FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Yara Rosa Veneri

RESPOSTA A DESASTRES EM CASO RANSOMWARE: ANÁLISE E PLANO DE RESPOSTA A DESASTRES

Americana, SP
2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Yara Rosa Veneri

RESPOSTA A DESASTRES EM CASO RANSOMWARE: ANÁLISE E PLANO DE RESPOSTA A DESASTRES

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação da Profa. Maria Cristina Aranda

Área de concentração: Segurança da Informação.

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

VENERI, Yara Rosa

Resposta a desastres em caso ransomware: análise e plano de resposta a desastres. / Yara Rosa Veneri – Americana, 2023.

75f.

Estudo de caso (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientadora: Profa. Dra. Maria Cristina Aranda

1. Gestão de sistemas, unidades e recursos da informação 2. Sistemas de informação - governança. I. VENERI, Yara Rosa II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 21
681.518.3

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Yara Rosa Veneri

RESPOSTA A DESASTRES EM CASO RANSOMWARE: ANÁLISE E PLANO DE RESPOSTA A DESASTRES

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 25 de junho de 2025.

Banca Examinadora:

Maria Cristina Aranda
Doutora
Fatec Americana "Ministro Ralph Biasi"

João Emmanuel D' Alkmin Neves
Doutor
Fatec Americana "Ministro Ralph Biasi"

Diógenes de Oliveira
Mestre
Fatec Americana "Ministro Ralph Biasi"

SUMÁRIO

RESUMO

O presente estudo tem como objetivo a análise e avaliação da resposta a desastres de segurança da informação em três empresas, no ramo de oleoduto, nas áreas de saúde e mercado financeiro, com foco em ataques de *ransomware*. Para este trabalho, foi realizado o estudo de caso de três instituições que sofreram incidentes dessa natureza. A proposta visa identificar as melhores práticas e estratégias para mitigar os impactos de ataques cibernéticos originados por *ransomware*, avaliando a eficácia das decisões tomadas pelas organizações estudadas durante os incidentes e propondo possíveis melhorias nas ações adotadas. Além disso, será elaborado - como segundo objetivo - um plano de resposta a desastres voltada a falhas relacionadas aos pontos de falha apresentado nos três estudos, integrando eficiência técnica e alinhamento com os objetivos do negócio. Esse plano de resposta a desastres é baseado em uma empresa real, a qual não será mencionada por motivos de segurança e confidencialidade. A metodologia adotada incluirá o estudo de casos e a revisão bibliográfica, explorando aspectos teóricos e práticos relacionados à resposta a desastres. O estudo de casos abordará o tema da resposta a desastres voltada a ataques de *ransomware*, destacando boas práticas que devem ser integradas para mitigar incidentes com esse tipo de vetor. Também foi estruturado um plano específico para de contingência para incidentes para uma empresa de desenvolvimento de software. A pesquisa reforça a importância de um plano de resposta a desastres robusto e adaptável, alinhado ao planejamento estratégico do negócio, enfatizando também a necessidade de investimentos contínuos em cibersegurança e resiliência organizacional.

Palavras-chave: Segurança da informação; Resposta a incidentes; Ransomware; Violação de dados.

ABSTRACT

The present study aims to analyze and evaluate the disaster response to information security incidents in three companies, operating in the oil pipeline sector, healthcare, and financial markets, with a focus on ransomware attacks. For this work, case studies were conducted on three institutions that experienced such incidents. The objective is to identify best practices and strategies to mitigate the impacts of cyberattacks caused by ransomware, assessing the effectiveness of the decisions made by the organizations studied during the incidents and proposing possible improvements to the adopted actions.

In addition, as a secondary objective, a disaster response plan will be developed, targeting the failure points identified in the three case studies, integrating technical efficiency with alignment to business objectives. The adopted methodology will include case study analysis and a literature review, exploring both theoretical and practical aspects related to disaster response. The case studies will address disaster response strategies aimed at ransomware attacks, highlighting best practices that should be incorporated to mitigate incidents involving this type of threat vector.

A specific contingency plan for incidents was also structured for a software development company. The research reinforces the importance of a robust and adaptable disaster response plan, aligned with the organization's strategic planning, while also emphasizing the need for continuous investment in cybersecurity and organizational resilience.

Keywords: Information security; Incident response; Ransomware; Data breach.

1. INTRODUÇÃO

A notória e constante evolução da tecnologia tem impulsionado a digitalização e o dinamismo das informações em todos os aspectos da vida humana. No contexto organizacional, a dependência digital dos sistemas corporativos é evidente. Com a expansão do digital, a superfície de ataque segue em constante crescimento, resultando no aumento das ameaças cibernéticas e das vulnerabilidades. Isso torna a segurança da informação e a proteção de dados elementos indispensáveis para a sustentabilidade e o sucesso das organizações.

No entanto, a proteção de informações ultrapassa o âmbito de ferramentas de segurança implementadas por equipes técnicas. Dentro disso inclui-se a capacidade de realizar uma resposta ágil em casos de incidentes que possam causar interrupções de operações.

Atacantes realizam a utilização de uma grande variedade de métodos para explorar meios lógicos falhos para obter acesso não autorizado a redes corporativas. É recorrente acontecer ataques a organizações explorando *phishing* (técnica de fraude onde o atacante engana a vítima para que ela forneça informações sensíveis) e *spear phishing* (forma mais direcionada de *phishing*, onde o atacante personaliza a mensagem com informações específicas sobre a vítima para aumentar as chances de sucesso), sendo que esses envolvem o uso do *e-mail* como ferramenta para manipular suas vítimas, conseguindo assim induzir e acessar *sites* maliciosos ou a realização de *downloads* de anexos infectados.

Conforme apresentado no Relatório de Investigação de Violação de Dados da Verizon (Verizon, 2024), 68% dos incidentes relacionados à violação de dados tiveram como ponto de origem o envolvimento humano não malicioso, ou seja, pessoas que foram vítimas de ataques de engenharia social ou cometeram erros acidentais.

Com o aumento desses incidentes, segundo o especialista em segurança cibernética da IBM, Crume (2024), o impacto financeiro médio de uma violação de dados foi de aproximadamente US$5 milhões no ano de 2024. Ainda segundo a apresentação do especialista, com base no Relatório de Custo de uma Violação de Dados 2024, foi evidenciado que organizações que não possuem um plano de resposta a desastres gastam, em média, cerca de US$2,66 milhões a mais na mitigação dos danos causados por esse tipo de incidente.

Entre os tipos mais graves e recorrentes de incidentes de violação de dados está o ataque de *ransomware*. Em 2024, de acordo com Ismael Rocha, especialista em *threat intelligence* da ISH (ISH, 2024), a América Latina vem enfrentando atualmente um aumento contínuo e significativo nas ocorrências desse tipo de ataque, tendo registrado, no segundo

semestre, um crescimento de 32% (com 1.294 casos confirmados) e um aumento de 10% em comparação com o segundo trimestre de 2023.

A necessidade de um plano de resposta a desastres estruturado, adaptado à realidade e às necessidades de cada organização, é um dos principais motivos pelos quais as organizações têm priorizado esse tema. Um PRD (Plano de Recuperação ao Desastre) tem como objetivo explicar como a organização deve agir em caso de desastres, ou bruscas interrupções, para que consiga recuperar suas atividades e funcionalidades dos seus sistemas de TI (Tecnologia da Informação) para garantir a continuidade do negócio. Esse plano é muito importante para minimizar o tempo de inatividade, perda de dados e impacto das atividades em caso de ocorrências com falhas de *hardware*, ataques cibernéticos ou desastres naturais.

A questão norteadora desse estudo se apoia em quais são as melhores práticas e medidas que as empresas, principalmente as que possuem sistemas críticos, podem estabelecer para prevenir, mitigar e responder a incidentes de violação de dados.

O trabalho traz como objetivo principal a realização de três análises de resposta a desastres em empresas que foram afetadas por ataques *ransomware*, onde este estudo visa identificar boas práticas e estratégias para mitigar os impactos dos ataques, avaliar a eficácia das ações tomadas pelas equipes de cada caso e propor melhorias. Em conjunto, como objetivo secundário, o desenvolvimento do plano de resposta a desastres traz o plano em ação tríplice (Preventiva, Contingencial e Recuperatória) para falhas recorrentes nos três casos expostos analisados. A partir disso, será possível entender a estrutura e melhores práticas no que diz respeito à construção de um PRD conforme as normas e *frameworks* mundialmente conhecidos, e também as melhores práticas de reação a falhas especificadas no plano.

As hipóteses para a fragilidade dos planos incluem o despreparo significativo das equipes responsáveis por incidentes e pela Segurança da Informação, aliado a comitês de risco com capacitação insuficiente e conhecimentos superficiais em resposta a desastres de cibersegurança.

A partir de análises de planos encontrados na Internet, nota-se que não apresentam qualquer modelagem ou alinhamento com o plano de negócios da empresa, sendo, em sua maioria, baseados em modelos genéricos disponíveis na Internet.

Além disso, contribuem para essa fragilidade a ausência de treinamentos contínuos, a falta de simulações práticas de incidentes, bem como a carência de ferramentas adequadas para monitoramento e resposta em tempo real, a comunicação interna ineficiente durante crises e a baixa priorização financeira de investimento em cibersegurança e resiliência operacional auxiliam para um cenário propício à vulnerabilidades.

O percurso metodológico deste trabalho se deve através de estudo de casos disponibilizados na Internet, com revisão bibliográfica sobre a temática inicial aqui proposta.

Os casos utilizados para esta pesquisa referem-se a três organizações, cujos nomes não são divulgados (não foi possível entrar em contato com as empresas para que seja solicitado a liberação do uso dos nomes), todas vítimas de ataques de *ransomware* realizados de formas distintas e com respostas igualmente diferentes. A partir dos casos expostos, foi desenvolvido um PRD (Apêndice A), apresentando como uma organização irá responder e se recuperar de um desastre ou interrupção significativa seguindo as boas práticas de normas e *frameworks*. Focando nos procedimentos de resposta, nas estratégias de recuperação, nos papéis e responsabilidades e na comunicação. A partir dessas ações a empresa terá como benefícios a redução do tempo de inatividade, a proteção de dados e ativos e a melhoria de sua resiliência.

Com o passar dos anos, as empresas têm enfrentado a necessidade constante de se modificar e adaptar diante da ascensão tecnológica e com ela surgem também os perigos digitais. Isso faz com que as organizações, independentemente do ramo de atuação ou do tamanho, precisem se precaver e proteger contra as ameaças presentes na Internet.

Na era digital, o volume de transmissão de dados e informações é extremamente elevado, e esses dados se tornam verdadeiros "objetos de desejo" para organizações criminosas e indivíduos mal-intencionados.

O trabalho está organizado em quatro capítulos, sendo que o capítulo I a introdução do trabalho, capítulo II fundamentação teórica, o capítulo III é o percurso metodológico e o capítulo IV conterá os resultados, análise e discussão dos dados.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Segurança da Informação

Segurança da informação é um conjunto de regras, práticas e tecnologias voltadas para a proteção de dados e de sistemas contra qualquer tipo de acesso indevido, ações que infringem sua integridade e que causam indisponibilidade.

É necessário pontuar que a segurança da informação não se limita apenas ao ambiente digital, mas também abrange medidas físicas e organizacionais para evitar vazamentos, ataques e falhas operacionais.

Com o aumento de incidentes de segurança, essa área está cada vez mais se colocando em lugar de destaque e importância, onde em algumas organizações é considerada como um dos pilares estratégicos dentro do plano de negócio. Principalmente no que diz respeito ao grande volume de dados processados digitalmente e o aumento das ameaças cibernéticas (CERT.br, 2023; GOV.BR, 2024).

O conceito da base da Segurança da Informação que orienta todos os profissionais durante a implantação de políticas e mecanismos, é a tríade CIA (Confidencialidade, Integridade e Disponibilidade).

- **Confidencialidade:** Ela possui o papel de assegurar que todas as informações sejam acessadas por pessoas ou sistemas autorizados. Com isso são adotadas algumas medidas para cumprimento desse pilar, como criptografia, controle de acesso e MFA (Múltiplo Fator de Autenticação) (GSI, 2023).
- **Integridade:** Refere-se à exatidão da confiabilidade dos dados, dando garantia que as informações não sejam alteradas ou corrompidas, de modo não autorizado, distinguindo-se da forma de origem. Seja por ataques cibernéticos ou erros humanos (CERT.br, 2024).
- **Disponibilidade:** O objetivo é garantir que as informações e sistemas sempre estejam disponíveis para os usuários devidamente autorizados (CERT.br, 2024).

Os incidentes de *ransomware* envolvem uma variedade de riscos para a segurança da informação, afetando diretamente os fundamentos de confidencialidade, integridade e disponibilidade. Nos incidentes de *ransomware*, a confidencialidade é violada quando *hackers* sequestram informações sigilosas e ameaçam expor caso o pagamento do resgate não seja realizado. A integridade é comprometida pela possibilidade de alteração ou eliminação de informações específicas, comprometendo a continuidade das operações comerciais. Além disso, a disponibilidade dos sistemas é prejudicada, uma vez que os dados são codificados,

impossibilitando o acesso legítimo e resultando em perdas financeiras e operacionais (ANPD, 2024).

2.2 Software malicioso

Os *softwares* maliciosos, também chamados de *malwares*, são descritos como todo e qualquer *software*, programa ou código que foi projetado com a premissa de causar danos, prejudicar ou explorar qualquer dispositivo, serviço, rede e seus usuários. Ataques cibernéticos envolvem, em grande maioria dos casos, algum tipo de *malware*, como *ransomware*, *adware*, *vírus*, *worms*, Trojan, *spywares* e *rootkits*.

Esses *malwares* se infiltram em alvos de várias maneiras, aproveitando vulnerabilidades e usuários que têm atitudes descobertas. A maneira mais frequente de contaminação acontece através de anexos ou *links* maliciosos que, ao serem acessados, instalam o *malware* no dispositivo. De acordo com o Relatório de Segurança Cibernética (Palo Alto Networks, 2024), os golpes de *phishing* são especificamente um dos principais meios de contaminação por malware, contribuindo para mais de 70% da eficácia de invasão de sistemas corporativos.

A obtenção de arquivos de fontes duvidosas ou alteradas também é um dos principais métodos de contaminação. De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2024), os *malwares* podem ser propagados através de arquivos que parecem inofensivos, como documentos PDF ou arquivos escondidos, que, ao serem baixados e executados, danificam o ambiente digital.

Com o aumento de usuários em redes sociais e aplicativos de mensagens instantâneas, essas plataformas se transformaram em fontes de contaminação, com *links* maliciosos disfarçados de conteúdos perigosos que levam os usuários a clicar neles. Segundo o Relatório de Ameaças Cibernéticas da Check Point Research (2024), os ataques baseados em engenharia social, como o *phishing* em mídias sociais e aplicativos de mensagens, tiveram um aumento de 40% no ano de 2024, aproveitando a confiança dos usuários nesses meios.

Outra forma de entrada é a falta de atualizações de *software* e sistemas de segurança desatualizados, pois *malwares* se aproveitam de vulnerabilidades conhecidas para se propagarem. De acordo com o Relatório de Segurança Cibernética (Palo Alto Networks, 2024), 60% dos ataques de *malware* em ambientes empresariais são causados pela exploração de vulnerabilidades que já possuem correções disponíveis, mas que não foram instaladas.

Referente aos impactos, caso ocorra a concretização de infecção por *malware*, podem ser devastadoras, tanto para usuários em seus equipamentos próprios, quanto para empresas e

organizações. O furto de dados protegidos e sensíveis é uma das consequências mais sérias e preocupantes de um ataque de *malware*, já que essas informações podem ser utilizadas para fraudes ou comercializadas na *dark web*. De acordo com o Relatório de Ameaças Cibernéticas da Symantec (Symantec, 2024), “o furto de informações e sua movimentação na Internet obscura persiste como uma das principais ameaças à privacidade e segurança de pessoas e organizações, com o número de incidentes que envolvem dados sensíveis aumentando anualmente” (Symantec, 2024, p. 16).

O *malware* tem a capacidade de causar a perda de informações relevantes, seja através da eliminação, corrupção de arquivos ou criptografia, como acontece em ataques de *ransomware*. No contexto organizacional, pode levar à interrupção das operações, resultando na redução da produtividade, modificação de sistemas componentes e até mesmo paralisação de tarefas. De acordo com o Relatório de Impacto de Ransomware da Palo Alto Networks, o impacto das organizações afetadas por *malware* é específico, resultando em prejuízos financeiros crescentes em setores que dependem de sistemas digitais para suas atividades cotidianas (Palo Alto Networks, 2024, p. 12).

2.3 Violação de dados

Considere-se como uma violação de dados, ou *data breach*, quando dados (pessoais ou empresariais) são furtados ou obtidos através de *software* sem autorização do proprietário do dado mesmo que de maneira acidental.

Segundo a Microsoft (Microsoft, 2024), uma violação de dados é um incidente de segurança onde dados protegidos, sensíveis ou protegidos são acessados ou expostos sem permissão. Os ataques cibernéticos, muitas vezes impulsionados por lucros financeiros, têm como alvo vários setores, como o governo, a saúde, a educação e as finanças, explorando vulnerabilidades como, *softwares* desatualizados ou senhas vulneráveis.

