Dataset Reports 3:1 (2024)
ISSN 2965-1182

RESEARCH ARTICLE

DATASET REPORTS

Política de resposta a incidentes cibernéticos e estratégias de aderência à legislação brasileira

Cyber incident response policy and strategies for compliance with Brazilian regulation

Fabio José Buchedid Vazquez [a*]

[a] Fundação Escola Nacional de Seguros, 20031-205, Rio de Janeiro, Rio de Janeiro, Brasil.

Resumo
Com o crescente aumento dos riscos cibernéticos, a proteção de dados e a conformidade com a legislação têm se tornado prioridades cruciais para organizações no Brasil. Este artigo explora a importância da política de resposta a incidentes cibernéticos e apresenta estratégias eficazes para garantir a aderência às normas legais brasileiras. Os riscos cibernéticos, que incluem ataques a sistemas e vazamentos de dados, têm mostrado um crescimento exponencial, afetando tanto empresas quanto indivíduos. A Lei Geral de Proteção de Dados (LGPD) impõe exigências rigorosas sobre a proteção de informações pessoais, com penalidades severas para violações. A política de resposta a incidentes é uma ferramenta essencial para mitigar esses riscos, permitindo que as organizações detectem, respondam e se recuperem de ataques cibernéticos de forma eficaz. Este artigo detalha as melhores práticas para desenvolver e implementar essas políticas, abordando desde a identificação e avaliação de riscos até a comunicação e o treinamento das equipes envolvidas. Além disso, discute a integração dessas práticas com os requisitos da LGPD, destacando a necessidade de uma abordagem proativa para a conformidade. Ao adotar estratégias robustas de resposta a incidentes e garantir a conformidade com a legislação, as organizações podem não apenas proteger seus ativos e dados, mas também fortalecer sua posição no mercado e aumentar a confiança de clientes e parceiros.

Palavras-chave: Política de resposta a incidentes. Riscos cibernéticos. Conformidade legal. Lei Geral de Proteção de Dados. LGPD. Proteção de dados. Encarregado. Estratégias de segurança.

Abstract
With the growing increase in cyber risks, data protection and compliance with legislation have become crucial priorities for organizations in Brazil. This article explores the importance of cyber incident response policies and presents effective strategies for ensuring adherence to Brazilian legal standards. Cyber risks, including attacks on systems and data breaches, have shown exponential growth, affecting both businesses and individuals. The General Data Protection Regulation (GDPR) imposes strict requirements on personal data protection, with severe penalties for violations. A cyber incident response policy is an essential tool for mitigating these risks, allowing organizations to effectively detect, respond to, and recover from cyber-attacks. This article details best practices for developing and implementing these policies, covering risk identification and assessment, as well as team communication and training. Additionally, it discusses how to integrate these practices with GDPR requirements, highlighting the need for a proactive approach to compliance. By adopting robust incident response strategies and ensuring legal compliance, organizations can not only protect their assets and data but also strengthen their market position and enhance trust with clients and partners.

Keywords: Incident response policy. Cyber risks. Legal compliance. General Data Protection Regulation. GDPR. Data Protection. Data Protection Officer. DPO. Security strategies.

Graphical Abstract

*Corresponding author: Fabio J. B. Vazquez. E-mail address: fabio.vazquez@gmail.com
Submitted: 12 September 2024; Accepted: 18 September 2024; Published: 19 September 2024.

ROYALDATASET

1. Introdução

Riscos cibernéticos, ou cyber risks, estão se tornando cada vez mais frequentes e prejudiciais. O número desses ataques aumenta exponencialmente a cada ano, resultando em prejuízos que chegam a bilhões de reais. Esses riscos não afetam apenas empresas, mas também indivíduos, frequentemente devido a práticas inseguras, como o uso de senhas fracas e a ausência de autenticação de dois fatores. Duo, Zhou e Abusorrah (2022) destacam que as ameaças a sistemas cibernéticos físicos são uma preocupação crescente, com recentes avanços e desafios na área de segurança.

