ACME Truques Financeiros

RELATÓRIO DE GESTÃO DE AMEAÇAS, VULNERABILIDADES E RISCO

Versão	Data	Responsável	Revisor Responsável	Descrição
1.0	20/12/2024	Adyellen Alves	Daniel Durante	Elaboração do relatório de gestão de ameaças, vulnerabilidade e riscos.
1.1	21/12/2024	Adyellen Alves	Daniel Durante	Adição das referências bibliográficas e agradecimentos

1. INVENTÁRIO DOS ATIVOS TECNOLÓGICOS

Descrever as ameaças, vulnerabilidades e riscos identificados no ambiente da ACME Truques Financeiros, com objetivos de disponibilizar as medidas mitigatórias e avaliar o impacto no negócio, incluindo ativos tecnológicos, processos e práticas de segurança.

1.1. Contexto

A ACME Truques Financeiros foi alvo de um ataque cibernético que resultou na exposição de dados sensíveis de clientes. Como uma empresa listada na bolsa, é crucial atender às exigências da CVM e BACEN para evitar futuras ocorrências, garantir a confiabilidade e transparência junto aos clientes e investidores.

1.2. Objetivos

Implementar e detalhar processos fundamentais de cibersegurança, conforme descritos abaixo:

- Gestão de Ameaças, Vulnerabilidade e riscos: Garantindo que todas as ameaças, vulnerabilidades e riscos sejam identificadas, avaliadas e tratadas;
- Plano de ação: Definição de um plano estratégico para mitigar os riscos

2. INVENTÁRIO DOS ATIVOS TECNOLÓGICOS

- 2 Firewalls
- 2 Servidores Web
- 2 Roteadores
- 1 Servidor de Banco de Dados
- 2 Servidores de Desenvolvimento
- 1 Servidor de Diretório (AD)
- 2 Servidores de Aplicação
- 1 Servidor de Email
- 1 Sistema de acesso às faturas de cartões de crédito (clientes e funcionários)
- 1 Sistema de processamento de números de cartões de crédito (funcionários apenas)
- 100 Estações de Trabalho (notebooks) com acesso remoto via VPN

Observações:

- Todos os servidores e sistemas estão na mesma rede.
- O servidor de banco de dados armazena informações de cartões de crédito.

3. GESTÃO DE AMEAÇAS

Tem como objetivo listar as ameaças identificadas no ambiente, classificando-as conforme a sua natureza (internas, externas, naturais, etc.).

3.1. Livro caso de Uso

#	Nome do Caso de Uso	Regra	Fonte de Dados	Probabilidade	Impacto	Gravidade
1	Acesso não autorizado	Identificar múltiplas tentativas de Login com falhas de um mesmo IP	Logs de Active Directory ou firewall	Alta	Alta	Alta
2	Extração de dados sensíveis	Identificar o tráfego de saída de informações para emails ou servidores externos	Logs de Firewall ou proxies	Média	Alta	Alta
3	Tentativa de degradação do serviço via DDos - Bot Herder	Identificar aumento abrupto de 50% acima de requisições esperadas	Logs do CDN	Alta	Alta	Alta
4	Tentativas de Phishing em E-mails	Identificação de e-mails e presença de anexos maliciosos	Logs de email (Microsoft Defender) e logs de tráfego Web (Firewall ou Akamai)	Alta	Alta	Alta
5	IPs maliciosos	Identificar e correlacionar IPs que estão em blacklists	Firewalls, Akamai, IDS/IPS	Média	Alta	Alta
6	Fraude de transações	Identificar e correlacionar transações suspeitas através do perfil do cliente	Logs de transações	Alta	Alta	Alta
7	Vulnerabilidade em APIs	Identificar aumento abrupto de requisições suspeitas e excesso de falhas	Logs de APIs, Kibana, WAF	Alta	Alta	Alta
8	Manipulação de versionamento de código - insider	Identificar novos clientes que não passaram pela jornada completa de criação de conta	Logs de APIs, WAF	Baixa	Média	Média