Os dados mais visados pelos crimes cibernéticos englobam informações pessoais (PII - Informações de Identificação Pessoal), registros de saúde (ISP - Informações de Saúde Protegidas), propriedade intelectual (PI - Propriedade Intelectual), informações financeiras e operacionais. A segurança dessas informações requer ações de segurança sólida, como criptografia, autenticação robusta, atualização de *software* e sensibilização dos usuários.

Segundo Kosinski (2024), gerente geral de vendas de produtos de tecnologia da IBM Américas, os conceitos de 'violação de dados' e 'violação' são comumente confundidos com 'ataque cibernético'. Contudo, nem todos os ataques cibernéticos são vistos como violação de dados. Este tipo de incidente acarreta problemas graves e prolongados, como prejuízos à

imagem, financeiros, indiretos nas atividades, consequências jurídicas e perda de direitos autorais.

De acordo com o relatório da IBM (IBM, 2024) sobre o custo das violações de dados, o impacto financeiro global, em 2024, dessas ocorrências atingiu a marca de 4,88 milhões de dólares. Esse valor alarmante destaca a vulnerabilidade de organizações de todos os portes e setores, com variações significativas nos custos de remediação. Nos Estados Unidos, conforme relatado no mesmo relatório da IBM, o custo médio de uma violação chega a 9,36 milhões de dólares, enquanto na Índia esse valor é de 2,35 milhões de dólares. Setores altamente regulamentados, como saúde e bancos, enfrentam consequências ainda mais severas, com custos médios de violação de 9,77 milhões de dólares no setor de saúde. Os custos decorrentes de uma violação de dados apresentam perda de negócios, detecção e contenção, resposta pós violação e notificação, sendo a perda de negócios a mais significativa, com um custo médio de 1,47 milhão de dólares. A detecção e contenção da violação representam um custo médio de 1,63 milhão de dólares, enquanto as despesas pós violação somam 1,35 milhão de dólares. Os custos de notificação, embora menores, atingiram a marca de 430.000 dólares. A complexidade e o tempo utilizado para o reporte de violações, conforme exigido por regulamentações como a LGPD no Brasil, Lei CIRCIA nos EUA e o GDPR na Europa, destacam a importância de uma resposta rápida e eficaz a esses incidentes (IBM, 2024).

A exploração de falhas em *softwares* e a infecção por *malware* são outros métodos frequentes para o roubo de informações que se beneficiam da reutilização de senhas. A ausência de criptografia e a configuração restrita de aplicativos ou servidores da *web* também podem levar à divulgação de informações sigilosas.

2.4 Ransomware

Ransomware é um tipo de *malware* que, além de sequestrar informações sigilosas, também podem sequestrar as máquinas das vítimas, mantendo os ativos sequestrados sob controle da organização criminosa até que o resgate seja pago. Segundo ao relatório de ameaças gerado pela Unit 42 (Palo Alto, 2024) efetua a infiltração nos sistemas por meio de *phishing*, anexos maliciosos ou exploração de vulnerabilidades em RDP e *softwares* obsoletos.

O *remote desktop protocol* (RDP) é um protocolo criado pela Microsoft que permite a execução de conexão remota entre *endpoints* e servidores. Caso esteja mal configurado ou aconteça sua exposição para a internet sem controles adequados para sua proteção, ele acaba

sendo um elo frágil dentro do ambiente e permitindo ser explorado por indivíduos maliciosos para implantação de *malwares*, como o *ransomware*.

Existe uma diversidade de variantes de *malwares*, permitindo assim facilidade em se adaptar conforme suas futuras vítimas. Variantes surgem constantemente e com modificações que dificultam a detecção e aumentam sua capacidade de adaptação nos ambientes. As variantes principais de *ransomware* atualmente são: Lockbit 3.0, Black Basta, Clop,Hive e Royal. Tais variantes são muito utilizadas pelos cibercriminosos para ameaçar empresas e instituições governamentais no mundo todo.

Outra variante conhecida, como WannaCry, traz um impacto enorme como resultado dos ataques em organizações pelo mundo, causando a interrupção de operações e exigindo montantes de pagamento.

Os custos financeiros podem ser elevados e não se restringem apenas ao valor do resgate, mas também aos gastos com recuperação de dados e reestruturação da infraestrutura. Mesmo que a vítima não ceda à pressão do resgate, os custos com investigação, reestruturação, consultorias em segurança, e aquisição de novas ferramentas de proteção podem ser substanciais. De acordo com o Relatório de Ameaças da Unit 42 da Palo Alto Networks (Palo Alto Networks, 2024), o valor médio do resgate pago por organizações atacadas em 2023 foi estimado em US$740.000, com alguns casos atingindo mais de US$20 milhões.

Os *malwares* são frequentemente infiltrados por meio de *e-mails* suspeitos, anexos indevidos ou explorando vulnerabilidades em RDP. De acordo com o Relatório da Sophos (Sophos, 2024), mais de 85% dos ataques de *ransomware* começaram através de técnicas de *phishing* e exploração de RDPs vulneráveis, tirando proveito das brechas de segurança para se disseminar na Internet

Quando adentrado no sistema, ele escaneia arquivos para criptografar, exclui as versões de origem e acaba deixando uma nota de resgate exigindo pagamento (geralmente em criptomoedas para garantir anonimato).

Algoritmos de criptografia sofisticados e furtivos fazem com que a recuperação dos dados sem a chave de descriptografia seja extremamente difícil. Dependendo do *malware*, mesmo equipes de segurança avançada têm dificuldade em quebrar esses esquemas de criptografia. Para analisar o funcionamento do código do *ransomware* e determinar como ele infectou o sistema é necessário planejar a recuperação e restauração dos backups ou utilizando ferramentas especializadas para a recuperação.

Destaca-se a importância de medidas preventivas robustas e *backups* eficazes para mitigação impostos por ataques de *ransomware*.

2.5 Incidente de cibersegurança

Incidente de cibersegurança são eventos que afetam a confidencialidade, integridade ou disponibilidade da informação. Esses incidentes podem ser intencionais ou não intencionais, segundo a ISO/IEC 27035 (ABNT, 2023 *apud* Target Normas, 2023), um incidente é descrito como um evento ou série de eventos indesejados, ou inesperados, que possuem a possibilidade de prejudicar a segurança da informação e operações do negócio, requerendo que seja efetuado uma resposta imediata.

Dentro da área de segurança da informação, os incidentes podem ser categorizados conforme sua natureza e consequência

- ***Malware***: Conforme comentado anteriormente são programas mal-intencionados concebidos para infringir a integridade, confidencialidade ou disponibilidade de sistemas e dados. Dentro das categorias estão incluídos *vírus*, *worms*, *trojans*, *spywares* e *ransomware*. O *ransomware*, particularmente, tem sido sobressaído como uma das ameaças mais frequentes e danosas nos anos recentes. De acordo com o relatório Verizon Data Breach Investigations (Verizon, 2023).
- ***Phishing***: Método de engenharia social para adquirir informações confidenciais ou credenciais.

  Normalmente esse tipo de ataque visa se passar por entidades confiáveis. Segundo o Relatório de Tendências de Ameaças Cibernéticas da Cisco (2024), 80% dos ataques bem-sucedidos tiveram a ferramenta *phishing* como seu primeiro movimento.
- Ataque DDoS: Atua para a realização de sobrecarga de requisições em sistemas ou rede de modo simultâneo, quebrando assim o pilar de disponibilidade e deixando os serviços indisponíveis. Conforme a Cloudflare em seu relatório de DDoS Threat Report (Cloudflare, 2023), os ataques que foram baseados em HTTP tiveram um aumento de 80% desde o último trimestre de 2023, demonstrando uma crescente e significativa sofisticação e frequência.
- Acesso não autorizado: Situação em que indivíduos não autorizados possuem acesso indevido a informações confidenciais e restritas. Essa ação é consequência de credenciais de baixa complexidade, autenticação inadequada ou ferramentas de controle de acesso falhos.

Conforme apresentado pelo NIST SP 800-61 Rev. 3 (NIST, 2023) o procedimento de resposta a incidentes é muito importante para a mitigação de impactos de incidentes de segurança, garantindo a continuidade do negócio. O fluxo de resposta a incidentes pode ser descrito em cinco etapas estruturadas, que visam garantir a pronta resposta e recuperação diante de um evento de cibersegurança, sendo elas:

- Preparação*:* Envolve a implementação de políticas de segurança da informação, treinamento da equipe para lidar com ocorrências de incidentes, como CSIRT e SOC, e implementação de *frameworks* como NIST Cybersecurity Framework (CSF) 2.0;
- Detecção (Identificação)*:* Identificação de anomalias por meio de sistemas de monitoramento, como SIEM's (solução que coleta, analisa e correlaciona eventos de segurança gerados em dispositivos e aplicativos de TI, ajudando a detectar ameaças e gerenciar incidentes de forma centralizada.) e sistema de monitoramento de rede (Zabbix, Wazuh, Naggios, entre outros). Também é efetuado a realização de análise dos dados para confirmar o evento e compreender seu escopo;
- Contenção*:* Isolamento dos sistemas alvos comprometidos para evitar a movimentação lateral do ataque. Essa contenção pode durar um curto ou longo espaço de tempo, dependendo da criticidade do sistema afetado.
- Recuperação e Erradicação*:* Responsável pela tomada de medidas para executar a recuperação dos sistemas afetados, correção de falhas de segurança e minimizar o tempo de inatividade. Também é de grande importância a remoção de artefatos maliciosos e a correção das vulnerabilidades exploradas pelo atacante.
- Lições aprendidas*:* Essa fase apresenta para a equipe quais lições foram apresentadas no pós-resposta, garantindo que a equipe tenha uma melhoria contínua do processo de resposta a incidentes. A aprendizagem é adquirida a partir de uma revisão e análise das ocorrências do evento, com isso é possível que a equipe de Segurança da Informação amadureça a partir da identificação dos pontos fracos e fortes do seu plano de resposta a desastres.

2.6 Normas e regulamentações relevantes

Com o aumento de ameaças e a crescente preocupação das organizações em relação à privacidade de dados, normas e regulamentações surgiram com o objetivo de fornecer diretrizes claras de como a proteção, gerenciamento e utilização de informações de modo seguro.

2.6.1 ISO/IEC 27001: Sistema de Gestão de Segurança da Informação (SGSI)

A ISO é uma norma internacional que apresenta uma definição de padrões e diretrizes para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI). A ISO/IEC 27001 possui o principal objetivo a prevenção da confidencialidade, integridade e disponibilidade das informações, apresentando uma abordagem sistemática para a realização da gestão de riscos de segurança da informação, conforme apresentado pela ABNT (ABNT, 2024 *apud* Target Normas, 2024).

O ciclo de melhoria contínua proposto pela norma baseia-se no modelo PDCA (*Plan-Do-Check-Act*), onde a organização deve realizar o planejamento, implementação, monitoramento e aprimoramento dos controles e políticas de segurança. Conforme a própria norma, são abordados os principais pontos:

- Análise e tratamento de riscos;
- Definição de políticas de segurança da informação;
- Atribuição de responsabilidades;
- Gerenciamento de ativos e controle de acessos;
- Conformidade com requisitos legais e contratuais.

A norma apresenta um grande compromisso das organizações para a proteção de dados, apresentando-se como diferencial competitivo dentro do mercado.

2.6.2 ISO/IEC 27002 - Controles de Segurança da Informação

Conforme a norma ISO/IEC 27002 (ABNT, 2022 *apud* Target Normas, 2022), a norma é um complemento para a 27001, oferecendo um guia de boas práticas para a realização da implementação de controles de segurança da informação. Na norma é estabelecido o como deve ser realizado, fornecendo uma base prática para os controles estipulados na norma.

A norma divide os controles em domínios, onde eles irão tratar de tópicos diferentes:

- Controles organizacionais;
- Controle de pessoas;
- Controles físicos;
- Controles tecnológicos.

Esses controles são acompanhados por objetivos e orientações para a sua adição. Esses controles devem basear-se na análise de contexto e riscos da organização.

2.6.3 NIST Cybersecurity Framework

O NIST Cybersecurity Framework, ou CSF, foi criado pelo National Institute of Standards and Technology, é um conjunto de diretrizes, práticas e padrões para realização da gestão de riscos de segurança (NIST, 2024). Utilizado de modo amplo por organizações de diversos setores ao redor do mundo, trazendo uma estrutura dividida em cinco partes: Identificar, Proteger, Detectar, Responder e Recuperar.

Possuindo uma abordagem flexível o NIST permite a personalização conforme as necessidades do negócio, sendo um framework valioso para empresas que almejam alinhar seus processos às melhores práticas de segurança de modo prático e seguro.

2.6.4 COBIT e ITIL

COBIT e ITIL, mesmo que seu foco não seja em segurança da informação, são *frameworks* atuais, globalmente usados e fundamentais para as atividades da governança, riscos e conformidade (GRC),

- **COBIT 2019:** Conforme apresentado pela ISACA (2023), ele se apresenta como um *framework* para a criação de valor a partir da tecnologia da informação, tendo como foco seu desempenho, conformidade e alinhamento estratégico.
- **ITIL 4:** *Framework* que apresenta orientações da gestão de serviços de TI, tendo como base a criação de valor e o cliente. Facilitando a integração entre práticas ágeis, DevOps e governança (Axelos, 2023).

Esses *frameworks* agregam para a estruturação de processos robustos de GRC, cumprindo requisitos legais e normativos, além de aprimorar a qualidade e a eficiência dos serviços de TI.

2.6.5 MITRE ATT&CK

O MITRE ATT&CK, criado pela MITRE Corporation, é uma base de conhecimento e constantemente atualizada, que registra e explica as ações de atacantes cibernéticos observadas no mundo. Ao contrário de abordagens reativas que se focam apenas em indicadores de comprometimento (IoCs) como hashes ou IPs maliciosos, o MITRE ATT&CK concentra-se no comportamento dos adversários. Ele classifica esse comportamento em uma matriz de táticas e técnicas, o que possibilita um entendimento mais detalhado de como os ataques são realizados.

As táticas refletem os objetivos de alto nível que um adversário pode atingir durante um ataque, incluindo acesso inicial, execução, persistência, escalada de privilégios, evasão de defesa, acesso a credenciais, descoberta, movimento lateral, coleta, exfiltração e impacto. Dentro de cada tática, existem diversas técnicas específicas que descrevem como o adversário pode atingir aquele objetivo tático.

2.6.6 HIPAA

O Health Insurance Portability and Accountability, ou HIPAA, é uma lei federal dos Estados Unidos aprovada em 1996 para a proteção de informações de saúde das pessoas, definindo normas para a privacidade e a segurança de dados médicos. Apesar de ser uma lei válida nos Estados Unidos, ela tem impacto global nas empresas multinacionais e serve como modelo para leis similares em outras nações (HHS, 2023), visando garantir a confidencialidade, integridade e disponibilidade das informações de saúde.

A lei está separada em diferentes títulos legais, com destaque para o segundo título apresentado como ‘Simplificação Administrativa no âmbito da segurança da informação'. Nele é definido orientações essenciais para a proteção de informações de saúde, seguindo três normas principais: Diretriz de privacidade, Diretriz de segurança e a Diretriz de notificação de violação. Essas normas trazem requisitos obrigatórios para o tratamento de informações de saúde, principalmente em forma eletrônica, aplicando-se tanto a entidades cobertas, como hospitais, clínicas, laboratórios e operadoras de planos de saúde, como a terceiros que efetuam o processamento ou acesso de dados sensíveis em nome dessas instituições.

Cada framework, lei ou norma aqui abordado define um conjunto específico de proteções administrativas, técnicas e físicas, visando garantir a confidencialidade, integridade e disponibilidade das informações, em acordo com os princípios de boas práticas de segurança da informação.

3 CASOS DE INCIDENTES DE RANSOMWARE

3.1 Empresa do setor de oleodutos

O primeiro caso real é o de uma organização privada estadunidense responsável pela operação do maior sistema de oleodutos de produtos refinados do país. Esse sistema transporta aproximadamente 2,5 milhões de barris de combustível por dia, suprindo a demanda do leste dos Estados Unidos, sendo assim um ponto importante para a economia do país.

A empresa sofreu um ataque de *ransomware* no dia 07 de maio de 2021, onde acabou gerando a paralisação das operações ativas por completo. A responsabilidade do ataque foi tomada pelo grupo DarkSide, especializado em ataques de ransomware como serviço (*RaaS – Ransomware as a Service*), onde eles implantaram o *ransomware* nos sistemas de tecnologia da informação da vítima, impactando operações administrativas, financeiras e logísticas.

O vetor do ataque foi uma credencial de VPN legada sem autenticação multifator, cuja credencial foi vazada (comprometida e publicada) em fóruns da *dark web*. Essa conta permitia com que fosse feito o acesso remoto à rede interna, o que facilitou a infiltração. Assim que entraram no sistema, os invasores traçaram um mapa da infraestrutura e realizaram movimentos laterais, acessando diversos domínios, servidores e bases de dados internos. Nesse procedimento, os atacantes recebem privilégios elevados, acessos a arquivos exclusivos e, por fim, instalam o *ransomware* em servidores de produção.

O *malware* usado era uma variante criada pelo grupo DarkSide que realizava a criptografia de arquivos e impedia o acesso de usuários legítimos. Simultaneamente, os *hackers* intensificaram para as vítimas o risco de exposição pública caso o resgate não fosse pago, um método denominado dupla extorsão.

