ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

MAJ (REP DOM) YESICA ELISABET **JOSE** HEREDIA,

Impacto da atuação do CSIRT-Defesa na Força Aérea da República Dominicana, no período 2019-2020.

Rio de Janeiro
2022

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO DE COMANDO E ESTADO-MAIOR

MAJ YESICA ELISABET **JOSE** HEREDIA, FARD.

Impacto da atuação do CSIRT-Defesa na Força Aérea da República Dominicana, No Período 2019-2020.

Trabalho de conclusão de curso apresentado como requisito parcial para aprovação, no Curso Avançado de Comando e Estado-Maior.

Linha de Pesquisa: Poder Militar.

Orientador: LUIZ GUSTAVO **SCHENK** - Cel Av R1.

Rio de Janeiro
2022

RESUMEN

La presente investigación trata sobre el impacto de la creación del CSIRT-Defensa frente a las amenazas cibernéticas de la infraestructura tecnológica a las que se enfrenta la Fuerza Aérea de República Dominicana y la protección de los servicios críticos que pueden afectar la Defensa Nacional y el buen funcionamiento de las operaciones. El mundo de las TIC en el ámbito castrense ha evolucionado de una forma asimétrica, desde una simple herramienta a mejorar la productividad administrativa hasta construir un medio estratégico a través de la creación de un equipo de respuestas a ataques cibernéticos y la atención a los ataques o guerras electrónicas para proteger el ciberespacio. Para esto se realizó un cuestionario a técnicos y expertos en materia de ciberseguridad y Ciberdefensa, como instrumento para obtener datos y las informaciones obtenidas utilizados desde una perspectiva fenomenológica, esta investigación caracterizará por ser no experimental, específicamente, del tipo longitudinal descriptivo, dando como resultado en su análisis de datos, el impactado la actuación del CSIRT-Defensa en la protección de los servicios y sistemas de tecnología de la información y comunicación de la FARD, así como el desarrollo de la creación y la concientización del buen uso de buenas prácticas de la ciberseguridad.

Palabras claves: Amenazas, Cibernéticas, Seguridad Cibernética, Defensa Cibernética, Seguridad y Defensa Nacional, CSIRT-Defensa**.**

RESUMO

Esta pesquisa trata do impacto da criação do CSIRT-Defesa contra as ameaças cibernéticas da infraestrutura tecnológica enfrentadas pela Força Aérea da República Dominicana e a proteção de serviços críticos que podem afetar a Defesa Nacional e o bom desempenho da operação. O mundo das TIC no campo militar evoluiu de forma assimétrica, desde uma simples ferramenta para melhorar a produtividade administrativa até a construção de um ambiente estratégico através da criação de uma equipe de resposta a ataques cibernéticos e atenção a ataques ou guerra eletrônica para proteção do ciberespaço. Para isso, foi feito um questionário a técnicos e especialistas na área de cibersegurança e ciberdefesa, como instrumento de obtenção de dados e as informações obtidas utilizadas de uma perspectiva fenomenológica, esta pesquisa será caracterizada por ser não experimental, especificamente, do tipo longitudinal descritivo, resultando na sua análise de dados, o impacto da atuação do CSIRT-Defesa na proteção dos serviços e sistemas de tecnologia da informação e comunicação da FARD, bem como o desenvolvimento da criação e conscientização para o bom uso de práticas de cibersegurança.

Palavras chaves: Ameaças, Cibersegurança, Defesa Cibernética, Guerra Cibernética, Segurança e Defesa Nacional, CSIRT-Defesa.

LISTA DE TABELAS

LISTA DE GRAFICOS

LISTA DE ABREVIATURAS E SIGLAS

CSIRT – Equipe de Reposta a Incidentes Cibernéticos.

FARD – Força Aérea da República Dominicana.

FA – Forças Armadas.

TIC – Tecnologia da informação e Comunicação.

ENISA – Agência Europeia para a Segurança das Redes e da Informação.

SUMÁRIO

1 INTRODUÇÃO

Esta pesquisa revelará o impacto da ação CSIRT-Defesa contra ameaças cibernéticas enfrentadas por instituições militares, sendo a Força Aérea da República Dominicana uma delas. Após a criação do CSIRT-Defesa, a FARD evoluiu de forma assimétrica, desde a utilização de uma simples ferramenta tecnológica até à implementação das melhores práticas de cibersegurança nos seus sistemas de informação, reforçando as capacidades do seu pessoal e do setor militar em geral. Para lidar com as novas ameaças que ameaçam a segurança e a defesa da nação.

