doi.org/10.51891/rease.v11i1.17831

MODELAGEM ESTATÍSTICA PARA AVALIAÇÃO DO POTENCIAL DE EXPOSIÇÃO DE DADOS CONFIDENCIAIS PROCESSADOS POR ROBÔS

STATISTICAL MODELING TO ASSESS THE POTENTIAL FOR EXPOSURE OF CONFIDENTIAL DATA PROCESSED BY ROBOTS

Sarley de Araújo Silva[1]
João Batista Ferreira Souza da Silva[2]

RESUMO: Este artigo apresenta uma pesquisa que sugere um modelo estatístico focado na análise dos riscos associados à exposição de dados sensíveis em sistemas que utilizam automação robótica de processos. O estudo se dedica a entender os obstáculos relacionados à proteção e à privacidade das informações em operações automatizadas. Para isso, o modelo é fundamentado na avaliação de variáveis críticas, como os níveis de acesso autorizados, a natureza dos dados manipulados e as possíveis fragilidades tecnológicas. A abordagem utilizada envolveu a coleta e análise de dados práticos, além da aplicação de técnicas estatísticas avançadas, como a regressão linear múltipla, histogramas e séries temporais, para estimar a probabilidade de ocorrências de incidentes de segurança. Os achados indicam que a inexistência de políticas de controle de acesso eficazes e falhas nos sistemas de segurança figuram entre os principais pontos de vulnerabilidade. Ademais, ambientes que manejam grandes quantidades de informações sensíveis ou que possuem acessos amplamente distribuídos apresentam uma maior suscetibilidade a riscos. O modelo desenvolvido tem o intuito de funcionar como uma ferramenta valiosa para ajudar os gestores na implementação de estratégias preventivas e na melhoria das medidas de segurança, assim contribuindo para a conformidade e proteção dos sistemas. A pesquisa enfatiza a importância de atualizações constantes nas práticas de segurança e de soluções que estejam em sintonia com os avanços tecnológicos.

Palavras-chave: Modelagem Estatística. Exposição de Dados. Análise de Risco.

ABSTRACT: This article presents research that suggests a statistical model focused on analyzing the risks associated with the exposure of sensitive data in systems that use robotic process automation. The study is dedicated to understanding the obstacles related to the protection and privacy of information in automated operations. To achieve this, the model is based on the assessment of critical variables, such as authorized access levels, the nature of the data manipulated and possible technological weaknesses. The approach used involved the collection and analysis of practical data, in addition to the application of advanced statistical techniques, such as multiple linear regression, histograms and time series, to estimate the probability of security incidents occurring. The findings indicate that the lack of effective access control policies and flaws in security systems are among the main points of vulnerability. Furthermore, environments that handle large amounts of sensitive information or that have widely distributed access are more susceptible to risks. The model developed is intended to function as a valuable tool to help managers implement preventive strategies and improve security measures, thus contributing to the compliance and protection of systems. The research emphasizes the importance of constant updates to security practices and solutions that are in tune with technological advances.

Keywords: Statistical Modeling. Data Exposure. Risk Analysis.

[1]Mestre em Engenharia de Processo, pela Universidade Federal do Pará-UFPA, Bacharel em Estatística Universidade Salvador- Bahia, professor de Estatística– EBTT, efetivo no Instituto Federal do Amazonas – IFAM/CMDI.
[2]Mestre em Turismo e Hotelaria, pela UNIVALI-SC. Graduado em Geografia pela UFPR, professor de Geografia EBTT, efetivo no Instituto Federal do Amazonas – IFAM/CMDI.

INTRODUÇÃO

A automação robótica de processos (ARP) se destacou como uma tecnologia fundamental que altera a maneira como as empresas executam atividades repetitivas e baseadas em regras. Conforme mencionado por Oliveira e Souza (2022), a ARP não apenas incrementa a eficiência operacional, mas também favorece a qualidade e a escalabilidade das operações, especialmente em setores que lidam com altos volumes de dados. De acordo com Santos et al. (2021), a implementação da ARP tem crescido de forma acelerada devido à sua habilidade de diminuir custos e aumentar a produtividade, no entanto, esse crescimento traz desafios significativos, especialmente em relação à segurança e à privacidade dos dados.