Apesar do sistema industrial (OT - Tecnologia Operacional) não sofrer danos diretos, foi escolhido por interromper toda a operação como uma medida de contenção, visando evitar a propagação do vírus no parque de máquinas e nos sistemas vitais de controle. A escolha foi fundamentada na possibilidade de que o *ransomware*, por sua capacidade de disseminação, pudesse abranger áreas de integração entre TI e OT e impactar o funcionamento automático de válvulas e sensores. A atividade foi feita pela impossibilidade de identificar imediatamente quais sistemas estavam em risco e quais sistemas se mantiveram seguros.

O ataque evidenciou que sua infraestrutura cibernética apresentava sérias vulnerabilidades, principalmente no setor de TI. A falta de uma autenticação forte, a preservação de acessos antigos, a ausência de visibilidade sobre credenciais violadas e a falta de controles preventivos sólidos apontam para uma infraestrutura operacional vulnerável em

relação à segurança da informação, especialmente quando confrontada com as demandas contemporâneas de defesa cibernética em contextos de missão crítica.

Destaca-se assim a falta de ligação entre as diretrizes corporativas de segurança da informação e as táticas operacionais de continuidade dos negócios. É evidente na demora nas primeiras horas após a detecção do ataque, bem como na demanda por assistência externa para a contenção e investigação do incidente.

3.1.1 Vulnerabilidades exploradas e método de ataque

O ponto de entrada dos atacantes no sistema deu-se por uma conta VPN que, mesmo não estando em uso, permanecia ativa e não possuía proteção de MFA integrada. Foi constatado que as credenciais associadas a essa conta de VPN estavam comprometidas, já que havia acontecido anteriormente um vazamento de banco de dados onde ela estava disposta, e essas informações estavam acessíveis na *dark web*.

Com a entrada dos atacantes por meio da credencial falha, os *hackers* fizeram movimentações laterais dentro da rede da organização. Desta forma, foram exploradas muitas falhas de segurança existentes entre os diferentes ambientes da rede. Tendo como resultado dessas ações, os atacantes conseguiram escalar seus privilégios, alcançando níveis elevados de acesso de forma rápida.

Além dessas falhas técnicas a empresa revelou uma deficiência estratégica crucial: a empresa não dispunha de um programa de gerenciamento de riscos cibernéticos estabelecido e amadurecido. Esse programa não incluía a análise regular e proativa de novas ameaças, o que deixou a organização vulnerável a ataques previsíveis.

É reconhecível que a combinação de conta de VPN ativa e desprotegida por MFA, e com credenciais expostas publicamente, com ausência de ações proativas para monitoramento de credenciais, constituem a principal falha que permitiu o acesso inicial. Essa inexistência de cuidado com as credenciais impediu que fosse identificado de modo antecipado o perigo iminente, sendo assim uma falha direta na aplicação da norma ISO/IEC 27001 que aborda a remoção ou o ajuste tempestivo dos direitos de acesso, principalmente a revogação de acessos de modo imediato dos acessos que não são mais necessários.

As ações subsequentes dos atacantes, como a movimentação lateral e a escalada de privilégios, não só exploraram, mas também expuseram as vulnerabilidades nos controles de interrupção e segregação entre redes e sistemas. Conclui-se que a ausência de uma segregação eficaz e detalhada da rede facilitou o avanço dos invasores, permitindo que eles se movessem

de áreas menos críticas para segmentos mais sensíveis da infraestrutura, onde estavam os servidores com dados críticos.

A falta de ferramentas eficientes para gerenciar privilégios de acesso é outro aspecto. Isso evidencia deficiências na conformidade com o controle específico de gestão de privilégios especiais. A velocidade com que os atacantes conseguiram elevar seus privilégios é um sinal claro da ausência de mecanismos de validação contínua e de uma separação de funções eficaz na gestão de TI, que são princípios fundamentais de segurança.

Por fim, a constatação de que não havia um programa de gerenciamento de riscos definido e operacional é a falha mais significativa. Isso vai contra o princípio básico da ISO 27001, que estabelece a necessidade de realizar avaliações de risco de segurança em intervalos planejados ou sempre que mudanças significativas no ambiente ou no cenário de ameaças se tornem evidentes. Dado que o *ransomware* é uma ameaça bem conhecida e amplamente documentada na indústria, a incapacidade da organização de antecipar e se preparar para se proteger adequadamente contra esse tipo de risco é especialmente grave e demonstra uma negligência em sua postura.

3.1.2 Medidas de prevenção existentes: acertos e falhas

Antes do incidente, a empresa já havia adotado algumas medidas consideradas fundamentais na área de segurança. Dentre essas medidas, estavam a realização periódica de *backups* de dados, o uso de *firewalls* para gerenciar o tráfego na borda da rede e uma tentativa de segmentação da rede, visando separar os ambientes de tecnologia da informação (TI) dos de tecnologia operacional (OT). Essas medidas preexistentes, de fato, foram úteis, pois permitiram que a empresa recuperasse parcialmente os dados afetados pelo incidente e, igualmente importante, ajudaram a restringir a propagação imediata do ataque aos sistemas industriais (OT), que costumam ser críticos.

Foi constatada a falta de um processo de MFA e a ausência de um sistema ou procedimento formal para o monitoramento constante de credenciais que estejam vulneráveis ou comprometidas. Um ponto crucial que surgiu foi a apresentação da não existência de um plano de ação para resposta a desastres no geral.

Significativas falhas na arquitetura e na estratégia de segurança da organização, mesmo considerando as medidas básicas que já se encontravam em vigor. A ausência de um processo de MFA em uma conta VPN, utilizada para acesso externo, é um indicativo claro de uma deficiência importante na gestão de identidades e acessos. O MFA é, atualmente, uma medida de segurança fundamental e indispensável para proteger acessos remotos, sendo

crucial para a redução efetiva do risco de invasões que explorem o comprometimento de credenciais.

A falta da implementação do monitoramento contínuo de credenciais poderia ter alertado a equipe de segurança previamente sobre a existência de credenciais comprometidas ou fracas em circulação, permitindo uma ação corretiva ou preventiva antes que estas fossem efetivamente exploradas pelos atacantes.

Além disso, a falta de um plano de resposta a desastres para ataques cibernéticos representa uma falha significativa no planejamento estratégico de continuidade de negócios e na resiliência cibernética da empresa. Essa omissão não só dificultou, mas também tornou significativamente mais complexa a tomada de decisões e a coordenação das ações de resposta nos momentos iniciais e mais críticos do ataque. A falta de um guia claro e testado para essa situação certamente aumentou o impacto do incidente e atrasou uma recuperação mais rápida e eficaz.

3.1.3 Estratégia de detecção e resposta: eficiência e fragilidades

Embora o ataque tenha sido identificado de forma relativamente rápida, não há evidências públicas que confirmem que essa detecção inicial foi feita por meio de ferramentas automatizadas de identificação de ameaças, como sistemas SIEM (gerenciamento de eventos e informações de segurança), EDR (resposta e detecção de *endpoint*) ou SOAR (orquestração, automação e resposta em segurança). A detecção do incidente foi reativa, o que não impediu a movimentação lateral dos atacantes na rede interna nem a infiltração e exfiltração de dados.

No que tange à resposta imediata ao caso, a empresa afetada tomou a decisão drástica de interromper completamente suas atividades operacionais. Esta ação envolveu o desligamento brusco dos sistemas OT e de TI. Verificou-se que a instituição não possuía um plano de resposta a desastres (PRD) formalmente validado antes do ocorrido. Adicionalmente, é perceptível a ausência de uma estrutura interna dedicada e formalizada para o gerenciamento de incidentes de segurança, como uma equipe de resposta a desastres ou um centro de operações de segurança (SOC).

Um fato notável foi a ação da empresa de pagar o resgate solicitado, que totalizava 4,4 milhões de dólares em criptomoedas, mesmo após ter feito cópias de segurança de seus sistemas anteriormente. A empresa conseguiu retomar suas operações em cinco dias após o ataque. Entretanto, esse processo de recuperação foi caracterizado por uma série de ações improvisadas e uma grande dependência de consultorias externas. Informações divulgadas pela própria organização posteriormente ao incidente indicaram que suas estratégias de

detecção e os processos de tomada de decisão estavam, de fato, desalinhados com as boas práticas e os *frameworks* de segurança de mercado.

O incidente demonstra claramente a coexistência de uma capacidade de reação emergencial com uma carência fundamental de uma estratégia organizada e proativa para a detecção e resposta a ameaças cibernéticas. A falta de uma estrutura forte de monitoramento contínua e intensificada de incidentes de segurança não apenas prejudicou a organização em seu ambiente interno.

A natureza reativa da detecção do incidente é um forte indicativo de que as camadas de segurança existentes não eram adequadamente configuradas ou careciam de especificidade para identificar comportamentos atípicos e maliciosos. Isso inclui falhas em detectar acessos indevidos a volumes significativos de arquivos, o uso de comandos administrativos de forma não usual ou reservada, ou tentativas de elevação de privilégios não autorizadas. É apontado a falta ou uma configuração deficiente e limitada de tecnologias cruciais no arsenal de defesa moderno.

A decisão drástica de interromper completamente as atividades, por meio do desligamento brusco dos sistemas, embora possa ter sido eficiente em um primeiro momento para conter a propagação do *ransomware*, evidenciou uma ausência preocupante de planejamento e de mecanismos automatizados para uma resposta coordenada e potencialmente menos disruptiva. A falta de um plano de resposta a desastres (PRD) validado e testado complicou severamente as primeiras ações estratégicas pós-detecção e gerou uma dependência imediata e custosa de suporte externo.

O pagamento do resgate, apesar de haver cópias de segurança, levanta questionamentos sobre a confiança da empresa na integridade e acessibilidade dessas informações. Isso indica problemas na realização e na verificação dos *backups*. Essa falta de preparo prejudicou a otimização e agilidade que poderiam ter sido alcançadas com um planejamento mais sólido e recursos internos apropriados.

3.1.4 Impactos do incidente

A interrupção brusca das operações de um importante duto de combustíveis desencadeou uma crise de abastecimento que reverberou por diversos estados norte-americanos. Este evento manifestou-se em postos de combustível através da escassez de produtos e da formação de longas filas de motoristas. Consequentemente, observou-se um aumento considerável nos preços dos combustíveis. Aeroportos e transportadoras tiveram

suas operações afetadas, mostrando a grande interdependência entre infraestruturas digitais e cadeias logísticas críticas.

No contexto corporativo, a empresa enfrentou perdas financeiras diretas e prejuízos consideráveis à sua imagem. O governo dos Estados Unidos reagiu de forma intensa ao incidente e como resposta, foram implementadas novas diretrizes que exigem padrões mínimos de cibersegurança para operadores de dutos e outras infraestruturas vitais. Entre essas medidas, destacam-se a exigência de notificação de incidentes cibernéticos e a execução de auditorias de segurança.

Conclui-se então que a paralisação das operações do duto demonstrou de forma inequívoca a vulnerabilidade das cadeias de suprimentos críticas a interrupções em infraestruturas digitais. O incidente serviu como um catalisador para uma reavaliação da segurança cibernética em setores importantes. A resposta governamental, ao impor padrões mínimos de cibersegurança e notificações compulsórias, reflete o reconhecimento da necessidade de uma postura mais proativa e regulamentada para proteger infraestruturas críticas contra ameaças digitais. As perdas financeiras e reputacionais sofridas pela empresa operadora também mostram a importância da gestão de riscos cibernéticos como um componente essencial da governança corporativa.

3.1.5 Lições aprendidas

O caso em questão mostrou que uma empresa teve sua cadeia de suprimentos afetada pela falta de medidas de segurança consideradas fundamentais. Foi demonstrado que a primeira credencial inativa usada no ataque foi uma credencial de uma VPN legada. Também foi observado que a empresa não possuía um monitoramento contínuo e eficiente contra ameaças, como serviços de detecção de senhas comprometidas ou análise de comportamento de usuários. Isso poderia ter alertado sobre a exposição de dados da organização em vazamentos públicos. Ficou evidente uma falha na preparação para incidentes, devido à falta de um plano de resposta sólido, testado e atualizado.

Com isso, existe uma necessidade de fortalecer as defesas cibernéticas em organizações críticas. Primeiramente, destaca-se a necessidade da implementação rigorosa de autenticação multifator em todos os acessos remotos. Justifica-se essa medida pelo fato de que, mesmo sendo um controle de segurança relativamente simples, o MFA poderia ter bloqueado o acesso inicial do invasor, impedindo a exploração da credencial comprometida.

Em segundo lugar, ressalta-se a importância crucial de uma gestão de identidade e acesso (IAM) eficiente. O fato de o ataque ter se originado a partir de uma credencial inativa

de VPN legada evidencia a falha nesse processo. Portanto, a implementação de políticas de ciclo de vida de contas, incluindo revisões periódicas de permissões e a desativação automatizada de contas obsoletas, é fundamental para mitigar riscos semelhantes.

A preparação para incidentes não pode ser negligenciada. Possuir um plano de resposta a desastres bem definido, testado regularmente e atualizado, com clara atribuição de funções, responsabilidades e procedimentos para tomada de decisão, é crucial.

3.2 Ataque *ransomware* a uma empresa de tecnologia para o setor de saúde

O segundo caso deste estudo é o de uma das maiores empresas do setor de tecnologia voltado para a área da saúde dos Estados Unidos. Ela atua como elo intermediário entre clínicas, hospitais, laboratórios, farmácias e operadoras de planos de saúde, sendo responsável pelo processamento de grande número de informações médicas anualmente, incluindo atividades de autorizações de exames, encaminhamentos clínicos, faturamento, processamento de pagamentos e gestão de registros eletrônicos de saúde. A organização foi alvo de um ciberataque de grande escala no dia 21 de fevereiro de 2024, sendo classificado como um incidente de *ransomware* duplo (quando o atacante não apenas criptografa os sistemas afetados, mas também realiza a exfiltração de dados sensíveis, utilizando a ameaça de vazamento como arma para extorsão).

A autoria desse crime foi vinculada ao grupo BlackCat/ALPHV, grupo conhecido por atuar contra infraestruturas críticas com ferramentas sofisticadas. O ataque à empresa de tecnologia causou a paralisação completa dos sistemas principais da empresa, tendo assim como resultado a paralisação dos serviços de autorizações médicas e de processamento de pagamentos em escala nacional. Consequentemente, clínicas e farmácias foram diretamente afetadas, gerando atrasos em tratamentos e prejuízos financeiros para instituições de saúde e pacientes.

3.2.1 Vulnerabilidades Exploradas e Método de Ataque

A companhia relatou que cibercriminosos acessaram sua rede remotamente usando credenciais válidas, provavelmente obtidas por *spear phishing* direcionado a usuários privilegiados, com *e-mails* contendo *links* para páginas de *login* falsas. Com as credenciais, os atacantes acessaram os sistemas internos via RDP sem disparar alarmes, por ser um *login* autenticado.

Ferramentas legítimas do sistema operacional (PowerShell, WMI, Tarefas Agendadas) foram usadas para controle remoto e execução de *scripts*. A movimentação lateral ocorreu

discretamente, utilizando credenciais administrativas internas, muitas vezes armazenadas em texto simples, e explorando vulnerabilidades conhecidas não corrigidas, como *PrintNightmare* e falhas no *Active Directory*. Após a infiltração de dados, o *payload* do *ransomware* foi distribuído coordenadamente com ferramentas como Cobalt Strike e Mimikatz, criptografando sistemas em vários setores da infraestrutura.

Com os fatos expostos, é perceptível que os fatos deste incidente conduzem a importância sobre as táticas dos atacantes e as fragilidades exploradas, justificando aprimoramentos em segurança. O êxito do *spear phishing* como vetor inicial evidencia a contínua eficácia da engenharia social direcionada e a necessidade crítica de elevar a conscientização dos usuários, o que justifica investimentos persistentes em treinamentos para a identificação de fraudes. O acesso não detectado via RDP, mesmo autenticado, aponta para lacunas no monitoramento de comportamento e na configuração de alertas, tornando imperativa a implementação de ferramentas de análise comportamental e uma revisão criteriosa das políticas de alerta.

3.2.2 Medidas de prevenção existentes: acertos e falhas

A entidade possuía um conjunto de ações de segurança básicas e insuficientes para lidar com ameaças de alto nível, como o *ransomware*. A utilização de *firewalls* perimetrais, antivírus comerciais, políticas de senhas e orientações para *backups* programados estavam entre as medidas de controle existentes. Também existia um plano de continuidade de negócios e uma política de resposta a desastres, em nível teórico.

Em relação às vulnerabilidades e falhas exploradas durante o ataque, a implementação da autenticação multifator não era uma atividade comum, pois não incluía todas as modalidades de acesso remoto aos sistemas da organização. De maneira especialmente crítica, foi apresentada a possibilidade de obter acessos com privilégios administrativos usando apenas as credenciais básicas de nome de usuário e senha.

Outro ponto de fragilidade constatado foi a segregação da rede, que se mostrou inadequada. A empresa também não contava com um sistema de monitoramento contínuo de segurança que incorporasse funcionalidades de análise de comportamento dos usuários e das entidades presentes na rede. Em relação às práticas de *backup*, embora fossem executadas, elas não estavam suficientemente resguardadas por um isolamento lógico ou físico robusto.