Um estudo americano prevê que, se as empresas não começarem a tomar medidas preventivas, em breve uma a cada três empresas acabarão sendo alvo dos riscos cibernéticos. De acordo com a Aon plc (s.d.), o risco cibernético figura entre as dez principais preocupações dos executivos, conforme indica a pesquisa Global de Gerenciamento de Riscos (Global Survey). Li e Liu (2021) revisam as tendências emergentes e desenvolvimentos recentes em cibersegurança e ressaltam a crescente importância da proteção contra ataques cibernéticos.

A análise das regulamentações de cibersegurança nos Estados Unidos e no Brasil, realizada por Brustolin (2019), oferece uma visão sobre as abordagens regulatórias distintas e suas implicações. Ghelani (2022) realiza uma revisão das ameaças cibernéticas e suas implicações futuras, destacando a necessidade de uma abordagem abrangente para enfrentar esses desafios.

Neste sentido, é essencial compreender o conceito de risco, definido como a probabilidade de um perigo, com ou sem ameaça física, que pode causar danos financeiros ou colocar vidas em perigo. Os perigos virtuais são variados e a prevenção é crucial. Falhas como o uso de senhas fracas, falta de atualizações de software e falhas na programação são vulnerabilidades que podem ser exploradas por invasores (Blum, Vainzof, & Moraes, 2021; Hurel & Lobato, 2022).

2. Riscos

É importante definir o que é um risco: “risco é a probabilidade de um perigo, com ou sem ameaça física, que possa causar danos financeiros ou ainda pôr a vida de alguém em perigo.” E quais são os perigos virtuais? São muitos, a chave é entender quais são as ameaças e como se prevenir. Eis alguns exemplos:

> - As senhas são um dos principais riscos. Utilização de senhas fracas como sequências numéricas, datas de aniversário e outros, são facilmente quebradas com algoritmos.
>
> - Manter softwares inadequados ou sem atualização também são uma grande fonte de brechas para invasão de hackers;
>
> - Manter portas do computador aberto são um chamariz para invasores. Contrate uma equipe de TI qualificada para fazer um diagnóstico nos computadores de sua empresa e encontrar e corrigir possíveis debilidades;
>
> - Falhas em programação presentes no site ou sistemas também podem permitir ataques via SQL injection e outros.

Os riscos virtuais podem causar danos à reputação de uma empresa, reduzir sua credibilidade, ou ainda, tornar todo um sistema inoperante. A responsabilidade por dados de terceiros tem também se tornado uma crescente fonte de preocupação à medida que cada vez mais as empresas estão dependentes da tecnologia para gerenciar seus negócios e informações. Hoje, praticamente todas as empresas trabalham com dados pessoais e corporativos, como número de cartão de crédito, identidade, endereço, registros médicos, passaporte, lista de clientes, orçamento, planos de negócios, planos de marketing etc.

As informações ficam mais expostas a vazamento ou roubo de informação com o avanço da tecnologia com o armazenamento em nuvem (cloud computing), redes sociais e até mesmo pelos hábitos de mobilidade e conceito de produtividade onde a maioria dos profissionais utilizam celulares, tablets e notebook para trabalhar.

A promessa do deep learning é concretizar sistemas preditivos que se difundem e se adaptam bem, melhoram continuamente à medida que novos dados são adicionados e são mais dinâmicos do que sistemas preditivos baseados em regras de negócios. Você não mais adapta um modelo, você o treina.

Com a Lei geral de proteção de dados, as empresas correm ainda maiores riscos, uma vez que o vazamento de dados pessoais pode gerar multas milionárias para as empresas, podendo chegar ao valor de R$ 50 milhões.

Assim, o objetivo deste artigo é conscientizar as organizações sobre este risco iminente divulgando as melhores práticas a serem adotadas para a gestão dos riscos cibernéticos.