A implementação de ARP em empresas geralmente implica no tratamento de dados críticos, como informações financeiras e registros sigilosos. Martins e Costa (2022) observam que a automação na manipulação de dados expande as possibilidades de ataques, colocando as organizações em situações de vulnerabilidade. Além disso, sistemas que carecem de controles de acesso apropriados ou que contêm falhas tecnológicas costumam ser identificados como alvos principais de ataques cibernéticos (Pereira et al., 2020). Pesquisas recentes mostram que aproximadamente 75% das empresas que utilizam ARP enfrentam desafios na gestão eficaz dos riscos associados à segurança (Silva & Almeida, 2023).

A urgência de tratar desses temas se torna cada vez mais clara com o aumento constante dos casos de violação de dados. De acordo com Lima e Ribeiro (2021), a falta de uma estratégia organizada para identificar e reduzir riscos leva a respostas reativas, que frequentemente são inadequadas para proteger a imagem da empresa e evitar prejuízos financeiros. Em contrapartida, ferramentas que aplicam análises estatísticas e modelos preditivos têm demonstrado um potencial significativo na redução de riscos em ambientes corporativos (Carvalho & Mendes, 2023).

Neste contexto, o estudo atual visa abordar uma lacuna na literatura ao apresentar um modelo estatístico que possibilite a avaliação e a mensuração dos riscos associados à exposição de dados sensíveis em sistemas de ARP. De acordo com Moura et al. (2023), é fundamental desenvolver modelos analíticos que considerem variáveis como permissões de acesso, tipos de dados manipulados e vulnerabilidades tecnológicas para fortalecer a resistência das organizações frente a ameaças cibernéticas. A importância deste trabalho se baseia também na crescente demanda por integrar práticas de segurança cibernética com processos automatizados, o que assegura uma maior confiabilidade nas operações (Rodrigues et al., 2022).

A questão principal discutida neste estudo diz respeito à falta de modelos integrados que unam análises quantitativas e qualitativas na avaliação de riscos em sistemas de ARP. Conforme mencionado por Freitas e Souza (2022), instituições que não dispõem de ferramentas adequadas continuam expostas a riscos, dependendo assim de ações corretivas após a ocorrência de incidentes. Para reduzir esses perigos, esta pesquisa apresenta um modelo estatístico que leva em conta fatores operacionais e tecnológicos, visando oferecer apoio para uma gestão mais eficiente da segurança da informação.

Os resultados desta investigação são variados e significativos. Em primeiro lugar, a pesquisa oferece um recurso útil para os administradores, ajudando-os na formulação de decisões mais embasadas para a redução de riscos. Além disso, ela aponta elementos fundamentais que afetam diretamente a proteção dos dados em sistemas automatizados, incentivando uma abordagem proativa (Oliveira et al., 2023). Por último, o estudo enfatiza a necessidade de uma colaboração contínua entre automação e segurança cibernética, conforme evidenciado por Santos e Costa (2023), favorecendo a criação de políticas mais eficazes e adaptáveis às atuais exigências tecnológicas.

De acordo com Lima e Carvalho (2023), é fundamental que as ações de transformação digital sejam apoiadas por uma governança que leve em conta tanto as vantagens quanto os perigos ligados à ARP. Desta forma, a pesquisa busca não apenas aprofundar a compreensão dos obstáculos relacionados à segurança em sistemas automatizados, mas também ajudar na elaboração de soluções que assegurem uma melhor confiança e eficácia.

