Journal of Technology & Information

O PLANO DE CONTINUIDADE DE NEGÓCIOS APLICADO A *RANSOMWARE* EM EMPRESAS MULTINACIONAIS

THE BUSINESS CONTINUITY PLAN APPLIED TO RANSOMWARE IN MULTINATIONAL COMPANIES

Recebido: 02/02/2023 | Revisado: 21/02/2023 | Aceito: 30/09/2023 | Publicado: 01/10/2023

Stephany Victoria Nascimento da Silva
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-2089-0517
Stephany.victoria@outlook.pt

Irapuan Glória Junior
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-2973-3470
ijunior@ndsgn.com.br

Resumo

Nos últimos quatro anos, o *malware* denominado *Ransomware*, que visa sequestrar dados, impossibilitando o acesso a estes até que seja pago uma quantia em resgate, tem ganhado cada vez mais visibilidade vitimando grandes empresas mundiais. Um ataque cibernético pode ocasionar a parada total da operação de uma empresa causando prejuízos na medida que esta fica fora de suas atividades. O Plano de Continuidade de Negócios visa ser um procedimento detalhado, permitindo a continuação das principais atividades ou aplicações de uma organização em meio a cenários previstos que causem disrupção. A pesquisa é qualitativa, com uso da metodologia de Estudo de Casos e visa entender o cenário dos processos de segurança relacionados à Continuidade de Negócios em empresas Multinacionais do setor de TI a fim de considerar sua aplicabilidade e eficiência em cenários de *Ransomware*.

Palavras-chave: Continuidade; Negócios; Ataque; Cibernético; Segurança; *Ransomware*.

Journal of Technology & Information

Abstract

In the last four years, malware called Ransomware, which aims to hijack data, making it impossible to access them until a ransom is paid, has gained increasing visibility, victimizing large mundials companies. A cyber attack can bring a company's operation to a complete halt, causing losses as it is out of business. The Business Continuity Plan aims to be a detailed procedure, allowing the continuation of the main activities or applications of an organization in the midst of foreseen scenarios that cause disruption. The research is qualitative, using the Case Study methodology and aims to understand the scenario of security processes related to Business Continuity in Multinational companies in the IT sector in order to consider its applicability and efficiency in Ransomware scenarios.

Keywords: Continuity; Business; Attack; Cyber; Security; Ransomware.

1. Introdução

Ao longo dos anos com a evolução da tecnologia e suas ferramentas de facilitação para o dia a dia foi criando-se um cenário de dependência digital, tanto para usuários comuns, quanto para organizações, que dependem destas para atividades do cotidiano, visto que, sem a tecnologia da informação o processo de desenvolvimento dessas atividades se torna muito mais trabalhoso e custoso (Cabral, 2021).

O advento da pandemia do COVID-19 ocasionou maior dependência tecnológica devido ao fato de que aquilo que não era informatizado precisou ser, empresas inclusive, se viram obrigadas a adotar o regime *Home office*, porém juntamente com as ferramentas de facilitação, o crime cibernético também evoluiu e melhorou suas práticas, aproveitando dessa exposição e relação de dependência (Nagli, 2020).

De 2020 até 2021, as denúncias de ataques cibernéticos em empresas aumentaram em 220% (Brasil, 2021), apesar de possuírem muita estrutura e investimentos em procedimentos de Segurança da Informação, grande parte desses alvos foram empresas multinacionais (Nascimento & Gloria Júnior, 2023).

Um reflexo disso foi que em 2021 grandes empresas como Lojas Renner, CVC e Atento, tiveram suas operações interrompidas devido a um ataque *Ransomware* no Brasil (Report, 2022).

O ataque sofrido pela Renner foi um grande marco na segurança da informação nacional, pois graças a sua repercussão, o assunto ganhou visibilidade (Gaidargi, 2021). A empresa divulgou um comunicado informando que havia ocorrido um ataque cibernético em seu ambiente de TI e que este causou indisponibilidade em parte de seus sistemas e operação. Esta também ressaltou que rapidamente acionou os protocolos e procedimentos existentes de controle e segurança para bloquear o ataque e minimizar eventuais impactos (Upx, 2021).

Outro caso importante para a segurança da informação nacional foi o caso da empresa de viagens CVC. que diferente da Renner só conseguiu obter o reestabelecimento normal das operações 10 dias após o ataque cibernético (ABC, 2019).

Cerca de 850 lojistas da CVC informaram dúvidas e inseguranças relatadas por clientes que compraram na empresa antes da invasão cibernética, e demonstraram preocupação, se seus dados de cartões e pessoais, estavam seguros após a invasão ou se foram violados, comprometidos ou vendidos pelos criminosos. Apesar de a empresa não ter exposto os prejuízos causados durante esse período de interrupção, estima-se que este foi extremamente alto, visto que o prejuízo aumenta de acordo com o tempo que a organização fica fora do ar. (Branco, 2021).

Diante deste contexto, o presente trabalho possui como questão de pesquisa: “Como o Plano de Continuidade de Negócios pode ser aplicado para evitar ataques Cibernéticos em empresas multinacionais?”. Os objetivos são: (1) Entender o motivo das multinacionais ainda serem grandes alvos de *Ransomware* e (2) Sugerir ações para a criação e aplicação de um PCN adaptado para cenários de ataque *Ransomware*.

2. Referencial Teórico

2.1. Segurança da Informação

A informação deve ser protegida adequadamente pois é um ativo essencial para o funcionamento dos Negócios de uma organização (Macarenhas & Araújo, 2019). Esta existe em uma organização de várias formas, eletronicamente, por meio de anotações em papéis, documentos ou até mesmo em conversas formalizadas por meio de correio eletrônico ou plataformas corporativas (ISO, 2013).

Desta forma, proteger a integridade das informações, confidencialidade e disponibilidade, permite com que o ambiente informacional da organização seja assegurado, sendo uma atividade básica da segurança da informação, controlá-lo (Macarenhas & Araújo, 2019).

Atualmente a informação pode ser considerada o ativo e recurso mais crítico de uma organização pois informações sob controle de pessoas de má-fé ou até mesmo concorrentes comerciais podem causar grande comprometimentos a uma instituição, danificando sua imagem frente a terceiros e clientes e até mesmo prejudicando seus processos institucionais, podendo até causar a inviabilização da continuidade de uma organização (TCU, 2012).