9	Conexão de dispositivos USB não autorizados	Identificar o plugin de dispositivos USB	Logs DLP	Média	Média	Média
10	Detectar Ransomware	Identificar e bloquear tentativas de malware	Firewalls e IDS/IPS	Alta	Alta	Alta
11	Vulnerabilidade de Software	Identificar vulnerabilidades no software	CVE	Alta	Alta	Alta
12	Treinamento em Segurança	Realizar treinamento de segurança e conscientização	Plataformas de e-learning e simulação de phishing	Alta	Média	Média
13	Resposta a Incidentes	Monitoração de dados em tempo real e alertas de segurança	Logs de Dynatrace, SIEM	Alta	Alta	Alta
14	Monitoramento de Users com acesso privilegiados - Insider	Monitoração das atividades e acessos simultâneos	Logs do IAM, SIEM, firewall	Alta	Alta	Alta
15	Gerenciamento de Patches	Monitoração e aplicação de patches de segurança	Ferramenta de gerenciamento de patches	Média	Alta	Alta

3.2. Tecnologias de mercado monitoração e/ou tratamentos de ameaças cibernéticas

#	Fabricante	Produto	Justificativa
Firewall	Fortinet FortiGate	Fortinet	Ferramenta robusta na qual oferece funcionalidades como: inspeção de pacotes, controle de aplicativos e proteção contra ameaças de rede.
DLP	Symantec Data Loss Prevention	Broadcom	Ferramenta que fornece proteção de dados, com possibilidade de criação de políticas de DLP e com isso diminuindo complexibilidade. Além de facilitar a conformidade com as leis globais de proteção de dados e requisitos regulatórios.
EDR	CrowdStrike Falcon	CrowdStrike	Fornece proteção durante todo o ciclo de vida da ameaça, combinando aprendizado de máquina, IA e análise comportamental. Eliminando a complexidade e simplificando a implantação por ser nativo na nuvem. Além de ser reconhecido por sua eficácia, rapidez e resposta rápida a

			ameaças de endpoints.

4. GESTÃO DE VULNERABILIDADES

Tem como objetivo detalhar as vulnerabilidades encontradas nas infraestruturas, sistemas, processos e pessoas.

4.1. Vulnerabilidades, detecção e mitigação

#	Vulnerabilidade	Detecção	Mitigação	CVE	Pontuações CVSS	CWE
1	SQL Injection	Detectado através de WAF tráfego malicioso com tentativas de SQL injection	Criação de políticas em gateways, atualização de patches, boas práticas de codificação segundo a OWASP	CVE-2024-56053	7.6	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
2	Vazamento de dados de APIs	Monitoramento de logs com ferramentas que analisam o tráfego de APIs	Implementação de políticas de segurança com autenticação e autorização adequadas, require SSL/TLS, requerimento de certificado digital	CVE-2021-44228	9.3 e 10.0	CWE-20, CWE-400, CWE-502, CWE-917
3	Controle de Acesso Quebrado (Broken Access Control)	Detectado através de logs de acesso com falhas e padrões suspeitos	Utilizar autenticação de múltiplo fator (MFA), monitorar logs de acesso	CVE-2024-22234	7.4	CWE-284: Improper Access Control
4	Escalação de Privilégios Vertical e Horizontal	Detectado através de monitoramento de políticas de segurança de controle de acesso e testes de penetração	Realizar o princípio do menor privilégio, aplicar MFA e aplicação de patches	CVE-2024-56053	7.6	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