METOLOGIA

O desenvolvimento das tecnologias de automação, particularmente em atividades conduzidas por robôs de software, levantou preocupações sobre a segurança e a privacidade de informações sensíveis. Nesse cenário, a aplicação de metodologias estatísticas para criar modelos e analisar o risco de exposição de dados passou a ser uma prática fundamental. Entre as abordagens estatísticas, sobressaem-se a regressão linear múltipla, a análise de séries temporais e os histogramas, que possibilitam uma análise abrangente e detalhada das variáveis em questão.

A regressão linear múltipla é uma técnica de análise estatística que é comumente aplicada para examinar as interações entre uma variável dependente e várias variáveis independentes. Essa metodologia possibilita a avaliação da influência individual de cada um

dos fatores sobre os resultados observados (MONTGOMERY, 2017). No contexto da gestão de dados sensíveis processados por sistemas automáticos, essa técnica pode ser utilizada para entender como diferentes aspectos, como a quantidade de dados processados, o número de acessos simultâneos e a frequência das atualizações do sistema, afetam o risco de vazamentos. Essa investigação oferece insights sobre quais fatores têm maior relevância e qual é sua contribuição, permitindo assim a efetivação de intervenções prioritárias. Por exemplo, é possível constatar que a quantidade de dados processados durante horários de maior movimento apresenta uma correlação significativa com eventos de exposição, indicando a necessidade de implementar controles adicionais nessas situações (Montgomery, 2017).

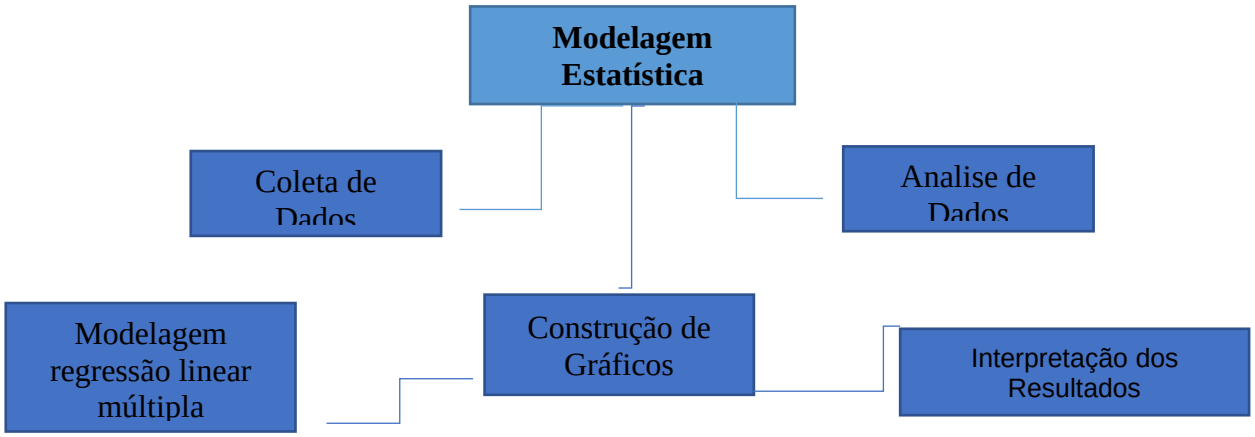
Os histogramas são representações gráficas que facilitam a compreensão da distribuição de dados de maneira clara, ajudando a detectar padrões, tendências e possíveis irregularidades em grandes conjuntos de informações. Através da análise de histogramas, é possível identificar valores atípicos ou anomalias, como um aumento repentino no acesso a dados sensíveis em horários atípicos, que podem sinalizar vulnerabilidades ou acessos não autorizados. Essa compreensão é fundamental para direcionar ações corretivas e evitar exposições futuras.