3. Política de resposta a incidentes e estratégia de aderência à legislação

Em conformidade com a Lei Geral de Proteção de Dados Pessoais - Lei Nº 13.709, de 14 de agosto de 2018, artigo 50 (planejamento estratégico):

> “Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.”

Articular defesas em camadas, nos mecanismos de inteligência: conceitualmente, diante da amplitude e complexidade do papel da segurança, é comum estudarmos os desafios em camadas ou fases, particionando todo o trabalho para tornar mais claro o entendimento de cada uma delas. Elencamos as seis defesas da segurança:

I. Defesa 1, **Desencorajar**: esta é a primeira das cinco defesas de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos e humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas, já são efetivos nesta fase.

II. Defesa 2, **Dificultar**: o papel desta defesa é complementar à anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Como por exemplo, podemos citar os dispositivos de autenticação para acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, senhas, smartcards e certificados digitais, além da criptografia, uso de blockchain, firewall, sistema de inteligência artificial para entender “behavior” (comportamento) atípico de uma possível intrusão.

III. Defesa 3, **Discriminar**: aqui o importante é se cercar de recursos que permitam identificar e gerir acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e bancos de dados. Os processos de avaliação e gestão do volume de uso de recursos, como e-mail, impressora, ou até mesmo fluxo de acesso físico aos ambientes, são alguns exemplos das atividades desta defesa.

IV. Defesa 4, **Detectar**: mais uma vez agindo de forma complementar às suas antecessoras, esta defesa deve munir a solução de segurança de dispositivos que sinalizem, alertem e instrumentem os gestores da segurança na detecção de situações de risco. Seja

em tentativa de invasão, uma possível contaminação de vírus, o descumprimento da política de segurança da empresa, ou cópia e envio de informações sigilosas de forma inadequada. Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como antivírus e o sistema de detecção de intrusos, que reduzirão o tempo de resposta à incidentes.

V. Defesa 5, **Deter**: esta quinta defesa representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta defesa, ativando seus mecanismos de controle, é um sinal de que as defesas anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são exemplos.

VI. Defesa 6, **Diagnosticar**: apesar de representar a última defesa, esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança da informação. Pode parecer o fim, mas é o elo de ligação com a primeira defesa, criando um movimento cíclico e contínuo. Devido a esses fatores esta é a defesa de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto aspectos tecnológicos quanto físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa.

Percebemos que tais defesas estão no escopo do Gerenciamento de processos de negócio (ou "Business Process Management"), que se resumem numa tríade da inteligência da empresa: pessoas, processos e tecnologia, mas para que seja uma gestão exitosa, observamos a necessidade de inclusão de um quarto item: a comunicação.

Mas ainda assim, a quebra de segurança é inevitável, podendo alguma das defesas acima serem transpostas, o que chamamos de "incidente". Durante um incidente, onde é constatado a violação da segurança, há necessidade de ações administrativas e técnicas para lidar com o problema e mitigá-lo.

4. Antes do incidente: planejamento tático

Recomendamos fortemente que a empresa busque o mais alto nível de compreensão de sua infraestrutura de tecnologia da informação para saber como reagir quando um incidente de segurança ocorrer. O "day zero attack", termo proveniente do inglês para descrever a ameaça de uma vulnerabilidade de segurança desconhecida para o qual não existe ainda uma correção, e os desenvolvedores, por desconhecerem a ameaça, não tiveram oportunidade de lidar com o problema e trabalhar em uma possível correção.

Existem Ferramentas de Diagnóstico de Risco Cibernético que ajudam a identificar os principais fatores internos e externos que podem afetar seu nível de exposição a riscos cibernéticos. Além disso, ela ajudará a enxergar drivers relevantes de risco cibernético e fornecerá orientações práticas referentes à estrutura de governança que a empresa pode adotar como parte de uma estratégia eficaz de gerenciamento de riscos cibernéticos.