5	Falta de Inspeção Profunda de Pacotes nos Firewalls	Detectado através de testes de penetração, análise dos logs de Firewall e monitoração de tráfego de rede	Atualizar e configurar firewalls adequadamente, segmentação de rede, usar ferramentas de detecção e prevenção de intrusão (IDS/IPS)	CVE-2020-1988	6.8 e 8.8	CWE-352: Cross-Site Request Forgery (CSRF)
6	Falta de Segmentação da Rede	Detectado através de testes de penetração	Implantar firewall, VPNs, aplicação de microsegmentação	CVE-2020-0601	5.8 e 8.1	CWE-295: Improper Certificate Validation
7	VPN com Autenticação de Dois Fatores Ausente	Detectado através de testes de penetração e auditoria de segurança	Habilitar autenticação de dois fatores utilizando OTP ou Google Authenticator, aplicar expiração de senhas e criar regras para senhas fortes	CVE-2020-10189	10.0 e 9.8	CWE-502: Deserialization of Untrusted Data
8	Falta de Criptografia de Dados Sensíveis	Detectado através de testes de penetração e auditoria de segurança	Implementação de criptografia em repouso e em trânsito utilizando protocolos TLS/SSL, auditoria e monitoração do acesso ao banco de dados	CVE-2020-14181	5.0 e 5.3	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
9	Antivírus Desatualizados	Detectado através de incidentes de segurança e testes de penetração	Implementação de atualizações automáticas, proteção em camadas, auditorias regulares e simulações de malware	CVE-2020-1350	10.0	CWE: não se aplica
10	Porta RDP Aberta e Exposta	Detectado através de monitoramento de tráfego de rede e teste de intrusão de IDS/IPS	Fechar a porta RDP através de firewall, utilizar VPN, MFA, atualização de patches	CVE-2018-0841	9.3 e 8.8	CWE: não se aplica
11	XSS (Cross-Site Scripting)	Detectado através de monitoramento de logs e varredura	Uso de headers (HTTPS) e certificados,	CVE-2016-10033	7.5 e 9.8	CWE-77: Improper Neutralization of Special Elements

		com burp suite	monitoração de logs, configuração de autenticação e autorização			used in a Command ('Command Injection')
12	Ausência de Plano de Resposta a Incidentes	Detectado através de auditoria de segurança	Implementar SIEM, realizar testes de penetração regularmente	CVE-2021-22986	10.0	CWE-918: Server-Side Request Forgery (SSRF)
13	Falta de Testes Regulares de Penetração	Falta de conformidade com PCI DSS ou ISO 27001	Estabelecer uma política de testes de penetração regulares, teste em diferentes camadas, contratar consultorias para testes de penetração	CVE-2021-22986	10.0	CWE-918: Server-Side Request Forgery (SSRF)
14	Sistemas Legados sem Suporte e Atualizações	Detectado através de auditoria de segurança e logs de segurança dos servidores	Aplicação de patches, monitoramento contínuo, conscientização interna para versionamento dos sistemas legados	CVE-2017-0144	9.3	CWE-306, CWE-94
15	Backups Não Criptografados ou Armazenados no Mesmo Ambiente	Detectado através de auditoria de segurança	Aplicação de criptografia em todos os backups, automatização de backups e auditorias frequentes	CVE-2021-22910	9.8	CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)
16	Configuração de Roteadores com Credenciais Padrão	Detectado através de análise de configuração de roteador e testes de penetração	Aplicação de configuração adequada	CVE-2020-10135, CVE-2019-14899	4.8	CWE-290, CWE-757, CWE-300
17	Vulnerabilidade XXE (XML External Entity)	Detectado através de análise de code review e análise de logs	Utilização de parses seguros	CVE-2017-12149	7.5	CWE-502: Deserialization of Untrusted Data
18	Vulnerabilidade CSRF (Cross-Site Request Forgery)	Detectado através de análise de code review e análise de logs	Utilização de tokens, autenticação de sessão	CVE-2018-11776	9.3	CWE: não se aplica

19	Man-in-the-Middle (MITM)	Detectado através de monitoramento de certificados SSL e análise de padrões de tráfego anômalo	Verificação de certificados SSL/TLS, uso de autenticação de múltiplos fatores (MFA)	CVE-2019-1234	7.5	CWE-300: Improper Authorization
20	Zero-Day Exploits	Detectado através de monitoramento de comportamento anômalo, testes de penetração e auditoria de segurança	Aplicação de patches, uso de detecção de intrusão e prevenção (IDS/IPS), uso de WAF	CVE-2024-0001	9.3	CWE-552: Exposure of Information Through Sent Data

