SEGURANÇA DE DADOS EM APLICAÇÃO WEB

DATA PROTECTION IN WEB APPLICATION

Wiliam Carlos Galvão, FATEC Santana de Parnaíba,
wiliam.galvao@fatec.sp.gov.br

Elson Santos da Costa, FATEC Santana de Parnaíba,
costaelson@hotmail.com

Resumo

O mundo está cada vez mais digital, independentemente do setor, seja na área hospitalar, na indústria, no agronegócio, nos serviços, entre outros. Em todos esses campos, a tecnologia está sendo utilizada para aumentar a eficiência, melhorar a competitividade e obter uma compreensão mais profunda dos clientes. Enormes volumes de dados fluem pela rede, incluindo muitos dados confidenciais e estratégicos que requerem precauções e uma estratégia de segurança sólida para garantir que somente os devidamente autorizados possam acessá-los, modificá-los ou atualizá-los conforme necessário. A Lei de Proteção de Dados (LGPD) foi estabelecida com o objetivo de padronizar a maneira como os dados são manipulados e tratados. Ela exige que as empresas implementem políticas internas padronizadas para cumprir a lei e proteger suas informações contra vazamentos ou acessos não autorizados, atribuindo direitos e responsabilidades claros. Nesta pesquisa, foi empregada a metodologia de Estudo de Caso, por meio da realização de testes de vulnerabilidade para identificar possíveis falhas na aplicação. Após a análise dos resultados, foram identificadas sete vulnerabilidades, e foram propostas soluções. Isso destaca a importância de adotar boas práticas, juntamente com normas e leis, a fim de criar um ambiente seguro que reduza os riscos e previna possíveis ataques.
Palavras-chave: Segurança da Informação, Ataques Cibernéticos, LGPD, Lei Geral de Proteção de Dados, ISO.

Abstract

The world is becoming increasingly digital, regardless of the sector, whether it's in healthcare, industry, agribusiness, services, and others. In all of these fields, technology is being used to enhance efficiency, improve competitiveness, and gain a deeper understanding of customers. Enormous volumes of data are flowing through the network, including a lot of confidential and strategic data that require precautions and a robust security strategy to ensure that only those duly authorized can access, modify, or update them as needed. The Data Protection Law (LGPD) was established with the aim of standardizing how data is handled and treated. It requires companies to implement standardized internal policies to comply with the law and protect their information from leaks or unauthorized access, assigning clear rights and responsibilities. In this research, the Case Study methodology was employed by conducting vulnerability tests to identify potential application flaws. After analyzing the results, seven vulnerabilities were identified, and solutions were proposed. This underscores the importance of adopting best practices, along with standards and laws, in order to create a secure environment that reduces risks and prevents potential attacks.

Keywords: Information Security, Cyber Attacks, LGPD, General Data Protection Law, ISO.

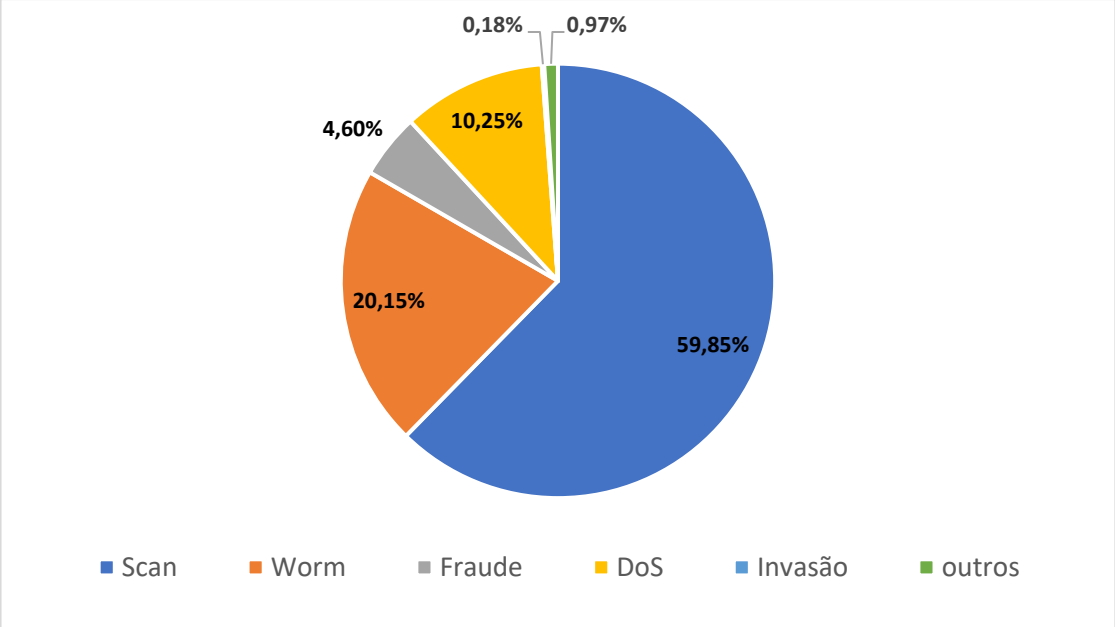
1. Introdução

Atualmente, as empresas reconhecem que não é suficiente oferecer um produto de qualidade a um preço competitivo. É necessário ir além disso. Isso implica em conhecer profundamente o cliente, compreender seus gostos e necessidades, aproximá-lo e transformá-lo em mais do que apenas um cliente; ele se torna um parceiro que agrega valor ao produto ou serviço, proporcionando experiências que fortalecem sua fidelidade à marca (KOTLER & KELLER, 2012).

Conforme Kotler, Hermawan e Iwan (2021) apontam, o avanço da tecnologia trouxe consigo maior facilidade e rapidez nos processos, tornando-se um aliado valioso para as empresas na capacidade de compreender, quase em tempo real, as demandas de seus clientes. Essa compreensão possibilita o desenvolvimento de campanhas direcionadas para atrair e manter a fidelidade desses clientes.

A segurança dos dados é uma grande preocupação, no ano de 2021, houve um aumento de 950% de ataques cibernéticos em relação há 2020 (Fortinet, 2022). No Brasil em 2020 a CERT.br, Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil em seu relatório final, indica um aumento nos números de incidentes, demonstrado na figura 1, São dados preocupantes que indicam alto risco de roubos ou acessos não autorizados à dados sigilosos (CERT.BR, 2022).