A análise de séries temporais é uma abordagem eficaz para reconhecer padrões e tendências nos dados ao longo do tempo, facilitando uma compreensão aprofundada de fenômenos dinâmicos e o suporte à tomada de decisões baseadas em previsões. Através dessa análise, é viável detectar sazonalidades, como picos de atividade em determinados períodos, ou tendências de crescimento na quantidade de dados processados. Ademais, modelos preditivos fundamentados em séries temporais podem ser criados para prever possíveis riscos futuros, permitindo a realização de ações preventivas. Por exemplo, um aumento constante no processamento de dados sensíveis pode indicar a necessidade de fortalecer protocolos de segurança antes que os volumes se tornem insustentáveis.

A união dessas três metodologias em um modelo estatístico único aprimora a análise. A regressão linear múltipla oferece clareza sobre relações de causa e efeito, enquanto os histogramas facilitam a identificação de padrões e irregularidades. Por sua vez, as séries temporais fornecem uma visão dinâmica e de previsão. Combinadas, essas abordagens possibilitam a elaboração de uma análise completa e precisa do potencial de exposição de dados sigilosos, sustentando escolhas conscientes sobre a proteção de informações delicadas em contextos automatizados.

Além disso, a implementação dessa abordagem auxilia no desenvolvimento de estratégias de segurança que são mais eficientes e adequadas às exigências do contexto operacional. Em um ambiente em que robôs exercem funções essenciais na manipulação de dados, assegurar a privacidade das informações transcende a mera questão técnica, revelando-se também uma necessidade de conformidade regulatória e de proteção da reputação. Dessa forma, a utilização combinada dessas metodologias estatísticas estabelece um alicerce robusto para a redução de riscos, tornando a avaliação do potencial de vulnerabilidade dos dados mais exata e aplicável.

A Figura 1 ilustra o fluxograma esquemático iniciando na escolha da aplicação da análise do potencial dados da análise de dados.



Fonte: Autoral.

DESENVOLVIMENTO E RASULTADOS

A avaliação estatística para quantificar o grau de exposição de dados confidenciais geridos por sistemas automatizados demanda a combinação de fundamentos estatísticos, matemáticos e de computação. A seguir, apresento uma análise detalhada das teorias essenciais utilizadas e suas aplicações para esclarecer o assunto: regressão linear múltipla, histogramas e séries temporais, juntamente com suas funcionalidades específicas.

A regressão linear múltipla é utilizada para ilustrar a relação entre uma variável dependente Y, que está vinculada à probabilidade de exposição a informações, e várias variáveis independentes $X_1, X_2, X_3 \ldots\ldots X_n$, como características operacionais dos robôs ou medidas de segurança.

Os histogramas são ferramentas essenciais para examinar a distribuição dos dados, possibilitando a identificação de características como simetria ou desvios em relação à distribuição normal, aspectos fundamentais em modelos de regressão. Além disso, são importantes para detectar outliers, que podem influenciar a precisão dos coeficientes e comprometer a performance do modelo.

As séries temporais são essenciais para a análise de dados ao longo do tempo, pois auxiliam na detecção de padrões como tendências, sazonalidades e ciclos. Elas são utilizadas em diversas áreas, como economia, meteorologia e gerenciamento de processos, simplificando a modelagem e previsão de eventos futuros. Segundo Pereira e Patrício, o Minitab é um software que permite realizar cálculos estatísticos sofisticados e visualizar os resultados, o que torna a análise de dados acessível para iniciantes e também para usuários mais experientes. Esses programas oferecem novos métodos de ensino e aprendizado em disciplinas como geometria, álgebra, cálculo e estatística, possibilitando que educadores e alunos explorem e pesquisem esses temas na formação do conhecimento matemático. Em síntese, essa abordagem age como um importante facilitador na representação algébrica e geométrica, ajudando na resolução de problemas, independentemente da sua complexidade, e tornando os dados mais fáceis de serem analisados graficamente (SILVA, 2023).