Tecnicamente é fundamental efetuar exercícios de "Pentest", termo proveniente do inglês que é abreviação de "Penetration Test" que significa "Teste de Penetração". Os testes de penetração são exercícios simulados de um ataque real cujo objetivo é avaliar a segurança de um sistema ou uma rede, tais como:

- Rede IP (IP é acrônimo de Internet Protocol). No contexto de uma rede IP, para que os hosts (computadores, notebooks, impressora, ou outro dispositivo "smart" IOT – Internet of Things – Internet das Coisas) da rede tenham condições de se comunicar, é necessário que essa rede possua um mecanismo de identificação. Essa identificação utilizada nos hosts das redes de computadores é o que conhecemos como endereço IP.
- Websites;
- Serviços de correio eletrônico;
- Bancos de dados.

O objetivo é respaldar-se em processos de avaliação de riscos à privacidade, como alicerce de modelo de gestão voltado à conformidade; como ação constante e preventiva, no ecossistema de proteção de dados.

Para o "Pentest", pode-se adquirir softwares no mercado, a exemplo do "Nessus", que é uma ferramenta muito poderosa da "Tenable" para verificação de falhas e vulnerabilidades de segurança; ou pode-se contratar equipe terceirizada nesse sentido, mantendo um "SOC – Security Operations Center", como plano de proteção de cybersecurity para empresas que buscam reduzir a exposição das informações e mitigar os riscos internos e externos. Podendo contratar "SOC-as-a-Service", que seria um conjunto de tecnologias e infraestruturas capazes de prevenir, detectar e responder a incidentes e ameaças de cybersecurity. Em outras palavras, o SOC coleta eventos de diferentes fontes, faz a análise, identifica anomalias e refina esse processo para gerar alertas. No mercado temos o exemplo da "RealProtect", que oferece soluções "SOC-as-a-Service".

4.1 Caçar as ameaças e não esperar ser atacado ("threat hunter")

Todos os funcionários devem estar cientes que qualquer vulnerabilidade ou ação diferenciada nos sistemas ou nas máquinas devem ser relatadas imediatamente à TI e ao Encarregado, tais como:

- phishing, mensagem eletrônica enviada por criminosos digitais, seja por e-mail, SMS, Whatsapp, Telegram, "banner clickbyte", etc, e que parece legítimo, mas que é uma tentativa de buscar uma ação inadvertida da vítima, que temo como consequência um incidente de violação de segurança;
- caixas de diálogo estranhas ou novas, que podem ser uma isca para aceite de uso inadvertido de software malicioso, para instalação de malware, para rastreabilidade oculta de dados;
- o objetivo mais comum dessas abordagens, é violar o sistema para obtenção de informações sigilosas (portanto, muitas vezes valiosas), pelo clique em links ou imagens dos e-mails phishing, se utilizando de um tipo de software nocivo ransomware, que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate (como em um sequestro) normalmente em criptomoedas, para que o acesso possa ser restabelecido. Caso não ocorra o mesmo, arquivos podem ser perdidos e até mesmo publicados.

A área de TI deverá elaborar *guidelines* explicando quais padrões e medidas técnicas devem ser seguidas pelos funcionários:

- jamais permitir uso de quaisquer dispositivos de memória, seja por fita magnética, disquete, zip drive, drive externo, token de memória, pen drive que não seja autorizado pela TI;
- jamais permitir o download e/ou instalação de software não autorizado pela TI, seja ele freeware, demo, ou do tipo "try before you buy" e/ou pago;
- a gestão de TI deve ser ter controle e monitoramento por "endpoint", estabelecendo políticas de acesso a sites e instalação de softwares, de forma restritiva e de gestão centralizada.

Caso o funcionário verifique alguma ação diferente nas máquinas ou sistemas da empresa, deverá relatar a situação suspeita, informando o dia e horário que teve início. A Notificação deve ser encaminhada para a área de TI e para o Encarregado.