Figura 1 – Incidentes Reportados



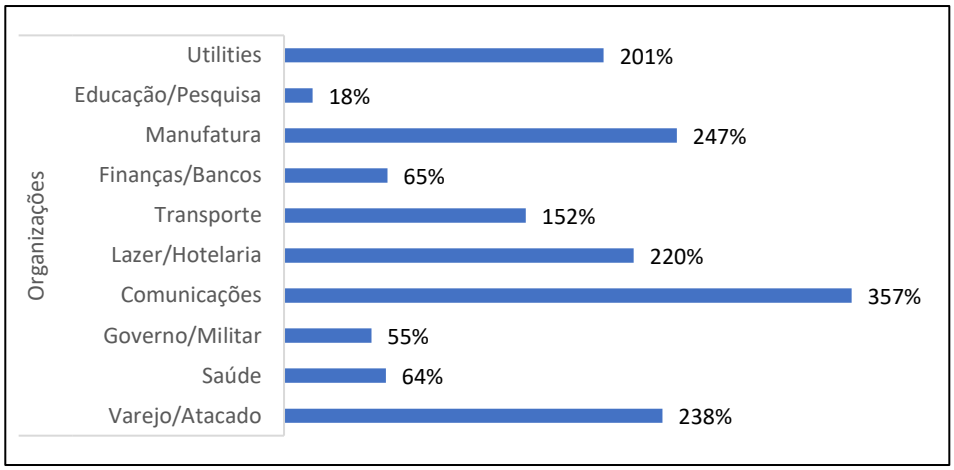
Fonte – Realizado pelo próprio autor

A Figura 1 demonstra os principais incidentes e a respectiva proporção relatados no período de janeiro de 2020 à dezembro de 2020.

O relatório de segurança Fortinet (2022) cita que o Brasil foi o segundo país da América Latina a sofrer mais ataques cibernéticos na ordem de 88,5 bilhões. Este maior volume tem ligação direta pelo aumento do trabalho remoto, impulsionado pela pandemia.

No Brasil, houve um aumento na ordem de 77% de ataques às organizações, no período de 2020 a 2021 (Check Point Research, 2021). A Figura 2 indica os ataques separadas por organizações.

Figura 2 – Incidentes Reportados



Fonte – Realizado pelo próprio autor

Apesar da alta de ataques, as empresas precisam entender e alinhar suas estratégias em conjunto com as tecnologias na implementação de táticas e operações de marketing para atrair clientes, oferecendo mais que apenas produtos ou serviços, desta forma terão clientes fiéis a marca (KOTLER; HERMAWAN; IWAN, 2021).

Neste contexto, este artigo busca responder à **Q**uestão de **P**esquisa (**QP**): “Os dados manuseados nas aplicações *web* estão seguros contra-ataques cibernéticos e vazamentos de informações?”. Os objetivos são: (1) Apresentar métodos de segurança para mitigar os riscos; (2) Discutir sua eficiência.

2. Referencial Teórico

2.1. International Organization for Standardization

InternationalOrganization for Standardization (ISO), possui sede na Suíça desde a sua criação no ano de 1946, 160 países são associados a ISO, sendo representados pelos seus órgãos de normalização (INMETRO, 2022).

O objetivo da organização Internacional de Normalização é criar normas que incentivam as boas práticas de gestão, avanço tecnológico e propagar conhecimentos para manter um padrão a ser seguido e assim facilitar o comércio mundial (INMETRO, 2022).

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2022). As normas ISO são critérios estabelecidos entre os membros associados que visam padronizar as ações, atividades e processos com o objetivo de melhorar eficiência, reduzir falhas na produção, aumentar a qualidade de produtos e serviços e garantir a segurança dos sistemas de acordo com os princípios de Confidencialidade, Integridade e Disponibilidade (CIA) (ISO, 2022).

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. (2022). A ABNT representa o Brasil na organização ISO e é uma instituição privada sem fins lucrativos. Além disso, a ABNT participa da Comissão Pan-Americana de Normas Técnicas (COPANT) e é membro da Comissão Eletrotécnica Internacional (IEC) (ABNT, 2022).

A ABNT trabalha na certificação de produtos e desenvolve estudos, pesquisas para atender as necessidades das empresas brasileiras para melhorias nos processos, qualidade, melhoria de eficiência e diminuição dos impactos ambientais (ISO, 2022).

2.2. Ciberataques

Os ciberataques consiste em obter acessos, roubar ou danificar arquivos que possuam algum tipo de valor, estes ataques podem ocorrem em organizações privadas, públicas ou até com pessoas físicas, se utilizando de conhecimento técnicos avançados de programação e lógica (CARVALHO, 2005).

Os oito primeiros meses do ano de 2021, houve um aumento de 23% de ataques no Brasil, identificando uma tendência de aumento em relação ao ano anterior, colocando o país como um dos focos de crimes virtuais (KASPERSKY, 2021).

Esse é um dado preocupante, que coloca em xeque a segurança de sistemas críticos, podendo causar milhões de reais em prejuízos quando o ataque obtém sucesso, um caso famoso que ocorreu no ano de 2021, foi com a grande empresa JBS em sua filial dos Estados Unidos, que teve seus dados sequestrados através do ataque tipo *Ransoware*, criptografando seus servidores, segundo a empresa, informa que seu departamento de TI atuou para restabelecer seus servidores e sistemas (JBS, 2021).

2.3. Segurança da Informação

De acordo com Silva (2009), a Segurança da Informação envolve a criação de um documento contendo medidas a serem implementadas para proteger as informações e sistemas de informações. O objetivo é garantir a integridade, disponibilidade, não repúdio, autenticidade e confidencialidade dessas informações.

A Autenticidade, de acordo com Silva (2009), refere-se à garantia de que a informação ou usuário é genuíno, permitindo a identificação do sistema ou usuário e aumentando a proteção contra acessos não autorizados e fraudes.

De acordo com Carvalho (2005), o pilar de segurança da Disponibilidade assegura que a informação ou sistema esteja prontamente acessível em qualquer momento solicitado.