4.2. Tecnologias de mercado para detecção e orquestração de vulnerabilidades

#	Fabricante	Produto	Justificativa
1	CrowdStrike	Falcon Spotlight	Falcon Spotlight é uma solução de gerenciamento de vulnerabilidades que integra detecção em tempo real e orquestração de resposta.
2	Palo Alto Networks	Cortex XSOAR	Cortex XSOAR é uma plataforma de orquestração de segurança que integra a detecção de vulnerabilidades com automação de resposta. A solução permite que as equipes de segurança coordenem e automatizem respostas a incidentes, gerenciem vulnerabilidades e melhorarem o tempo de remediação. Ele é altamente flexível, permitindo integrações com várias fontes de dados de segurança, como sistemas de SIEM, firewalls e outras ferramentas de gerenciamento de vulnerabilidades.
3	Qualys	Qualys Vulnerability Management	Plataforma baseada em nuvem, fornece visibilidade em tempo real, integração com outras soluções de segurança e automação para detecção e remediação.

5. GESTÃO DE RISCOS

Tem como objetivo realizar a combinação de ameaça e vulnerabilidade identificada, avaliando o risco que ela representa para a organização..

5.1. Sugestão de Metodologia/Framework:

1. **NIST (RMF):**

O Risk Management Framework (RMF) fornece um processo que integra atividades de gerenciamento de risco de segurança, privacidade e cadeia de suprimentos cibernética no ciclo de vida de desenvolvimento do sistema. A abordagem baseada em risco para seleção e especificação de controle considera eficácia, eficiência e restrições devido a leis, diretivas, ordens executivas, políticas, padrões ou regulamentos aplicáveis. O gerenciamento de risco organizacional é fundamental para programas eficazes de privacidade e segurança da informação; a abordagem RMF pode ser aplicada a sistemas novos e legados, qualquer tipo de sistema ou tecnologia (por exemplo, IoT, sistemas de controle) e dentro de qualquer tipo de organização, independentemente do tamanho ou setor.

Preparar	Atividades essenciais para **preparar** a organização para gerenciar riscos de segurança e privacidade
Categorizar	**Categorizar** o sistema e as informações processadas, armazenadas e transmitidas com base em uma análise de impacto
Selecione	**Selecione** o conjunto de controles NIST SP 800-53 para proteger o sistema com base na(s) avaliação(ões) de risco
Implement	**Implementar** os controles e documentar como os controles são implantados
Avaliar	**Avaliar** para determinar se os controles estão em vigor, operando conforme o esperado e produzindo os resultados desejados
Autorizar	Um alto funcionário toma uma decisão baseada em risco para **autorizar** o sistema (a operar)
Monitor	**Monitorar** continuamente a implementação do controle e os riscos ao sistema

2. **OCTAVE (Avaliação Operacionalmente Crítica de Ameaças, Ativos e Vulnerabilidades):**

É um framework com foco em segurança cibernética e avaliação de vulnerabilidades. A metodologia é voltada para a avaliação de riscos críticos operacionais e tecnológicos, identificando ativos essenciais e ameaças potenciais.

Fases OCTAVE

Fase 1: Criar Perfis de Ameaças Baseados em Ativos – Esta é uma avaliação organizacional. A equipe de análise determina o que é importante para a organização (ativos relacionados à informação) e o que está sendo feito atualmente para proteger esses ativos. Em seguida, a equipe seleciona os ativos mais importantes para a organização (ativos críticos) e descreve os requisitos de segurança para cada ativo crítico. Por fim, ele identifica ameaças a cada ativo crítico, criando um perfil de ameaça para esse ativo.