Com as informações expostas, o conjunto de ações de segurança básicas que eram adotadas pela entidade mostrou-se manifestamente insuficiente para fazer frente a ameaças cibernéticas de alto nível e sofisticação, como o *ransomware* moderno, frequentemente

gerenciado por grupos organizados como o ALPHV. As falhas reveladas durante e após o incidente foram consideráveis e indicam deficiências sistêmicas na estratégia de segurança da organização.

Permitir acessos administrativos apenas com nome de usuário e senha facilitou enormemente um potencial de invasão, representando uma negligência de um controle de segurança que é fundamental e amplamente recomendado no cenário atual de ameaças.

A segregação ineficaz da rede foi outra falha crítica. Essa deficiência possibilitou que um invasor, uma vez comprometido um ponto de entrada inicial, pudesse transitar lateralmente com relativa liberdade entre diversos ambientes da rede, incluindo sistemas críticos de administração financeira e aqueles contendo dados clínicos sensíveis. Tal movimentação ampliou exponencialmente o raio de impacto e a severidade do ataque.

A existência de ferramentas de SIEM mal configuradas transformou-se em um problema paradoxal e adicional. Em vez de ajudar na detecção, essas ferramentas, por causa da correlação ineficaz de eventos e do alto número de falsos positivos, provavelmente causaram um "ruído" excessivo e uma possível complacência, comprometendo a habilidade da equipe de identificar ameaças reais em meio a um grande volume de alertas sem relevância.

A questão dos *backups* é particularmente emblemática das deficiências de planejamento e execução observadas. A falta de isolamento lógico adequado dos dados copiados tornando-os igualmente vulneráveis ao ataque de *ransomware*. Com isso essa falha possibilitou sua criptografia pelos atacantes em conjunto com os sistemas de produção primários, neutralizando uma das principais linhas de defesa e recuperação contra esse tipo de ameaça. Além disso, a falta de uma política clara e a ausência de testes regulares e rigorosos de recuperação de desastres dificultou consideravelmente o processo de restauração de sistemas e dados após o ataque. Essa omissão resultou em um aumento do tempo de inatividade, agravou os prejuízos financeiros e operacionais e gerou dúvidas sobre a possibilidade de recuperação.

3.2.3 Estratégia de detecção e resposta: eficiência e fragilidades

A organização fundamentava sua capacidade de detecção de ameaças em um conjunto de ferramentas e processos considerados tradicionais e limitados. Estas práticas incluíam o uso de *software* antivírus de prateleira, a implementação de *firewalls* configurados predominantemente com regras estáticas, o monitoramento isolado de *logs* de diferentes sistemas e a criação manual de alertas de segurança.

No decorrer do caso, é constatado também que a organização não possuía uma estrutura de monitoramento contínuo suficientemente madura, nem dispunha de sistemas de detecção de ameaças que fossem baseados em análise de comportamento de usuários e entidades.

A situação de detecção foi particularmente agravada pelo fato de os atacantes terem utilizado credenciais válidas para realizar suas movimentações dentro da rede, o que tornou a distinção entre atividades legítimas e maliciosas consideravelmente mais complexas para as ferramentas e processos existentes. Adicionalmente, a empresa não dispunha de uma solução dedicada à análise comportamental.

No que tange às ações de resposta ao incidente, a companhia tomou a iniciativa de recrutar especialistas em forense digital e implementou algumas medidas de contenção para mitigar os danos. Contudo, ficou evidente a falta de um centro de operações de segurança (SOC) interno ou de uma equipe de monitoramento terceirizada que estivesse disponível em regime de 24/7. Um dos problemas mais salientes observados nos momentos iniciais da resposta ao incidente foi a comunicação desordenada e pouco eficiente entre os diferentes setores da empresa.

Diante do exposto, a falha principal neste caso não reside apenas na ocorrência técnica imediata ou na exploração de uma vulnerabilidade específica, mas, fundamentalmente, na falta de uma estrutura de segurança integrada, proativa e resiliente. A estratégia de identificação e resposta a desastres empregada pela organização infectada não evidenciou estar à altura da complexidade e sofisticação das ameaças cibernéticas atuais. Além disso, essa abordagem não está em sintonia com os princípios de resiliência que são cada vez mais exigidos, especialmente em organizações de setores críticos como o da saúde, onde a continuidade dos serviços é vital.

Este caso destaca a necessidade urgente de uma transição dos modelos de segurança convencionais e reativos para uma estratégia moderna, fundamentada em inteligência sobre ameaças (*Cyber Threat Intelligence*), automação de processos de segurança e uma capacidade de resposta orquestrada e bem definida. Esses elementos são fundamentais para enfrentar ameaças persistentes de forma eficiente e para reduzir consideravelmente o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR) a incidentes de segurança, minimizando, dessa maneira, os danos à organização.

3.2.4 Impactos do Incidente

Como consequência direta da alta complexidade do ataque cibernético, a empresa enfrentou uma interrupção ampla e grave de seus serviços fundamentais. Essa interrupção não se restringiu apenas à empresa alvo do ataque, mas gerou um efeito dominó, impactando

diretamente milhares de instituições de saúde que dependiam dos sistemas da empresa para suas atividades diárias. Através das informações disponíveis, os estabelecimentos de saúde ficaram impossibilitados de realizar processos fundamentais, como autorizações de procedimentos médicos, o faturamento de serviços já prestados e o recebimento de pagamentos vitais para sua sustentabilidade.

Os efeitos diretos dessas interrupções operacionais foram sérios e de grande alcance. Como resultado dessas interrupções, muitos tratamentos médicos sofreram atrasos ou adiamentos significativos. Várias instituições de saúde que dependiam dos sistemas da empresa atacada sofreram perdas financeiras e operacionais significativas.

Na esfera econômica, o prejuízo financeiro total atribuído ao incidente foi estimado em um valor aproximado de 870 milhões de dólares.

No contexto jurídico e regulatório, a empresa foi obrigada a cumprir uma série de requisitos obrigatórios para lidar com as implicações legais da violação de dados. Isso envolveu a exigência de fazer notificações formais e minuciosas à autoridade de saúde competente dos EUA. Além disso, a empresa precisou informar individualmente os pacientes cujos dados pessoais e informações de saúde foram comprometidos ou violados durante o incidente, tudo em estrita conformidade com as diretrizes e exigências da Lei de Portabilidade e Responsabilidade em Saúde (HIPAA), uma legislação rigorosa sobre a privacidade e segurança das informações de saúde.

Diante do exposto, conclui-se que os efeitos do ataque cibernético foram profundos e de múltiplas faces, um resultado direto e esperado de um incidente de tamanha sofisticação direcionado a uma infraestrutura crítica e sensível como a do setor de saúde. A ligação clara entre a interrupção dos sistemas da empresa afetada e o impacto negativo direto na prestação de serviços de saúde a milhares de pacientes demonstra a seriedade sistêmica e a possibilidade de uma crise generalizada que esses ataques podem causar.

O prejuízo astronômico representa um golpe no balanço financeiro, apenas quantifica parcialmente o dano real. Este dano se estende de forma imensurável à confiança dos pacientes no sistema de saúde, à estabilidade operacional de inúmeras instituições que dependem de terceiros e à integridade e confidencialidade de dados extremamente sensíveis.

3.2.5 Lições aprendidas do caso

A análise post-mortem do incidente, baseada nos fatos referenciados anteriormente neste estudo, revelou que a organização operava com uma série de deficiências significativas em sua arquitetura de segurança da informação.

Um dos pontos mais críticos foi a falta de implementação da autenticação multifator de forma universal, especialmente para todas as credenciais administrativas e para os acessos remotos à rede corporativa. Além disso, a segregação da rede existente revelou-se limitada e ineficiente.

Ficou claro que não havia uma estrutura de defesa em profundidade, o que, na prática, permitiu que uma única credencial comprometida facilitasse uma movimentação lateral extensa e preocupante em várias partes da rede interna.

Outra observação relevante foi a ausência, por parte da empresa, de um sistema de monitoramento de segurança contínuo que inclua a capacidade de analisar o comportamento de usuários e entidades. Apesar de a infraestrutura tecnológica da organização contar com ferramentas de SIEM, constata-se que elas estavam mal configuradas. Essa configuração imprópria levava a uma correlação de eventos de segurança ineficazes e, gerava muitos alertas falsos positivos, dificultando a detecção de ameaças reais.

No que diz respeito à proteção de dados através de *backups*, embora cópias de segurança fossem programadas e realizadas, os dados não eram armazenados em locais que garantisse seu isolamento lógico ou físico adequado, nem contavam com controles de imutabilidade. Adicionalmente, não existia uma política clara e formalizada para a execução de testes regulares e completos de recuperação de desastres. Durante a resposta ao incidente, existiu uma falta de clareza na estrutura de liderança e na tomada de decisões, um descompasso significativo na comunicação entre as equipes técnicas e áreas comerciais, além de atrasos na comunicação com parceiros externos e entidades reguladoras importantes.

Conforme os fatos referenciados, é possível identificar falhas na arquitetura de segurança da informação da empresa, que levaram à ocorrência e severidade do incidente. Esses erros também mostraram a necessidade urgente de revisar as políticas e estratégias de defesa cibernética. Esse caso enfatizou a necessidade de uma estratégia de segurança constante, flexível e adaptável, voltada para a gestão de riscos e proteção de ativos digitais em situações críticas.

A ausência de MFA para acessos constitui uma falha grave no cumprimento das práticas recomendadas por normas como a ISO/IEC 27001, que exigem controles de acesso rigorosos e em múltiplas camadas. A prática da organização de usar apenas usuário e senha para acessos sensíveis é inadequada diante de ataques modernos, nos quais adversários obtêm credenciais por *phishing* ou vazamentos de dados.

Uma lição importante deste caso é a necessidade de ter uma visão completa e em tempo real do ambiente de segurança. A organização não dispunha de ferramentas para

acompanhar e avaliar atividades incomuns em *endpoints* e servidores. Soluções como EDR e XDR teriam permitido a identificação precoce de atividades suspeitas, como uso impróprio do *PowerShell*, movimentação lateral por meio do RDP e execução de comandos privilegiados (técnicas documentadas no *framework* MITRE ATT&CK).

Além das falhas técnicas apresentadas, o caso revelou deficiências na governança de TI e de segurança da informação, e na comunicação interna durante o incidente. A falta de uma liderança clara, com papéis definidos, descompasso entre equipes técnicas e áreas de negócio, e atraso na comunicação com parceiros e reguladores prejudicaram a resposta e a reputação institucional. Destaca-se que uma resposta eficaz deve ter um plano estruturado, testado, validado e atualizado regularmente.

As medidas estruturantes tomadas pela organização após o evento, a formação de um SOC interno para monitoramento e resposta, a revisão integral e criteriosa da política de acessos privilegiados e a implementação de soluções como o SOAR são ações positivas e que evidenciam um importante e necessário alinhamento com os princípios da resiliência cibernética. Essa perspectiva de resiliência, pelo que entendo, vai além da mera prevenção e detecção de ameaças, focando principalmente em garantir a continuidade das operações essenciais do negócio e a habilidade de recuperação dos serviços de maneira eficiente e oportuna, mesmo diante de falhas ou comprometimentos resultantes de um ataque cibernético em ambiente financeiro crítico.

3.3 Incidente LockBit 3.0 em ambiente financeiro crítico

No terceiro caso do estudo apresenta uma instituição financeira norte-americana, a qual oferece serviços com ênfase em custódia, liquidação e financiamento de operações com ativos de renda fixa, principalmente o Tesouro americano.

Como uma instituição de infraestrutura crítica, a empresa desempenha um papel estratégico na estabilidade do sistema financeiro, sendo intermediária entre instituições bancárias e regulatórias e seus investidores. Na data de 23 de novembro de 2023 foi vítima de um ataque severo de origem *ransomware*, o qual foi conduzido pelo grupo criminoso LockBit. A empresa teve suas operações de liquidação de ativos comprometidas pelo incidente, onde o ataque em questão causou a interrupção das operações normais da empresa, causando uma paralisação nas operações financeiras e exigindo medidas emergenciais por parte de instituições parceiras. A empresa trouxe o evento a público rapidamente, dadas suas implicações no ecossistema financeiro.

O grupo autor do incidente é conhecido por seu modelo de operações *ransomware-as-a-service* (RaaS), em que afiliados utilizam a infraestrutura fornecida pelo

grupo principal (LockBit) para a efetivação dos ataques, muitas vezes envolvendo extorsão dupla.

3.3.1 Vulnerabilidades exploradas e método de ataque

A investigação conduzida pela empresa, revelou que o ataque foi perpetrado utilizando uma variante específica do *ransomware* conhecida como LockBit 3.0. Este *malware* é amplamente reconhecido no cenário de cibersegurança global como um dos mais sofisticados e perigosos *ransomwares* em atividade até o presente momento (2025).

Os atacantes conseguiram acessar o ambiente da organização inicialmente explorando portas do protocolo de área de trabalho remota. Essas portas estavam abertas e expostas diretamente à internet pública, representando uma configuração de alto risco. Essas portas RDP, de forma crítica, não estavam protegidas por um firewall configurado adequadamente para filtrar e restringir acessos não autorizados, nem estavam localizadas em um segmento de rede isolado que pudesse limitar o impacto de uma possível exploração. Uma vez estabelecido o acesso facilitado a essas portas RDP expostas, os criminosos se beneficiaram do uso de credenciais de acesso válidas previamente obtidas.

O fator crítico que facilitou a exploração foi a constatação de que o ambiente comprometido não possuía a implementação de MFA para os acessos, especialmente aqueles realizados de forma remota ou que envolviam contas com privilégios administrativos. O objetivo dessas movimentações era identificar e alcançar ativos de maior valor estratégico dentro da organização e, fundamentalmente, obter acesso a credenciais com privilégios ainda mais elevados, como as de administrador de domínio. Posteriormente a ferramenta Cobalt Strike foi utilizada para estabelecer persistência no ambiente comprometido, garantindo o acesso contínuo dos atacantes, e para facilitar a gestão remota e o controle dos sistemas já infectados.

Em seguida, os invasores exfiltraram dados confidenciais usando comunicação criptografada para evitar detecção. Depois, criptografaram sistemas críticos com o ransomware LockBit 3.0, causando a paralisação completa das operações.

A exposição das portas RDP constituiu uma séria violação das práticas de segurança fundamentais recomendadas por especialistas e entidades internacionais. Isso gerou um vetor de ataque de alto risco e fácil exploração, demonstrando deficiências significativas na gestão da superfície de ataque externa da organização. A falta de MFA para acessos remotos e contas privilegiadas intensificou a vulnerabilidade, uma vez que esse mecanismo, sugerido

por normas e *frameworks* de segurança, teria dificultado o uso indevido de credenciais adquiridas por atacantes.

Diante das ameaças atuais, a dependência exclusiva de nome de usuário e senha é considerada obsoleta. Ademais, a habilidade dos invasores de se mover lateralmente na rede aponta para outras vulnerabilidades na segurança interna.

Como resultado, a exfiltração de dados confidenciais e a criptografia generalizada dos sistemas causaram a paralisação total das atividades da organização. Conclui-se, assim, que a organização falhou em proteger sua superfície de ataque externa, expôs portas RDP desnecessariamente, não implementou MFA em contas críticas, facilitando a exploração de credenciais comprometidas, e não adotou segmentação de rede e monitoramento interno que pudessem limitar a movimentação lateral dos atacantes.

A dependência de senhas simples também contraria as diretrizes básicas de segurança da informação. Esse incidente evidencia a necessidade de uma abordagem de segurança em camadas, que não apenas dificulte o acesso inicial, mas também limite o impacto de uma invasão e permita detectar e responder rapidamente a atividades maliciosas, reforçando a importância de revisar e aprimorar continuamente a segurança de forma holística.

3.3.2 Medidas de prevenção existentes: acertos e falhas

Durante o incidente, alguns controles de segurança positivos foram observados na organização em questão. A existência de uma segmentação de rede implementada entre suas várias unidades operacionais globais foi um dos principais controles observados. Uma unidade da empresa localizada no continente asiático ficou completamente imune ao ataque, evidenciando a eficácia dessa segmentação. Além disso, conseguiu manter suas operações normalmente durante todo o período crítico do incidente. Esse evento evidenciou a eficácia das práticas de contenção de incidentes e de separação de áreas organizacionais.

A manutenção de *backups* de segurança dos dados críticos foi outro ponto positivo. Além de estarem criptografadas, essas cópias eram guardadas em locais afastados da origem da ameaça e isoladas da rede principal. Como um benefício adicional significativo, essa estratégia de *backup* possibilitou a retomada parcial dos serviços essenciais após as etapas iniciais de contenção do ataque.

No entanto, em contraste com esses pontos positivos, foram identificadas falhas significativas e críticas na estratégia de prevenção de ameaças da organização. Destaca-se a ausência de MFA em sistemas críticos, além da falta de um processo formalizado e forte de gestão de vulnerabilidades. Essa deficiência ficou evidente com a presença de versões de

software desatualizadas e a ausência de atualizações de segurança importantes. Também foi identificada a ausência de um inventário completo, preciso e confiável dos ativos de informação, o que dificulta a identificação dos recursos que precisam ser protegidos.

A eficácia da segmentação de rede é claramente demonstrada pela resiliência da unidade asiática, que manteve suas operações ininterruptas durante o incidente. Isso evidencia a aplicação correta e cuidadosa das práticas de separação de áreas organizacionais e contenção de incidentes. Esta é uma demonstração prática de como uma arquitetura de rede bem projetada pode reduzir consideravelmente o alcance e as consequências de um comprometimento.