Segundo Silva (2009), o princípio de Não-Repúdio desempenha um papel crucial ao garantir que uma ação concluída não possa ser negada, o que proporciona confiabilidade às informações obtidas por meio de transações eletrônicas. Esse princípio é especialmente relevante para aplicações web envolvidas no comércio eletrônico.

A Integridade garante que a informação esteja na sua forma original quando for armazenada ou enviada, protegendo contra modificações não autorizadas (IBM, 2021).
A Confidencialidade permite que a informação ou sistema deve ser acessado somente por pessoas autorizadas, permitindo segregar os níveis de acesso de acordo com sua necessidade (IBM, 2021).

2.4. Open Web Application Security Project

Open Web Application Security Project (OWASP) é uma entidade privada sem fins lucrativos que tem por objetivo pesquisar e desenvolver melhorias de segurança dos softwares (OWASP, 2022). A organização OWASP tem um projeto onde, são analisados vários trabalhos de desenvolvimento de softwares para encontrar vulnerabilidades ranqueá-las, é criado um documento com recomendações para os processos de desenvolvimento para mitigar os riscos de segurança, estes dados
analisados é elaborador por especialistas em segurança da informação e organizações que contribuem com a entidade (OWASP, 2022).

A lista Top 10 OWASP apresentada na Tabela 1 tem sua última edição lançada em 2021 e apresentou as seguintes vulnerabilidades:

Tabela 1 – *TOP* 10 OWASP – Baseado em Owasp*Top 10*

#	Vulnerabilidades Encontradas
A01	Controle de acesso quebrado
A02	Falhas de criptografias
A03	Injeção
A04	Design inseguro
A05	Configuração incorreta de segurança
A06	Componentes vulneráveis e desatualizados
A07	Falhas de identificação e autenticação
A08	Falhas de software e de integridade dados
A09	Falhas de registro e monitoramento de segurança
A10	Falsificação de solicitação (SSRF)

Fonte: Owasp

3. Metodologia

Este artigo utilizou, conforme Tabela 2, a metodologia Estudo de Caso, pois proporcionou expor de forma prática o problema para retratar de forma real soluções adequadas por abordar especificações técnicas e desenvolvimento (YIN, 2014).

Tabela 2 – Características da Pesquisa

Item	Conteúdo	Autor (a)
QP	Os dados que transitam nas aplicações web estão seguros contra-ataques cibernéticos e vazamentos de informações?	
Natureza	Qualitativo	MARTINS; THEÓPHILO (2009)
Metodologia	Estudo de Caso	YIN (2014)

Fonte – Realizado pelo próprio autor

3.1 Procedimentos Para Desenvolvimento do Ambiente

Os procedimentos seguirão da seguinte forma:

Etapa 1: Criar ambiente. No portal Microsoft criar o ambiente de teste CRM Dynamics;

Etapa 2: Teste de Vulnerabilidade. Realizar o teste de vulnerabilidade utilizando a ferramenta OWASP ZAP;

Etapa 3: Avaliar os resultados. Através dos resultados obtidos pela ferramenta de teste, identificar as falhas através da avaliação dos dados;

Etapa 4: A partir da Questão de Pesquisa, validar as propostas;

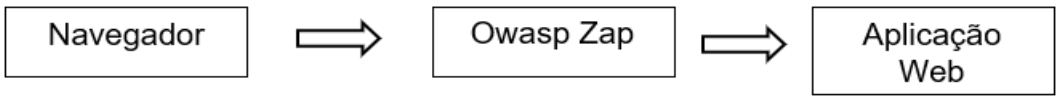
Etapa 5: Análise dos Resultados.

3.2 Desenvolvendo Ambiente de Teste

A ferramenta utilizada para realizar análise de vulnerabilidade é a OWASP ***Z**AP **A**TTACK **P**ROXY* (ZAP), é um software para scanear aplicações web de código aberto muito utilizado para verificar vulnerabilidades, trabalha entre o navegador e *web application*, se colocando em uma posição conhecida como *man-in-the-middle*, desta forma ele irá inspecionar as mensagens trocadas entre navegador e aplicação, modificar o conteúdo e encaminhar para o destino e analisar o comportamento da aplicação (OWASP, 2022).

Na Figura 3 é possível identificar como a ferramenta Owasp Zap trabalha para coletar as informações e realizar o teste de vulnerabilidade:

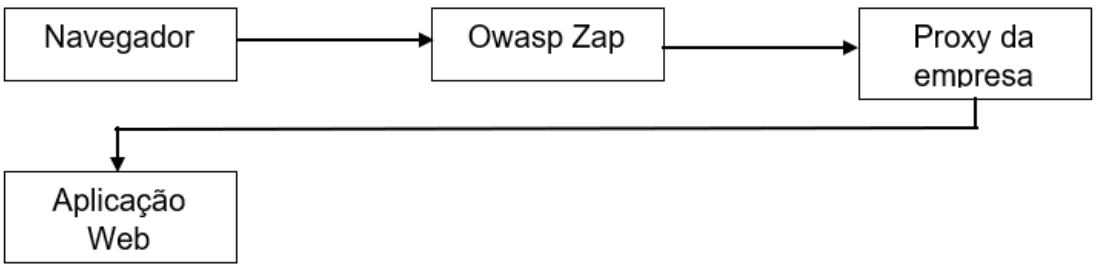
Figura 3: Owasp Zap Sem Proxy



Fonte – Realizado pelo próprio autor

A Figura 4 ilustra de forma sequencial o funcionamento da ferramenta Owasp ZAP.

Figura 4: Owasp Zap Com Proxy



Fonte – Realizado pelo próprio autor

De acordo com Dynamics Cloud (2022), o ambiente de teste selecionado foi o CRM Microsoft Dynamics 365, uma solução baseada em nuvem. Nesse contexto, a segurança do ambiente é responsabilidade da Microsoft, que implementa medidas como firewalls, regras de segurança para acesso aos servidores e atualizações regulares, entre outros aspectos.

No ambiente *CRM* é possível realizar qualquer ação, adicionar ou remover usuários de grupo, criar bancos de dados no ambiente *Microsoftdataverse*, gerenciar recurso criados no ambiente e definir políticas de prevenção contra perdas de dados (MICROSOFT, 2022).