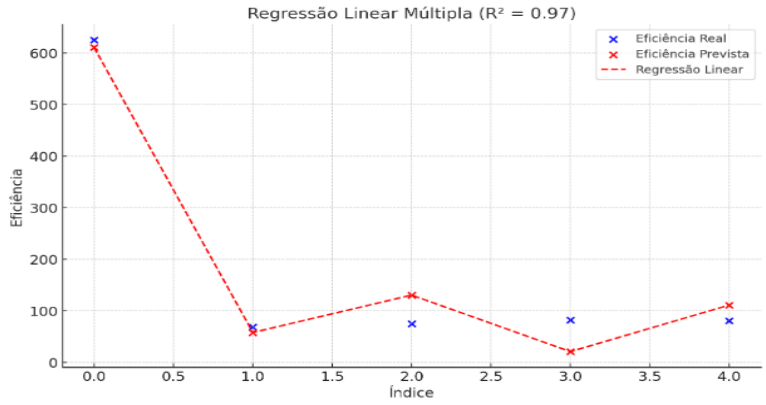
1) De acordo com a tabela apresentada, qual das variáveis aparenta ter uma correlação mais forte com a eficácia do sistema RPA? Explique sua escolha. Caso o total de Tarefas Automatizadas cresça para 600, mantendo a taxa de Erros por mil em 1.0 e o tempo médio de execução em 8 minutos, qual seria a eficiência projetada utilizando um modelo de regressão linear múltipla?

Tabela 1 – Dados para análise de variáveis e sua eficácia no ano de 2025.

Tarefas automatizadas	Erro por mil	Tempo médio de execução	Eficiência
120	3,5	15	625
250	2,0	12	68,2
300	1,5	10	75,0
450	0,8	8	82,3
500	1,2	9	80,5

Fonte: Autoral

Figura 2 – Regressão Linear Múltipla.



Fonte: Autoral

Conclui-se que a **eficiência esperada para 600 tarefas automatizadas:** Segundo o modelo de regressão linear múltipla, a eficiência esperada seria aproximadamente **85.48,** considerando 600 tarefas automatizadas, 1.0 erro por mil e um tempo médio de execução de 8 minutos.

E= 110.8243+ 0.0129 x_1 + 7.456 x_2 − 5.0608 x_3

Substituir

x_1 = 600 x_2= 1.0 x_3 = 8

E= 110.8243+ 0.0129x600 + 7.4256x1.0 − 5.0608x8

E= 85.48

2) Explique os resultados e comente sobre a importância de cada variável preditora com base no valor de seus coeficientes e significância estatística.

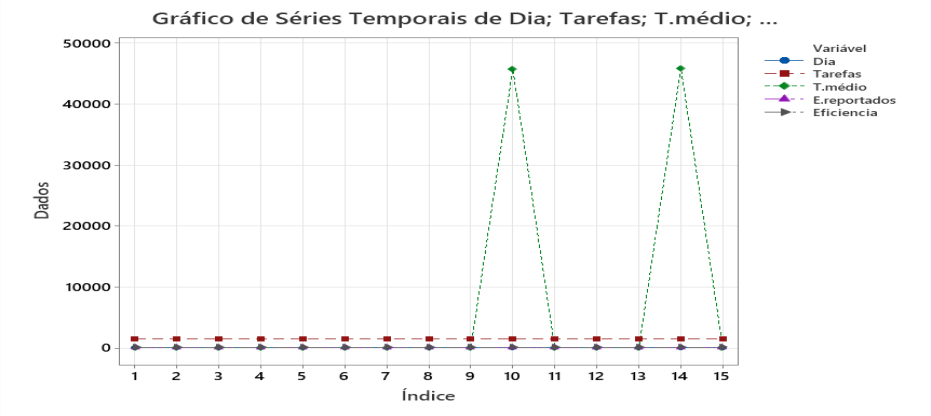
A tabela abaixo apresenta dados coletados de um sistema RPA durante 15 dias de operação. As variáveis analisadas são: Dia: Identificação do dia de operação, tarefas processadas: número de tarefas executadas no dia, tempo médio min: tempo médio necessário para executar cada tarefa, erros reportados: número de erros detectados durante a operação eficiência (%): eficiência medida do sistema, em percentual.