Para que este ativo tão importante seja protegido, as empresas devem ter um setor de segurança da informação, onde políticas devem ser criadas, implementadas, controladas, monitoradas e atualizadas regularmente para normatizar e assegurar a integridade dos ativos de informação. Essas políticas buscam priorizar as áreas de negócio, principalmente quando são utilizadas tecnologias nestas para o desenvolvimento de trabalhos (Federal, 2022).

De um modo geral, a segurança da informação é um requisito obrigatório, de forma a minimizar os riscos associados a uma atividade ou negócio e assegurar a conformidade com disposições legais ou de natureza regulatória, como é o caso de regulamentos comunitários ou provenientes da legislação nacional (Gouveia, 2016).

2.2. *Ransomware* em empresas multinacionais

Uma das preocupações dos executivos e consumidores por sua constante aparição na mídia atualmente é o sequestro de dados, que criptografa as informações de um computador e só o desfaz em troca de um resgate em cripto moeda (Liska & Gallo, 2019).

A história do *Ransomware* começa em 1998, quando sua primeira variação, denominada *Aids InfoDisk (*AIDS), foi desenvolvida em Harvard pelo biólogo Dr. Joseph Popp (Kelly, 2020).

Porém este não parou por aí, e até mesmo em 2023, é considerado uma das maiores ameaças para multinacionais. Em 2021 foram entrevistadas 800 multinacionais com mais de 500 funcionários e identificado que um terço das maiores empresas do mundo já foram vítimas de ataques *Ransomware.* (IDC International Data Corporation,2021).

É possível afirmar que em multinacionais esse *malware* ganhou visibilade a partir de 2017, quando cibercriminosos se aproveitaram de uma vulnerabilidade em computadores não atualizados do Windows, criptografando mais de 220.000 computadores em cerca de 150 países (Zandt, 2021).

O Wannacry foi apenas o início de uma chamada “epidemia de *Ransomwares*” que afeta grandes empresas até os dias atuais. Embora seja comum pensar que empresas multinacionais, devido ao seu tamanho e orçamento elevado para investir em segurança da informação, seriam menos propensas a sofrer ataques de *Ransomware*, a realidade é bem diferente (Burton, 2021).

Figura 1 – Wannacry attack baseado em Burton, A. (2021).

Grandes empresas multinacionais como Nissan (Cohen, 2021), Renault (Cohen, 2021), Canon (Alecrim, 2020) , Kia Motors (Privacytech, 2021), Toyota (CNN Brasil, 2021), Ferrari (Silva, 2023), Nvidia (Arntz, 2022), e Fleury (Tadeu, 2023) foram vítimas de *Ransomware* nos últimos 6 anos. Acredita-se que ataques a outras empresas não citadas ocorreram, mas devido à vergonha de não obter planos de resposta e muito tempo de sequestro de dados, estas não divulgaram o ocorrido (Martins, 2022).

Em 2017, as empresas Renault e Nissan tiveram suas operações interrompidas em algumas unidades pelo *Ransomware* Wannacry. Mesmo que estas tenham imediatamente desconectado os sites que relatavam infecções da rede para evitar a propagação do *Ransomware*, ambas ficaram 3 dias sobre ataque (Cohen, 2021)

Um dos casos mais críticos de *Ransomware* em multinacionais no ano de 2020, foi na empresa Canon que ficou cerca de 8 dias sob ataque. Além de ter 10TB de dados sequestrados, a empresa teve grande parte de seus sistemas interrompidos como e-mail corporativo, o site da companhia, a conta da empresa no Microsoft Teams e até a plataforma de armazenamento de vídeos e fotos nas nuvens. Ainda em 2020, a Honda teve fábricas paralisadas no mundo inteiro, consequente de um ataque *Ransomware* (Alecrim, 2020).

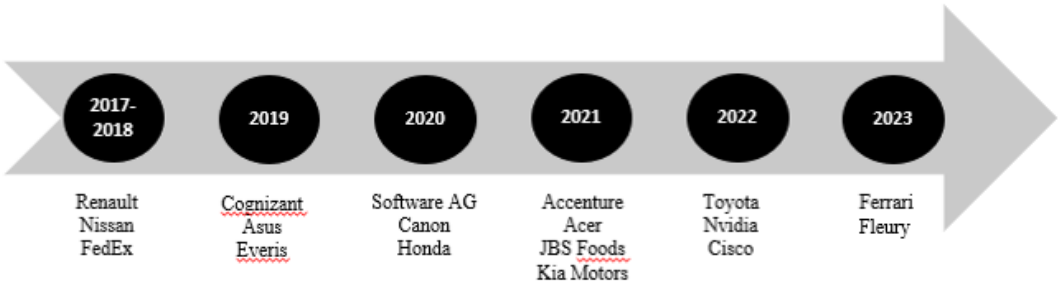
Já em 2021 a empresa JBS *Foods* pagou cerca de U$11 milhões em resgate após um ataque *Ransomware* (G1, 2021). Enquanto isso, a empresa Kia *Motors* teve seus sistemas centrais interrompidos e foi cobrada em US$ 20 milhões em Bitcoins para ter seus arquivos descriptografados e não ter dados confidenciais vazados online (Privacytech, 2021).

No Japão, a Toyota teve todas as suas fábricas fechadas por um dia, atrasando a produção de 13 mil veículos devido a um ataque *Ransomware* no ano de 2022 (CNN Brasil, 2022). Ainda no mesmo ano a empresa NVIDIA foi atacada e teve dados de e-mail e senha de 70 mil funcionários divulgados. A equipe criminosa que realizou o ataque afirma ter divulgado os dados pois acusam ter sido atacados de volta pela empresa (Arntz, 2022).

Em 2023, a empresa Ferrari teve dados, como nomes, endereços e telefones vazados após se recusar a pagar o resgate em um ataque *Ransomware*. Apenas um número limitado de sistemas foi acessado pelos criminosos e a empresa contratou uma empresa forense para investigação do caso (Silva, 2023).