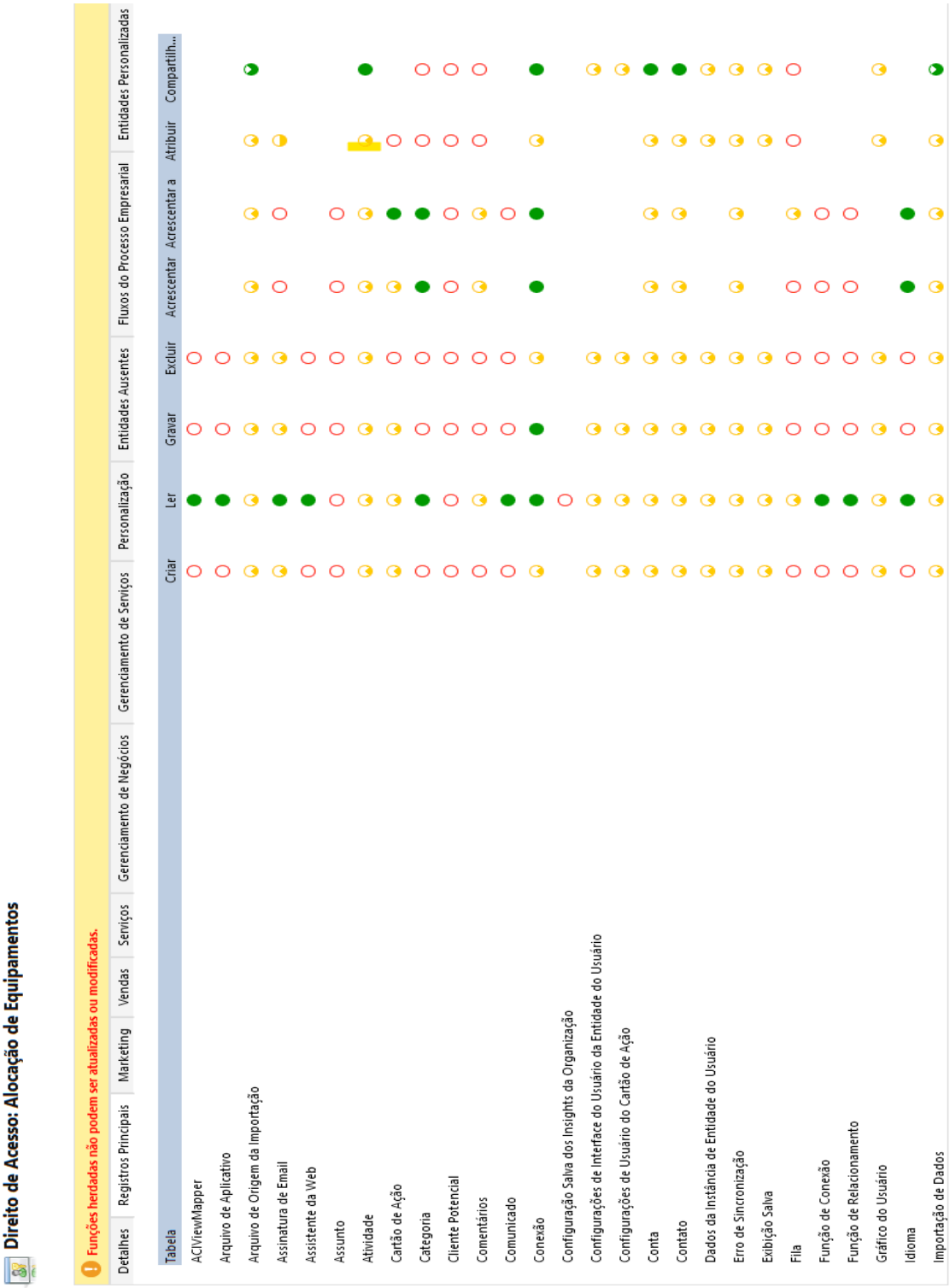
Realizado a criação do ambiente CRM, segue dados:

Ambiente CRM endereço: https://org89ca8cb4.crm2.dynamics.com/ (Ambiente *trial* para teste);

- Configurado os componentes: O ambiente possui uma solução de nome “Treinamento” e um aplicativo Alocação de Equipamentos de TI para teste;
- Aplicado as configurações de segurança (Criar, atualizar, visualizar e exclusão) – Esta etapa foi criado um grupo de nome: Alocação de Equipamentos para definir os níveis.

A Figura 5 representa os níveis de acessos aos recursos do ambiente, é possível classificar para cada componente a forma de como o usuário que possuir no seu perfil o grupo Alocação de Equipamentos o grau de permissões que no *Dynamics* são classificados pelas chaves representadas por círculos pintados:

Figura 5: Direitos de Acesso



Fonte – Realizado pelo próprio autor

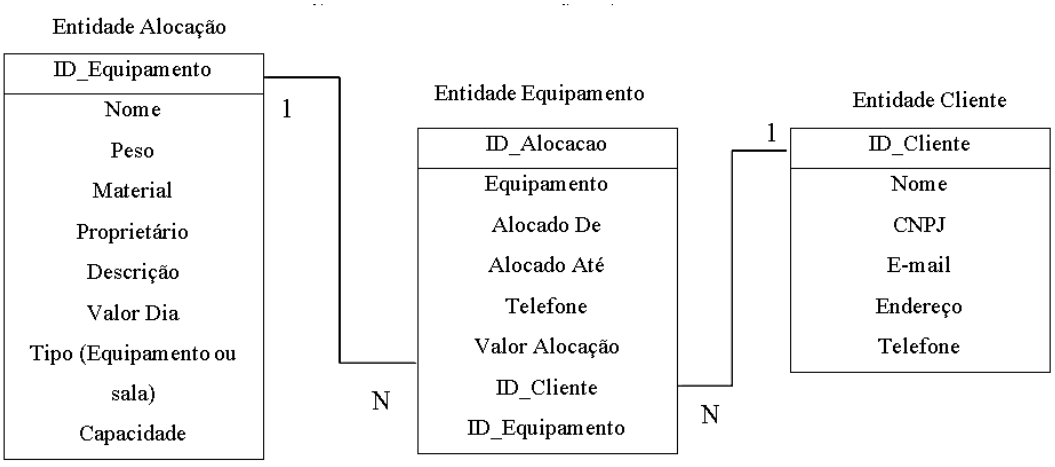
As chaves possuem os valores:

- Usuário: Esta chave indica que somente o usuário que criou o registro poderá atualizá-lo;
- Unidade de Negócio: Os usuários que pertence a unidade de negócio onde o registro foi criado poderá atualizá-lo;
- Divisão Primárias, secundárias: Os usuários poderão atualizar os registros de Unidades de Negócios e usuários que estiverem abaixo dela;
- Organização, esta chave indica que terá acesso irrestrito para manusear o registro conforme sua necessidade.