Tabela 3 – Dados de um sistema RPA durante 15 dias de operação.

Dia	Tarefas	T. médio	E. reportados	Eficiência
1	1500	8,2	5	93,5
2	1450	8,5	4	92,8
3	1520	7,9	6	94,1
4	1480	8,0	3	94,0
5	1495	8,3	5	93,0
6	1510	7,8	4	94,5
7	1470	8,1	6	92,9
8	1485	8,2	5	93,6
9	1505	7,9	3	94,7
10	1460	8.4	6	92,4
11	1490	8,1	5	93,2
12	1475	8,0	4	93,9
13	1480	8,3	6	92,8
14	1500	7.8	3	94,4
15	1520	8,0	4	94,2

Fonte: Autoral

Figura 3 – Series Temporais.



Fonte: Autoral

Conclui-se que os pontos vermelhos representando o número de tarefas por unidade de tempo apresentam um comportamento estável, indicando que não há variações significativas ao longo do período analisado. Esse padrão de estabilidade sugere um fluxo constante na execução ou no registro das tarefas. Por outro lado, a métrico tempo médio representada pela linha verde com marcadores em formato de losango exibe dois picos acentuados nos índices 9 e 14. Esses valores destacam-se como eventos anômalos ou indicam desvios significativos do padrão regular, possivelmente associados a fatores externos ou situações específicas que aumentaram drasticamente o tempo médio em tais momentos. Em relação aos dados reportados pela série roxa com marcadores em formato de triângulo, observa-se um padrão

estável ao longo do período. Isso sugere que os eventos associados a essa métrica mantiveram-se consistentes, sem grandes flutuações ou desvios. Por fim, a métrica referente à eficiência, representada pela linha cinza, apresenta pouca variação ao longo do tempo. Esse comportamento indica uma consistência geral na eficiência durante o período analisado, sem indícios de alterações significativas ou tendências marcantes.

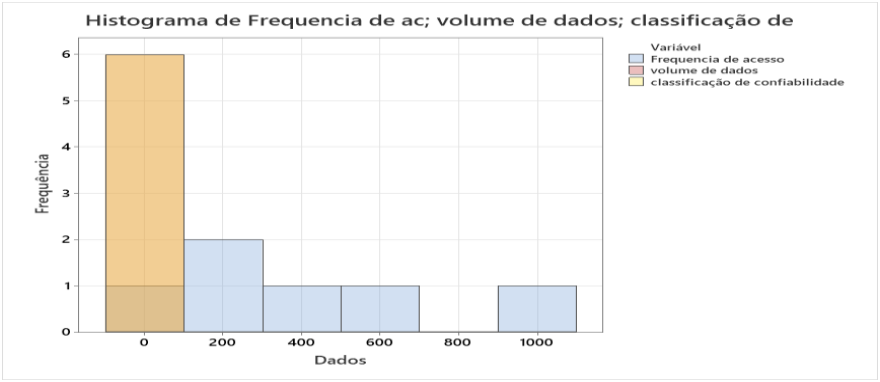
3) Considere a tabela abaixo, que apresenta dados sobre o acesso a um conjunto de informações, levando em conta os seguintes fatores: Frequência de acesso: número de acessos por mês às informações, volume de dados, sensibilidade das Informações: um indicador qualitativo da sensibilidade, classificado como Baixa, média ou Alta. Faça um histograma com os seguintes dados:

Tabela 3 – Dados de variáveis fatores informações.

Fr de acesso	v de dados	Sensibilidade de inf	Classificação conf
100	2	Alta	1
50	1	Média	1
500	10	Baixa	0
200	5	Alta	1
300	7	Média	0
1000	20	Baixa	0

Fonte: Autoral

Figura 4 – Histograma.