Já o grupo Fleury do setor de saúde foi vítima de *Ransomware* duas vezes em um período de menos de um ano, sendo o último ataque em 2023. Pacientes ficaram sem acesso à seus exames e não há uma certeza de venda de dados, estes podem ter sidos vendidos ou não. (Tadeu, 2023)

Fluxograma 1- – Linha do tempo de *Ransomware* em multinacionais



É surpreendente notar que até mesmo empresas de tecnologia multinacionais são afetadas por *Ransomware*, o que sugere que mesmo organizações com conhecimento avançado sobre segurança podem ser vítimas. Como é o caso da Cognizant, uma das maiores provedoras globais de serviços de TI, que teve seus dados sequestrados enquanto fazia a transição do método de trabalho para *Home-Office* (Yasar, 2021).

Em 2019, a empresa Everis, de consultoria do grupo NTT Data foi vítima do *Ransomware* Bitpaymer, não houve vazamento de dados, mas os funcionários foram liberados mais cedo para que a equipe de crises pudesse agir. As lições foram aprendidas e a empresa investiu fortemente em segurança da informação, tanto que foi uma das pioneiras na prestação de serviços relacionados à implementação da LGPD em outras empresas (Chieco, 2019).

Em 2020 a empresa Software AG precisou atender clientes via e-mail como contingência, pois seus sistemas habituais foram criptografados por *Ransomware*, a empresa confirmou vazamento de dados de servidores e de notebooks de funcionários. Em paralelo estava sendo anunciado na internet 19TB de dados de uma grande empresa foram comprometidos (Redação, 2020).

O maior resgate já solicitado em casos de *Ransomware* foi o da Acer em 2021, os criminosos solicitaram U$50 milhões em troca dos dados criptografados e vazaram saldos bancários de membros da empresa para provar o sequestro, já que essa negava para a mídia (Soares, 2021).

Em 2022, um outro tipo de *Ransomware* sofisticado foi descoberto em placas-mãe da Asus fabricadas e infectadas em 2019, esperando somente ser conectado a um computador-cliente para sequestrar seus dados (Alecrim, 2022).

Em 2022, até mesmo a gigante de redes de computadores Cisco foi vítima de um ataque destes. Os criminosos tomaram conta das credenciais do google de um funcionário e conseguiu se disfarçar de várias organizações confiáveis, convencendo a vítima a aceitar um push de MFA, obtendo acesso à VPN e roubando cerca de 2,8GB de dados da empresa (Winder, 2022).

Em empresas que não possuem um Plano de Continuidade a gestão de crises pode se tornar complicada. Poucas empresas na região possuem um plano de continuidade do negócio (BCP) ou de recuperação de desastres (DRP) (Kezter, 2023). Nos estados unidos estima-se que em 6 meses, mais de 5 bilhões de bitcoins tenham sido pagos como resgate para quadrilhas de *Ransomware* (Nunes, 2023).

Em 2021 a existência de backups era vista como a solução para ataques *Ransomware*, pois impossibilitam o acesso aos dados da vítima, caso estes fossem perdidos os backups anulariam os impactos (Hoff, 2022).

Esperava-se que a estratégia da realização de backups eliminasse a chamada "epidemia de *Ransomware*'s" porém, na metade de 2022, foi identificado que 72% das empresas globais tiveram seus arquivos de armazenamento comprometidos em ataques *Ransomware*, indiciando uma evolução e sofisticação destes (Dermatini, 2022).

Backups inadequados são parte desta problemática em cenários de *Ransomware*. Por justificativas de reduzir custos, algumas empresas não revisam e testam seus procedimentos de backup, ocasionando uma impossibilidade de restauração em caso de contingência. Pela mesma justificativa também há casos em que o plano de backup é eficiente, mas não cobre alguma aplicação ou sistema específico que talvez não seja mapeado em primeira instância como crítico, mas que forneça dados para um sistema crítico (IT,2021).

Outra parte desta problemática é causada pelo fato de que todo backup cuja localização é acessível ao sistema de arquivos da máquina está em risco. A maioria dos produtos de backup modernos para Windows usa cópias de sombra e pontos de restauração do sistema. Vários tipos de *Ransomware*, como Locky e Crypto, são conhecidos por destruir cópias de sombra e restaurar dados de ponto. Portanto como mesmo o *Ransomware* mais avançado não pode sobrescrever um backup que não esteja armazenado em uma unidade local de armazenamento, o melhor modo para proteger os backups dos *Ransomware* é a nuvem. (Advisor, 2022).

2.3. Setor de TI

Em meados dos anos 2000 as empresas consideravam a Tecnologia da Informação como custo alto e que não gerava o retorno esperado (Beal, 2009). Isso acontecia devido ao fato de que eram investidas quantias em equipamentos que não eram muito utilizados. Este cenário foi mudando conforme os valores dos computadores foram diminuindo e a sua utilização facilitada, permitindo com que as organizações passassem a buscar infraestruturas cada vez mais voltadas a tecnologia, permitindo que fossem realizadas não somente automação de tarefas, mas gestão de dados, conexões entre pessoas, escritórios e organizações, comunicação e até mesmo controle de equipamentos (Alves, 2022).

Diante do novo cenário que as empresas estão vivenciando, a informação e o conhecimento fundem-se e superam expectativas e necessidades, para que entre empresa e colaboradores, exista senso comum, no que diz respeito, ao alcance dos objetivos planejados, havendo uma troca mútua de interesses. Com isso, a organização permanecerá por mais tempo no mercado altamente competitivo. Através destas variáveis, a área de Tecnologia da Informação tem assumido um novo papel: o de contribuir substancialmente com a gestão integral dos negócios. (Teófilo & Seget, 2016).

Na conjuntura contemporânea as empresas mais destacadas no mercado investem no setor de TI usando-o para melhoria da experiência do colaborador e do cliente através de implantação de soluções (Tutida, 2021).

Isso acontece porque quando o departamento de TI é gerido de forma estratégica, a fim de atuar como elaborador de soluções e não apenas como apoio, as melhorias trazidas por ela podem diminuir os custos da operação (Telecom, 2021).

O departamento de TI tem como uma de suas principais responsabilidades garantir que as informações não sejam vazadas, atualmente grande parte das informações de uma empresa são criadas e compartilhadas através da internet e dispositivos tecnológicos (Tutida, 2021).

Porém, como parte das inúmeras consequências de um processo de industrialização tardio, o Brasil precisou se adaptar de forma rápida à tecnologia, negligenciando a estruturação de segurança no desenvolvimento desta. Desta forma, procedimentos proativos referentes à segurança da informação acabam sendo vistos como gastos desnecessários ou sendo desenvolvidos de maneiras superficiais, justificada pelo baixo custo apenas com o intuito de cumprimento de requisitos de auditorias, ocasionando uma forte cultura de vulnerabilidade nas empresas do país. (Bertolli, 2020).

