identificação, resposta e que sejam evitados novos incidentes. Em uma organização estruturada, esses incidentes estão sob a alçada da equipe de gerenciamento de incidentes (*incident management team* – IMT), do sistema de comando de incidentes (*incident command system* – ICS) ou da *equipe de resposta a incidentes* (*incident response team* – IRT). A falta de gerenciamento eficaz de incidentes pode interromper as operações de negócios, bem como as partes interessadas;

• *planejamento de contingência*: um plano de contingência corre quando suas operações comerciais regulares são interrompidas por um evento significativo.

Os planos de contingência garantem a entrega contínua e imediata de produtos e serviços, operações de negócios no local e fora do local e satisfação do cliente;

• *recuperação de desastre (DR)*: a recuperação de negócios refere-se a um plano, arranjo e procedimento avançado implementado pelas operações após um desastre. Visa recuperar os processos de negócio da organização em torno de espaços de trabalho, pessoal, equipamentos e instalações, entre outros.

Figura 9 – *Business continuity management*.



Fonte: elaborado por Andrey G. Oliveira e Allan Kovalscki.

5.4.3 Análise de impacto nos negócios (BIA)

A análise de impacto nos negócios (BIA) é uma série de métodos analíticos para entendimento do ambiente de negócios e seus componentes de maneira que sejam sistematizados os efeitos potenciais de uma interrupção nas opera-

ções comerciais críticas devido a emergências, incidentes ou acidentes, como: disputas trabalhistas, falha de fornecedor, turbulência política, ataques terroristas, desastres naturais ou causados pelo homem, ataques cibernéticos e falhas de utilidade.

Como a BIA concentra-se em minimizar os efeitos dos riscos mencionados, quando é modelada e criada, deve ser incluída no BCP, especificamente como um componente de planejamento que concentre estratégias de redução de riscos e identificação de vulnerabilidades.

A BIA resulta em um relatório que descreve a abrangência dos riscos e seus impactos nas operações comerciais, não obstante a verificação de cada componente sistêmico e a dependência do negócio acerca dele.

O processo de construção e elaboração do BIA está destacado na figura 10 e dividido em 4 fases.

A fase 1 envolve:

- descrição dos objetivos e escopo;
- equipe de projeto BIA (interna e externa);
- comitê executivo.

Já a fase 2 compreende:

- aquisição de informação (entrevistas e questionários);
- inventário e mapa de relacionamento;
- coleta de ativos e componentes críticos.

A fase 3, por sua vez, considera:

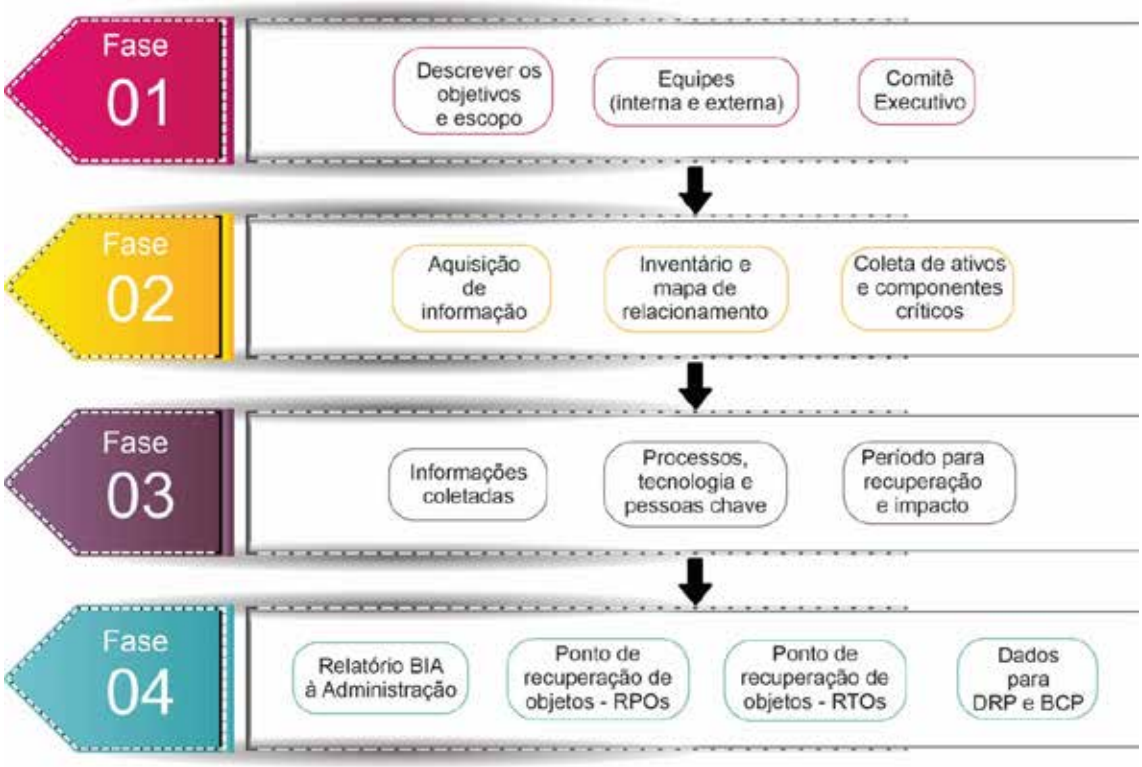
- as informações coletadas;
- a lista priorizada de processos ou funções de negócios, por importância;