De maneira semelhante, a estratégia de manter *backups* criptografados e geograficamente dispersos, que possibilitou a recuperação parcial dos serviços, foi um benefício evidente, evidenciando um planejamento regular e uma execução eficaz nesse aspecto específico da segurança de dados e continuidade dos negócios. Contudo, os erros e omissões na prevenção foram cruciais e determinantes para o êxito da ofensiva cibernética. A ausência de MFA em sistemas de acesso à distância e em contas privilegiadas prejudicou um dos fundamentos mais importantes da segurança de acesso moderna.

A ausência de um processo sólido e contínuo de gestão de vulnerabilidades foi outro ponto crítico identificado. Um programa eficiente deve identificar, classificar, priorizar e corrigir vulnerabilidades de maneira contínua e proativa. O ataque expõe a falta de cuidado no processo de atualização e manutenção dos sistemas, que estavam utilizando versões de *software* desatualizadas e sem atualizações de segurança. De acordo com a norma ISO/IEC 27001, a presença de vulnerabilidades técnicas conhecidas e não gerenciadas constitui uma não conformidade em relação à necessidade de uma gestão sistemática de vulnerabilidades, o que compromete a capacidade de defesa da organização contra ataques que aproveitam falhas já identificadas.

Esse caso destaca a importância de uma estratégia de segurança cibernética equilibrada e abrangente. Não é suficiente implementar controles isolados, é fundamental investir na gestão de acessos, na gestão proativa de vulnerabilidades e em um inventário de ativos de informação que seja completo e atualizado, a fim de criar uma defesa robusta e capaz de se adaptar ao cenário atual de ameaças.

No entanto, em contraste com esses pontos positivos, foram identificadas falhas significativas e críticas na estratégia de prevenção de ameaças da organização. Destaca-se a ausência de MFA em sistemas críticos de acesso remoto e em contas administrativas, além da falta de um processo formalizado de gestão de vulnerabilidades. Essa deficiência ficou

evidente com a presença de versões de software desatualizadas e a ausência de atualizações de segurança importantes. Também foi identificada a ausência de um inventário completo, preciso e confiável dos ativos de informação, o que dificulta a identificação dos recursos que precisam ser protegidos.

3.3.3 Estratégia de detecção e resposta: eficiências e fragilidades

A detecção do comprometimento pela entidade foi possível em um estágio bastante avançado do ataque durante a investigação do incidente cibernético que afetou a organização. A identificação formal do incidente ocorreu apenas após a confirmação visual do comprometimento generalizado dos sistemas, seguida da apresentação da nota de resgate pelos *hackers* responsáveis pelo ataque. Essa sequência de detecção tardia é um indicativo claro de problemas.

É apresentado também a ausência de uma estrutura de supervisão de segurança que pudesse ser considerada robusta. Faltavam mecanismos baseados na análise e correlação eficaz de eventos de segurança provenientes de múltiplas fontes, bem como o uso sistemático e atualizado de indicadores de comprometimento (IOCs) para identificar atividades suspeitas de forma proativa.

Em relação à resposta da organização ao incidente, nota-se que a ação de resposta foi iniciada somente após a ocorrência do ataque e sua descoberta tardia. Essa resposta envolve ações como a contratação de empresas externas especializadas em forense digital para investigar a extensão e a origem da violação, e a recuperação de desastres para ajudar na restauração dos sistemas e dados impactados. Entretanto, um aspecto fundamental foi a falta de um plano formal, abrangente e detalhado para a gestão de incidentes de segurança.

Com as informações expostas, a estratégia de detecção de ameaças empregada pela entidade mostrou-se extremamente ineficaz e claramente insuficiente para o atual cenário. O fato de o incidente só ter sido detectado após a confirmação dos danos generalizados e apresentação da nota de resgate pelos criminosos evidência a ausência de um monitoramento de segurança constante, abrangente e proativo. Essa lacuna é particularmente grave no que diz respeito à falta de um sistema que integre notificações e alertas baseados na análise do comportamento de usuários e sistemas, sendo capaz de detectar desvios de padrões normais que possam sinalizar uma intrusão em seus estágios iniciais.

Essa situação crítica de detecção tardia evidencia a falta ou a configuração inadequada de ferramentas modernas e essenciais para a cibersegurança. Quando essas ferramentas são integradas e monitoradas por profissionais qualificados, é possível identificar, relacionar e

conter ameaças complexas de maneira proativa. Se essas ações tivessem sido identificadas e analisadas oportunamente, o ataque poderia ter sido contido antes da criptografia dos dados, diminuindo consideravelmente seu impacto.

Além disso, a falta de uma estrutura robusta de supervisão de segurança, capaz de analisar eventos e utilizar indicadores de comprometimento (IOCs) de forma proativa e automatizada, agravou a situação e prejudicou a resposta ao incidente.

Essas falhas iniciais afetaram negativamente todo o ciclo de resposta, estendendo o tempo de inatividade dos sistemas, elevando os custos e prejudicando a imagem da instituição. Este caso destaca a importância de investir tanto em tecnologias de detecção avançadas quanto em processos de resposta a desastres bem estabelecidos e maduros, com treinamento contínuo das equipes e definição clara de papéis e responsabilidades.

3.3.4 Impactos do incidente

Sob uma perspectiva estritamente operacional, o incidente causou a suspensão das vendas de ativos financeiros. Essa interrupção teve um impacto direto no funcionamento normal de um dos mercados financeiros mais sensíveis do mundo. A recuperação das operações habituais da organização após o incidente exigiu um esforço significativo e de várias facetas. Esse esforço incluiu a destinação de treinamentos e recursos específicos para a complexa recuperação de sistemas críticos comprometidos, a realização de uma análise forense minuciosa para compreender a extensão, a origem e a metodologia, a comunicação intrincada com diferentes partes interessadas e a colaboração imprescindível com as entidades reguladoras do setor. Todas essas medidas acarretam custos consideráveis para a organização, que podem ser categorizados como diretos e indiretos.

Além disso, o contexto geral do incidente indicou que não havia mecanismos eficazes para a detecção precoce do ataque. Também se tornou claro que não havia uma estratégia de resposta a desastres organizada e definida previamente, que pudesse ser acionada de maneira ágil e eficaz.

Os impactos resultantes deste incidente de segurança foram consideráveis e se manifestaram de forma contundente tanto no aspecto técnico-operacional quanto no estratégico-reputacional da organização. A interrupção das vendas de títulos do Tesouro americano é um exemplo claro e alarmante da gravidade operacional que um ciberataque pode alcançar. Este tipo de indisponibilidade, mesmo que temporária, tem o potencial de prejudicar o fluxo monetário global, desestabilizar a liquidez e provocar instabilidades momentâneas,

porém significativas, nos mercados secundários, afetando a confiança dos investidores e a precificação de ativos em escala.

O incidente expôs falhas importantes e preocupantes na estrutura de governança corporativa, nos processos de administração de riscos e nos planos de manutenção e continuidade dos negócios da organização afetada. A ausência de uma capacidade de detecção antecipada eficaz e a falta de uma estratégia de resposta a desastres devidamente organizada, documentada e, crucialmente, testada, indicaram que a organização possivelmente subestimava a criticidade da segurança cibernética ou não havia implementado adequadamente os controles preventivos e reativos necessários para enfrentar ameaças dessa sofisticação. A complexidade e o custo elevado do processo de recuperação apenas reforçam a importância crítica de um preparo prévio robusto, que inclua simulações de crise e planos de resposta bem definidos.

Igualmente, o impacto na reputação da entidade foi evidente e particularmente danoso, dadas as características do setor em que atua. No setor financeiro, onde a confiança e a credibilidade são ativos intangíveis, porém absolutamente essenciais e de difícil e demorada reconstrução uma vez abalados, a percepção de fragilidade na segurança da informação ou na capacidade de gestão de crises pode ter consequências severas e duradouras.

Este caso é um estudo valioso sobre a interconexão intrínseca entre segurança cibernética, resiliência operacional, governança de riscos e a sustentabilidade da confiança no ecossistema financeiro. Demonstra que a negligência ou a subestimação dos riscos cibernéticos pode levar a consequências que vão muito além das perdas financeiras imediatas, comprometendo a estabilidade de mercados e a reputação construída ao longo de anos.

3.3.5 Lições aprendidas do caso

O episódio em questão proporcionou ensinamentos essenciais que transcendem a organização diretamente afetada, oferecendo aprendizados valiosos que reverberam por todo o setor financeiro e por outras organizações que administram infraestruturas críticas. Destaca-se a importância premente da compreensão, adoção e aplicação efetiva do modelo de arquitetura *Zero Trust*. Essa metodologia de segurança parte do princípio de que nenhum usuário, dispositivo ou aplicação deve ser automaticamente considerado confiável, independentemente de sua localização, sendo, portanto, um pilar indispensável para a construção de uma segurança moderna e robusta. Sua aplicação prática exige a implementação rigorosa e granular de controles de acesso baseados em contexto (incluindo fatores como identidade do usuário, tipo de dispositivo, localização, sensibilidade do recurso acessado e o momento do

acesso), à exigência de autenticação contínua e adaptativa, e a verificação dinâmica e periódica da integridade e da postura de segurança dos dispositivos e sistemas que interagem com os dados e aplicações da organização.

Ademais, é fundamental que as empresas invistam em ferramentas de monitoramento de segurança e resposta que sejam atuais, integradas e que possam oferecer uma visão detalhada do ambiente. Quando adequadamente implementadas e integradas às plataformas de SIEM e soluções de SOAR, soluções como EDR e NDR podem coletar e correlacionar eventos de diversas fontes, identificar comportamentos anômalos que sinalizem uma intrusão em curso e gerar alertas acionáveis, enriquecidos com contexto, para as equipes de segurança.

Em conclusão, é fundamental criar, manter e, principalmente, revisar regularmente um plano de resposta a desastres e um plano de continuidade de negócios. Esses planos são essenciais para direcionar as ações da organização durante e após uma crise, garantindo a resiliência operacional e minimizando danos. Para que esses planos sejam verdadeiramente eficazes e não apenas documentos formais, é preciso conduzir simulações e exercícios práticos regularmente, considerando diversos cenários de crise cibernética. Essa capacitação ajuda consideravelmente a diminuir o tempo de resposta, reduzir perdas financeiras e operacionais, além de preservar a reputação e a confiança na instituição.

4. CONCLUSÃO

A partir da análise dos três casos estudados conclui-se que existe uma predominância do erro do fator humano e da exploração de falhas básicas de configuração como portas de entrada para os ataques. Um vetor predominante nos casos foi a falta de MFA, demonstrando que a negligência de controles de acesso robustos continua sendo um elo fraco na segurança organizacional e um ponto muito bem explorado pelos atacantes.

No estudo do caso 1, a senha exposta sem proteção extra foi o ponto de partida. No caso 2, a empresa de tecnologia em saúde, o ataque começou com credenciais privilegiadas obtidas através de ataques de *phishing*. Em contrapartida, no caso 3, o acesso foi simplificado através de portas RDP abertas e o uso de credenciais autênticas. Ademais, dois dos três ataques envolvem movimentos laterais utilizando ferramentas como o Cobalt Strike, evidenciando a elevada competência técnica dos atacantes. Além desses aspectos, observa-se que em dois dos três casos no roubo de dados utilizando-se criptografia, atividade essa conhecida como extorsão dupla.

Ao analisar os casos discutidos, nota-se padrões constantes de falhas e vulnerabilidades em cada organização, onde cada detalhe foi crucial para a ocorrência e efetividade dos ataques. Tais aspectos foram expostos à luz das normas, diretrizes e práticas recomendadas já esclarecidas neste estudo.

Dentro do primeiro caso que foi abordado que é possível concluir que as principais falhas de segurança foram a inexistência de um meio de multi autenticação em acessos remotos e a utilização de autenticação a partir de credenciais simples (usuário e senha), comprometendo assim o controle de acesso e deixando facilitado a utilização de credenciais válidas ou reutilizadas. Esse tipo de risco vai contra as recomendações estipuladas pelo NIST SP 800-63B, principalmente no que diz respeito a ativos críticos. Foi identificado também uma omissão perante controles de gestão de credenciais de autenticação, os quais são previstos dentro da ISO 27001.

Com o decorrer da movimentação do atacante, é nítido que existia uma ausência de segregação eficaz entre os ambientes de TI e OT, descumprindo um dos controles da ISO/IEC 27001, que trata da importância de restringir o fluxo de tráfego entre redes. A utilização de redes sem esse tipo de controle permitiu que o incidente se expandisse. A implementação de segregação lógica com *firewalls* internos, micro segmentação baseada em identidade ou uma arquitetura *Zero Trust* teria auxiliado para que o raio de ataque fosse reduzido, e traria um gerenciamento de riscos mais fácil e em tempo real.

Outro aspecto crítico identificado foi a ação realizada pela equipe de segurança da vítima, que desconectou abruptamente a rede OT para conter o ataque. No entanto, isso causou uma interrupção ampla das operações. A falta de um plano estruturado de resposta ao incidente, conforme estabelecido nos requisitos da NIST SP 800-61 Rev.3, resulta na implementação de uma ação drástica e totalmente desorganizada. A presença de um plano que inclua uma avaliação de impacto e segmentação de ativos permitiria uma decisão seletiva e a manutenção parcial dos serviços essenciais, reduzindo dessa forma o efeito dominó no setor.

No segundo caso, uma companhia da área de tecnologia da saúde revelou sérias vulnerabilidades nos mecanismos de detecção e proteção. Uma das primeiras dificuldades identificadas é a falta de uma solução de detecção e reação, como SIEM ou EDR, que permite um acompanhamento constante e reconhecimento de comportamentos anormais no ambiente. Esta falta leva à perda do controle sobre os registros de eventos de segurança da informação, além de exigir um sistema para a geração de relatórios de incidentes de segurança. Ademais, afeta os pontos de detecção e reação propostos pelo NIST. Neste contexto, a integração das plataformas de prevenção e a automação de respostas seriam imprescindíveis, como podemos observar dentro de um XDR.

Ao deixar *backups* conectados à rede comprometida, tornando esse ponto crítico e permitiu que os mesmos fossem criptografados igualmente pelos atacantes. Essa falha vai contra as boas práticas de isolamento lógico e físico de *backups* de segurança com proteção contra modificações ou exclusões intencionais ou acidentais. Também neste cenário, a melhor estratégia seria implementar *backups*, armazenados em locais isolados, com testes regulares de restauração como parte do plano de continuidade de negócios.

Se constatou também a ausência de controle sobre acessos privilegiados, possibilitando que os invasores ascendessem rapidamente aos privilégios. A falta de um sistema de PAM (Gerenciamento de Acesso Privilegiado) e a não implementação do princípio do menor privilégio configuram infrações ao controle da ISO/IEC 27001, bem como às orientações do NIST SP 800-53. A solução perfeita implicaria na implementação de acesso *just-in-time*, com autenticação forte, monitoramento constante e expiração automática de permissões elevadas.

Em última análise, a resposta foi desorganizada e fundamentada em medidas emergenciais, demonstrando a falta de treinamentos e simulações de incidentes anteriores (simulação), prejudicando a comunicação e o processo de tomada de decisões durante o ataque. De acordo com as diretrizes do NIST SP 800-84 e da ISO 22301, é crucial que os planos de resposta sejam constantemente testados e que todos os interessados estejam

capacitados para trabalhar em conjunto e sob pressão psicológica. Esta abordagem tem sido consistentemente reforçada nas publicações mais recentes do setor de segurança da informação e continuidade de negócios.

Para a instituição financeira, caso 3, impactada pelo grupo LockBit 3.0, as principais falhas técnicas estão relacionadas a falhas estruturais na administração de riscos e na estrutura de segurança. O comprometimento começou com a exposição direta do protocolo RDP à Internet, sem a necessidade de VPN, autenticação multifator ou limitações de IP. Esta configuração vai de encontro à ISO/IEC 27001 e ao CIS Control, que condenam a utilização de serviços administrativos expostos ao público. Sugere-se o uso de *gateways* seguros, com *Zero Trust Network Access* (ZTNA), *hosts* base e MFA como requisitos para qualquer acesso à distância, além de bloqueios baseados em geolocalização e análise de comportamento.

A falta de um sistema de SIEM e EDR impediu a identificação antecipada do ataque, prejudicando gravemente os procedimentos de prevenção. Apenas após a criptografia total dos sistemas e o recebimento da nota de resgate, o incidente foi identificado, configurando uma falha nos domínios *Detect* e *Identify* do NIST CSF. A utilização de telemetria comportamental e detecção heurística, juntamente com a inteligência de ameaças, teria facilitado a detecção do comportamento atípico.

Além disso, a instituição não possuía um plano de continuidade de negócios devidamente testado e integrado ao plano de resposta a desastres, resultando na interrupção das operações de liquidação de ativos, impactando diversas partes no mercado financeiro. A ISO 22301 e a ISO/IEC 27031 estabelecem a exigência de elaborar planos de continuidade a partir de análise de risco e análise de impacto e de envolver partes interessadas externas nos testes. A implementação dessas diretrizes teria possibilitado o funcionamento parcial de serviços vitais, mesmo em situação de ataque, com um sistema mudando automaticamente para outro como contingência.