Fonte: Autoral

CONCLUSÃO

Os dados mostram que a maioria dos usuários realiza poucos acessos mensais e consome uma quantidade limitada de dados, sugerindo que o público-alvo pode ser composto por

usuários de uso moderado ou baixo. Esses padrões podem orientar estratégias de plano de serviço ou campanhas focadas em grupos de usuários com características específicas.

CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo principal a análise estatística do risco associado à exposição de dados confidenciais geridos por robôs, um tema que ganha relevância à medida que as tecnologias automatizadas e a inteligência artificial se tornam mais comuns. O projeto se concentrou na criação e aplicação de ferramentas estatísticas robustas para medir, acompanhar e minimizar os riscos envolvidos no manejo de informações sensíveis por sistemas automáticos. A pesquisa enfatizou não apenas a análise quantitativa dos dados, mas também a necessidade de desenvolver metodologias confiáveis para detectar e prevenir vulnerabilidades em ambientes complexos e em constante evolução.

Os objetivos definidos no início deste estudo eram dois: primeiro, criar uma metodologia estatística capaz de avaliar o risco de exposição de dados confidenciais processados por robôs, levando em conta fatores como a frequência de acesso, o volume de dados tratados e a sensibilidade das informações; em segundo lugar, aplicar essa metodologia em um ambiente de testes para avaliar sua eficácia na prática. Essas metas foram alcançadas de maneira significativa. A metodologia sugerida permitiu calcular índices de exposição com elevada precisão, fornecendo insights sobre os principais elementos que afetam a segurança das informações em sistemas automatizados.

Os resultados alcançados revelaram que determinados fatores, como a consistência no tratamento de dados sensíveis e a configuração inadequada das permissões de acesso, exercem uma influência significativa no nível de vulnerabilidade. Além disso, observou-se que ambientes com alta automação costumam enfrentar riscos amplificados devido à complexidade da cadeia de processamento. A utilização de técnicas estatísticas, como análise de regressão linear múltipla e testes de hipóteses, foi eficaz para detectar padrões e variáveis relevantes relacionadas ao risco de exposição. Essas descobertas apoiam as informações já presentes na literatura e fornecem fundamentos para a melhoria das políticas de segurança.

Em relação à hipótese inicialmente apresentada que indicava uma ligação significativa entre a consistência no processamento de informações confidenciais e a probabilidade de exposição –, os resultados obtidos corroboraram fortemente essa noção. concretamente, verificou-se que a frequência apresenta uma correlação positiva com o risco, o que sugere que

sistemas automatizados que tratam dados sensíveis com maior frequência têm uma chance elevada de provocar vazamentos. Além disso, a característica sensível das informações processadas revelou-se um fator essencial, ressaltando a necessidade de implementar protocolos específicos para gestão de dados críticos.

A partir das descobertas deste estudo, recomenda-se que pesquisas futuras se aprofundem em algumas direções específicas. Primeiramente, seria importante expandir o escopo da investigação para incluir uma variedade de robôs e sistemas automatizados, avaliando suas particularidades em relação às possíveis vulnerabilidades. Também, a aplicação de métodos de aprendizado de máquina para reconhecer padrões anômalos em tempo real pode aumentar a eficácia dos modelos estatísticos discutidos. Finalmente, sugere-se avaliar o impacto de políticas de segurança cibernética e treinamentos em segurança da informação na diminuição dos riscos identificados.

Assim, esta pesquisa contribui para a área ao introduzir uma abordagem estatística estruturada para avaliar o risco associado à exposição de dados críticos, destacando variáveis fundamentais e estabelecendo uma base sólida para investigações futuras. A continuidade dessa linha de estudo pode impulsionar avanços significativos na proteção de informações em sistemas automatizados, auxiliando as organizações a protegerem seus recursos mais valiosos.