• a determinação da tecnologia e do pessoal necessários para manter as operações em um nível ótimo;
• o período para recuperação e impacto.

Por fim, a fase 4 compreende:

• apresentação do Relatório BIA à administração;
• ponto de recuperação de objetos (*recovery point objets* – RPOs);
• tempo de recuperação de objetos (RTOs);
• dados para DRP e BCP.

Figura 10 –Fases do BIA.



Fonte: elaborado por Andrey G Oliveira e Allan Kovalscki.

5.4.4 Recuperação de desastres – *disaster recovery* (DR)

A recuperação de desastre é uma área de planejamento de segurança que reflete a capacidade de uma organização de restaurar dados e aplicativos de negócios após um evento. Envolve um conjunto de procedimentos e políticas destinadas a recuperar ou restaurar a infraestrutura tecnológica crítica. O *business continuity* tem o foco no negócio e elementos que levem que ele que não estejam indisponíveis; logo, o DR é parte desse modelo que procura ter uma estratégia centrada em dados com foco na recuperação e na restauração de dados perdidos, sistemas, TI ou pessoas responsáveis pela reconstrução de *data centers*, servidores ou outros componentes críticos da infraestrutura de TI.

Os objetivos do DR, demostrados na figura 11, são os seguintes:

• *redução do tempo de inatividade*: objetiva diminuir o tempo de recuperação que inclui danos à marca, insatisfação do cliente e perda de receita;

• *redução de perdas acumuladas*: mitigação de interrupções ou aceleração do retorno da operação levam à diminuição do impacto aos sistemas;

• *recuperação de dados perdidos*: retorno de dados perdidos devido a uma falha de hardware, ataques de vírus e malware, danos acidentais e desastres naturais.

Figura 11 – Objetivos do DR.

Fonte: elaborado por Andrey G. Oliveira e Allan Kovalscki.

5.4.5 Plano de recuperação de desastres – *disaster recovery* (DRP)

O plano de recuperação possui itens objetivos como *tempo de recuperação de objetos** (RTO), definido como o tempo máximo tolerável que um computador, um sistema, uma rede ou um aplicativo podem ficar inativos após uma falha ou desastre.

O dono do processo é avaliado pelo BIA, sendo que a métrica do RTO corrobora a expectativa do negócio. O item pode ser medido em segundos, minutos, horas ou dias. Isto posto, um RTO determina até que ponto o desastre interrompe as operações normais e a consequente perda de receita por unidade de tempo e, portanto, é crucial para o DRP.

* A expressão objeto refere-se a qualquer item como hardware, software, sistema, integração ou mesmo processo dependente de diversos itens anteriormente destacados.

Outro conceito fundamental é o ponto de recuperação do objeto (RPO), que é o prazo máximo no qual uma organização perde dados após uma grande interrupção de TI. Ele determina a quantidade aceitável de perda de dados que uma empresa pode sofrer em caso de interrupção. Um RPO define metas para projetar um BC, um DR ou alta disponibilidade (HA) e, portanto, é crucial para o DRP; já o RPO pode ser medido a partir do momento em que os serviços de hospedagem ficam indisponíveis, por exemplo.

Pré-definir um RPO para um determinado sistema pode auxiliar a determinar qual frequência mínima de backup deve-se ter ou mesmo quais itens são utilizados em políticas de retenção e tecnologias de restauração. Como um RTO, um RPO permite que os administradores de sistemas e analistas de segurança escolham os procedimentos ideais e tecnologias de DR mais alinhadas com a necessidade de negócio.

Os conceitos destacados neste artigo trazem boas práticas para o uso de ambientes que possam assegurar que empresas e governos possam retornar ou mesmo ter suas operações com disponibilidade mínima e com o menor impacto possível. Não obstante, essas ações fazem parte de um sistema integrado com outros *frameworks*, como o de Zero Trust, gerando procedimentos, processos, serviços, comunicações e tecnologias que venham proteger ambientes tecnológicos, produtos e serviços.

Adicionalmente, a ISO 22313:2012 fornece orientação baseada em boas práticas internacionais para planejar, estabelecer, implementar, operar, monitorar, revisar, manter e melhorar continuamente um sistema de gestão documentado que permite que as organizações se preparem, respondam e se recuperem de incidentes perturbadores quando eles surgem, assim como o NIST SP 800-34 nos traz uma visão de recuperação de desastre e um guia de contingência.