Outro ponto negligenciado foi a auditoria contínua de vulnerabilidades e análise de riscos cibernéticos. A não identificação de falhas básicas, como serviços abertos sem controle de acesso, revela o não cumprimento dos controles de gestão de riscos de segurança da informação e gestão de vulnerabilidades técnicas da ISO/IEC 27001. A implementação de um programa de gestão de vulnerabilidades baseado em risco, com varreduras periódicas, análises de configuração e testes de intrusão, teria mitigado as condições que favoreceram o ataque.

Finalmente, na instituição financeira, a confidencialidade foi violada pelo vazamento de informações financeiras e senhas, usado como parte da tática de extorsão do grupo *LockBit*. A exposição ocorreu devido à falta de DLPs (Prevenção de Perda de Dados) e de

mecanismos de monitoramento de dados delicados. A integridade foi seriamente comprometida, tanto no nível de dados quanto no de sistemas, com alterações nos registros de transações e deterioração de serviços vitais. A ausência de registros confiáveis e a ausência de trilhas de auditoria verificáveis complicaram a avaliação do alcance do dano, violando os princípios do controle de identificação de eventos. No que diz respeito à disponibilidade, as consequências foram significativas: a instituição precisou interromper operações de custódia e liquidação, impactando negativamente o mercado financeiro. A reação foi restrita e reativa, resultando em contenção tardia e comunicação ineficaz com os interessados. A entidade não empregava a arquitetura *Zero Trust*, não empregava a vigilância constante de eventos nem possuía uma segmentação lógica sólida.

A solução ideal demandaria a aplicação de uma estratégia proativa de detecção e reação, combinada com um plano de continuidade operacional apto a isolar domínios impactados e transferir serviços vitais para locais seguros temporários.

Trazendo para a perspectiva da tríade de segurança da informação, isso nos possibilita uma análise correta dos efeitos nos ativos de informação, da efetividade das medidas de proteção implementadas e da maturidade operacional das entidades impactadas. Ao analisar cada componente da tríade, podemos reconhecer padrões constantes de erros e brechas nos processos de contenção, erradicação e recuperação, além de sugerir orientações corretivas em conformidade com os *frameworks* de renome internacional.

No caso da empresa de oleoduto, houve um impacto indireto na confidencialidade. Apesar dos invasores terem inicialmente afirmado que não vazaram dados, existem evidências de que informações operacionais e credenciais foram expostas. A falta de criptografia de dados confidenciais em repouso e a falta de controles de acesso rigorosos contribuíram para essa situação. A segurança dos sistemas não foi diretamente comprometida, já que o *ransomware* não chegou a impactar os sistemas de OT. Contudo, a integridade operacional foi comprometida pela decisão da equipe de segurança de interromper as operações bruscamente, sem confirmação técnica de contaminação nos ambientes industriais, o que sugere uma falha na coordenação fundamentada em provas. No que diz respeito à disponibilidade, o efeito foi severo, a interrupção das atividades afetou o fornecimento de combustível em grande parte da costa leste dos Estados Unidos. A reação impulsiva tomada destacou a ausência de um plano de continuidade de negócios e de um plano de resposta a desastres validado. Uma estratégia que utilizasse segregação de redes, avaliação de impacto e contenção seletiva teria mantido, mesmo que de forma parcial, a operação de sistemas vitais.

No incidente contra a companhia de tecnologia em saúde, a confidencialidade foi seriamente afetada. Antes da criptografia, dados confidenciais de pacientes e documentos médicos foram vazados, evidenciando que o *ransomware* atuou em um esquema de dupla extorsão. Esta falha indica a falta de uma criptografia eficiente para dados em repouso e em movimento, além de políticas de controle de acesso ineficientes. A integridade dos sistemas foi comprometida devido à modificação ou criptografia de arquivos e bases de dados, sem a possibilidade de verificação ou reversão imediata. A falta de mecanismos de garantia de integridade, tais como *hashes* e cópias de segurança inalteráveis, piorou a situação. A disponibilidade foi significativamente comprometida: sistemas de prontuário eletrônico, agendas de atendimento e processos hospitalares foram suspensos. A reação do time de segurança demonstrou falta de preparo e coordenação, ao tentar reativar cópias de segurança que também estavam encriptadas. A prática ideal seria o uso de *backups* protegidos por segregação lógica, cópias inalteráveis e testes de restauração regulares, conforme estabelecido pelas normas ISO/IEC 27031 e CIS Control.

A partir do que foi exposto, observa-se que as três empresas não possuem planos de resposta a desastres documentados e adequados para suas atividades, um ponto crítico que as deixou vulneráveis e expôs as falhas em seguir as melhores práticas e diretrizes de segurança. A ausência de um PRI eficaz resultou em reações desorganizadas aos ataques, exacerbando os impactos causados por vulnerabilidades básicas, como a falta de autenticação multifator (MFA), segregação de rede deficiente e gestão inadequada de acessos privilegiados. É fundamental que as organizações compreendam que a segurança cibernética exige um planejamento estratégico proativo, investindo não só em tecnologia, mas também na criação, documentação e testes regulares de planos de resposta a desastres, além do treinamento contínuo de suas equipes, para garantir a resiliência e a proteção de seus ativos em um cenário de ameaças cada vez mais complexo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS *apud* TARGET NORMAS. **NBR ISO/IEC 27001:2022/Em 1:2024: Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos**. São Paulo: Target Normas, 2024. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/abnt-nbriso-iec27001-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-sistemas-de-gestao-da-seguranca-da-informacao-requisitos. Acesso em: 05 de maio de 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS *apud* TARGET NORMAS. **NBR ISO/IEC 27002:2022: Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação**. São Paulo: Target Normas, 2022. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/21529/abnt-nbriso-iec27002-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-controles-de-seguranca-da-informacao. Acesso em: 05 de maio de 2025

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS *apud* TARGET NORMAS. **NBR ISO/IEC 27031:2023: Tecnologia da informação — Técnicas de segurança — Diretrizes para a prontidão para a continuidade de negócios da tecnologia da informação e comunicação.** São Paulo: Target Normas, 2023. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/34728/abnt-nbriso-iec27031-tecnologia-da-informacao-tecnicas-de-seguranca-diretrizes-para-a-prontidao-para-a-continuidade-de-negocios-da-tecnologia-da-informacao-e-comunicacao. Acesso em: 06 de maio de 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS *apud* TARGET NORMAS. **NBR ISO/IEC 27035-1:2023: Tecnologia da informação - Gestão de incidentes de segurança da informação - Parte 1:** Princípios e processos. São Paulo: Target Normas, 2023. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/13740/abnt-nbriso-iec27035-1-tecnologia-da-informacao-gestao-de-incidentes-de-seguranca-da-informacao-parte-1-principios-e-processo. Acesso em:02 de abril de 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS *apud* TARGET NORMAS. **NBR ISO/IEC 27035-2:2023: Tecnologia da informação - Gestão de incidentes de segurança da informação - Parte 2:** Diretrizes para planejar e preparar a resposta a incidentes. São Paulo: Target Normas, 2023. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/13741/abnt-nbriso-iec27035-2-tecnologia-da-informacao-gestao-de-incidentes-de-seguranca-da-informacao-parte-2-diretrizes-para-planejar-e-preparar-a-resposta-a-incidentes. Acesso em: 02 de abril de 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS *apud* TARGET NORMAS. **NBR ISO/IEC 27035-3:2021: Tecnologia da informação - Gestão de incidentes de segurança da informação - Parte 3:** Diretrizes para operações de resposta a incidentes de TIC. São Paulo: Target Normas, 2021. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/13148/abnt-nbriso-iec27035-3-tecnologia-da-informacao-gestao-de-incidentes-de-seguranca-da-informacao-parte-3-diretrizes-para-operacoes-de-resposta-a-incidentes-de-tic. Acesso em: 02 de abril de 2025

BRASIL. **Estratégia nacional de cibersegurança**. Brasília, DF: Gabinete e Segurança Institucional da Presidência da República, 2024. Disponível em: https://www.gov.br/gsi. Acesso em: 26 mar. 2025.

CERT.BR. **Cartilha de segurança para Internet:** dicas rápidas. São Paulo: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2023. Disponível em: https://cartilha.cert.br/dicas-rapidas/. Acesso em: 26 de maio de 2025.

CERT.BR. **Cartilha de segurança para Internet:** proteção de dados. São Paulo: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2022. Disponível em: https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf. Acesso em:26 de maio de 2025.

CISCO. **Cybersecurity threat trends report 2024**. San Jose: Cisco Systems, Inc., 2024. Disponível em: https://www.cisco.com. Acesso em: 04 de abril de 2025.

CHECK POINT RESEARCH. **Relatório de segurança cibernética 2024:** Aumento de ransomware, evolução das táticas de guerra cibernética e uso estratégico de IA na defesa. Tel Aviv: Check Point Software Technologies, 2024. Disponível em: https://research.checkpoint.com/2024/2024s-cyber-battleground-unveiled-escalating-ransomw are-epidemic-the-evolution-of-cyber-warfare-tactics-and-strategic-use-of-ai-in-defense-insigh t s-from-check-points-latest-security-re/. Acesso em: 4 de janeiro de 2025.

CLOUDFLARE. **O que é uma violação de dados?** San Francisco: Cloudflare, Inc., 2024. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/glossary/data-breach/. Acesso em: 4 de maio de 2025.

DEPARTMENT OF HEALTH & HUMAN SERVICES. **Health Information Privacy: HIPAA for Professionals**. Washington, DC: HHS.gov, 2023. Disponível em: https://www.hhs.gov/hipaa/for-professionals/index.html. Acesso em: 4 de maio de 2025.

DOC MANAGEMENT. **Brasil é principal alvo de onda de ataques de ransomware contra a América Latina, afirma ISH Tecnologia**. DocManagement, 6 de julho de 2024. Disponível em: https://docmanagement.com.br/06/07/2024/brasil-e-principal-alvo-de-onda-de-ataques-de-ra n somware-contra-a-america-latina-afirma-ish-tecnologia. Acesso em: 4 de maio de 2025.

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. **Política nacional de segurança da informação**. Brasília, DF: GSI, 2024. Disponível em: https://www.gov.br/gsi. Acesso em: 26 de março de 2025.

IBM SECURITY. **Cost of a data breach report 2024**. Armonk: IBM, 2024. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 01 de abril de. 2025.

KOSINSKI, Renato. **Violação de dados:** o que é, quais os tipos e como evitá-la. IBM Brasil, 2024. Disponível em: https://www.ibm.com/blogs/ibm-brasil/violacao-de-dados-o-que-e-quais-os-tipos-e-como-evi t a-la. Acesso em: 24 de janeiro de 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Cybersecurity framework 2.0**. Gaithersburg: NIST, 2024. Disponível em:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: 26 de março de 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Digital Identity Guidelines – Authentication and Lifecycle Management (SP 800-63B)**. Gaithersburg: NIST, 2020. Disponível em: https://pages.nist.gov/800-63-3/sp800-63b.html. Acesso em: 14 de janeiro de 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-61 Revision 3:** Computer security incident handling guide. Gaithersburg: NIST, 2023. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf. Acesso em: 06 de novembro de 2024.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Guia de Boas Práticas para Segurança Cibernética**. São Paulo: NIC.br, 2023. Disponível em: https://www.nic.br/publicacoes. Acesso em: 4 de dezembro de 2024.

MICROSOFT. **O que é uma violação de dados?** Redmond: Microsoft Corporation, 2024. Disponível em: https://www.microsoft.com/security/blog/what-is-a-data-breach/. Acesso em: 4 maio 2025.

PALO ALTO NETWORKS. **Unit 42 ransomware threat report 2024**. Santa Clara: Palo Alto Networks, 2024. Disponível em: https://unit42.paloaltonetworks.com/2024-ransomware-threat-report/. Acesso em: 7 de novembro de 2024.

SYMANTEC. **Relatório de ameaças cibernéticas 2024**. Mountain View: Broadcom Inc., 2024. Disponível em: https://www.broadcom.com/company/newsroom/press-releases?filtr=cybersecurity. Acesso em: 26 de março de 2025.

VERIZON. **Data Breach Investigations Report 2023**. New York: Verizon Communications, 2023. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 02 de abril de 2025.

FORTINET. **O que é a estrutura MITRE ATT&CK ?.** Sunnyvale, California: Fortinet, 2023. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/mitre-attck#:~:text=Defini%C3%A7% C 3%A3o%20MITRE%20ATT&CK,uma%20organiza%C3%A7%C3%A3o%20e%20classifi c a r%20ataques. Acesso em: 10 de junho de 2025.

APÊNDICE A

PLANO DE RESPOSTA A DESASTRES DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. Objetivo

O objetivo principal deste Plano de Resposta a Desastres de Segurança da Informação é definir uma estratégia sistemática e estruturada para a gestão de quaisquer incidentes que possam colocar em risco a segurança dos ativos de informação da AXTI. Este plano tem como objetivo facilitar a identificação rápida de ameaças, seguida de uma análise eficiente e uma reação eficaz, com o objetivo principal de reduzir qualquer efeito negativo nas operações empresariais, nas finanças, na situação jurídica e na imagem da empresa. Adicionalmente, busca assegurar a pronta recuperação dos serviços e sistemas que possam ser afetados, garantindo a manutenção das operações essenciais. Um aspecto crucial é a coleta de evidências de maneira forense, essencial para apoiar investigações internas e possíveis litígios jurídicos. É igualmente crucial aprender com cada incidente, aplicando as lições obtidas para melhorar continuamente os controles de segurança em vigor e o plano de resposta em si. Por fim, este documento reafirma o compromisso da AXTI em assegurar a aderência a todas as exigências legais, regulamentares e contratuais relevantes, tais como a LGPD, GDPR e os períodos máximos toleráveis de interrupção (MTPD's) firmados com os clientes.

2. Aplicabilidade desse plano

Este plano de resposta a desastres tem um alcance amplo dentro da empresa aqui denominada como AXTI, a fim de preservação de imagem. As suas orientações e processos se aplicam a todos que interagem com os recursos da empresa, incluindo funcionários efetivos, fornecedores, consultores externos e todos os demais que, no desempenho de suas funções, manuseiam ou acessam aos ativos de informação e sistemas de propriedade ou gestão da AXTI. O plano também é aplicável a todos os ativos de informação da organização, sejam eles digitalizados ou não (físicos). Isso inclui, mas não se restringe a infraestrutura de tecnologia da informação, dados de clientes, informações corporativas sigilosas, propriedade intelectual e sistemas empregados no processo de criação de *software*. Adicionalmente, abrange todos os incidentes de segurança da informação que afetem a confidencialidade, integridade ou disponibilidade dos dados e sistemas da empresa, independentemente de sua natureza ou origem, incluindo, mas não se limitando a:

- Sistemas de desenvolvimento e produção de *software*.
- Infraestrutura de TI local e em nuvem.
- Dados de clientes e dados corporativos.
- Propriedade intelectual e código-fonte.
- Dispositivos de usuários finais (*endpoints*).
- Redes de comunicação.

3. Controle de documento

Este documento é revisado todos os anos pela área de propriedade, com a colaboração da área de conformidade. A última revisão com modificações foi executada conforme as datas indicadas na tabela a seguir:

Versão	Data	Descrição	Autor
1.0	Abril/2025	Criação inicial do Plano de Resposta a desastres	@yara.veneri
2.0	Maio/2025	Ajustes e atualizações em conformidade as ISOs 27001:2024, 27002:2022, 27005:2022, 27035:2023	@yara.veneri

4. Gestão de incidentes

4.1. Classificação de Incidentes

Os incidentes com base em seu impacto potencial e real nos negócios, nos pilares de segurança da informação e nos requisitos legais e regulatórios. A orientação de priorização da resposta e o procedimento de escalonamento será efetuado com base na mesma classificação, como crítico, alto, médio ou baixo.

Crítico: Categoria de incidente de segurança que levou às seguintes falhas:

- Interrupção total das operações de desenvolvimento chave ou da entrega de *software* aos clientes;
- Vazamento em larga escala de código-fonte crítico, dados de clientes de produção, ou chaves de criptografia mestras.
- Violação regulatória grave com alta probabilidade de multas significativas;
- Perda financeira substancial;
- Dano reputacional extremo e perda de confiança de clientes e investidores;
- Mobilização total e imediata do time de resposta a incidentes, onde devem ser solucionados com um MTPD de 4 horas.

Alto: Categoria de incidente de segurança que levou às seguintes falhas:

- Impacto severo em funções críticas de desenvolvimento, entrega de projetos importantes ou suporte ao cliente;
- Possível violação regulatória;
- Perda financeira significativa;
- Dano reputacional considerável;
- Mobilização e resposta urgente do time de resposta a incidentes, onde deve ser solucionado dentro de um MTPD de 6 horas.

Médio: Categoria de incidente de segurança que levou às seguintes falhas:

- Impacto moderado em algumas funcionalidades de desenvolvimento ou entrega;
- Perda de dados não críticos ou internos;
- Pequeno risco de não conformidade ou dano reputacional.;
- Mobilização e resposta em tempo hábil, onde deve ser solucionado dentro de um MTPD de 36 horas.

Baixo: Categoria de incidente de segurança que levou às seguintes falhas:

- Impacto mínimo ou localizado, sem interrupção significativa dos fluxos de trabalho;
- Nenhum dado sensível ou de cliente envolvido;
- Consequências financeiras ou reputacionais desprezíveis;
- Pode ser tratado através de procedimentos operacionais padrão, mas é necessário realização de registro e monitoramento contínuo.
- MTPD de baixo risco, podendo ser resolvidos em 72 horas.