A missão das Forças Armadas da República Dominicana está consagrada em sua Carta Magna, onde estabelece que, além de proteger os fatores e nosso espaço aéreo e interesses da nação, também enfrenta um novo cenário onde os novos combates do futuro. As Forças Armadas da República Dominicana exigem a promoção de uma cultura de segurança e defesa no mundo da tecnologia, para se adaptar aos novos tempos com flexibilidade e versatilidade.

A criação do CSIRT-Defesa foi chocante no mundo das TIC e muito mais para as instituições militares, onde muda completamente uma doutrina aplicada em três menções: estratégica, operacional e tática, apresentando um quinto domínio que é vital no uso de armas e tecnologia aplicada aos campos de batalha, como o novo cenário da guerra eletrônica, o ciberespaço e a proteção da infraestrutura crítica de um setor.

1.1 Hipótese

A Força Aérea da República Dominicana, além de sua função principal de Defesa do Espaço Aéreo, tem o objetivo e identificar ameaças cibernéticas físicas e virtuais que afetam a soberania do país.

A criação de uma equipa de resposta a incidentes cibernéticos procura estabelecer os mecanismos necessários para o desenvolvimento da Segurança Nacional, procurando a escala ao longo do tempo para obter um país mais seguro em termos de ciberespaço e cibersegurança.

A Força Aérea hoje também se preocupa com a grande mudança tecnológica de muitas aeronaves, com mudanças análogas às digitais, cuidando de suas informações, dispositivos eletrônicos que armazenam informações relevantes e que estão expostos a solicitações de informações, assim, também têm procurado fortalecer e sensibilizar o capital humano, as áreas tecnológicas, juntamente com o CSIRT-Defesa das nossas Forças Armadas.

Esta investigação abordará o impacto que a Força Aérea da República Dominicana obteve com as novas regulamentações e até mesmo com o resultado que será obtido após a aprovação das diferentes estratégias e protocolos a serem seguidos em conjunto com as outras instituições militares setor, para contrariar estes ataques que podem limitar e colocar em risco o nosso Espaço Aéreo e a Defesa Nacional.

1.2 Objetivos

Identificar como as boas práticas de segurança cibernética foram fortalecidas após a criação de uma equipe de resposta a incidentes cibernéticos da Força Aérea da República Dominicana.

Para atingirmos o objetivo geral e com o intuito de balizar as ações da pesquisa foram definidos os objetivos específicos abaixo:

a) Identificar os procedimentos de CSIRT-Defesa para a gestão de incidentes cibernéticos.
b) Incidência do CSIRT-Defesa sobre as melhores práticas de cibersegurança Força Aérea da República Dominicana.
c) Analisar a estrutura de cibersegurança na Força Aérea da República Dominicana.

1.3 Justificativa do Estudo

Este estudo representa um mecanismo de grande importância pois, por meio dele, será possível identificar oportunidades de melhorias, conseguir idenficar as ameaças com maior incidência e desenvolver um esquema que tenha tanto equipamento que merece, quanto capital humano e técnico que é necessário para enfrentar as ameaças cibernéticas de maior risco no ciberespaço, influenciando significativamente a segurança na defesa nacional.

Uma vez que o CSIRT-Defesa na República Dominicana tem forçado a criação de uma consciência e cultura em cibersegurança, de acordo com a estratrégia nacional de cibersegurança que saiu por decreto presidencial, onde seus pilares são a criação de consciência, mostra o impacto de enfatizar as fases das diferentes instituições, como a Força Aérea Dominicana, como uma instituição com infraestrutura aeronáutica critica relevante, tem sido positivo no reforço dessas capacidades.

1. Revisão literária

2.1 Quadro teórico

A editora Wiley Blackwell (2021) aponta que os avanços tecnológicos criam desafios para a segurança global, que deixam até os países mais poderosos do ponto de vista militar vulneráveis a ataques cibernéticos.

Nesse sentido, é notória a intenção dos países de se prepararem para a guerra eletrônica e, embora se deva observar que as antigas regras dos conflitos internacionais não são aplicadas ou não foram desenvolvidas, é aí que reside um dos grandes desafios dos governos ainda e é encontrar soluções políticas estáveis para lidar com possíveis ameaças cibernéticas que ameaçam a segurança e a defesa da nação, isso se traduz em estabelecer novos padrões globais de comportamento aceitável no ciberespaço, especialmente das Forças Armadas de todo o mundo.