INCIDENT

6
GESTÃO DE INCIDENTES

Primeiramente, cabe esclarecer que existem vários tipos de incidentes, sendo importante diferenciá-los com base em metodologias reconhecidas para isso. Dessa forma, encontram-se listados os tipos de incidentes a seguir:

• *Incidente de TI*: a *information technology infrastructure library* (Itil) define um incidente de TI como a interrupção não prevista de um serviço de TI ou ainda a queda da qualidade de um serviço de TI;

Incidente de Segurança da Informação: um único ou uma série de eventos indesejados ou inesperados de segurança da informação (ISO 27000:2014 seção de número 2.35, p. 2), que têm uma probabilidade significativa de comprometer as operações do negócio e de ameaçar a segurança da informação (ISO 27.000, seção 2.36, p. 2);

• *Incidente de Segurança da Informação com Dados Pessoais*: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, as quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Em que pese todos os tipos de incidentes devam ser geridos com um mesmo método, cabe lembrar algumas questões quanto aos incidentes de segurança com dados pessoais, quais sejam:

• a LGPD determina que a comunicação do incidente (Comunicação [...], 2024) de segurança seja feita em prazo razoável (art. 48, § 1.º), conforme ainda será definido pela ANPD;

• a realização da comunicação demonstrará transparência e boa-fé e será considerada em eventual fiscalização;

• após o conhecimento do evento adverso e havendo risco relevante, comunicar a ANPD no prazo de 2 dias úteis a partir da data do conhecimento do incidente.

A seguir, listamos alguns exemplos de incidentes de segurança para melhor entendimento:

a) uso impróprio:

• uso de e–mail corporativo para spam ou promoção de negócios pessoais;
• instalação de softwares não autorizados;
• uso de pen-drive de forma não autorizada;
• impressão não autorizada de documentos;

b) vazamento de dados:

• exposição não autorizada de dados pessoais e informações privadas;
• credenciais roubadas ou comprometidas;

c) tentativas de acesso não autorizado a sistemas ou dados como, por exemplo:

• tentar ou realizar acesso utilizando credenciais de terceiros;
• má utilização de um sistema;
• provocar falhas no sistema que impeçam um acesso autorizado;

d) ataques de negação de serviço:

• forçar um sistema a reinicializar ou consumir excessivamente recursos (como memória ou processamento por exemplo), de forma que ele não possa mais fornecer seu serviço;

• obstruir mídia de comunicação entre os utilizadores de forma a não se comunicarem adequadamente;

e) vírus e outros códigos maliciosos;

f) sequestro de dados (*ransomware*);

g) desfiguração de sites;

h) modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do proprietário;

i) desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

6.1 GESTÃO DE INCIDENTES DE SEGURANÇA

O gerenciamento de incidente de segurança é um processo, em que se registram os incidentes de segurança e de privacidade ocorridos e que armazene informações como:

• descrição dos incidentes ou eventos;

• informações e sistemas envolvidos;

• medidas técnicas e de segurança utilizadas para a proteção das informações;

• riscos relacionados ao incidente e as medidas tomadas para mitigá-los.

A ISO/IEC 27035–1:2016, p. 3-4, abrange as cinco fases principais para a gestão de incidentes de segurança da informação, como indica a figura 12.

Figura 12 – Fases da gestão de incidentes de segurança da informação.

Fonte: elaborado por Allan Kovalscki.

A ISO 27.035 está dividida em três partes diferentes: ISO/IEC 27035-1, ISO/IEC 27035-2 e ISO/IEC 27035-3. Cada parte aborda aspectos específicos do gerenciamento de incidentes de segurança da informação (Isim). A seguir apresentamos uma breve descrição de cada parte:

i) ISO/IEC 27035-1:2016 – Parte 1: conceitos e princípios gerais:

• esta parte estabelece os conceitos e princípios gerais para o Isim, define os termos relacionados a incidentes de segurança da informação;

• fornece uma estrutura para o Isim, incluindo a abordagem do ciclo de vida do incidente;

• oferece orientações sobre a preparação e a melhoria contínua do Isim;

ii) ISO/IEC 27035-2:2016 – Parte 2: diretrizes para implementação do Isim:

• esta parte fornece diretrizes práticas para implementar o Isim em uma organização;

• aborda aspectos específicos do ciclo de vida do incidente, incluindo detecção, relato, avaliação, resposta e revisão;

• oferece orientações sobre a preparação e a resposta a incidentes, incluindo a coordenação com partes externas;

iii) ISO/IEC 27035–3:2013 – Parte 3: Diretrizes para Cooperação entre Organizações:

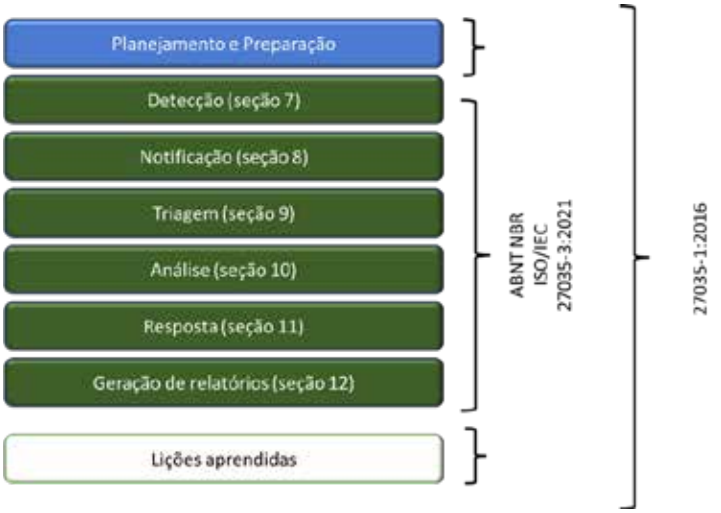
• esta parte trata da cooperação entre organizações no contexto do Isim;

• fornece orientações sobre a colaboração e a comunicação eficazes entre organizações durante e após incidentes de segurança da informação;

• aborda a troca de informações e a coordenação de atividades relacionadas a incidentes entre diferentes entidades.

A figura 13 exibe um gráfico para ilustrar melhor cada fase do ciclo de vida das operações de resposta a incidentes com as respectivas normas.

Figura 13 – ciclo de vida das operações de resposta a incidentes.



Fonte: elaborado por Allan Kovalscki, adaptado da ISO 27035-3:2021, p. 5.

Entrando mais a fundo no ciclo de vida das operações de resposta a incidentes, temos:

• *planejamento e preparação*: a gestão de incidentes requer um adequado planejamento e preparação. Devemos realizar atividades preparatórias, tais como: formular e produzir uma política de gestão de incidentes e comprometimento da alta administração, análise de risco, plano de gestão de incidentes, estabelecimento de equipe de resposta a incidentes, plano de testes e outros;

• *detecção*: as operações de detecção de incidentes requerem que haja um ponto de contato (PoC) para receber informações e uma metodologia estabelecida para a equipe detectar eventos de segurança da informação. A detecção é importante porque inicia as operações de resposta a incidentes.

Os incidentes de segurança da informação podem ser identificados internamente por um indivíduo ou por ferramentas de segurança cibernética, ou ainda

serem informados por fontes externas. Esses incidentes podem ser reconhecidos de diversas maneiras e categorizados nos seguintes três métodos:

i) técnicos:

• sistemas de detecção e prevenção de intrusões (IDPS);

• ferramentas de segurança para terminais, como software antivírus;

• ferramentas de análise de logs de segurança ou sistemas de gestão de informações e eventos de segurança (Siem);

ii) de pessoas:

• usuários internos ou externos, incluindo equipe não relacionada à TI ou à segurança, ou clientes;

iii) organizacional:

• departamento de TI, incluindo o centro de operações de rede e o suporte técnico de TI;

• prestadores de serviços gerenciados;

• equipe de respostas a incidentes de segurança (CSIRT);

• outras unidades e funcionários que possam detectar anomalias durante o trabalho diário;

• meios de comunicação de massa (jornal, televisão etc.);

• websites (websites de informações sobre segurança pública, websites de pesquisadores de segurança, websites de arquivo de desfiguração etc.).

6.1.1 Notificação

A geração de relatório de incidentes é usada para todos os tipos de eventos, para fins de comunicação de incidentes. A geração de relatório de incidentes consiste em três fases, que podem ser descritas como:

i) *operação de notificação de incidentes*: o evento de segurança de TIC detectado, que é um incidente em potencial, é relatado (geração de relatório de eventos) da fonte (pessoas, aviso de organização externa ou alerta do sistema) ao PoC;

ii) *geração de relatório de incidente interno*: dependendo das características do incidente, vários tipos de geração de relatórios internos são incluídos como parte da geração de relatório de incidentes (ver seção 12 da ABNT NBR ISO/IEC 27035-3:2021, p. 30);

iii) *geração de relatório de incidentes externos à organização*: pode precisar relatar certos tipos de incidentes a terceiros externos à organização (para fins de regulamentação), ou às autoridades, ou a outras partes identificadas (como fornecedores, clientes etc.). Isso também pode fazer parte da operação do incidente, mas também pode ser separado, dependendo da estrutura da gestão de incidentes e das características do incidente (ver seção 12 da ABNT NBR ISO/IEC 27035-3:2021, p. 31).