Os funcionários devem ser alertados para não desligarem as máquinas nem efetuarem qualquer alteração. O importante é interromper qualquer atividade em andamento (colocar a máquina offline) e limitar a comunicação com os sistemas afetados, mas sem apagar as pistas ou contaminar as evidências.

Equipe de TI deve constatar minimamente se realmente é uma possível incidente de violação de segurança. Caso positivo, notificar imediatamente o Encarregado.

A necessidade de capacitação e aculturamento em segurança da informação, para todos os colaboradores da corporação, é um fator crítico de sucesso: treinar e superar, até conseguir atingir um nível mínimo de entendimento e máximo em excelência.

Implementar é adquirir, configurar e aplicar os mecanismos de controle de segurança a fim de atingir o nível de risco adequado. Comumente esta atividade faz parte de uma orientação obtida pela análise de riscos ou por sugestões de normas específicas de segurança (baseadas na Norma ISO 27001). O universo de controles aplicáveis é enorme, pois estamos falando de mecanismos destinados à segurança física, tecnológica e humana. Se pensarmos no "peopleware", ou seja, no capital humano como um dos elos mais críticos e relevantes para a redução dos riscos, teríamos, por exemplo, os seguintes controles:

- seminários de sensibilização;
- cursos de capacitação;
- campanhas de divulgação da política de segurança;
- crachás de identificação;
- procedimentos específicos para demissão e admissão de funcionários;
- procedimentos específicos para tratamento de recursos terceirizados;
- termo de responsabilidade: deixar claro para todos os colaboradores, mesmo em caso de desligamento da empresa, aspectos civis e criminais da Lei 12.737 de 30/11/2012 (Lei Carolina Dieckmann);
- termo de confidencialidade: deixar claro para todos os colaboradores, mesmo em caso de desligamento da empresa, aspectos civis e criminais da Lei 13.709 de 14/08/2018 (LGPD);
- softwares de auditoria de acessos;
- softwares de monitoramento e filtragem de conteúdo;
- plano de continuidade dos negócios, após ataque cibernético ou por vazamento de dados (data breaches);
- contratação de Seguro de Riscos Cibernéticos (Cyber Insurance);
- contratação de Seguro D&O – Responsabilidade Civil para Diretores e Administradores. Esta é uma categoria de seguro que visa proteger o gestor da empresa (presidente, conselheiro, diretor ou gerente) diante uma possível responsabilização pessoal a terceiros decorrente de seus atos enquanto tomador de decisões – abrange inclusive o DPO - Data Protection Officer;
- simulação de Incidentes à segurança – SIS.

Para cada projeto na empresa, se aculturar no "Security by design", que é um conceito de grande importância para a indústria de segurança da informação. Significa pensar em segurança desde o escopo de desenvolvimento de um novo software, prevendo toda possibilidade de riscos aos quais aquela aplicação pode estar sujeita.

Conhecida a gestão de compliance, pontos fortes e fracos dos atuais controles de sistemas de informação, físico, lógico e humano, da empresa; elaborar um "check list" dos passos identificados quando se tem uma incidência de ataque cibernético, ou vazamento de dados ("data breaches"). Esse checklist será o balizador para oficialmente detectar um "incidente" de violação de proteção à privacidade de dados, pode ser elaborado por quem tem a visão total dos fluxos de processos da empresa ou conjuntamente, os quais sugerimos a participação dos seguintes sujeitos:

- DPO - Data Protection Officer, o Encarregado, responsável por auxiliar as empresas que fazem tratamento de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade.
- CRO - Chief Risk Officer, responsável por permitir a governança eficiente e eficaz de riscos significativos e oportunidades relacionadas a uma empresa e seus vários segmentos;
- BISO - Business Information Security Officer, responsável pela Segurança da Informação, é quem avalia os riscos e impactos nos negócios;
- CISO - Chief information security officer, responsável por estabelecer e manter a visão, estratégia e programa da empresa para garantir que os ativos e tecnologias da informação sejam adequadamente protegidos.