Além disso, argumenta que, embora os Estados-nação permaneçam centrais, os atores não estatais estão desempenhando um papel cada vez mais importante na construção de normas de segurança cibernética, complementando a ação do Estado e, até certo ponto, compensando a inação do Estado quando a cooperação chega a um impasse. (Wiley Publishing em Política & Políticas, 2021)

As ameaças contra as nações se tornaram tão diversificadas que algo abstrato como o ciberespaço se tornou o novo teatro de operações militares devido à incidência que os ataques cibernéticos poderiam causar nesse cenário, podendo limitar desde os provedores de saúde que compromete o atendimento ao paciente, como a capacidade de vender combustível ou alimentos em um supermercado.

A Casa Branca da Estados Unidos (2021), observou que:

> O ransomware representa um risco significativo para infraestrutura crítica, serviços essenciais, segurança pública e consumidor. Proteção e privacidade e prosperidade econômica. Tal como acontece com outras ameaças cibernéticas, a ameaça de ransomware é complexa e global por natureza e requer uma resposta compartilhada. A capacidade de uma nação de efetivamente prevenir, detectar, mitigar e responder a ameaças de ransomware dependerá, em parte, da capacidade, cooperação e resiliência dos parceiros globais, do setor privado, da sociedade civil e do público em geral. (Casa Branca da Estados Unidos, 2021)

A Revista It Now (2015), argumenta que, em todo o mundo, os governos e as Forças Armadas estão cada vez mais dependentes da cibernética: as pessoas, *hardware* e *software* que suportam o fluxo e a gestão da informação. Essa dependência crescente dá aos adversários oportunidades novas e mais exploráveis para cumprir sua missão.

2.1 Quadro histórico

As Forças Armadas de todos os países, se modernizaram à medida que as ameaças se diversificam, por exemplo. Keohane e Nye (2000), apontam que todas as

armas modernas contêm recursos de processamento digital, seja uma unidade de processamento de computador atualizada em um radar, a tecnologia digital que permite que os bloqueadores modernos se adaptem ao seu ambiente eletromagnético ou o software usado por alvos e planejadores de combate para atribuir armas e planejar campanhas.

As informações de combate, anteriormente transmitido via analógica e prejudicadas por limitações de tamanho e logística, agora são entregues via pacotes de código binário via satélite, cabo de fibra óptica e transmissões de rádio. Essas informações digitais são armazenadas e processadas por meio de data centers repletos de servidores, roteadores, software de processamento, aplicativos de software e acesso convencional de combatentes.

A informação tornou-se tão totalmente integrada na forma como os Estados modernos combatem a guerra que não pode ser separada das táticas, operações ou estratégia. Ou seja, o setor militar sofreu e está passando por uma nova revolução, como afirma, Lynn (2010), que se refere a isso ao enfatizar diferentemente da revolução da infantaria ou da artilharia, a revolução da informação ele não apenas criou e é criando guerreiros da informação, mas ele informou todos os guerreiros convencionais.

São soldados de infantaria, controladores de tráfego aéreo avançados, especialistas em munições, pilotos e pessoal de guerra que dependem de tecnologias e informações digitais para realizar operações convencionais.

É virtualmente impossível separar a guerra moderna das capacidades digitais. Como o ex-secretário de Defesa dos EUA Lynn (2010), afirmou, “a tecnologia da informação permite quase tudo que os militares fazem. . . [isto] evoluiu de uma ferramenta administrativa para melhorar a produtividade do escritório para um ativo estratégico nacional por direito próprio “.

Intimamente ligado ao aumento de armas e operações habilitadas digitalmente está o domínio agora difundido da guerra centrada em rede. As implicações do Ministério da Defesa não são apenas extrapoladas para os quatro domínios geralmente conhecidos, mar, ar, espaço e terra, mas o ciberespaço é considerado o novo teatro de operações militares.

Cebrowski e Garstka (1998) argumentam que “a guerra centrada em rede surgiu

> no início da década de 1990, e os proponentes imaginaram uma revolução nos assuntos militares que usaria a tecnologia da informação para executar operações militares rápidas e abrangentes enquanto afastava o pessoal do perigo do combate corpo a corpo". As tecnologias digitais podem criar disseminação de inteligência quase em tempo real, estabelecer os meios para o rastreamento constante da força azul e permitir decisões rápidas e abrangentes por e-mail e bate-papo. Os defensores da guerra em rede argumentavam que a revolução digital mudaria fundamentalmente o equilíbrio da vitória militar para os estados que fossem capazes de alcançar o domínio da informação. Consequentemente, a guerra centrada em rede que evoluiu a partir desses preceitos é altamente precisa, integrada e dinâmica. Ele é extraordinariamente capaz."