6.1.2 Triagem

A triagem é o processo de classificação, categorização, correlação, priorização e atribuição de eventos recebidos, relatórios de incidentes, relatórios de vulnerabilidade e outras solicitações de informações gerais. Isso pode ser compara-

do à triagem em um hospital, em que os pacientes que necessitam ser atendidos imediatamente são tratados com maior prioridade e, portanto, são separados daqueles que ainda podem esperar por assistência.

O processo de triagem envolve os seguintes estágios:

i) *determinação da gravidade do incidente*: baseia-se no impacto aos negócios da organização, nos *hosts* envolvidos, no método de atividade de ataque usado, no tempo dos "ataques" e no(s) número(s) de referência;

ii) *correlação com outros relatórios*: a correlação analisa quantos relatórios estão ligados a um incidente específico. Isso pode ajudar a determinar o escopo e a gravidade da atividade;

iii) *priorização*: se o evento não fizer parte de um incidente em andamento, depois de categorizado, ele será passado para o estágio de priorização. Certas categorias de eventos podem realmente ter as suas próprias prioridades predefinidas. Muitas vezes, pode ser necessário uma análise adicional para determinar a prioridade. Os critérios de decisão de priorização podem envolver o seguinte:

- nível de perigo para a vida humana;
- impacto na reputação;
- paradas ou danos nas operações;
- proteção de informações confidenciais;
- limitação de perdas financeiras;
- manutenção da integridade da infraestrutura;
- ameaça aos sistemas CSIRT;
- ameaça à infraestrutura crítica;
- tipo de atividade;
- escopo da atividade;

• relacionamento com outras atividades contínuas relacionadas à segurança e não relacionadas à segurança.

6.1.3 Atribuição

Se as informações forem notáveis ou suspeitas, são atribuídas a alguém no processo de análise e repassadas para esse processo. Convém que seja observado que a categorização e a prioridade, assim como a atribuição, podem ser alteradas quando o evento é analisado no processo de resposta.

6.1.4 Análise

A análise de incidentes é definida como a série de etapas analíticas adotadas ao tentar verificar quais são a causa e o efeito de um incidente. Existem diferentes tipos de análises técnicas que podem ser conduzidas ao lidar com um incidente. Exemplos incluem, mas não estão limitados aos seguintes:

i) *análise de sistema* – o processo de adquirir, preservar e analisar artefatos do sistema (por exemplo, arquivos de log ou informação do registro) que possam auxiliar na determinação da causa do incidente e no desenvolvimento de roteiros de ação;

ii) *análise de rede* – o processo de coletar, examinar e interpretar tráfego de rede para identificar e responder aos eventos que violam a política de segurança ou a postura dos recursos conectados à rede ou à infraestrutura de rede, e usados para dar apoio à investigação de incidentes de segurança de computadores;

iii) *análise de malware* – o processo de identificar, analisar e caracterizar artefatos reportados de software (por exemplo, assinaturas de vírus, worms, ca-

valos de Troia etc.), suspeitos de constituir técnicas e métodos dos adversários para auxiliar em ações e em estratégias de mitigação em profundidade, ações de contrainteligência e atividades de aplicação da lei;

iv) *análise forense* – a análise forense em incidentes de informação refere-se ao processo sistemático de coleta, preservação, análise e apresentação de evidências digitais relacionadas a incidentes de segurança da informação. O objetivo principal dessa análise é determinar a natureza do incidente, identificar as partes envolvidas, entender a extensão do impacto e fornecer insights para evitar incidentes futuros.

6.1.5 Resposta

O principal propósito de uma resposta a um incidente é conter, erradicar e recuperar um incidente. Os objetivos primários para o processo de resposta são:

i) parar ou minimizar os efeitos ou danos do ataque, mantendo a continuidade da missão operacional;

ii) assegurar a recuperação efetiva e oportuna dos sistemas, de forma a prevenir que incidentes semelhantes ocorram novamente;

iii) reforçar a postura defensiva e a prontidão operacional da organização;

iv) assegurar que atividades de resposta ocorram de uma maneira que protejam quaisquer dados, de acordo com o seu nível de sensibilidade;

v) oferecer apoio à caracterização de ataques, rápida e completa;

vi) desenvolver e implementar cursos de ação;

vii) remediar ou mitigar a atividade;

viii) recuperar os sistemas para o nível operacional normal;

ix) melhorar os processos de infraestrutura e de tratamento de incidentes.

6.1.6 Geração de relatórios

A geração de relatório de incidentes é uma parte importante da avaliação e das decisões de incidentes para coordenar as respostas corretas. É uma parte essencial das operações de incidentes que os canais e formatos de geração de relatórios sejam estabelecidos para obter respostas rápidas a um incidente. Além disso, as organizações analisam incidentes para descobrir questões ou problemas que coloquem seus clientes e outros clientes em risco.