2.4. Sistema de Gestão de Continuidade de Negócios

O Sistema de Gestão de Continuidade de Negócios (SGCN) utiliza de diversas estruturas organizacionais, incluindo a elaboração de políticas, atividades de planejamento, responsabilidades, procedimentos, processos e recursos para a elaboração de um sistema que garanta a disponibilidade dos principais recursos e funcionalidades de uma empresa durante uma disrupção e o seu passo-a-passo seguro até a sua volta à normalidade (Campos, 2020).

Para a existência de um SGCN, primeiramente é necessária a elaboração de uma política de continuidade para definir quais os padrões e diretrizes devem ser utilizados na elaboração e realização dos procedimentos associados (Sullivan, 2022).

O Plano de Continuidade de Negócios é o principal produto de um bom SGCN pois ele será o passo-a-passo tanto da continuidade dos recursos críticos quanto da invocação dos outros procedimentos associados, como por exemplo, os Planos de Recuperação de Desastres – que definem como mandar os processos e aplicações para seus ambientes de contingência (ISO, 2012).

Para elaboração dos procedimentos necessários em um SGCN é de extrema importância que avaliações de riscos e ameaças para o negócio sejam feitas, pois através destas será possível definir os cenários previstos pelos planos que serão desenvolvidos. (ISO, 2012).

É necessário também que sejam mapeados os processos e aplicações críticas para definição do que é realmente necessário em caso de contingência. Após definido torna-se essencial uma avaliação de impacto em função do tempo, para que seja analisado quanto tempo estes recursos podem ficar fora do ar e quanto de dados pode ser perdido sem grandes prejuízos. Esses valores são chamados também de *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO), e essa avaliação geralmente é nomeada como *Business Impact Analysis* (BIA) (ISO, 2015).

No dia 11 de setembro de 2011, os Estados Unidos foi vítima de um ataque terrorista onde uma empresa composta por dois prédios conhecidos por “Torres Gêmeas” foi atingida por um avião, destruindo-a. Essa empresa guardava os dados em um prédio e os *backups* no prédio ao lado. Portanto, quando ocorreu o incidente, e que deixou de existir, pois perdeu seus dados sem a possibilidade de continuar em outro endereço (Spaniol, 2019).

Este incidente das torres gêmeas foi extremamente importante na história da definição de diretrizes de proteção de dados, pois através dele, definiu-se que é de grande recomendação que uma empresa armazene seus *backups* em locais consideravelmente distantes de seus originais, para em caso de desastres de grandes proporções, estes não sejam afetados (Januário, 2017).

Além da previsão de cenários, possíveis impactos e alinhamento destes com as rotinas de *backup*, é de extrema importância que a organização monitore seus sistemas, para que esta possa ser capaz de identificar e avaliar um incidente, abrindo uma sala de crise e dando início ao SGCN (ISO, 2012).

É obrigação legal que a organização comunique as partes impactadas e autoridades necessárias em casos de incidentes de segurança da informação, portanto, esta deve estabelecer procedimentos que definam estratégias de comunicação em caso de riscos reais ou iminentes (ISO, 2015).

3. Metodologia

A metodologia aplicada foi estudo de caso (YIN, 2021), pois o estudo tem como objetivo realizar o entendimento dos procedimentos de contingência existentes em uma empresa do setor de TI, para elaboração de uma lista de ações para implementação de um Plano de Continuidade de Negócios. Na Tabela , são apresentadas as características utilizadas para a realização do estudo.

Tabela 2 - Características do Estudo

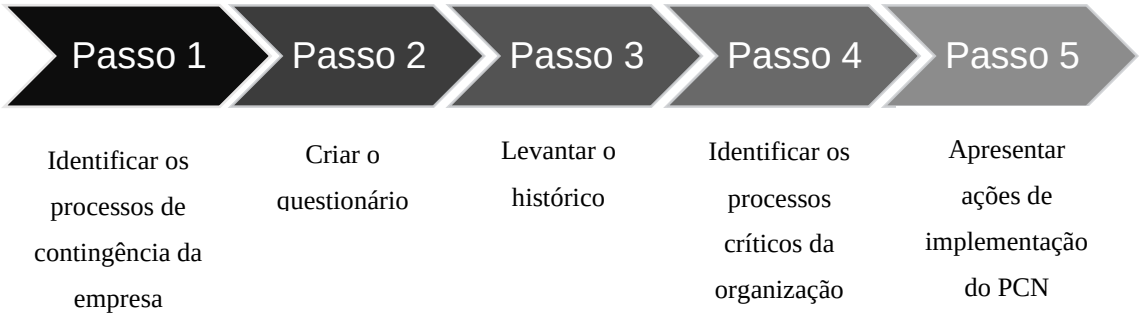
Item	Descrição	Autor(es)
Questão de Pesquisa	- Como o Plano de Continuidade de Negócios pode ser aplicado para evitar ataques Cibernéticos em uma empresa no setor de TI?	
Natureza	- Qualitativa	GIL (2022)
Metodologia	- Estudo de Caso	YIN (2021)
Coleta de Dados	- Entrevista - Análise documental	TEÓPHILO; MARTINS (2016)
Unidade de análise	- Empresas do setor de TI	

3.1. Processo Metodológico

As etapas desta pesquisa, conforme Figura , são:

- **Passo 1: Criar o questionário**. Foi criado um questionário para o levantamento de dados a ser empregado aos funcionários-chaves (Apêndice B);
- **Passo 2: Identificar os processos de contingência da empresa**. Serão levantados por meio de documentos digitais e entrevistas (Apêndice A) os processos utilizados na empresa;
- **Passo 3: Levantar o histórico**. Foi obtido o histórico de ataques cibernéticos da empresa, entender os procedimentos realizados e elaborar uma linha do tempo com a evolução da área de segurança e lições aprendidas;
- **Passo 4: Identificar os processos críticos da organização**. Mapear os processos de maior impacto para a organização.
- **Passo 5: Apresentar Ações de Implementação do PCN**. Foi elaborada uma lista de ações para implementação de um Plano de Continuidade de Negócios.