Dafoe e Garfinkel (2019), inferem que as capacidades criadas pela revolução da informação significam que mais armas não criam mais efeitos de forma aditiva, mas sim aumentos exponenciais de eficácia. Os estados habilitados para a revolução da informação podem atingir grandes distâncias, projetar poder no horizonte e realizar ataques de precisão por meio da rápida fusão habilitada por computador de uma infinidade de sensores. Alguns desses sensores incluem radares tradicionais que coletam usando técnicas analógicas. No entanto, com a revolução da informação veio também a proliferação de centros de fusão de sensores digitalizados, coletores de sinais digitais passivos e exploração de redes de computadores.

A fusão de sensores, possibilitada pelos avanços na computação, permite que os estados anulem as limitações inerentes de um sensor para gerar soluções de direcionamento, alerta precoce e consciência situacional de sensores que não podem rastrear, direcionar ou orientar individualmente para locais.

E à medida que a revolução da informação avança e as tecnologias evoluem, 'Big Data', computação quântica, inteligência artificial, autonomia, a proliferação de redes virtuais e computação em nuvem e microprocessamento criam enormes oportunidades de detecção, direcionamento e controle para estados capazes de aproveitar recursos de informação.

2.1 Quadro referencial

Em nível global, prevalece o interesse das Forças Armadas em fortalecer suas capacidades cibernéticas para poder enfrentar as ameaças cibernéticas, que ocorrem no

ciberespaço, quinto cenário das operações militares. Um exemplo chave disso é a Espanha, já que o Exército de Defesa Cibernética (ECD09) das Forças Armadas é formado por militares especialistas em telecomunicações por computador, que fizeram cursos militares e civis avançados em segurança das TIC. Seu treinamento consiste em atacar computadores inimigos, enquanto defendem os seus, dentro de uma rede criada expressamente para isso. Além disso, há o Centro de Resposta a Incidentes de Segurança Computacional (CSIRT), que é uma equipe de técnicos especialmente treinados para resolver e gerenciar incidentes de informática de alto impacto.

O relatório de segurança cibernética do BID (2016), afirmou que, dado o crescente número de usuários da Internet e a disponibilidade de serviços de comércio eletrônico, a República Dominicana enfrenta cada vez mais ameaças cibernéticas. Nesse sentido, é importante mencionar que o governo dominicano, apesar de até o momento não ter uma estratégia de segurança cibernética, nem ter governança nesse sentido, relatou 963 casos de roubo de identidade (phishing) em 2013, bem como 432 casos de furto de dados bancários entre 2009 e 2008.

As agências internacionais de cibersegurança, como a ENISA, asseguram que, em consequência da pandemia de COVID-19, revelam que as organizações a nível global consideram a ciberespionagem (ou espionagem promovida pelos Estados-nação) como uma ameaça crescente que afeta os setores industriais, bem como os a infraestruturas vitais e estratégicas, incluindo administrações públicas, empresas de energia, ferrovias, prestadores de serviços de telecomunicações, hospitais, bancos e até o setor militar.

Mas talvez o exemplo por excelência seja a China e seu exército cibernético de reservistas. No passado, o papel pretendido para as forças de reserva era apoiar o Exército Popular de Libertação (EL) na defesa contra qualquer intervenção estrangeira. Em vez disso, hoje eles têm a capacidade de empregar armas eletrônicas e de informação para atingir um adversário em outro continente. Portanto, entre suas funções estão: interromper o sistema de informação, sabotar a estrutura de condução das operações, enfraquecer a capacidade de contra-ataque, dispersar as forças, armas e fogo do inimigo, conseguindo ao mesmo tempo a concentração das forças, armas e fogo das próprias unidades, confundem o oponente e simultaneamente lançam um ataque surpresa de informação para que ele tome uma decisão errada ou execute uma ação

errada (Thomas 2001, p. 76).