Para o armazenamento dos dados será utilizado o *Microsoft Dataverse*, é uma solução baseada em nuvem para ser o repositório central dos dados, ele permite escalar recursos conforme necessidade (MICROSOFT, 2022).

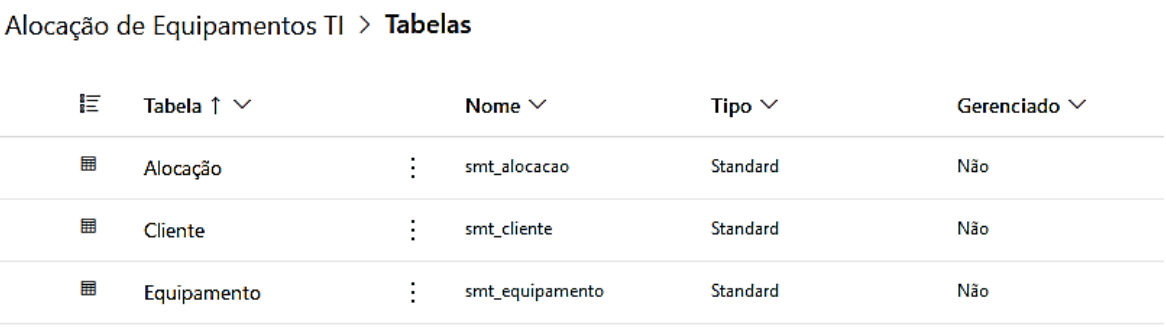
Foram criadas três tabelas no *Microsoft Dynamics* como demonstra a Figura 6, estas tabelas são denominadas como entidades.

Figura 6 – Tabelas *Microsoft Dynamics*



Fonte – Realizado pelo próprio autor

Figura 7 – Descrição das Entidades Criadas



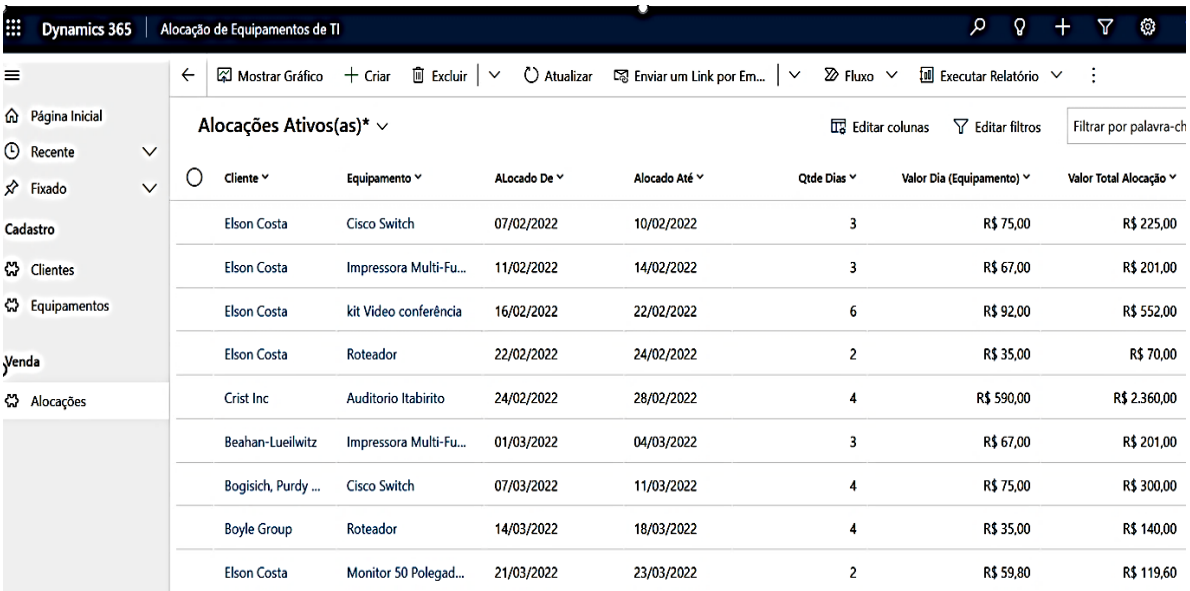
Alocação de Equipamentos TI > **Tabelas**

Tabela ↑	Nome	Tipo	Gerenciado
Alocação	smt_alocacao	Standard	Não
Cliente	smt_cliente	Standard	Não
Equipamento	smt_equipamento	Standard	Não

Fonte – Realizado pelo próprio autor

O ambiente possui um aplicativo *Model Driven* chamado de Alocação de Equipamentos de TI para que os dados das alocações sejam armazenados e gerados relatórios demonstrados na Figura 7. Na Figura 8 podemos visualizar sua interface e os campos preenchidos com informações de vários clientes compostos por nome do cliente, equipamento alocado, período e valores.