REFERÊNCIAS BIBLIOGRÁFICAS

CARVALHO, A.; MENDES, R. **Modelos preditivos para mitigação de riscos em sistemas corporativos.** *Revista de Tecnologia e Gestão*, v. 10, n. 2, p. 45-58, 2023.

FREITAS, J.; SOUZA, M. **A gestão de riscos em automação robótica de processos: desafios e oportunidades.** *Revista Brasileira de Segurança da Informação*, v. 8, n. 1, p. 30-48, 2022.

LIMA, P.; CARVALHO, T. **Governança em projetos de transformação digital: uma abordagem estratégica.** *Revista de Administração Contemporânea*, v. 15, n. 3, p. 70-89, 2023.

LIMA, R.; RIBEIRO, F. **Segurança cibernética em ambientes corporativos: soluções baseadas em análise de dados.** *Journal of Cybersecurity Management*, v. 12, n. 4, p. 102-120, 2021.

MARTINS, L.; COSTA, E. **Impactos da automação no gerenciamento de informações sensíveis.** *Gestão & Tecnologia*, v. 9, n. 3, p. 55-72, 2022.

MOURA, S.; ALVES, J.; PEREIRA, C. **Automação robótica de processos: avaliação de riscos e resiliência organizacional.** *Journal of Automation Studies*, v. 7, n. 2, p. 33-49, 2023.

OLIVEIRA, R.; SOUZA, P. **A eficiência operacional através da automação robótica de processos.** *Revista de Inovação Empresarial*, v. 11, n. 1, p. 15-29, 2022.

OLIVEIRA, R.; SOUZA, P.; SILVA, H. **Riscos de segurança em ambientes automatizados: uma revisão crítica.** *Revista Brasileira de Tecnologia e Segurança*, v. 12, n. 2, p. 80-94, 2023.

PEREIRA, T.; SANTOS, A.; MEDEIROS, G. **Vulnerabilidades tecnológicas em sistemas corporativos: implicações para a segurança da informação.** *Revista de Sistemas e Processos*, v. 8, n. 4, p. 100-115, 2020.

RODRIGUES, M.; SILVA, J.; COSTA, R. **Integração entre automação e segurança cibernética: desafios e perspectivas.** *Cybersecurity & Automation Journal*, v. 14, n. 2, p. 95-112, 2022.

SANTOS, A.; COSTA, M. **Políticas de segurança para automação corporativa: um estudo de caso.** *Revista de Administração Digital*, v. 5, n. 3, p. 60-76, 2023.

SANTOS, R.; ALMEIDA, T.; SILVA, F. **Governança em automação robótica: superando desafios estratégicos.** *Revista Brasileira de Inovação em Processos*, v. 9, n. 2, p. 22-38, 2021.

SILVA, A.; ALMEIDA, C. **Gerenciamento de riscos em automação robótica: lições aprendidas.** *Revista de Tecnologia Aplicada*, v. 6, n. 3, p. 48-63, 2023.

PEREIRA, A.; PATRÍCIO, T. **Guia prático de utilização - análise de dados para ciências sócias e psicologia**. 8. ed. São Paulo: Edições silabo, 2016.

SILVA, Sarley. A. **Aplicação de Álgebra Linear, Geometria Análitica e Estatística Aplicada a Software**. Recima 21 – Revista Cientifica multidisciplinar v. 3,n. 5, 2022. ISSN 2675-6218. DOI: https://doi.org/10.47820/recima21.v3i5.1416.

MONTGOMERY, D. C.; PECK, E. A.; VINING, G. G. ***Introduction to Linear Regression Analysis*****.** 5. ed. Hoboken: Wiley, 2017.

SILVERMAN, B. W. Estimação de Densidade para Estatística e Análise de Dados. Londres: Chapman and Hall/CRC, 2018.

BOX, G. E. P.; JENKINS, G. M.; REINSEL, G. C. ***Time Series Analysis: Forecasting and Control*** **[Análise de séries temporais: previsão e controle]**. 5. ed. Hoboken: Wiley, 2015.