Figura 3 - Procedimentos Metodológicos



3.2. Objeto de Estudo

A Empresa-Alpha é uma multinacional situada no estado de São Paulo, possui cerca de 500 colaboradores, possui mais de 10 anos no mercado.

A Empresa-Beta também está situada no estado de São Paulo e possui o mesmo porte da Empresa-Alpha, estando há mais de 20 anos no mercado.

Foram entrevistados dois profissionais em 2022 que possuem poder decisório na área de tecnologia e que estão nestas empresas há pelo menos 5 anos e na área de consultoria há no mínimo 15 anos.

3.3. Proposições

As proposições deste artigo baseado no referencial teórico, e apresentadas na Tabela 2, são:

Proposição 1: Políticas devem ser criadas, implementadas, controladas, monitoradas e atualizadas regularmente para normatizar e assegurar a integridade dos ativos de informação. Essas políticas buscam priorizar as áreas de negócio, principalmente quando são utilizadas tecnologias nestas para o desenvolvimento de trabalhos. (Fernandes, 2013)

Proposição 2: O backup dos sistemas deve ser armazenado em outro local. Em caso de destruição total do prédio ou até mesmo da cidade onde a empresa está localizada, manter os backups distantes impedirá a sua destruição, permitindo com que as informações sejam recuperadas e os processos da empresa continuados de maneira mais rápida e eficiente (Spaniol, 2019).

Proposição 3: Os processos e aplicações críticas da empresa devem ser mapeados. Para definição de escopo do plano de continuidade de negócios é preciso entender o que é essencial para continuação da operação, de acordo com a ISO/IEC 22301, para isso deve ser realizada uma análise de impacto nos negócios afim de entender quais são os processos críticos da organização que trazem maior impacto em casos de interrupções, e quais são os requisitos para seu funcionamento para que estes e passos a serem seguidos para sua continuidade possam ser identificados e documentados. (ISO, 2012).

Proposição 4: Devem ser realizadas avaliações de riscos e ameaças para o negócio. Por meio dos mapeamentos necessários para a elaboração de um Plano de Continuidade de Negócios é possível identificar as probabilidades de determinadas situações acontecerem de acordo com vários fatores externos e internos de uma organização e através disso determinar os cenários do plano, conforme a ISO/IEC 27005 (ISO, 2008)

Proposição 5: **É preciso avaliar os impactos dos processos e aplicações críticas em função do tempo.** Quanto maior o tempo que a operação de uma empresa fica fora do ar, maiores os prejuízos, sejam eles legais, financeiros e de imagem, se tornam. Segundo a ISO/IEC 22317 (ISO, 2015).

Proposição 6: As partes interessadas devem ser mapeadas e comunicadas. A organização deve estabelecer, implementar e manter procedimentos para alertar as partes interessadas potencialmente impactadas por um incidente de interrupção real ou iminente, conforme a ISO/IEC 22301. (ISO, 2012).

Proposição 7: A organização deve realizar a monitoração de ambientes. A organização deve ser capaz de identificar um incidente assim como sua possibilidade, de acordo com a ISO 22301, dessa forma é possível definir estratégias de prevenção e contenção antes mesmo destes acontecerem e acompanhá-los em tempo real (ISO, 2012).

Proposição 8: A organização deve manter ambientes de contingência. A organização deve ser capaz de levantar um segundo ambiente para realizar a continuidade dos negócios caso o primeiro se torne indisponível, conforme a ISO 22301 (ISO, 2012)

Tabela *1* **-** Relação de questões e preposições

Item	Proposições	Questões Relacionadas
1	Políticas devem ser criadas, implementadas, controladas, monitoradas e atualizadas regularmente para normatizar e assegurar a integridade dos ativos de informação	1,2, 8, 11, 12 e 13.
2	O backup dos sistemas deve ser armazenado em outro prédio	9
3	Os processos e aplicações críticas da empresa devem ser mapeados	4
4	Devem ser realizadas avaliações de riscos e ameaças para o negócio.	6
5	É preciso avaliar os impactos dos processos e aplicações críticas em função do tempo.	7
6	A organização deve estabelecer, implementar e manter procedimentos para alertar as partes interessadas potencialmente impactadas por um incidente de interrupção real ou iminente.	10
7	A organização deve realizar a monitoração de ambientes	3
8	A organização deve manter ambientes de contingência	5

4. Análise e Interpretação dos Resultados

Os resultados do estudo foram obtidos a partir de entrevistas com duas empresas e entendimento dos procedimentos destas. Foi realizada uma análise e comparação destes para entendimento de particularidades e convergências.

4.1. Funcionamento das Empresas

A área responsável pelos procedimentos de contingência da Empresa-Alpha é a área de Segurança da Informação. Esta é dividida em duas: Segurança da Informação interna e Segurança da Informação comercial, que é responsável pela prestação de serviços de segurança para outras empresas. Já a Empresa-Beta, assim como a Empresa-Alpha, fornece serviços de TI para outras empresas. Esta, possui o departamento de segurança da informação integrado com o departamento de TI, unificando os dois para a mesma equipe e gestor.

4.2. Sugestões

Durante o mapeamento da Empresa-Alpha foi mapeado que as áreas são muito independentes entre si, cada uma é responsável pelo próprio faturamento e gerenciamento de *budget*. Consequente desta independência não há comunicação efetiva e serviços prestados acabam sendo duplicados.

As políticas e procedimentos da CIA são à nível global, recebidas da matriz. Foi identificado que decorrente deste cenário não existem mapeamentos e procedimentos específicos para cada área do Brasil, ou seja, não foram identificados procedimentos de continuidade, apenas planos de intenções. É recomendável que seja feita uma mudança neste cenário, pois em caso de desastres e indisponibilidade do recurso-chave de recuperação, pessoas de outros departamentos ou funcionários sem domínio técnico dos ambientes não conseguiriam realizar os acionamentos e contingências de forma rápida, ocasionando o aumento de prejuízos e ressaltando a ineficiência do Plano de Continuidade de Negócios existente.

Foi identificado que mesmo funcionários de segurança da informação não possuem conhecimento sobre alguns procedimentos e análises de impacto da organização. É necessário conscientizar e treinar os funcionários à nível de gestão de todas as áreas acerca de continuidade de negócios. É recomendável realizar simulações de cenários de contingência periodicamente.