Figura 8 – Aplicativo *Model Driven* Alocação de Equipamentos de TI



Dynamics 365 | Alocação de Equipamentos de TI

Mostrar Gráfico | Criar | Excluir | Atualizar | Enviar um Link por Em... | Fluxo | Executar Relatório

Página Inicial
Recente
Fixado
Cadastro
Clientes
Equipamentos
Venda
Alocações

Alocações Ativos(as)*

Editar colunas | Editar filtros | Filtrar por palavra-ch

Cliente	Equipamento	ALocado De	Alocado Até	Qtde Dias	Valor Dia (Equipamento)	Valor Total Alocação
Elson Costa	Cisco Switch	07/02/2022	10/02/2022	3	R$ 75,00	R$ 225,00
Elson Costa	Impressora Multi-Fu...	11/02/2022	14/02/2022	3	R$ 67,00	R$ 201,00
Elson Costa	kit Video conferência	16/02/2022	22/02/2022	6	R$ 92,00	R$ 552,00
Elson Costa	Roteador	22/02/2022	24/02/2022	2	R$ 35,00	R$ 70,00
Crist Inc	Auditorio Itabirito	24/02/2022	28/02/2022	4	R$ 590,00	R$ 2.360,00
Beahan-Lueilwitz	Impressora Multi-Fu...	01/03/2022	04/03/2022	3	R$ 67,00	R$ 201,00
Bogisich, Purdy ...	Cisco Switch	07/03/2022	11/03/2022	4	R$ 75,00	R$ 300,00
Boyle Group	Roteador	14/03/2022	18/03/2022	4	R$ 35,00	R$ 140,00
Elson Costa	Monitor 50 Polegad...	21/03/2022	23/03/2022	2	R$ 59,80	R$ 119,60

Fonte – Realizado pelo próprio autor

Foram criados dados fictícios para a aplicação observado na Tabela 3, os testes de vulnerabilidades serão realizados neste ambiente.

Tabela 3 – Configuração básica do ambiente

Ambiente	Tipo	Banco de Dados
Treinamento	*SubscriptionBasedTrial*	5 GB

Fonte – Realizado pelo próprio autor

3.3 Programa de Recompensas para a Localização de Bugs da Microsoft MSRC

A *Microsoft* possui um programa de recompensas onde incentivam pesquisadores, profissionais da tecnologia a descobrirem vulnerabilidades nos seus produtos, serviços ou dispositivos da *Microsoft*. Se o relatório de vulnerabilidades enviado afetar um produto ou serviços e esteja alinhada ao programa de recompensa, será premiado com valores que podem chegar até US*$ 250.000*. (MICROSOFT MSRC, 2022)

4. Resultado

4.1. Teste de Vulnerabilidade

Realizado teste de vulnerabilidade no ambiente *CRM Trial* com a ferramenta Owasp zap para verificar as principais vulnerabilidades mais encontradas nas aplicações que estão descritas na Tabela 1 – Capítulo 2.4.

Os alertas gerados são classificados por cores:

- Cor vermelha: Alta;
- Cor Amarelo escuro: Médio;
- Cor Amarelo Claro: Baixo;
- Cor Azul: Informativo;
- Cor Verde: Falso Positivo.

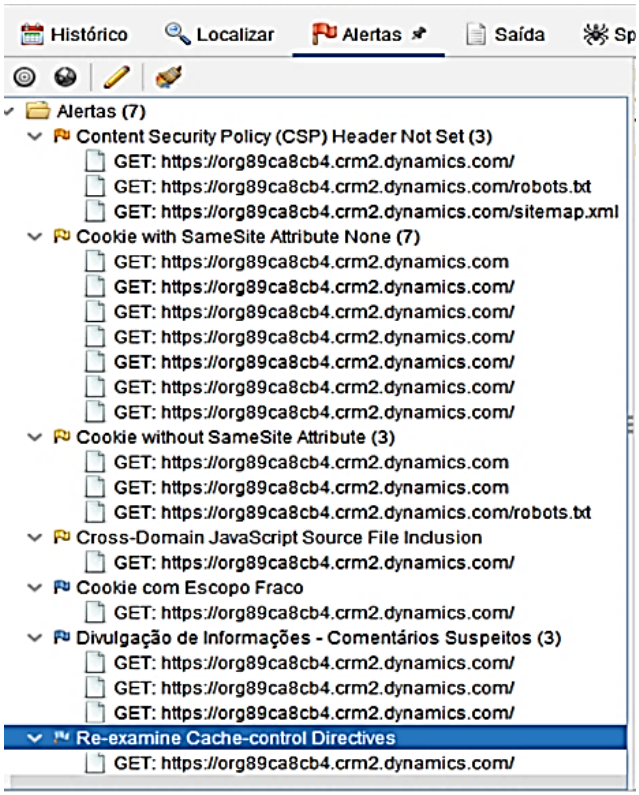
De acordo com OWASP ZAP (2022), a categorização é realizada pelo aplicativo, com base nas referências fornecidas pelo OWASP, CVE e CWE, as quais são apresentadas diretamente no aplicativo OWASP ZAP.

Foram encontradas 7 alertas nos testes realizados, onde:

- 1 Cor Amarela escura: Médio;
- 3 Cor Amarela claro: Baixo;
- 3 Cor Azul: Informativo.

Conforme mencionado pela OWASP ZAP (2022), é importante destacar que, embora a categoria de cor azul seja informativa, se não for corrigida, pode representar uma brecha que hackers podem explorar para realizar ataques que causam danos significativos à organização. Essa classificação de vulnerabilidade é claramente apresentada na lista Owasp Top 10.

Figura 9 – Tela de Resultado

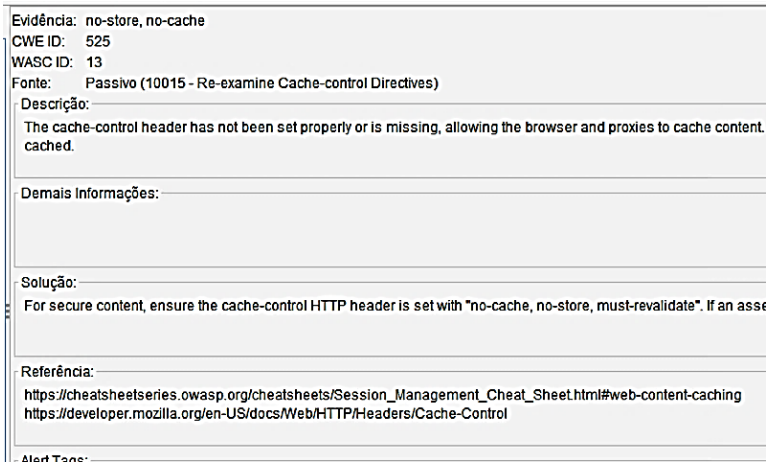


Fonte – Realizado pelo próprio autor

A Figura 9 lista os alertas gerados pelo teste, categorizando por riscos sendo identificados com bandeiras coloridas que indicam a sua classificação. Clicando nos alertas será aberto uma tela com as informações do risco encontrado, descrição e soluções.