O foco da ciberespionagem é promover situações geopolíticas e roubar segredos de Estado e comerciais, informações de domínio privado em campos estratégicos e direitos de propriedade intelectual, segundo a ENISA (2020), “71% das organizações lidam com ciberespionagem e outras ameaças de “caixa preta” e ainda estão aprendendo sobre eles.

Nesse sentido, é importante mencionar que as estatísticas de muitas empresas de segurança cibernética relatam, de acordo com os sensores que possuem em todo o mundo, os dados mostram que os sofisticados atores de ameaças estão incansavelmente adaptando suas táticas e adotando ameaças cibernéticas. a ponto de negar a operacionalidade, integridade e confidencialidade das informações nele contidas, tais como: Ransomware com um valor de cerca de 304,7 milhões até agora este ano, malware 32,2 milhões, entre outras ameaças cibernéticas que buscam ganho financeiro e prejuízo.

2.2 Quadro conceitual

Cibersegurança: É a proteção de dispositivos interligados, por meio do tratamento de ameaças que colocam em risco as informações que são processadas, armazenadas e transportadas pelos sistemas de informação que estão interligados.

Defesa cibernética: De acordo com a Junta Interamericana de Defesa, a defesa cibernética é o conjunto de capacidades defensivas, de exploração e ofensivas, focadas na defesa dos interesses nacionais contra ameaças cibernéticas de outros Estados que possam afetar a defesa nacional.

Defesa cibernética militar: São eventos de segurança que se aproveitam de uma violação de segurança e podem causar danos a uma infraestrutura tecnológica interna e externamente e se materializar pelo ciberespaço.

Inteligência de ameaças cibernéticas: É a atividade realizada através do ciberespaço (e ocasionalmente por outros meios), para obter informações e conhecimento de uma ameaça cibernética conhecida e/ou desconhecida ou de ameaças cibernéticas potenciais.

Guerra cibernética: Escalada das ações militares planejadas, organizadas, coordenadas e executadas pelas unidades de defesa cibernética em apoio às missões do Estado.

Ataque cibernético: É o uso deliberado de software especificamente projetado para causar danos a elementos do ciberespaço, podendo prejudicar sistemas computacionais como as redes sociais.

Inteligência de ameaças cibernética: É a atividade realizada através do ciberespaço (e ocasionalmente por outros meios), para obter informações e conhecimento de uma ameaça cibernética conhecida e/ou desconhecida ou de ameaças cibernéticas potenciais.

3 Metodologia

3.1 Projeto de pesquisa

Para a execução desta pesquisa será utilizada a técnica documental e exploratória, ou seja, uma coleta de informações a fim de esmiuçar e especificar um resultado. Será realizada uma série de resenhas literárias de publicações de instituições multilaterais, bem como nacionais, como reportagens, artigos de jornais e revistas, além de entrevistas, tudo com o objetivo de subsidiar este estudo. Portanto, esta pesquisa caracterizar-se-á por ser tanto qualitativa, uma vez que seus resultados serão obtidos por meio da análise teórica do material documental existente sobre o tema a ser estudado.

3.2 Tipo de pesquisa

A pesquisa será feita com abordagem qualitativa, com o método fenomenológico, fim de aprofundar esse aspecto através das experiências das autoridades que estão constantemente monitorando a sofisticação com que as ameaças evoluem no ciberespaço.

3.3 Operacionalização

Esta pesquisa será caracterizada por ser não experimental, especificamente, do tipo longitudinal descritivo, pois tentará descrever o problema do que será estudado e, dessa forma, poderá analisar como o desempenho do CSIRT -A defesa teve impacto na proteção dos serviços e sistemas de tecnologia da informação e comunicação da FARD.

3.4 Métodos e técnicas de coleta de dados

Em primeira instância, este estudo será realizado com a implementação da

ferramenta MAXQDA (All-in-One Qualitative & Mixed Methods Data Analysis Tool), oferecem instalações como triangulação de informações, contraste de ideias que facilita e organiza o processo de geração e agrupamento de códigos como resultado de informações em várias versões de arquivos, tais como: .pdf, .doc, .mp4, .png, entre outros, bem como Microsoft Word e Microsoft Excel, para gerenciamento de dados nos formatos que o MAXQDA propõe para a saída do resultado. Ressalta-se que as entrevistas serão realizadas por meio da plataforma de encontro virtual “Zoom”.