Convém que os seguintes requisitos e orientações sejam seguidos para a geração de relatório:

i) fornecer a definição de um incidente para a organização;

ii) fornecer uma explicação sobre porque convém que um indivíduo ou grupo tenha um relatório;

iii) identificar para quem ou para onde convém que o relatório seja enviado;

iv) fornecer uma explicação sobre como relatar;

v) fornecer uma descrição de quais informações críticas convém que sejam incluídas em um relatório;

vi) fornecer uma explicação sobre quando relatar.

6.1.7 Lições aprendidas

Ocorre quando os incidentes são resolvidos. Devem ser extraídas as lições aprendidas sobre como os incidentes e vulnerabilidades foram tratados, que melhorias podem ser introduzidas no processo e em situações futuras.

6.2 RELAÇÃO DA GESTÃO DE INCIDENTES COM A LGPD

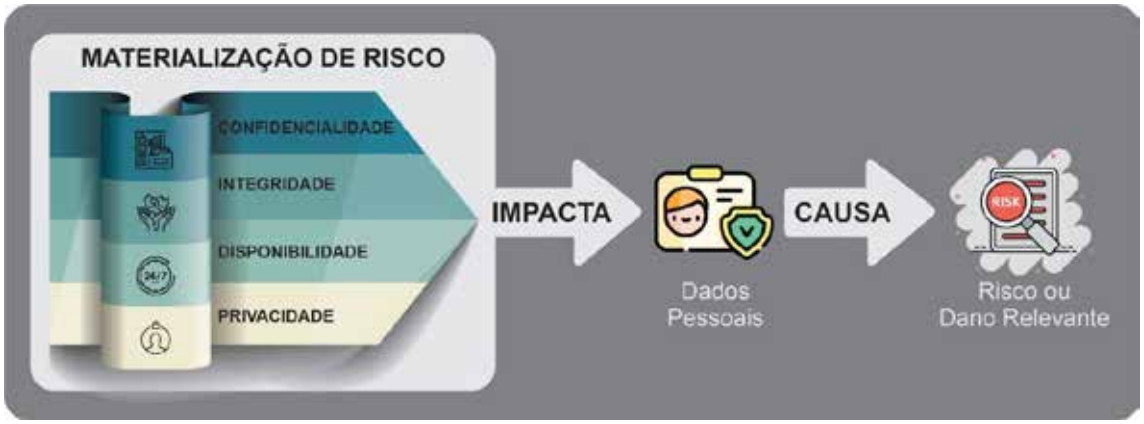
O artigo 48 da lei 13.709/2018 (LGPD) estabelece que “O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares”.

No dia 23/12/2022, a ANPD publicou orientações quanto à comunicação de incidente de segurança, tendo sido atualizada em 31/05/2023. Tal documento visa orientar quanto à comunicação da ocorrência aos titulares dos dados pessoais violados. Essa é uma importante medida de mitigação de danos, uma vez que os titulares poderão tomar conhecimento do ocorrido e adotar medidas de precaução para mitigar os riscos a que foram expostos em razão de possíveis incidentes.

Na ANPD, é a Coordenação–Geral de Fiscalização (CGF) quem recebe as comunicações de incidente de segurança e dá a elas o tratamento necessário, bem como é a responsável por fiscalizar e aplicar as sanções administrativas cabíveis.

Sendo assim, sempre que houver um incidente com dados pessoais, que sejam relacionados a alguma das perspectivas de risco listadas na ISO 27.001 e que traga risco ou dano relevante aos titulares, isso deverá ser comunicado à ANPD e aos titulares impactados.

Figura 14 – Critérios para comunicação de incidentes.



Fonte: elaborado por Allan Kovalscki, adaptado de Comunicação [...] (2024).

Assim, um incidente precisa ser comunicado se atender, cumulativamente, aos seguintes critérios:

- tenha a ocorrência confirmada pelo agente;
- envolva dados pessoais sujeitos à LGPD;
- acarrete risco ou dano relevante aos titulares dos dados.

Na avaliação de risco do incidente, devem ser considerados, dentre outros aspectos:

- contexto da atividade de tratamento de dados;
- as categorias e quantidades de titulares afetados;
- os tipos e quantidade de dados violados;
- os potenciais danos materiais, morais e reputacionais causados aos titulares;