Segundo OWASP ZAP. (2022), a Figura 10 apresenta as informações ao clicar no alerta, com informações sobre a vulnerabilidade encontrada e um breve relato de como corrigir o problema, ao pesquisar o código CWE (2022) é possível obter mais detalhes do risco bem como a solução no máximo detalhe.

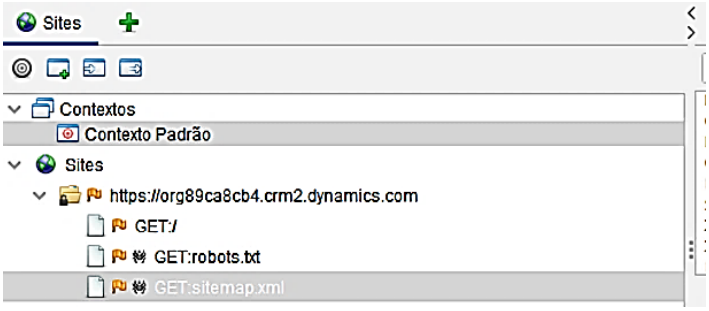
Figura 10 – Tela de Resultado



Fonte – Realizado pelo próprio autor

A Figura 11 faz parte dos resultados encontrados. No entanto, esta tela informa os itens testados, no caso deste estudo, a página da aplicação web e scripts que podem ser utilizados em conjunto de categorias e *templates* (OWASP ZAP, 2022).

Figura 11 – Tela de Resultado



Fonte – Realizado pelo próprio autor

Os resultados encontrados no aplicativo Owasp zap foram tabulados com informações que que identificam qual o nível de alerta conforme Tabela 4, vulnerabilidade, descrição e a possível solução.

Tabela 4: Resultado teste de Vulnerabilidade

Tag Alerta	Vulnerabilidade	Descrição	Classificação Top 10	CWE ID	Solução
Amarelo Escuro	*Security Misconfiguration*	Forma de configuração incorreta	5	693	Certificar seu servidor *web*, esteja configurado para definir o cabeçalho *Content-Security-Policy*, para obter o suporte ideal ao navegador: "*Content-Security-Policy*" para Chrome 25+, *Firefox* 23+ e *Safari* 7 +, etc.
Amarelo Claro	*Broken Access Control*	Cookie com o atributo *SameSite*definido como "*none*", dessa maneira é possível realizar ataques por falsificação de solicitação entre sites, inclusão de script entre sites etc.	1	1275	Definir atributo *SameSite* com o valor:*Iax* ou *atrict.*
Azul	*Software and Data Integrity Failures*	Cookie com escopo de domínio Pai.	8	565	Sempre definir o escopo dos cookies para FQDN
Azul	*Broken Access Control*	Comentários suspeitos que podem ajudar um invasor.	1	200	Remover todos os comentários que retornem informações que possam ajudar o invasor.

Fonte – Realizado pelo próprio autor

O teste de vulnerabilidade demonstra que, por mais que a aplicação seja bem projetada, bem estruturada e desenvolvida, sempre há pontos que podem se tornar vulneráveis. Importante entender que o teste de vulnerabilidade é uma parte da estratégia para se manter o ambiente seguro. É preciso instituir o gerenciamento de vulnerabilidades para conhecer melhor pontos de melhoria.

4.2. Gerenciamento de Vulnerabilidade

Segundo o ITEAM (2020), a vulnerabilidade é considerada um ponto de acesso potencial para invasões, acesso não autorizado e vazamento de dados quando descoberta por hackers. Essa vulnerabilidade pode ter origem na infraestrutura, desenvolvimento da aplicação ou banco de dados.

O gerenciamento de vulnerabilidade tem por objetivo criar processos para identificar as vulnerabilidades, classificar e indicar a solução adequada para correção dos itens elencados como vulneráveis (MICROSOFT, 2022).

A ISO 27002 é uma norma que fornece diretrizes de Segurança da Informação com práticas para gerenciamento de segurança, controles para ambientes críticos para desenvolvimento de processos para identificação e gerenciamento de riscos e vulnerabilidades (ISO, 2022).

O teste indica como primeiro passo, conhecer os pontos falhos, desta forma a empresa terá meios para desenvolver processos internos para melhorias contínuas, terá conhecimento dos ativos, possuindo um maior controle para avaliação das vulnerabilidades (MICROSOFT, 2022).

4.3. Discussão

Os resultados dos testes indicam que é importante ter um gerenciamento de vulnerabilidades das aplicações web, desta forma os dados que lá trafegam sempre estarão seguros e com o mínimo de risco para ataques e vazamentos de dados.

Muito importante ter um processo preventivo de melhoria contínua, sempre baseado nas melhores práticas de gestão de segurança da informação em conformidade com o que é praticado no mercado e regulamentado por entidades regulamentadoras (ISO - STANDARDS, 2022).

Conforme a ISO - STANDARDS (2022), a norma ISO 15408 desempenha um papel importante ao auxiliar os desenvolvedores na construção de aplicações seguras. Ela descreve os conceitos necessários para garantir a segurança dos sistemas, possibilitando uma avaliação mais detalhada.

Diante das questões que implicam na segurança da informação, o teste de vulnerabilidade demonstra que não podemos ficar satisfeitos com a segurança já aplicada mesmo que nunca tenham tido um ataque ou vazamentos, pelo contrário, sempre haverá pontos frágeis, muito importante estar atentos com as novas tecnologias e tendências na segurança da informação.

5. Conclusões

Segundo o Ministério da Cidadania (2022), a Lei Geral de Proteção de Dados (LGPD) foi instituída com o objetivo de salvaguardar a liberdade, privacidade e formação da personalidade de cada indivíduo. A LGPD oferece orientação tanto para empresas, governo e outras entidades sobre a maneira adequada de coletar, tratar, armazenar e manipular dados por meio de um conjunto de medidas que delineiam responsabilidades, penalidades e direitos das partes envolvidas.

Neste contexto, faz se necessário trabalhar para manter o ambiente seguro para estar aderente a Lei, bem como ter um ambiente seguro para aplicações onde, é desenvolvido um ciclo de melhoria por meio do Gerenciamento de Vulnerabilidades avaliando seus ativos para entender o perfil de risco de cada recurso.