- Fontes primárias. Coletados diretamente da realidade com nossos próprios instrumentos. Como legislação relacionada à Estratégia Nacional de Cibersegurança 2018-2021 na República Dominicana e seus planos complementares; conferência de empresas de segurança cibernética sobre ameaças cibernéticas à República Dominicana; relatórios panorâmicos sobre ameaças cibernéticas globais, estatísticas do observatório do Centro Nacional de Segurança Cibernética; entrevistas com autoridades nacionais competentes, entre outros.
- Fontes secundárias. Composto por documentos históricos sobre a preparação da República Dominicana e do mundo em termos de segurança cibernética.
- Fontes terciárias. Citações indexadas resumidas; resumos de outras pesquisas sobre ameaças cibernéticas; entre outros.

  Incluirá raciocínios, abordagens ou interpretações do autor; apresentados como comentários, críticas e conclusões derivadas dos documentos analisados, apresentados em linguagem escrita, bem como tabelas e gráficos que permitirão destacar aspectos significativos da investigação.

3.5 Critérios de seleção da amostra/participantes/informantes

Será utilizado o método de análise crítica qualitativa com análise de dados, a partir da abordagem fenomenológica, apoiada na comparação com o interesse de determinar o impacto da ação CSIRT-Defesa na proteção de serviços e sistemas de tecnologia da informação FARD informação e comunicação.

Tabela 1 — Operacionalização da hipótese

Variável	Indicador	Medição	Faixa de variabilidade
Variável dependente: (Y) Impacto.	Os efeitos do CSIRT-Defesa na FARD.	Implementação de boas práticas de cibersegurança.	Negativo=0; Positivo = 1
Variável independente:			
(X) Número de incidentes cibernéticos.	Incidentes cibernéticos relatados pela CSIRT-Defesa.	Número de incidentes cibernéticos resolvidos e em vigor.	07 incidentes relatados.
(Z) Conscientização sobre segurança cibernética.	Workshops ministrados à F	Número de membros da FARD que receberam as oficinas.	50 membros recorrentes da FARD.
(W) Número de ataques bloqueados.	Ataques cibernéticos que não tiveram sucesso FARD.	O número de eventos.	31 tipos de eventos.

Fonte: O autor.

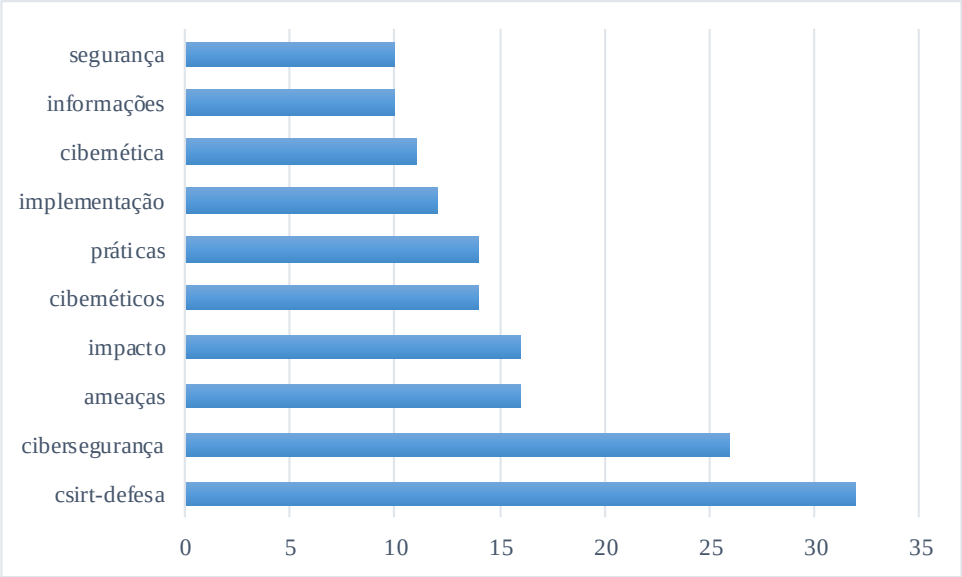
Tabela 2 — Operacionalização da hipótese em anexo

Questões de pesquisa.	Hipótese
Quais são os procedimentos CSIRT-Defesa para gerenciar incidentes cibernéticos?	O CSIR-Defesa, após identificar uma constatação que possa representar uma ameaça à infraestrutura tecnológica da FARD, faz um relatório e o encaminha ao departamento de Tecnologia da Informação da instituição afetada, tendo previamente estabelecido um ponto de contato para garantir a comunicação efetiva.
Qual a incidência do CSIRT-Defesa na implementação das melhores práticas de cibersegurança nas FARD?	A incidência da promoção do CSIRT-Defesa com base na Estratégia Nacional de Cibersegurança na criação da cultura para que cada setor implemente boas práticas de cibersegurança é positiva.