5. Durante o incidente: planejamento tático e operacional

A atuação da equipe deverá ser tática e operacional, ou seja, deve haver ações administrativas e técnicas, objetivando manter a continuidade dos negócios, para de forma precisa identificar fraudes, bloquear falhas, comunicação adequada e reestabelecer o serviço. Assim, podemos adotar os seguintes protocolos:

1 Convocar o Comitê de Privacidade de dados da empresa;
2 A depender do tamanho do incidente, será necessário convocar parceiros externos (empresa especializada para data breach, Assessoria de imprensa especializada, Empresa de Marketing e propaganda);
3 Formar um Comitê de Crise (é um time pequeno, normalmente composto por pessoal de TI, pessoal de Compliance – Jurídico e RH – para Comunicação) em uma Sala de Guerra, onde todas as informações vão ser encaminhadas, com o objetivo de detecção e análise do problema para ter um canal de comunicação facilitado com os Superiores (Diretoria e Presidência). Onde não poderá ser comunicada nenhuma informação fora daquele local. Serão definidas as ações organizativas; nesse momento será decidido, conforme amplitude detectada, a comunicação às Diretorias e a comunicação da indisponibilidade aos demais colaboradores, sem muito alarde para não gerar ansiedades.
4 Registrar todas as ações, desde a convocação do Comitê de Privacidade;
5 Levantar e reunir todas as informações do incidente. Definir se o problema foi interno dos funcionários ou externo.
6 Correção imediata da vulnerabilidade sistêmica, por patch de atualização, "shift-left" ou "pipeline" de desenvolvimento (correção técnica);
7 Monitoramento de eventos e mapear danos;
8 Avaliação do Comitê de Crise sobre ações urgentes, ações importantes e necessárias;
9 Confirmação do evento e necessidade de publicidade: cliente, funcionários, parceiros, ANDP e público em geral;
10 Alerta de incidente aos funcionários da empresa. Funcionários devem ser comunicados e notificados para que todos fiquem cientes do que aconteceu. Como aconteceu. Quais dados foram vazados e quais ações a empresa está tomando. Informar e nortear ações a serem realizadas, ações que devem ser evitadas e proibidas;
11 Levantar a necessidade de notificar os parceiros de negócio (operadores de dados) Alerta de incidente;
12 Medidas judiciais e pedido de instauração de inquérito policial;
13 Levantamento da necessidade de confecção do Relatório de impacto para a Autoridade Nacional de Proteção de Dados (ANPD)
14 Notificação à ANPD;
15 Alerta de incidente aos titulares dos dados;
16 Verifique a necessidade de o titular do dado realizar alguma ação afirmativa (cancelamento do cartão de crédito, por exemplo);
17 Alerta de incidente ao público em geral;
18 Prepare-se para respostas e para descrever as ações que a empresa está realizando para sanar ou mitigar o incidente;
19 Resposta ao incidente;
20 Respostas adicionais.

Neste mesmo sentido, apresentamos alguns exemplos de medidas técnicas:

I. Isolar Servidor afetado ou endpoint contaminado;
II. Alterar as senhas;
III. Alterar credenciais de bloqueio das máquinas e sistemas;
IV. Alterar regras do firewall da rede;
V. Executar plano de continuidade dos negócios, acionando Servidor(es) paralelo(s) com backup redundante (algo parecido com técnicas de recuperação de dados de sistema, em caso de desastres "disaster recovery").

6. Após o incidente ou vazamento: planejamento estratégico e tático

I. Conduzir análise criteriosa para determinar a causa raiz do incidente ou vazamento;
II. Propor processo de melhoria contínua para sanar aquela brecha de segurança;
III. Revisar as políticas e processos de segurança para avaliar sua efetividade. Caso necessário proponha alterações.