Qualquer software que seja mal desenvolvido possui vulnerabilidades que serão exploradas em algum momento. As aplicações web, são visadas por estarem disponíveis ao público, logo, implementar de maneira segura é fundamental. Além disto, há riscos das informações coletadas pela empresa de serem acessadas, vazadas, comprometendo todo o serviço realizado por ela. Caso haja o incidente, põem em risco a credibilidade e mostra para seus usuários, clientes a falta de gestão e competência da empresa em gerir com segurança o seu ambiente.

A utilização da ferramenta de escaneamento OWASP ZAP é parte de uma estratégia maior, o software encontra as vulnerabilidades para serem solucionadas, no entanto, é importante trabalhar para identificar a causa raiz que permitiu que esta vulnerabilidade ocorresse, diante deste contexto, propomos também um estudo mais aprofundado utilizando a ferramenta OWASP ZAP.

O gerenciamento de vulnerabilidade vem de encontro com esta proposta, conhecendo seus ativos e recursos, poderá de forma proativa reduzir os pontos vulneráveis. No entanto, este gerenciamento de vulnerabilidade, deve estar acompanhado com uma política de segurança da informação, que contemple processos, procedimentos, responsabilidades das áreas bem como as ações que serão tomadas, pontos focais quando um incidente ocorrer.

A ISO 27002 é um ótimo ponto de partida para as organizações implementarem Sistema de Gerenciamento de Segurança da informação (SGSI), com diretrizes e procedimentos auxiliando as organizações com as melhores soluções de acordo com os ambientes de riscos, porte e estratégias.

Em conjunto com o gerenciamento de vulnerabilidade, Políticas de Segurança, processos para avaliações de segurança, equipe bem treinada, o risco de algum ataque prosperar será mínimo, portanto, manter um ciclo que revise todos os processos em um ciclo de melhoria contínua, possibilita que as aplicações *web* seja sim, seguras e possa garantir os três principais pilares, Disponibilidade, integridade e Autenticidade.

Como contribuição futura será elaborado uma cartilha de boas práticas especificamente para modelos aplicados ao contexto do estudo.

Referências

ABNT - Brasil. ISO - Membros. Recuperado em 3 de junho de 2022, de https://www.iso.org/member/1579.html

Carvalho, L. G. de. Segurança de Redes, 2005. (2ª ed.). Editora Ciência Moderna.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, 2022. Recuperado em 28 de agosto de 2022, de https://www.cert.br/

Check Point Research. Cyber Attack Trends: 2022 Mid-Year Report, 2022. Recuperado em 20 de junho de 2022, de https://research.checkpoint.com/category/threatintelligence-reports/

CWE. CWE - Common Weakness Enumeration, 2022. Recuperado em 4 de junho de 2022, de https://cwe.mitre.org/index.html

Dynamics Cloud. Microsoft Dynamics 365 Cloud, 2022. Recuperado em 29 de abril de 2022, de https://dynamics.microsoft.com/pt-br/cloud-migration/

Fortinet. Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. Segurança, 2022. Recuperado em 2 de abril de 2022, de https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021

IBM. Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação. Segurança da Informação, 2021. Recuperado em 10 de setembro de 2022, de https://service.com.br/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao/

INMETRO. O que é ISO? Governo, 2022. Recuperado em 3 de junho de 2022, de http://www.inmetro.gov.br/qualidade/responsabilidade_social/o-que-iso.asp

ISO - International Organization for Standardization, 2022. ISO - Standards. Normalização. Recuperado em 3 de junho de 2022, de https://www.iso.org/home.html

Iteam. Vulnerabilidade de segurança e quais são as mais comuns. Segurança da Informação, 2022. Recuperado em 17 de setembro de 2022, de https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/

JBS. JBS USA E PILGRIM'S ANUNCIAM RESOLUÇÃO DE ATAQUE CIBERNÉTICO, 2022. Privado. Recuperado em 6 de dezembro de 2022, de https://ri.jbs.com.br/arquivos-cvm/avisos-comunicados-e-fatos-relevantes/

Kaspersky. O Panorama de Ameaças 2021 da Kaspersky, 2021. Recuperado em 24 de abril de 2022, de https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/

Kotler, P., & Keller, K. L. Marketing Estratégico Para Instituições Educacionais, 2012. (12ª ed.). Pearson - Prentice Hall.

Kotler, P., Hermawan, K., & Iwan, S. Marketing 5.0: Tecnologia para a humanidade, 2021. Editora Sextante.

Martins, G. de A., & Theóphilo, C. R. Metodologia da investigação científica para ciências sociais aplicadas, 2009.

Microsoft. 365. O que é o Dynamics 365? CRM, 2022. Recuperado em 22 de abril de 2022, de https://dynamics.microsoft.com/pt-br/what-is-dynamics365/

Microsoft. Gerenciar permissões e administração para o Dataverse, 2022. Recuperado em 29 de abril de 2022, de https://docs.microsoft.com/pt-br/learn/modules/get-started-security-roles/

Microsoft. O que é o Gerenciamento de Vulnerabilidades? Tecnologia, 2022. Recuperado em 29 de abril de 2022, de https://www.microsoft.com/pt-br/security/business/security-101/what-is-vulnerability-management

Ministério da Cidadania – Lei Geral de Proteção de Dados Pessoais (LGPD), 2022. Recuperado em 20 de junho de 2022, de https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd

Open Web Application Security Project. OWASP, 2022. Fundação. Recuperado em 20 de junho de 2022, de https://owasp.org/

OWASP ZAP. OWASP - Zap Attack Proxy (ZAP). Cibersegurança, 2022. Recuperado em 3 de setembro de 2022, de https://www.zaproxy.org/

OWASP. OWASP Top Ten. Segurança da Informação, 2022. Recuperado em 20 de junho de 2022, de https://owasp.org/www-project-top-ten/

Silva, L. H. R. da. Tecnologia em Redes de Computadores - Uso de GPO's na Segurança de Domínios Corporativos. Ciência Moderna, 2009.

Yin, R. K. Estudo de Caso. Planejamento e Métodos, 2014. (5ª ed.). Bookman.