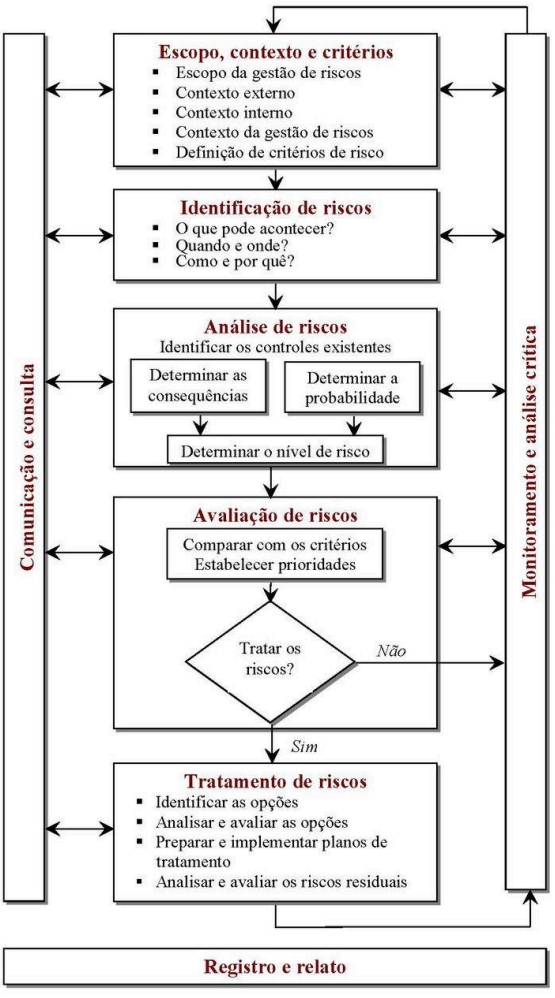
Fase 2: Identificar Vulnerabilidades de Infraestrutura – Esta é uma avaliação da infraestrutura de

informação. A equipe de análise examina rede caminhos de acesso, identificando classes de componentes de tecnologia da informação relacionados a cada ativo crítico. A equipe então determina até que ponto cada classe de componente é resistente a ataques de rede.

Fase 3: Desenvolver Estratégia e Planos de Segurança – Durante esta parte da avaliação, a equipa de análise identifica os riscos para a organização e decide o que fazer em relação aos mesmos. A equipe cria uma estratégia de proteção para a organização e planos de mitigação para abordar os riscos para os ativos críticos, com base em uma análise das informações coletadas.

5.2. Etapas do processo de gestão de riscos, objetivos e resultados esperados (ISO 31000)

Extraído do Manual de Implementação da ISO 31000:2018 *[clique para mais informações]*



Processo de Gestão de Riscos - Detalhamento

Risk Tecnologia Editora

- **Etapa 1: Comunicação e consulta**

Já que a gestão de riscos deve ser inclusiva, este é o momento onde as partes interessadas apropriadas serão conscientizadas para entenderem os riscos (comunicação) e retornarão com informações que auxiliarão a tomada de decisão (consulta).

- **Etapa 2: Escopo, contexto e critérios**

Nesta etapa ocorre a personalização do processo de gestão de riscos, pois a empresa deve definir quais atividades estarão cobertas pelo escopo e também qual é o contexto interno e externo destas atividades.

- **Etapa 3: Avaliação dos riscos**

Esta fase contempla a identificação, análise e avaliação dos riscos. Identificar significa encontrar, reconhecer e descrever os riscos. A análise consiste em compreender a natureza dos riscos e suas características, considerando, entre outras informações, a probabilidade, consequências, fatores temporais e volatilidade. Já a avaliação é a comparação entre os resultados da análise com os critérios que a empresa estabeleceu na etapa 2, servindo de suporte para o processo decisório e podendo levar a empresa a:

➔ Considerar opções de tratamento dos riscos;
➔ Realizar análises adicionais;
➔ Manter os controles existentes;
➔ Reconsiderar os objetivos.

- **Etapa 4: Tratamento dos riscos**

Aqui a empresa deve selecionar e implementar opções para abordar os riscos, avaliando a eficácia da ação adotada e decidindo se o risco remanescente é aceitável ou se deve ser realizado tratamento adicional.

É importante ressaltar também que as opções abaixo abrangem riscos que têm consequências negativas e / ou positivas. As opções de tratamento são as seguintes:

➔ evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;
➔ assumir ou aumentar o risco de maneira a perseguir uma oportunidade;
➔ remover a fonte de risco;
➔ mudar a probabilidade;
➔ mudar as consequências;
➔ compartilhar o risco (por exemplo, por meio de contratos, compra de seguros);
➔ reter o risco por decisão fundamentada.

- **Etapa 5: Monitoramento e análise crítica**

A empresa deve assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo de gestão de riscos de maneira contínua e em todos os estágios do processo e isso é tratado nesta etapa.