7. Melhoria contínua da qualidade: planejamento estratégico, tático e operacional

Alterar políticas de governança corporativa, manuais de procedimento e tudo que for necessário para correção da falha detectada para inibir novas ocorrências, disseminando a cultura da importância do tratamento da privacidade de dados e da proteção dos dados, baseado em um conjunto de controles internos, nos termos da Lei Geral de Proteção de Dados Pessoais - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, de modo a conferir segurança jurídica razoável de que os objetivos do negócio estão sendo alcançados dentro da legalidade e com eficiência nas operações.

Portanto, o processo sistemático de prevenção (simulação periódica e pentest), detecção da causa raiz de incidentes, proposta de saneamento das brechas e revisão dos processos de segurança, são uma espiral de melhoria contínua de qualidade, que permite à organização administrar seus ativos de conhecimento, e a mensurar com mais segurança a sua eficiência.

Reciclar periodicamente por mecanismos de comunicação adequado e rápido, e também treinamento aos colaboradores, acerca da importância e da criticidade no tratamento da segurança da informação, destacando as novas técnicas retro identificadas e as possibilidades de fraude em evidência no mercado (leitura sugerida: Data Breach Investigations Report, publicada anualmente pela Verizon), abordando também temas, tais como:

- ✓ engenharia social: é uma forma muito usada por cibercriminosos para descobrir informações pessoais de usuários – como senhas ou dados bancários – sem precisar explorar falhas de segurança de sistemas. De modo geral, a estratégia pode ser pensada como um meio de hackear os usuários, e não seus dispositivos, com o objetivo de convencê-los que estão cedendo as informações para pessoas ou serviços confiáveis. As táticas usadas incluem mensagens de e-mails e páginas falsas ou truques psicológicos para distrair as vítimas; e
- ✓ concorrência desleal: empresas concorrentes que querem vender mais, fomentando ataque cibernético ao seu rival comercial, podendo ocorrer inclusive falsos ransomwares, utilizando dados semelhantes, de base de dados própria, para prejudicar a imagem de sua empresa.

Seguem listados como propósito de alerta, os erros mais comuns praticados na hora de pensar em segurança da informação:

- ✓ atribuir exclusivamente à área tecnológica a segurança da informação;
- ✓ posicionar hierarquicamente essa equipe abaixo da diretoria de TI;
- ✓ definir investimentos subestimados e limitados à abrangência dessa diretoria;
- ✓ elaborar planos de ação orientados à reatividade;
- ✓ não perceber a interferência direta da segurança com o negócio;
- ✓ tratar as atividades como despesa e não como investimento;
- ✓ adotar ferramentas pontuais como medida paliativa;
- ✓ satisfazer-se com a sensação de segurança provocada por ações isoladas;
- ✓ não cultivar corporativamente a mentalidade de segurança;
- ✓ tratar a segurança como um projeto e não como um processo.

Sobre o processo decisório, do ponto de vista de um administrador, uma de suas funções mais importantes é exatamente a de decidir. Essa decisão que ocorre no presente não é um ato isolado, repentino, “ela é tanto um fim, quanto o início de uma ação”, fim do passado e início do futuro. Pelo exposto, notamos que existe algo ligando o passado ao futuro que nos auxilia no processo decisório e nos dá a capacidade de tomada de decisão. Chamaremos este sensor de previsão, definido como o “processo pelo qual a partir de informações existentes, admitidas certas hipóteses e através de algum método de geração, chegamos a informações sobre o futuro, com uma determinada finalidade”. Como casos especiais de previsão teremos a projeção, a predição e o planejamento, que diferem entre si pelas hipóteses admitidas, a saber:

- ➢ Projeção: futuro é continuação do passado – hipótese de permanência;
- ➢ Predição: futuro diferindo do passado por causas fora de nosso controle;
- ➢ Planejamento: futuro diferindo do passado por causas sob nosso controle.