Com que frequência o CSIRT-Defesa reporta vulnerabilidades a FARD?	Toda vez que uma nova descoberta é identificada, digamos, alguma política de segurança muito flexível ou uma vulnerabilidade em si.

Fonte: O autor.

Gráfico 1 — TOP 10 palavras mais frequentes

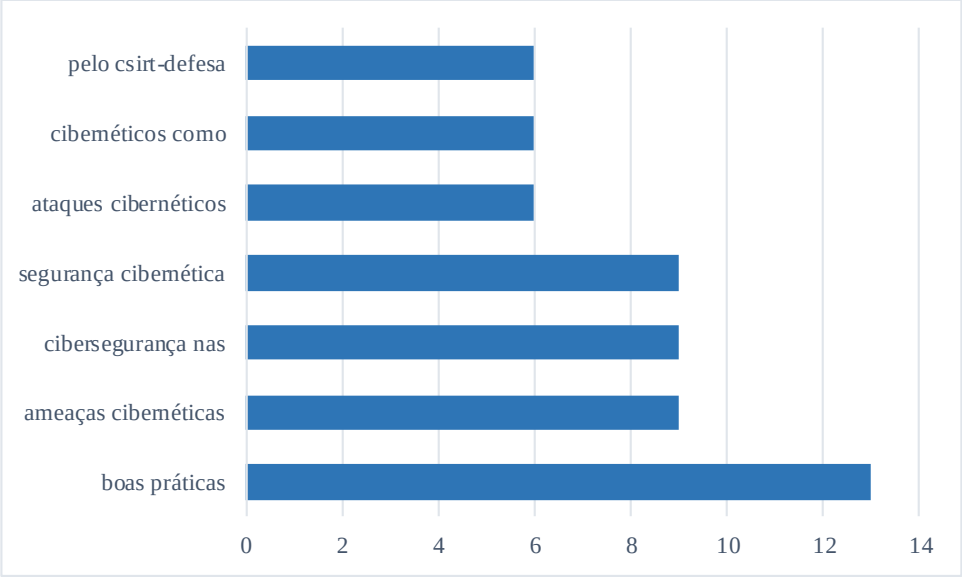


Fonte: O autor.

Ao entrevistar cinco profissionais e especialistas em Tecnologia da Informação e Comunicação e cibersegurança que prestam seus serviços no FF. AA da República Dominicana, especialmente na Força Aérea daquele país, a partir das perguntas e respostas, obteve-se a frequência de palavras que têm uma conotação importante nesta investigação, pois, em primeiro lugar, há CSIRT-Defesa.

Implica a sensibilização da comunidade servida no setor militar para a existência de uma equipe de resposta a incidentes cibernéticos para a proteção das infraestruturas críticas e de Tecnologias de Informação do referido setor. (Ver gráfico 1)

Gráfico 2 — TOP 7 de palavras combinadas mais frequentes



Fonte: O autor.

O Gráfico 2 mostra um top 7 de palavras frequentes, que, combinadas, obtêm maior significado, dentro das palavras combinadas mais recorrentes nas respostas das entidades entrevistadas, as "boas práticas" são exibidas em primeira instância, "ameaças" em segunda instância cibernética" e, em terceiro lugar, "cibersegurança". Isto, em correlação com a análise do gráfico anterior, leva-nos a inferir que o impacto do CSIRT-Defesa está relacionado com a promoção da implementação de boas práticas de cibersegurança para prevenir ameaças cibernéticas que assombram o seu ciberespaço, tendo em conta a importância de cibersegurança.

4 CONCLUSÃO

As Forças Armadas da República Dominicana buscam enfrentar a diversificação das ameaças cibernéticas no local de trabalho, na indústria, bem como aquelas que ameaçam a operação de infraestruturas críticas relevantes aos sistemas de defesa, informação e comunicação, realizadas por criminosos cibernéticos, para causar danos e assumir sistemas sem o consentimento do administrador.

A criação de um centro de atendimento a incidentes cibernéticos faz parte da agenda nacional, como forma de responder em tempo hábil às ameaças no ambiente de segurança cibernética e, assim, preparar e conscientizar para mitigar integralmente os danos que possam ser causados.