Durante o mapeamento da Empresa-Beta, por questões de confidencialidade, não foi possível realizar análise aprofundada de suas políticas, mas foi possível identificar que seu plano de continuidade de negócios, assim como a Empresa-Alpha, não se trata de um procedimento detalhado, e sim de um plano de intenções.

É recomendável que sejam documentados todos os seus procedimentos de continuidade e fluxos de acionamento, para que em caso de indisponibilidade das pessoas responsáveis pela continuidade de negócio com domínio dos ambientes, outro funcionário que não possua tanto conhecimento técnico consiga realizar o acionamento do plano.

4.3. Análise das Proposições

Proposição 1: Políticas devem ser criadas, implementadas, controladas, monitoradas e atualizadas regularmente para normatizar e assegurar a integridade dos ativos de informação. Em ambas as empresas, as políticas são mantidas e revisadas. Na Empresa-Alpha existem políticas globais, criadas pela equipe de segurança da informação interna e que são utilizadas a nível LATAM, não há adaptações para cada país.

Proposição 2: O backup dos sistemas deve ser armazenado em outro local. Em ambas as empresas os backups são armazenados em nuvem.

Proposição 3: Os processos e aplicações críticas da empresa devem ser mapeados. Não há conhecimento sobre este mapeamento na Empresa-Alpha. A Empresa-Beta tem um *Business Impact Analysis*.

Proposição 4: Devem ser realizadas avaliações de riscos e ameaças para o negócio. Na Empresa-Alpha, avaliações de riscos e ameaças são realizadas, porém não são abrangidos cenários de riscos lógicos, apenas físicos, como situações de incêndio, indisponibilidade de tecnologia e interrupção de fornecimento de serviços prestados por terceiros. Já na Empresa-Beta, há um *Business Impact Analysis*.

Proposição 5: **É preciso avaliar os impactos dos processos e aplicações críticas em função do tempo.** Os funcionários entrevistados não tinham conhecimento sobre a existência de um mapeamento de impacto na Empresa-Alpha. Já na Empresa-Beta, há um *Business Impact Analysis*.

Proposição 6: As partes interessadas devem ser mapeadas e comunicadas. Não há procedimento que compile todas as partes interessadas com a justificativa de que por se tratar de uma multinacional, existe um grande número destas tornando seu mapeamento complicado e um investimento não crítico.

Proposição 7: A organização deve realizar a monitoração de ambientes. A monitoração de ambientes é realizada constantemente, e há restrições de acessos aos funcionários em ambas as empresas.

Proposição 8: A organização deve manter ambientes de contingência. Na empresa Alpha existem ambientes de contingência, porém se houver um cenário de *Ransomware* a estratégia não é válida e a operação para. A empresa Beta possui e testa ambientes de contingência para este cenário constantemente.

4.4. Discussão

Ao analisar o cenário de duas grandes empresas no setor de consultoria foi possível identificar que apesar de bem estruturadas estas possuem um nível muito alto de confiança no conhecimento dos profissionais de seus ambientes, possuindo planos de intenções que não contemplam procedimentos de continuidade dos negócios, podendo ser uma problemática caso funcionários não acostumados com o ambiente e/ou de outras áreas precisem executar o plano sem domínio técnico, ocasionando um tempo maior de resolução de problemas, aumentando os prejuízos.

Visto que o plano de continuidade de negócios visa ser um procedimento mais claro e detalhado o possível para poder ter sua execução iniciada e entendida por qualquer profissional da organização, entende-se que isto é um risco pois em caso de desastres os profissionais que têm domínio do ambiente podem não estar disponíveis.

Essa problemática vem da autonomia das áreas consequente do tamanho das empresas, visto que, não há uma globalização de serviços e mapeamento e cada uma se torna responsável por estes, podendo haver divergências e duplicações. Este cenário pode ser consequente do crescimento da empresa, que pode vir da compra de outras menores - quando isso ocorre, geralmente não há uma revisão de aplicações, procedimentos e processos para elaboração de procedimentos detalhados que os incluam devido à necessidade de um alto investimento.

Ao questionar sobre problemáticas dentro do cenário de segurança da informação, ambos os gestores de TI entrevistados citaram que ao trabalhar com consultoria para outras empresas percebem uma relutância muito grande no investimento em políticas e procedimentos de contingência pois é muito comum as companhias acharem que cenários de ataque *Ransomware* é uma realidade distante, só se preocupando com a situação depois de sofrerem um ataque.

5. Conclusões

Empresas multinacionais são grandes alvos de criminosos cibernéticos pela possibilidade de grande ganho financeiro em um sequestro de dados, portanto é necessário um maior cuidado e investimento em Segurança da Informação. Investir em ações de continuidade e prevenção é o melhor caminho porque os criminosos podem vazar os dados mesmo com o pagamento sendo feito.

Esse investimento ganhou espaço no mercado recentemente por duas razões: cumprimento de requisitos de auditoria e a visibilidade de ataques cibernéticos na mídia.

Porém apenas ter procedimentos de contingência não é o suficiente. Estes precisam ser minimamente detalhados, testados, mantidos, revisados, atualizados, e recursos para contingenciamento devem ser mantidos, o que é um investimento constante, e é neste ponto que as empresas pecam.

Esta pesquisa possui como contribuições para teoria, novos eventos para serem pesquisados. A contribuição para prática é que gestores de TI e de processos possam incluir em seus planejamentos de continuidade as lacunas apresentadas neste trabalho. Futuros trabalhos incluem investigar outras empresas do mesmo setor e de setores complementares.

Referencial Bibliográfico

ABC, Diário do. (2021). Ataque cibernético prejudica vendas da CVC há cinco dias, SP. Editora Redação. https://www.dgabc.com.br/Noticia/3781374/ataque-cibernetico-prejudica-vendas-da-cvc-ha-cinco-dias.

Advisor, CISO. (2022). 72% dos ataques de *Ransomware* destroem o backup. https://www.cisoadvisor.com.br/72-dos-ataques-de-Ransomware-destroem-o-backup/.

Alecrim, E. (2020). Canon sofre ataque de ransomware e tem serviços derrubados. SP. https://tecnoblog.net/noticias/2020/08/07/canon-sofre-ataque-ransomware-maze-sistemas-sites-afetados/.

Alecrim, E. (2022). Malware sofisticado é descoberto em placas-mãe da Asus e Gigabyte. SP. https://tecnoblog.net/noticias/2022/07/27/malware-sofisticado-e-descoberto-em-placas-mae-da-asus-e-gigabyte/.