A classificação inicial pode ser modificada à medida que a partir dos eventos apresentados, a análise de impacto é alterada. O líder da equipe de resposta a incidentes (líder da equipe de segurança da informação) deve ser responsável por realizar a confirmação ou ajustar a classificação do incidente.

4.2 Notificação a órgãos reguladores e partes interessadas chave

Levando em conta o alcance mundial da AXTI e sua condição de empresa de capital aberto, esta seção explica os processos de notificação para entidades reguladoras e outros *stakeholders* relevantes, como a *Exchange Commission* (SEC) nos Estados Unidos conforme aplicável.

- Análise da Requisição de Notificação Regulatória:
  - Em colaboração com a alta administração e a equipe de resposta a incidentes, o departamento jurídico e de compliance determinará se um incidente de segurança da informação (especialmente aqueles categorizados como críticos ou altos, ou que envolvam violação de dados pessoais) requer a notificação aos órgãos reguladores. De acordo com as normas da SEC, os incidentes de cibersegurança devem ser notificados em até quatro dias úteis após a confirmação de sua materialidade. A avaliação da materialidade levará em conta o efeito nos negócios, financeiro, operacional e na reputação.
  - Outras entidades de proteção de dados: As notificações por violações de dados pessoais serão feitas de acordo com os prazos e critérios definidos por essas normas.

- Processo de notificação:
    1. A Equipe de Segurança da Informação notificará imediatamente o Departamento Jurídico e de Compliance sobre qualquer incidente classificado como alto ou crítico, bem como qualquer incidente que possa levar a uma possível violação de informações pessoais.
    2. Juntamente com o Departamento Jurídico e de Compliance, a Equipe de Segurança da Informação analisará a relevância e a exigência de comunicar aos reguladores financeiros e/ou autoridades de proteção de dados. Se for crucial a notificação, o Departamento Jurídico irá preparar e enviar a comunicação oficial, de acordo com as demandas específicas da entidade reguladora.
    3. A equipe de Relações com Investidores e Comunicação Corporativa será responsável pela coordenação da comunicação com investidores e o mercado, sob a supervisão do Departamento Jurídico e da Alta Direção.

4.3 Registro e notificação de incidentes

Os eventos de incidentes de segurança da informação que forem reportados ou detectados terão de ser registrados por meio de *tickets* dentro do Jira da AXTI. Eles podem ser registrados por qualquer colaborador. Os incidentes de segurança da informação incluem, mas não limita, os seguintes eventos:

- Compartilhamento de senha;
- Falha de *login*;
- Conta de usuário habilitada e desbloqueada;
- Ataque Pass The Hash;
- IOCs de comunicação suspeitos;
- Ataques de *Cross-Site-Scripting*;
- Uso indevido do PsExec.

O registro inicial deve conter:

- ID único do incidente;
- Data e hora da detecção e do registro;
- Fonte de *report* (usuário, ferramenta, etc.);
- Classificação inicial de severidade e atualizada;
- Descrição detalhada do incidente (o que, quando, como, onde);
- Sistemas, que estavam sendo manipulados;

- Tipos de dados que estavam sendo manipulados;
- Ações de resposta tomadas e *status*
- Analistas de segurança da informação designados para o caso.
- Impacto avaliado

4.4 Tratamento de incidentes de segurança

O tratamento do incidente deverá seguir as melhores práticas do ciclo de gestão de incidentes de segurança da informação, seguindo as cinco fases que compõem tal ciclo. Depois de detectar o incidente, a equipe de Segurança da Informação examina os registros de eventos e, caso seja necessário, a equipe se comunica com a equipe de infraestrutura e/ou com o empregado.

4.5 Coleta de evidência

O recolhimento e o tratamento de evidências precisam obedecer a processos que assegurem sua integridade, autenticidade, confiabilidade e completude.

- **Pessoa Autorizada**: Apenas integrantes da equipe de Segurança da Informação ou peritos forenses designados têm permissão para recolher e manipular provas.
- **Documentos (Cadeia de Custódia)**: Registrar todas as ações: quem executou, o que executou, quando, onde e como ocorreu qualquer alteração na custódia. É sugerido o uso de formulários de cadeia de custódia.
- **Prioridade de Volatilidade:** Recolher informações da memória RAM, caches e estado da rede antes de gravar dados nos discos rígidos.
- **Tipos de Provas:** Registros (sistema, aplicativo, rede, segurança), backups de memória, imagens de disco, arquivos duvidosos, registros de tráfego, ajustes de sistema e entrevistas.
- **Legalidade e Privacidade:** Assegurar que a coleta respeite as leis de privacidade (LGPD, GDPR e SEC) e os direitos dos indivíduos. Consultar o Departamento Jurídico quando necessário.

4.6 Lições aprendidas

Depois de solucionar cada incidente relevante (especialmente o crítico ou alto), a equipe de segurança da informação realizará uma avaliação pós-incidente.

- Analisar a resposta e o incidente cronologicamente;

- Determinar a causa raiz essencial;
- Analisar a efetividade das medidas de segurança e dos processos de reação;
- Reconhecer os aspectos positivos e negativos na resposta;
- Verificar se as medidas implementadas foram adequadas e eficazes;
- Sugerir medidas corretivas e preventivas para prevenir recaídas e potencializar a resiliência;
- Detectar a necessidade de atualização deste plano, dos playbooks, dos treinamentos ou dos instrumentos.

4.7 Comunicação em caso de incidente

No caso de incidentes, cabe à equipe de Segurança da Informação comunicar incidentes que possam afetar os clientes, num prazo de até 24 horas. É essencial formalizar incidentes através de sistemas de tickets para registro e auditorias futuras. Conforme a extensão e a gravidade do incidente, outras partes devem ser envolvidas. informadas, que incluem:

- Policiais (FBI, Polícia Federal, etc.);
- ANPD (se informações pessoais ou confidenciais de cidadãos brasileiros forem expostas);
- Agências europeias (GDPR) - caso haja impacto em dados PII europeus;
- Proprietários dos dados, quando apropriado;
- Outras entidades encarregadas de outras leis de proteção de dados ao redor do mundo.
- Globalmente, com base nos dados de cidadãos de outras nações impactadas;
- SEC (Comissão de Valores Mobiliários);
- Grupo de Contato com Investidores;
- Administração Superior da Empresa;
- Imprensa Internacional - com a assistência da equipe de comunicação.

4.8 Processo de Tratamento de Incidentes

3.8.1 Alertas de Incidentes de Segurança da Informação

A seguir, apresenta-se uma visão geral das ferramentas e serviços de segurança empregados na AXTI, detalhando seus respectivos escopos de atuação e os tipos de alertas gerados.

Procedimento Padrão de Escalonamento de Alertas

Para todos os as detecções das ferramentas mencionadas a seguir, o fluxo de escalonamento é o seguinte:

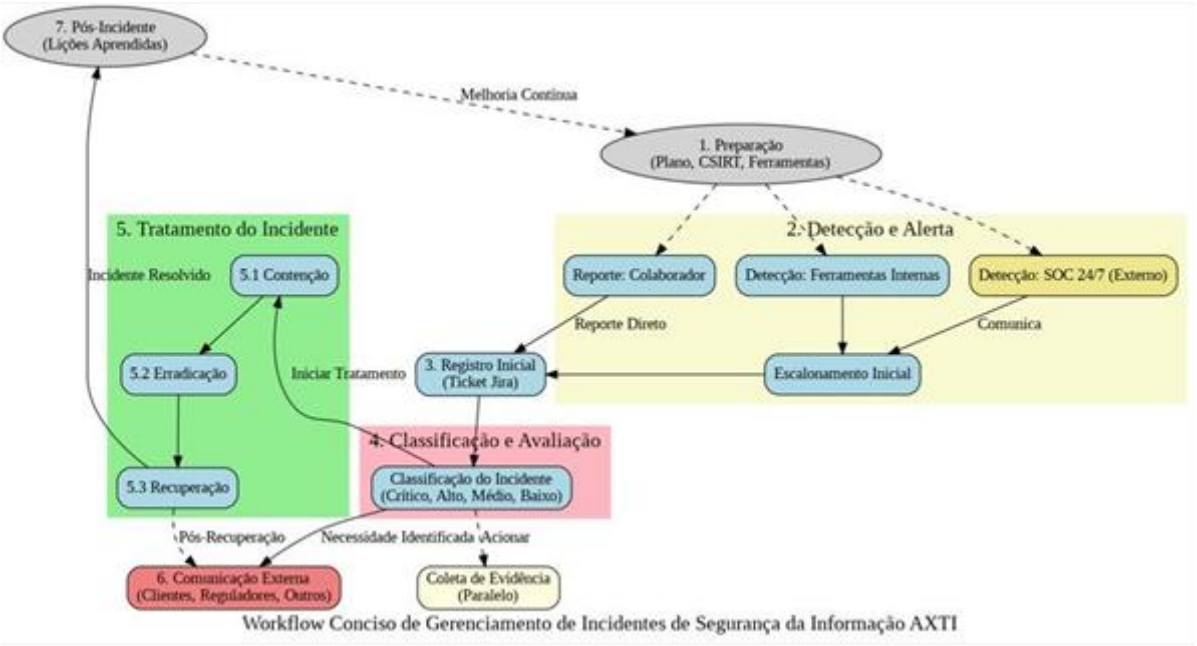
1. Analista de Segurança de Plantão
2. Analista de Infraestrutura de Plantão
3. Oficial Sênior de Segurança de Dados
4. Gerente de TI
5. Gerente Executivo de TI

Ferramentas e Serviços de Segurança

- **SHODAN**
  - ESCOPO: Realiza análises em IPs públicos dentro do intervalo da AXTI para identificar serviços potencialmente vulneráveis expostos à Internet;
  - ALERTAS: *e-mail*.
- **DARKTRACE**
  - ESCOPO: Examinar o tráfego da rede interna e do *GSuiti*, empregando Inteligência Artificial (IA), para identificar comportamentos atípicos ou que correspondam a ataques ao ambiente empresarial. Depois de identificados, os eventos são direcionados ao SOC (Centro de Operações de Segurança), de acordo com o procedimento padrão de gerenciamento de eventos.
  - ALERTAS: *e-mail*, Jira e telefone.
- **PRISMA CLOUD**
  - ESCOPO: Concentra a avaliação, identificação e, em certas situações, a reação automática a irregularidades detectadas nas soluções em nuvem empregadas no ambiente da AXTI.
  - ALERTAS: *e-mail* e Jira.
- **XDR**
  - ESCOPO: Sistema *antimalware* sofisticado que consegue relacionar comportamentos atípicos para lutar contra *malware*, *ransomware* e outras tentativas de ataques mal-intencionados.
  - ALERTAS: *e-mail*, Jira e Telefone.
- **THREAT INTEL**

    - ESCOPO: Serviço prestado por terceiros para salvaguardar a marca da AXTI na internet, incluindo a *dark web* e fóruns subterrâneos. Faz a supervisão de informações vazadas e dados divulgados sem permissão.
    - ALERTAS: *e-mail*.
- **SOC**
    - ESCOPO: Atividade exercida por uma empresa externa, disponível 24 horas por dia, 7 dias por semana (24/7), que ajuda na detecção de alertas emitidos. O SOC comunica-se com o Especialista em Segurança em serviço para que o incidente seja solucionado no menor período de tempo.
    - ALERTAS: *e-mail*, Jira e telefone.
- **DESKTOP CENTRAL**
    - ESCOPO: Serviço de inventário de ativos da AXTI, encarregado de supervisionar todos os bens da companhia. Administra atualizações, acesso e assistência à distância, seleção de softwares e produção de relatórios.
    - ALERTAS: Por aplicativo.
- **SPLUNK**
    - ESCOPO: Recolhe registros dos ativos mais importantes do ambiente e de ferramentas de monitoramento de ameaças. Examina esses registros e, por meio do SOC, emite alertas sempre que um padrão pré-estabelecido é detectado.
    - ALERTAS: *e-mail* e Jira.
- **OPENVAS**
    - ESCOPO: Executa verificações semanais nos projetos da AXTI. Vulnerabilidades que superam 7.0 (índice CVSS) são categorizadas como elevadas e precisam ser resolvidas pela equipe responsável pelo projeto em questão.
    - ALERTAS: Via aplicativo

4.9 Fluxo de Gerenciamento de Incidentes de Segurança



Workflow Conciso de Gerenciamento de Incidentes de Segurança da Informação AXTI

4.10 Tratamento de Incidentes de Segurança da Informação

O provedor de monitoramento SOC terceirizado envia um chamado com as informações e o analista de segurança da informação em serviço analisa e gerencia o aviso quando estiver dentro do âmbito de atuação. Se isso ocorrer, ele se comunica com o departamento encarregado para tratar do alerta.

4.11 Retenção de log

Os registros são enviados para o Splunk e mantidos até que seja necessária uma rotação. Os registros mais antigos são enviados para um bucket S3 na AWS, onde são mantidos por um período de 5 anos para possíveis auditorias ou eventos futuros.

5. Responsabilidades – Definição de papéis

- **Todos os colaboradores, fornecedores e terceiros:** Todos têm a obrigação e a responsabilidade de conhecer e aderir às políticas de segurança da informação da AXTI. Este grupo tem a responsabilidade de comunicar imediatamente ao time de Segurança da Informação em caso de suspeitas ou confirmação de qualquer incidente. Além disso, devem se envolver ativamente nos treinamentos e eventos de sensibilização sobre segurança da informação realizados e incentivados pela AXTI.
- **Equipe de Resposta a Incidentes de Segurança (Equipe de Segurança da Informação) e o Líder de Segurança da Informação**: São encarregados de manter e atualizar constantemente este plano de resposta a incidentes, além dos *playbooks* específicos para variados tipos de ameaças. A equipe Segurança da Informação supervisiona e comanda a resposta a todos os incidentes de segurança da informação, desde a primeira avaliação e categorização até a realização das etapas de contenção, eliminação e restauração. É também sua responsabilidade organizar a coleta e conservação de provas de maneira forense, liderar as reuniões de lições aprendidas, preparar os relatórios correspondentes e garantir que as lições sejam incorporadas para melhorar a postura de segurança. A equipe precisa estar sempre ciente das ameaças mais recentes, vulnerabilidades e métodos de resposta, além de oferecer formação e orientação sobre como lidar com incidentes para outras equipes e funcionários.
- **As Equipes de TI / Infraestrutura / Desenvolvimento (DevSecOps) e Operações:** Têm uma função vital no apoio técnico à resposta a incidentes. São encarregadas de estabelecer e preservar os controles de segurança técnica nos sistemas e na infraestrutura da organização. No decorrer de um incidente, é necessário oferecer todo o apoio necessário à Segurança da Informação, o que pode envolver a aplicação de correções emergenciais, a recuperação de sistemas e dados a partir de cópias de segurança, a obtenção de registros específicos e a execução de ações de contenção. Essas equipes também administram os procedimentos de cópia de segurança e restauração de dados, participam ativamente na avaliação e solução de incidentes que possam afetar os sistemas ou aplicações sob sua responsabilidade, e têm a responsabilidade de aplicar as sugestões de segurança derivadas das análises de lições aprendidas.

- **SOC Terceirizado:** Assume funções vitais na primeira linha de defesa e identificação. As suas responsabilidades principais envolvem o acompanhamento constante dos alertas de segurança gerados pelas ferramentas e sistemas especificados no âmbito do serviço, a execução da análise inicial e triagem desses alertas para detectar e confirmar possíveis incidentes de segurança, além da classificação inicial da severidade. Encarregado também de encaminhar rapidamente os incidentes confirmados para a equipe interna de Segurança da Informação da AXTI, de acordo com os procedimentos e prazos estabelecidos. Além disso, espera-se que o SOC apresente relatórios regulares sobre a situação de segurança, divulgue inteligência de ameaças pertinentes, auxilie a Segurança da Informação com informações e análises durante investigações mais complexas, e se envolva ativamente nos processos de aprimoramento constante ligados à detecção e resposta inicial a incidentes.

Todos os colaboradores da AXTI devem aderir a estas orientações e contatar a equipe de Segurança (sec@axti.com) em caso de incertezas sobre a implementação dessas diretrizes. Se houver exceções às diretrizes apresentadas anteriormente, a área deve entrar em contato com a equipe de segurança para uma avaliação de aprovação. As penalidades podem ser implementadas de acordo com o comportamento dos envolvidos em relação à nossa política de segurança e código de conduta ética, incluindo este documento ou outro, se aplicável. Todas as transgressões são passíveis de investigação e sanções disciplinares pela Comissão de ética e conduta.

6. Plano de resposta a desastres

A partir do exposto, propõe-se o seguinte plano de resposta a desastres simplificados. As diferenças básicas de um plano de resposta a desastres simplificado de um plano completo é que ele focará só nas ações essenciais, sendo assim menos detalhado e mais técnico do que o plano completo. Esse plano focará nas seguintes falhas: Ausência ou deficiência de segmentação de rede, Ausência de criptografia em dados sensíveis armazenados em banco de dados, Credenciais fracas, e Backups Inadequados.

Falha: Ausência ou deficiência de segmentação de rede

Ação Preventiva: Implementação de segmentação de rede baseada em firewalls e VLANs, com políticas de menor privilégio para o tráfego entre segmentos.
Área Responsável: Equipe de Redes e Segurança da Informação.
Periodicidade:

Revisão e otimização das regras de firewall: Trimestral.