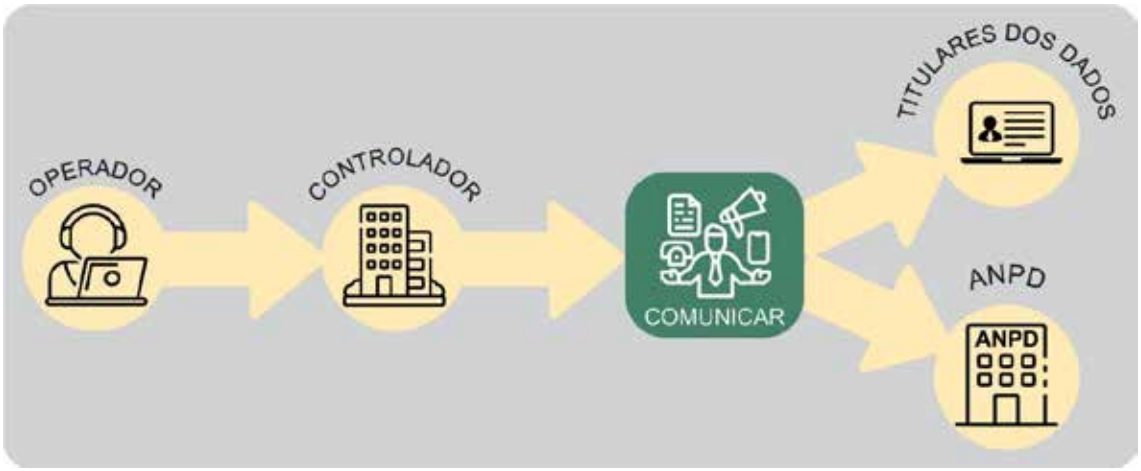
• se os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares;

• as medidas de mitigação adotadas pelo controlador após o incidente.

A obrigação legal de comunicar o incidente de segurança aos titulares e à ANPD é do controlador, nos termos do art. 48 da LGPD. No entanto, a obrigação de adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais estende-se a todos os agentes de tratamento de dados, inclusive aos operadores.

Quando um incidente de segurança ocorre, o operador deverá informar o fato, sem demora injustificada, ao controlador dos dados. Todas as informações necessárias à comunicação do incidente de segurança à ANPD e aos titulares deverão ser fornecidas pelo operador ao controlador.

Figura 15 – Obrigações quando ocorrer um incidente com dados pessoais .



Fonte: elaborado por Allan Kovalscki, adaptado de Comunicação [...] (2024).

Por fim, poderão ser aplicadas medidas preventivas e sanções, dentre outras situações, nos casos em que o controlador:

• não comunicar o incidente à ANPD e aos titulares em tempo razoável;
• não comunicar o incidente aos titulares de dados pessoais afetados;
• não adotar medidas de segurança técnicas e administrativas compatíveis aos riscos de suas atividades de tratamento de dados.

Dessa forma, observa-se que não basta ter um bom processo de gestão de incidentes da segurança da informação, mas também se deve atentar para as legislações vigentes, a fim de evitar impactos significativos às organizações, tanto na perspectiva financeira quanto à imagem legal e/ou operacional.

7
INTEGRAÇÃO, INTEROPERABILIDADE E INCLUSÃO DIGITAL

Precisamos destacar que, nas prefeituras do Brasil e na diversidade de nossos 5.568 municípios, temos disparidades econômicas e divergências tecnológicas, ou seja, diferentes equipamentos, tecnologias, sistemas operacionais, sistemas, métodos, metodologias, e precisamos lembrar de que, independentemente das divergências, precisamos ter métodos para fazer convergir as comunicações e as transferências dos dados e das informações.