Alves, C. (2022). A importância da tecnologia da informação nas empresas, SP. http://www.webartigos.com/artigos/a-importancia-datecnologia-da-informacao-nas-empresas/95285.

Arntz, P. (2022). Nvidia, the ransomware breach with some plot twists. USA. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi046aCiOT_AhVFq5UCHTlAC3sQFnoECAoQAQ&url=https%3A%2F%2Fwww.malwarebytes.com%2Fblog%2Fnews%2F2022%2F03%2Fnvidia-the-ransomware-breach-with-some-plot-twists&usg=AOvVaw1WlegD2O4ASWFTqnGcDshK&opi=89978449

Augustene, A. (2022). Explicando o que é o ataque WannaCry. Lituânia. https://nordvpn.com/pt-br/blog/o-que-e-Ransomware-wannacry/.

Bertolli, E. (2020) Por que a negligência ainda causa tantos incidentes de segurança?, SP. https://www.varonis.com/pt-br/blog/por-que-a-negligencia-ainda-causa-tantos-incidentes-de-seguranca.

Burdova, C. (2022). What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?. London, United Kingdom. https://www.avast.com/c-eternalblue.

Burton, A. (2021). Bitsight Research Roundup 2021. Boston, USA. BitSight Researches. https://www.bitsight.com/blog/bitsight-research-roundup-2021

Branco, D. (2021). CVC segue com prejuízos em vendas devido a ataque de *Ransomware*. Canaltech. https://canaltech.com.br/seguranca/cvc-segue-com-prejuizos-em-vendas-devido-a-ataque-de-Ransomware-198352/.

Brasil, CNN. (2021). Ataques cibernéticos a empresas brasileiras crescem 220% no 1º semestre de 2021. RJ.

https://www.cnnbrasil.com.br/economia/ataques-ciberneticos-a-empresas-brasileiras-crescem-220-no-1-semestre-de-2021/.

Cabral, G (2021). Depêndencia Digital. Equipe Brasil Escola. GO. https://brasilescola.uol.com.br/psicologia/dependencia-digital.htm#:~:text=A%20depend%C3%AAncia%20digital%20%C3%A9%20a,proporciona%20prazer%20f%C3%ADsico%20%C3%A0%20pessoa.

Campos, J. (2020). Consultoria SGCN Gestão de Continuidade de Negócio: Estrutura do Sistema de Gestão de Continuidade de Negócio (SGCN). RJ. https://www.pdcati.com.br/plano-de-continuidade-de-negocios/.

CNN Brasil. (2022). Ataque cibernético fechou todas as fábricas da Toyota no Japão por um dia. https://www.cnnbrasil.com.br/economia/ataque-cibernetico-fechou-todas-as-fabricas-da-toyota-no-japao-por-um-dia/.

Chieco, B. (2019). Everis sofre ataque de ransomware. https://www.mentebinaria.com.br/noticias/portal-mente-bin%C3%A1ria/everis-sofre-ataque-de-ransomware-r182/

Cohen, G. (2021). Throwback Attack: WannaCry ransomware takes Renault-Nissan plants offline. USA. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline/.

Dermatini, F. (2022). 72% das empresas tiveram backups atingidos durante golpes de *Ransomware*. SP. https://canaltech.com.br/seguranca/72-das-empresas-tiveram-backups-atingidos-durante-golpes-de-Ransomware-216768/.

G1. (2021). JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. RJ. https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml?utm_source=linkedin&utm_medium=share-bar-desktop&utm_campaign=materias

Gaidargi, J. (2021). Renner é vítima de *Ransomware* – E se fosse você?. SP. https://www.infonova.com.br/seguranca/renner-ransonware-consequencias-solucoes/.

Gouveia, B, L. (2016). Conceitos de Segurança da Informação e sua gestão. 1.1. Porto, Portugal: UFP. https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf.

Federal, Governo. (2022). Programa De Privacidade E Segurança Da Informação (PPSI). DF. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf.

Hoff, C. (2022). *Ransomware*: o backup seguro é a sua última linha de defesa. https://www.veeam.com/blog/pt-br/secure-backup-Ransomware-defense.html.

IDC, International Data Corporation. (2021). IDC's 2021 Ransomware Study: Where You Are Matters!. https://www.idc.com/search/v3/?query=IDC%E2%80%99s%202021%20Ransomware%20Study:%20Where%20You%20Are%20Matters!&siteContext=IDC&tab=Blogs&sortBy=relevancy&languages=eng&publishedWithin=0&inSubscription=false.

ISO, International Standarts Organization: ISO/IEC 27001, 27001:2013 23 (2013). https://www.iso.org/standard/54534.html.

ISO, International Standarts Organization—ISO/IEC 27005, 27005:2012 23 (2012).
https://www.iso.org/standard/80585.html.

ISO, International Standarts Organization—ISO/IEC 22301, 27005:2012 23 (2012).
https://www.iso.org/standard/50038.html.

ISO, International Standarts Organization—ISO/IEC 22313, 22313:2012 23 (2012).
https://www.iso.org/standard/50050.html.

IT, Service. (2021). Como as variantes de *Ransomware* estão neutralizando os backups de dados. RJ. https://service.com.br/como-as-variantes-de-Ransomware-estao-neutralizando-os-backups-de-dados/.

Januário, M. (2017). Backup fora da Empresa, como fazer do jeito certo!. SP. https://www.wan.com.br/backup-fora-da-empresa-como-fazer-do-jeito-

certo/.

Kelly, M, S. The bizarre story of the inventor of *Ransomware*. CNN Business. USA. https://edition.cnn.com/2021/05/16/tech/Ransomware-joseph-popp/index.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fcnn_latest+%28RSS%3A+CNN+-+Most+Recent%29.

Ketzer, E. (2023). Poucas empresas na América Latina possuem plano de recuperação contra ransomware. https://tiinside.com.br/25/01/2023/poucas-empresas-na-america-latina-possuem-plano-de-recuperacao-contra-ransomware/ .

Liska, A. & Gallo, T. (2019). SP. *Ransomware*: Defendendo-se da extorsão digital, SP: Editora Novatec. https://propi.ifto.edu.br/ocs/index.php/jice/10jice/paper/viewFile/9705/4320.