Auditoria da segmentação de rede: Anual**.**

Testes de penetração (pentest): Trimestral.

Esquema de Implementação: Mapeamento da estrutura da rede, determinação de áreas de segurança, configuração de listas de controle de acesso e regras de firewall. OpenVAS para realizar varreduras que detectem serviços abertos entre segmentos desnecessariamente. Shodan para analisar a exposição externa de segmentos. Prisma Cloud para assegurar a segmentação e as diretrizes de rede em contextos de nuvem.

Ação Contingencial: Em caso de comprometimento em um segmento, isolar imediatamente o segmento ou hosts infectados para evitar a propagação lateral para outras áreas da rede.
Área Responsável: Equipe de Resposta a Incidentes e SOC.
Pré-condições: Diagrama de rede atualizado com segmentos e capacidade de isolamento de rede, como desabilitar portas, reconfigurar VLANs, ativar regras de firewall de bloqueio.
Pós-condições: Propagação do incidente contida dentro do segmento afetado e outros segmentos da rede protegidos.
Esquema de Implementação: Operações para isolamento de rede. Darktrace e XDR são utilizados para identificar movimento lateral e anomalias na rede, ativando o isolamento de forma automática ou manual. Splunk para análise de registros e visualização do tráfego entre segmentos, determinando a origem da propagação.

Ação Recuperadora: Limpeza e restauração dos sistemas comprometidos no segmento afetado, validação das políticas de segmentação e reforço da arquitetura de rede.
Área Responsável: Equipe de Infraestrutura e Segurança da Informação.
Pré-condições: Ameaça eliminada do segmento; sistemas limpos prontos para restauração.
Pós-condições: Segmento restaurado e operacional; políticas de segmentação revisadas e reforçadas; risco de propagação minimizado para futuros incidentes.
Esquema de Implementação: Reconfiguração de dispositivos de rede; reconstrução de sistemas no segmento. Execução de varreduras de vulnerabilidades com OpenVAS e testes de penetração no segmento para validar a segmentação. Splunk para monitorar o tráfego pós-recuperação e garantir a conformidade com as novas políticas de segmentação. Prisma Cloud para revalidar configurações de rede em ambientes de nuvem.

Falha: Ausência de criptografia em dados sensíveis armazenados em banco de dados

Ação Preventiva: Implementação de criptografia em repouso para todos os dados sensíveis armazenados em bancos de dados e em trânsito (SSL/TLS para conexões).
Área Responsável: Equipe de DevSecOps e Segurança da Informação.
Periodicidade:

Revisão da política de criptografia: Anual.
Auditoria de conformidade com a política: Semestral.
Monitoramento da implementação: Continuo.

Esquema de Implementação: Configuração de TDE (Criptografia de Dados Transparente) em bases de dados; Implementação de certificados SSL/TLS em todas as comunicações; Gerenciamento de chaves de criptografia. No contexto da nuvem, o Prisma Cloud é empregado para garantir que os serviços de banco de dados e armazenamento estejam configurados com a criptografia ativada. OpenVAS para executar varreduras que identificam serviços de banco de dados sem criptografia.

Ação Contingencial: Em caso de comprometimento do banco de dados, isolar o servidor imediatamente, realizar uma avaliação da exposição dos dados não criptografados e notificar as partes interessadas, como DPO (Data Protection Officer), clientes, autoridades, se aplicável.
Área Responsável: Equipe de Resposta a Incidentes, DPO e SOC.

Pré-condições: Plano de resposta a incidentes; equipe capacitada para avaliação de exposição de dados; lista de contatos para notificação.

Pós-condições: Vazamento contido; Extensão dos dados expostos avaliada; processos de notificação iniciados.

Esquema de Implementação: Métodos de isolamento de banco de dados. Utilização do Splunk para analisar logs e identificar a causa raiz do comprometimento. XDR e Darktrace para detectar atividades incomuns no banco de dados ou movimentação de dados confidenciais.

Ação Recuperadora: Restaurar o banco de dados de um backup limpo e já com a criptografia ativada, ou aplicar a criptografia aos dados restantes, e reforçar os controles de segurança.

Área Responsável: Equipe de DevSecOps e Segurança da Informação.

Pré-condições: Banco de dados comprometido isolado ou limpo; backups criptografados ou plano de criptografia em massa.

Pós-condições: Dados sensíveis criptografados e protegidos; funcionalidade do banco de dados restabelecida; conformidade com requisitos de proteção de dados assegurada.

Esquema de Implementação: Execução de scripts de criptografia de banco de dados; validação da criptografia. Auditoria de conformidade com as regulamentações de proteção de dados usando ferramentas como Prisma Cloud (para nuvem). Splunk para monitorar a reativação e garantir a integridade dos dados e o cumprimento das políticas de criptografia.

Falha: Credenciais Fracas

Ação Preventiva: Implementação de políticas de senhas fortes (complexidade, rotação), autenticação multifator (MFA) em todos os sistemas críticos, e ferramentas de monitoramento de credenciais vazadas (Dark Web Monitoring).

Área Responsável: Equipe de Segurança da Informação e RH (para treinamento).

Periodicidade:

Revisão de políticas de senha/MFA: Semestral.

Treinamento e conscientização de usuários: Anual ou em onboarding.

Monitoramento de vazamento de credenciais: Contínuo.

Esquema de Implementação: Configuração de diretivas de domínio (GPOs). Implementação de solução de MFA em todos os sistemas e aplicações. Utilização de serviços de Threat Intel para monitorar vazamentos de credenciais corporativas na dark web e plataformas de nuvem,

integrando com Prisma Cloud para acessos em cloud. Varreduras com Shodan para identificar serviços expostos na internet com credenciais padrão.

Ação Contingencial: Reset imediato de senhas de contas comprometidas ou de alto privilégio, bloqueio de acessos suspeitos e desativação temporária de serviços com credenciais fracas expostas.
Área Responsável: Equipe de Segurança da Informação e SOC.
Pré-condições: Ferramentas de gestão de identidade e acesso (IAM); registros de acesso centralizados e supervisionados; processo de redefinição de senha em caso de emergência.
Pós-condições: acesso não autorizado impedido; contas comprometidas resguardadas; risco de acesso indevido controlado.
Esquema de Implementação: Comunicação e etapas para redefinir senhas em massa por meio do sistema de gerenciamento de usuários. Análise de registros no Splunk para determinar a magnitude do comprometimento de credenciais. Darktrace e XDR são utilizados para identificar o uso irregular de credenciais e atividades suspeitas em redes e endpoints, possibilitando um bloqueio rápido.

Ação Recuperadora: Auditoria completa de todos os acessos e permissões após o incidente, reforço das políticas de segurança, e retreinamento dos usuários afetados.
Área Responsável: Equipe de Segurança da Informação, Auditoria e SOC.
Pré-condições: Incidentes de segurança contidos e resolvidos; acesso a logs históricos de autenticação.
Pós-condições: Ambiente de acesso mais seguro e resiliente; credenciais auditadas e limpas; usuários conscientes das melhores práticas de segurança de credenciais.
Esquema de Implementação: Instrumentos de auditoria de acesso; análise de diretrizes de privilégios mínimos. Emprego do Splunk para realizar uma auditoria minuciosa dos registros de autenticação após o incidente. Reforço do treinamento de segurança de credenciais com base nas lições aprendidas.

Falha: Backups Inadequados

Ação Preventiva: Implementação e verificação regular de uma estratégia de backup 3-2-1, garantindo três cópias dos dados em dois tipos diferentes de mídia, com uma cópia sendo offline e imutável.
Área Responsável: Equipe de Infraestrutura e Segurança da Informação.

Periodicidade:

Revisão e validação da política de backup: Trimestral.

Testes de recuperação de backup: Semestralmente ou após grandes mudanças na infraestrutura.

Execução de backups: Diária/Contínua, conforme criticidade dos dados.

Esquema de Implementação: Implementação de soluções de backup automatizadas com verificação de integridade. Estabelecimento de janelas de backup e procedimentos para o transporte e armazenamento de mídias em um local externo. Estabelecimento de um ambiente de teste separado para simulações de restauração. Uso do Prisma Cloud para assegurar a conformidade e a integridade dos backups em ambientes de nuvem.

Ação Contingencial: Desconectar imediatamente sistemas e redes afetadas pelo incidente para evitar a propagação da criptografia ou exclusão de dados, e isolar os backups existentes.
Área Responsável: Equipe de Resposta a Incidentes e SOC.
Pré-condições: Plano de resposta a incidentes de segurança (IRP) documentado; ferramentas de monitoramento de rede e endpoints; capacidade de isolamento de rede.
Pós-condições: Propagação do incidente contida; extensão do dano avaliada; backups não comprometidos identificados para recuperação.
Esquema de Implementação: Procedimentos operacionais de contenção de incidentes; scripts para isolamento de rede. Utilização de Darktrace e XDR para detecção de anomalias, movimento lateral e isolamento automático ou semiautomático de hosts infectados. Splunk para correlacionar logs e identificar a extensão do comprometimento.

Ação Recuperadora: Restauração de sistemas e dados a partir dos backups imutáveis e testados, priorizando sistemas críticos para o negócio, em um ambiente seguro e limpo.
Área Responsável: Equipe de Recuperação de Desastres (TI/Infraestrutura), com apoio da Segurança da Informação e SOC.
Pré-condições: A análise forense inicial foi concluída para garantir a remoção da ameaça; o ambiente de recuperação foi limpo e preparado; o acesso aos backups foi assegurado.
Pós-condições: sistemas e dados foram recuperados e verificados quanto à integridade e funcionalidade; operações comerciais foram restabelecidas em um estado operacional aceitável; lições aprendidas foram registradas.
Esquema de Implementação: Plano de Recuperação de Desastres (DRP) minucioso; automação dos processos de restauração; testes de funcionalidade após a restauração;

confirmação de dados restaurados com as áreas de negócio. Splunk para validação após recuperação e XDR para supervisionar a reintegração de sistemas no ambiente.

7. Glossário

O glossário é uma ferramenta importante para garantir que todos os stakeholders entendam os termos e conceitos utilizados no Plano de Resposta a Desastres, facilitando a implementação e manutenção do plano.

Ameaça: Qualquer situação ou ocorrência que possa causar prejuízos a um ativo.
Ativo de informação: Qualquer recurso, tangível ou intangível, de valor para a AXTI e que demande proteção, incluindo informações, software, hardware, serviços e indivíduos.
AXTI: Todas as referências a "AXTI" incluem a AXTI Inc, bem como todas as empresas do Grupo AXTI.
Cadeia de Custódia: Processo que garante a integridade, autenticidade, confiabilidade e completude das provas, documentando minuciosamente todas as ações e quem as realizou.
Centro de Operações de Segurança (SOC): Equipe encarregada do acompanhamento, identificação, análise inicial, classificação e distribuição de alertas de segurança.
Comissão de Valores Mobiliários (SEC): A Comissão de Valores Mobiliários dos Estados Unidos requer que as empresas de capital aberto notifiquem incidentes de cibersegurança materiais.
Contenção: Estágio da resposta a incidentes em que medidas são implementadas para restringir o alcance, a gravidade e a duração de um incidente, bem como suas repercussões.
Cross-Site Scripting (XSS): Trata-se de uma vulnerabilidade que possibilita a um invasor inserir scripts maliciosos em páginas da web acessadas por outros usuários. Isso pode resultar no roubo de cookies, alteração não autorizada de sites ou redirecionamento para páginas maliciosas.
Darktrace: Uma plataforma de segurança cibernética fundamentada em inteligência artificial emprega aprendizado de máquina para identificar e reagir a ameaças em tempo real, reconhecendo comportamentos anômalos na rede que podem sinalizar um ataque.
Desktop Central: Uma solução integrada de gerenciamento de endpoints da ManageEngine que auxilia as empresas no gerenciamento, proteção e monitoramento de laptops, desktops, smartphones e tablets por meio de um console centralizado. Abrange recursos para gerenciamento de patches, implantação de software e administração de ativos.
Erradicação: Fase da resposta a incidentes onde a causa raiz do incidente é eliminada.
Equipe de Resposta a Incidentes: Equipe de Segurança da Informação da AXTI, encarregada de organizar as ações de resposta a incidentes.

Evento de segurança da informação: Ocorrência que indica uma possível violação de segurança da informação ou falha de controles.

Incidente de segurança da informação: Eventos de segurança da informação relacionados e identificados que podem prejudicar os ativos de uma organização ou comprometer suas operações. É incluso como incidente de segurança a perda ou roubo de informações, transferência de dados ou informações não autorizados a sistema ou repositórios de dados, interrupções não planejadas ou bloqueios de acesso a sistemas, alterações não autorizadas em dados, softwares, firmware, hardware ou sistemas, sem o devido registro de alteração e aprovação formal.

Indicador de Comprometimento (IOC): Elementos de informação ou artefatos forenses que indicam uma possível invasão ou ação mal-intencionada em um sistema ou rede.

Lei Geral de Proteção de Dados (LGPD): Lei brasileira que define normas para a coleta, guarda, processamento e divulgação de dados pessoais.

OpenVas: Um scanner de vulnerabilidades de código aberto e gratuito capaz de detectar falhas de segurança em sistemas e redes. Trata-se de um recurso valioso para conduzir avaliações de segurança e assegurar que os sistemas estejam resguardados contra vulnerabilidades identificadas.

Pass The Hash (PTH): Trata-se de uma técnica de ataque na qual um invasor utiliza o hash criptográfico de uma senha para se autenticar em um sistema ou serviço de rede. É uma prática comum em redes Windows e possibilita que o atacante se desloque lateralmente na rede sem a necessidade de decifrar a senha.

Período Máximo Tolerável de Interrupção (MTPD): Indica o período máximo que uma empresa pode tolerar a interrupção de um processo de negócio, serviço ou sistema essencial antes que os efeitos se tornem insustentáveis.

Pilares da Segurança da Informação: Divididos em Confidencialidade, Integridade e Disponibilidade (CID). Respectivamente a divisão, os pilares auxiliam na garantia de que a informação é acessível apenas por pessoas autorizadas, garantia da precisão e integralidade das informações e dos procedimentos de processamento, e assegurar que somente usuários autorizados possam acessar a informação e os ativos relacionados quando necessário.

Playbooks: Documentos que descrevem procedimentos específicos para gerenciar diversas ameaças ou incidentes.

Prisma Cloud: Uma plataforma completa de segurança em nuvem da Palo Alto Networks, que garante proteção para aplicações, dados e toda a infraestrutura em ambientes de nuvem

pública e híbrida. Ela auxilia na identificação de vulnerabilidades, na gestão de configurações e na garantia de conformidade.

Recuperação: Estágio da resposta a incidentes em que os sistemas, serviços e dados impactados são restabelecidos ao seu funcionamento normal e seguro.

Regulamento Geral de Proteção de Dados (GDPR): Norma europeia relativa à privacidade e à salvaguarda de dados pessoais de pessoas na União Europeia e no Espaço Econômico Europeu.

Resposta a incidentes: Ações implementadas para minimizar ou resolver um incidente de segurança da informação, incluindo aquelas voltadas para a proteção e restauração das condições habituais de funcionamento de um sistema de informação e dos dados nele armazenados.

Shodan: Um mecanismo de busca distinto do Google, pois indexa dispositivos conectados à internet e os serviços que eles oferecem. Pesquisadores de segurança e atacantes utilizam-no para identificar dispositivos com vulnerabilidades ou configurações inadequadas.

Sistema Comum de Pontuação de Vulnerabilidades (CVSS): Norma industrial para aferir a severidade de vulnerabilidades de segurança.

SOC (Security Operations Center): trata-se de uma estrutura centralizada em uma organização na qual equipes de segurança monitoram, identificam, analisam e respondem a ocorrências de segurança cibernética. O principal objetivo é resguardar os bens da empresa contra possíveis ameaças.

Splunk: Uma plataforma para operações de segurança e análise de dados que possibilita a coleta, indexação e análise de grandes volumes de dados gerados por máquinas. É comumente empregado para SIEM, monitoramento, resolução de problemas e inteligência operacional.

TDE (Transparent Data Encryption): Trata-se de uma tecnologia de segurança que, em tempo real, criptografa dados em repouso sem a necessidade de modificar as aplicações que utilizam esses dados. Caso os arquivos do banco de dados sejam comprometidos, ele contribui para a proteção de dados sensíveis contra acesso não autorizado.

Threat Intel (Inteligência de Ameaças): diz respeito a informações fundamentadas em evidências e contexto acerca de ameaças cibernéticas atuais ou em potencial. Inclui informações sobre TTPs (Táticas, Técnicas e Procedimentos) de atacantes, IoCs (Indicadores de Compromisso), vulnerabilidades e tendências, ajudando as empresas a se protegerem de forma proativa.

Violação de dados: Incidente de segurança que tem como resultado a exposição, acesso ou aquisição acidental ou ilegal de dados pessoais protegidos.

Vulnerabilidade: Ativo ou domínio que pode ser aproveitado por uma ou mais ameaças.

XDR (Extended Detection and Response): trata-se de uma estratégia de segurança cibernética que integra e relaciona informações de segurança provenientes de diversos pontos de controle (endpoints, rede, nuvem, e-mail), oferecendo uma visão mais abrangente e contextualizada das ameaças, o que possibilita uma detecção e resposta mais eficientes.