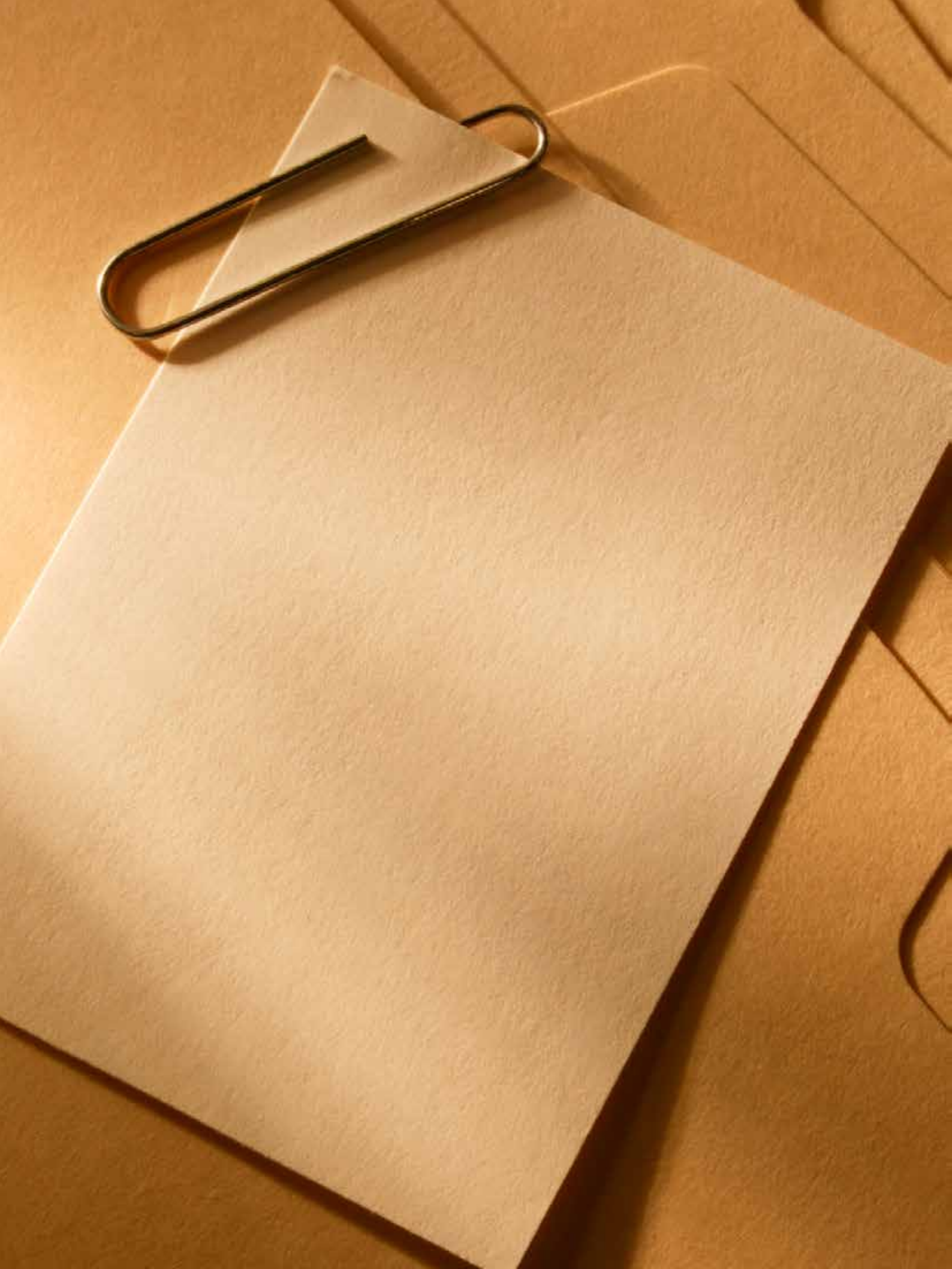
Temos, no Brasil, os manuais que abordam os padrões de interoperabilidade do governo eletrônico (ePING), nos quais temos todos os métodos e protocolos que viabilizam a comunicação de sistemas, serviços, programas e tecnologias para as atividades de tecnologia, comunicações e informações.

Outra importante referência são os modelos de acessibilidade governo (eMAG), que trazem orientações de acessibilidade, tamanho de cédulas, comunicabilidade, métodos de ajuda on-line, formas de acessibilidade para pessoas com deficiências visuais, tamanhos de cédulas, formas de comunicação e integração social.

Esses métodos também interagem com a Lei Geral de Proteção de Dados Pessoais, e nós temos que ter a percepção de que esse universo é maior do que os mundos jurídicos, tecnológicos, telemáticos, informáticos e das comunicações.

O nosso universo atua com pessoas, e pessoas movimentam produtos, serviços e capitais.

Os requisitos da Política Nacional de Proteção e Privacidade de Dados, ainda que entregues em meados do ano de 2022, ainda não foram devidamente apreciados, ponderados e objeto de sugestões de nossa Autoridade Nacional de Proteção de Dados.



REFERÊNCIAS

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jan. 2022.

CALDER, Allan; MATKINS, Steve. **IT Governance**: an international guide to data security and ISO 27.001/27.002. 6. ed. [*s.l.*]: Editora KoganPage, 2015.

CIASULLO, Maria Vincenza; LIM, Weng Marc. Editorial: Digital transformation and business model innovation: advances, challenges and opportunities. **Int. J. Quality and Innovation**, v. 6, n. 1, 2022.

COMUNICAÇÃO de incidente de segurança. **Autoridade Nacional de Proteção de Dados**, 18 set. 2024. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 10 out. 2024.

FEZZEY, Tyler; BARCHELOR, John H.; BURCH, Gerald F.; and REID, Randall. Cybersecurity Continuity Risks: Lessons Learned from the COVID–19 Pandemic. **Journal of Cybersecurity Education, Research and Practice**, v. 2022, n. 2, 2023.

POURMAJID, William; ZHANG, Lei; STEINBACHER, John; ERWIN, Tony; MIRANSKYY, Andriy. A reference architecture for observability and compliance of cloud native applications. **Computer Science**, Software Engineering, 2023. Disponível em: https://arxiv.org/abs/2302.11617. Acesso em: 19 dez. 2021.


IGCP
INSTITUTO LATINO-AMERICANO
DE GOVERNANÇA E COMPLIANCE PÚBLICO
RGB
DA GOVERNANÇA
À ESPERANÇA
MENTE ABERTA