Podemos combinar projeções, predições e planejamento para melhor nos prepararmos para as decisões do momento ou do futuro.

8. Conclusão

A política de resposta a incidentes e a estratégia de aderência à legislação são componentes cruciais para a proteção de dados e a segurança cibernética nas organizações. Em alinhamento com a Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018), é fundamental que as empresas implementem um planejamento estratégico robusto e adotem uma abordagem de defesa em camadas para mitigar riscos e responder efetivamente a incidentes. A aplicação de defesas em múltiplas camadas, desde desencorajar e dificultar até detectar e diagnosticar, fortalece a segurança e a resiliência das operações empresariais. O planejamento tático e operacional, que inclui a realização de exercícios de pentest e a capacitação contínua dos funcionários, assegura uma preparação adequada para lidar com incidentes. Durante um incidente, a ação coordenada de equipes especializadas e a comunicação eficaz são essenciais para minimizar os danos e restaurar a integridade dos sistemas. Após o incidente, a análise crítica da causa raiz e a implementação de melhorias contínuas garantem a evolução constante das práticas de segurança. A melhoria contínua da qualidade, por meio de revisões periódicas e atualizações das políticas de governança, é vital para manter a conformidade com a legislação e reforçar a proteção dos dados. O comprometimento com a educação e o treinamento dos colaboradores sobre segurança da informação e a conscientização sobre ameaças emergentes contribuem para um ambiente mais seguro e preparado. Dessa forma, as organizações não apenas atendem às exigências legais, mas também reforçam sua capacidade de gerenciar riscos e proteger seus ativos de informação de maneira eficaz.

Contribuições dos Autores

F.J.B.V.: Curadoria de Dados, Redação - Preparação do Rascunho Original; Edição, Revisão e Edição. O Autor leu e aprovou o manuscrito final.

Disponibilidade de Dados

Os dados que compõem este estudo estão disponíveis a partir da seguinte referência: Vazquez, Fabio José Buchedid. Política de Resposta a Incidentes. 2020. - Fundação Escola Nacional de Seguros – FUNENSEG (“ENS”), Escola Superior Nacional de Seguros (ESNS), Rio de Janeiro, 2020. https://doi.org/10.29327/44425290

Conflitos de Interesses

O autor declara que não tem interesses conflitantes.

Referências

AON (s.d.). Riscos Cibernéticos (Cyber Risk). Acesso em 18 de setembro de 2024. Disponível em: <https://www.aon.com/brasil/consulting/riscos-ciberneticos.jsp>.

Blum, R. O.; Vainzof, R.; Moraes, H. F. (2021). *Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e GDPR* (2. Ed). São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2021. 576 p.

Brustolin, V. (2019). Comparative analysis of regulations for cybersecurity and cyber defence in the United States and Brazil. *Revista Brasileira de Estudos de Defesa, 6*(2). https://doi.org/10.26792/rbed.v6n2.2019.75149

Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica, 9*(5), 784-800. http://dx.doi.org/10.1109/JAS.2022.105548

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A review. *Authorea Preprints*. https://doi.org/10.22541/au.166385207.73483369/v1

Kshetri, N., & DeFranco, J. F. (2020). The economics of cyberattacks on Brazil. *Computer, 53*(9), 85-90. https://doi.org/10.1109/MC.2020.2997322

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Palhares, F. (2020). *Temas Atuais de Proteção de Dados*. São Paulo. Revista dos Tribunais, 2020. 550 p.

Vazquez, F. J. B. (2003). Gestão do conhecimento aplicada em processos de e-banking. Monografia. Pós-Graduação em Administração Estratégica de Sistemas de Informação. Fundação Getúlio Vargas, FGV Management. Brasília, DF. https://doi.org/10.29327/44254525

Hurel, L. M., & Lobato, L. C. (2022). *Strategy for Cybersecurity Governance in Brazil*. Igarape Institute. 37 p.

DATASET REPORTS

journals.royaldataset.com/dr