- **Etapa 6: Registro e relato**

A ISO 31000 também enfatiza a importância de documentar o processo de gestão de riscos e os seus resultados, considerando as diferentes partes interessadas e, a partir disso, a empresa terá uma base para melhorar a comunicação e facilitar a tomada de decisão.

5.3. Tecnologia para Gestão de risco

Fabricante	Produto	Justificativa
Galvanize	Galvanize Risk Management Software	A Galvanize é amplamente utilizada por grandes organizações devido à sua capacidade de integrar análise de dados e conformidade regulatória, tornando-a uma escolha popular para empresas que enfrentam riscos complexos.

6. AGRADECIMENTOS

A realização deste relatório de gestão de ameaças, vulnerabilidades e risco é resultado de um longo percurso de aprendizado, dedicação e apoio recebido de diversas pessoas, as quais gostaria de expressar minha profunda gratidão.

Primeiramente, agradeço a Deus, permitindo-me superar os desafios e chegar até aqui.

À minha família, pelo amor incondicional, paciência e compreensão. Pois são a minha base e fonte de motivação constante para persistir e alcançar este objetivo.

Ao meu e professor, Dan Durante, que compartilharam seus conhecimentos, me guiou com sabedoria e generosidade. Além da enorme paciência e disponibilidade para tirar dúvidas. Suas orientações foram fundamentais para a construção deste trabalho e para o meu crescimento acadêmico e profissional.

A um grande amigo, Renato, que mesmo não sendo da área de cibersegurança, se disponibilizou em ler o relatório e se colocar como "empresa" para me dar feedback se o mesmo estava de fácil entendimento.

Agradeço também à instituição de ensino, por proporcionarem um ambiente de aprendizado enriquecedor e pelas oportunidades oferecidas.

Por fim, sou grato(a) a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho. Sem o apoio e a contribuição de cada um de vocês, esta etapa não teria sido possível.

Com gratidão,

Adyellen Alves.

7. REFERÊNCIAS BIBLIOGRÁFICAS

1. **CROWDSTRIKE**. *Falcon Spotlight*. 2023. Disponível em: https://www.crowdstrike.com/pt-br/resources/data-sheets/falcon-spotlight/.

2. **BROADCOM**. *Data Loss Prevention*. 2023. Disponível em: https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention.

3. **CROWDSTRIKE**. *Why CrowdStrike*. 2023. Disponível em: https://www.crowdstrike.com/en-us/why-crowdstrike/.

4. **FORTINET**. *Next Generation Firewall*. 2023. Disponível em: https://www.fortinet.com/br/products/next-generation-firewall.

5. **WEGALVANIZE**. *Wegalvanize*. 2023. Disponível em: https://www.wegalvanize.com/.

6. **NIST**. *Risk Management Framework (RMF)*. 2023. Disponível em: https://csrc.nist.gov/projects/risk-management/about-rmf.

7. **NIST**. *National Institute of Standards and Technology*. 2023. Disponível em: https://www.nist.gov/.

8. **CVE DETAILS**. *CVE Details*. 2023. Disponível em: https://www.cvedetails.com/index.php.

9. **OWASP**. *OWASP Code Review Guide*. 2023. Disponível em: https://owasp.org/www-project-code-review-guide/.

10. **MITRE**. *Common Weakness Enumeration (CWE)*. 2023. Disponível em: https://cwe.mitre.org/.

11. **BLOG DA QUALIDADE**. *Diretrizes para Gestão de Riscos com Base na ISO 31000*. 2023. Disponível em: https://blogdaqualidade.com.br/diretrizes-para-gestao-de-riscos-com-base-na-iso-31000/.

12. **ISO 31000**. *Processo de Gestão de Riscos*. 2023. Disponível em: https://iso31000.net/processo-de-gestao-de-riscos/#:~:text=Essas%20tr%C3%AAs%20etapas%20s%C3%A3o%3A&text=Comunica%C3%A7%C3%A3o%20e%20consulta%20%C3%A0s%20partes,nos%20'outputs'%20do%20processo.