Macarenhas, N. & Tenório P. & Araújo, W. (2019). Segurança da Informação: Uma visão sistémica para implantação em organizações. Editora UFPB, 160 p. ISBN 978-85-237-1473-4.

Martins, L. (2022). Ataques de ransomware estão mais complexos e caros para empresas. https://itforum.com.br/noticias/ataques-de-ransomware-estao-mais-complexos-e-caros-para-empresas/

Nagli. (2020). Pandemia na Pandemia: A Escalada de Ataques Cibernéticos pós Covid-19. Editora Brazilian Journal of Development, ISSN: 2525-8761. DOI 10.34117/bjdv8n4-375. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/46768/pdf .

Silva, S., & Glória Júnior, I. (2023). Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital. Journal of Technology & Information, 3(2). Disponível em: http://www.jtni.com.br/index.php/JTnI/article/view/84

Nunes, E. (2023). Ransomware: Confira como Grandes Empresas Lidaram com o Ataque. SP. VXN. https://vnx.partners/ransomware-confira-casos-em-grandes-empresas/

PrivacyTech. (2021). Kia Motors sofre ataque de ransomware de US $ 20 milhões. https://privacytech.com.br/noticias/kia-motors-sofre-ataque-de-

ransomware-de-us-20-milhoes,388292.jhtml.

Redação. (2020). Software AG confirma ransomware e vazamento de dados. SP. Ciso Advisor. https://www.cisoadvisor.com.br/software-ag-confirma-ransomware-e-vazamento-de-dados/ .

Report, Security. (2022). Brasil foi o 5º país com mais ataques cibernéticos em 2021. SP. Conteúdo Editorial. https://www.securityreport.com.br/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.ZCisl3vMLIU .

Silva, Bruno. (2023). Ferrari sofre ataque cibernético e dados de clientes são expostos. SP. Security Report. https://www.securityreport.com.br/ferrari-sofre-ataque-cibernetico-e-dados-de-clientes-sao-expostos/

Spaniol, B. (2019). Como o 11/9 mudou a trajetória da proteção de dados, SP. http://www.aliancatecnologia.com/conteudo/2015/09/como-o-119-mudou-a-protecao-de-dados .

Soares, L. (2021). Hackers invadem Acer com ransomware e exigem US$ 50 milhões como resgate. SP. https://olhardigital.com.br/2021/03/19/seguranca/hackers-invadem-acer-com-ransomware-e-exigem-us-50-milhoes-como-resgate/ .

Sullivan, E. (2021). Política de Continuidade de Negócios. Editora SearchStorage. USA. https://www.computerweekly.com/br/definicoe/Politica-de-continuidade-de-negocios.

Tadeu, E. (2023). Grupo Fleury sofre novo ataque cibernético em menos de um ano. SP. Ciso Advisor. https://www.cisoadvisor.com.br/grupo-fleury-sofre-novo-ciberataque-em-menos-de-um-ano/

TCU, Tribunal de Contas da União. (2012). Boas Práticas em Segurança da Informação. Brasília: Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p. v. 4.

Telecom, A. (2021). Qual é a importância da TI estratégica para o negócio? Entenda!. AL. https://blog.aloo.com.br/ti-estrategica/ .

Teófilo, R. & Freitas, L. & Seget. (2021). O uso de tecnologia da informação como ferramenta de gestão. SP. https://www.aedb.br/seget/arquivos/artigos07/652_SEGET%20roro.pdf .

Tutida, D. (2021). 5 atribuições do departamento de TI: do suporte à gestão. https://encontreumnerd.com.br/blog/atribuicoes-do-departamento-de-ti .

UPX. (2021). *Ransomware*: entenda o caso que abalou a Renner e conheça os diferentes tipos de ciberataques. https://upx.com/post/Ransomware-renner/ .

Winder, D. (2022). Cisco Hacked: Ransomware Gang Claims It Has 2.8GB Of Data. Forbes. https://www.forbes.com/sites/daveywinder/2022/08/13/cisco-hacked-ransomware-gang-claims-it-has-28gb-of-data/?sh=5f3b485e4043 .

Yasar, K. (2021). What You Need to Know About the Cognizant Maze Ransomware Attack. USA. https://www.makeuseof.com/know-about-cognizant-maze-ransomware/ .

Zandt, F. (2021). The Industries Most Affected by Ransomware. https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/ .

APÊNDICE A – Protocolo de Entrevista

O protocolo de entrevistas aplicado aos respondentes possui os seguintes passos:

- **Passo 1.** Realizar a introdução sobre o pesquisador e a pesquisa a ser feita;
- **Passo 2.** Descrever como será conduzida a entrevista;
- **Passo 3.** Ressaltar a preocupação da confidencialidade e privacidade dos entrevistados. Explicar como os dados coletados serão mantidos no anonimato;
- **Passo 4.** Iniciar as questões (Apêndice B);
- **Passo 5.** Perguntar se há alguma outra observação que será interessante para a pesquisa;
- **Passo 6.** Finalizar a entrevista.

APÊNDICE B – Questionário

Conteúdo: Planejamento estratégico

#	Pergunta
Q01	Existem políticas de Segurança da informação? Quais?
Q02	Há algum plano de respostas a incidentes?

Conteúdo: Planejamento tático

#	Pergunta
Q03	Como é realizada a monitoração de ambientes?
Q04	Existe um mapeamento dos processos críticos do negócio?
Q05	Em caso de interrupção, como funcionam os ambientes de contingência?
Q06	A empresa faz avaliação de riscos e ameaças existentes a continuidade da operação?
Q07	Existem avaliações de impactos legais, de imagem e financeiros em caso de disrupção?
Q08	É mantida uma rotina de conscientização e treinamentos?
Q09	Quais os principais aspectos existentes na política de backups?

Conteúdo: Comunicação

#	Pergunta
Q10	Foram definidas estratégias de comunicação com fornecedores, clientes e mídia em caso de disrupção?

Conteúdo: Histórico

#	Pergunta
Q11	Qual é a sua experiência com ataques *Ransomware*?
Q12	Como foi o procedimento de respostas?

Q13	Quais foram as mudanças implementadas após o ocorrido?
Q14	Como profissional do mercado de segurança da informação, de acordo com a sua experiência em consultoria, como você enxerga o cenário atual das empresas em relação à planos de continuidade e procedimentos de contingência em casos de *Ransomware*?