Por tais ameaças, a Força Aérea também está enfrentando essa evolução tecnológica, da mudança analógica para a digital em nossas aeronaves, sistemas de vigilância, equipamentos eletrônicos e equipamentos de comunicação e a reestruturação de uma nova infraestrutura. O crescimento dos ataques cibernéticos, por meio da web, tornou-se um ponto de preocupação para a instituição, que precisa manter o uso de boas práticas de segurança, buscando a implementação e conscientização do uso destas em seus espaços jurisdicionais.

Operações em um alcance seguro nas missões ou operações realizadas pela instituição. Após realizar a análise de dados e entrevistar especialistas e técnicos em segurança cibernética da Força Aérea da República Dominicana, o impacto do CSIRT-Defesa é reconhecido como positivo, devido ao uso de boas práticas de segurança cibernética, sensibilização, formação e reforço em cibersegurança, gestão da informação e os diversos protocolos que ligam o CSIRT-Defesa ao FARD.

Após a utilização das boas práticas de cibersegurança, reflete-se a organização e bom funcionamento da equipa tecnológica, bem como do staff, cumprindo a estratégia nacional de cibersegurança, para lidar com ameaças cibernéticas e criar um espaço mais seguro.

REFERÊNCIAS

AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA (2019). **Ataques baseados na Web. ENISA Threat Landscape**, 6. Disponível em: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-cti-overview

DIREÇÃO DE DEFESA AÉREA. **Manual de Doutrina Operacional, FARD.**

JOURNAL OF STRATEGIC STUDIES, **O paradoxo capacidade/vulnerabilidade e revoluções militares: Implicações para computação, cibernética e o início da guerra**, Edited by Todd S. Sechser, Neil Narang, Volume 42 (2019), (6), 841–863.

JOURNAL OF STRATEGIC STUDIES. **Issue 6: Emerging Technologies and Strategic Stability.** Edited by Todd S. Sechser, Neil Narang and Caitlin Talmadge. Volume 42, 2019.

LYNN, W. (2010). **Defending a New Domain: The Pentagon's Cyber Strategy.** Council on Foreign Relations, 89(5), 97-108.

POLITICS & POLICY MAGAZINE (2021). **Norm Entrepreneurship in Global Cybersecurity.** Wiley Blackwell. 49(5), p1121-1145.

REPÚBLICA DOMINICANA. Decreto Nº. 230, de 19 de janeiro de 2018. que dispõe sobre da Estratégia Nacional de Cibersegurança (2018-2021). **Diário Oficial 10912 da República Dominicana,** Santo Domingo**,** DR, 2018.

REPÚBLICA DOMINICANA**. Constituição (1844). Constituição da República Dominicana: p**romulgada em 6 de novembro de 1844, Diário Oficial 10561, 14 de junho de 2015.

REPÚBLICA DOMINICANA. Decreto Nº 189, de 15 de abril de 2007, que dispõe sobre a Diretriz de Segurança e Defesa Nacional. **Diário Oficial 10414 da República Dominicana,** Santo Domingo**,** DR, 2007.

ANEXOS

QUESTIONÁRIO-RESPOSTA

Esta informação será utilizada para efeitos de análise e interpretação da incidência do CSIRT-Defesa como equipa de resposta a incidentes cibernéticos e implementação de boas práticas de cibersegurança nas FARD.

Impacto do desempenho do CSIRT-Defesa na Força Aérea da República Dominicana, período 2020-presente.

Questionário:

1- Como o CSIRT-Defesa tem impactado a implementação de boas práticas de cibersegurança nas FARD?

RESP: 1.1- Desde a sua criação, o CSIRT-Defesa lançou workshops de formação sobre questões de cibersegurança, newsletters com boas práticas em tratamento de dados e cibersegurança, continuidade de negócios, entre outros temas relacionados. Da mesma forma, a publicação de infográficos com dicas e recomendações sobre cibersegurança; tudo isso com o objetivo de implantar uma cultura de cibersegurança em todas as dependências das Forças Armadas. FF. AA.

RESP: 1.2- Graças à criação da Diretoria de Defesa Cibernética (CSIRT-Defesa) do Centro de Comando, Controle, Comunicações, Informática, Segurança Cibernética e Inteligência (C5i) das Forças Armadas. A Força Aérea da República Dominicana (FARD) recebeu denúncias de vulnerabilidades e recomendações para proteger seus ativos tecnológicos a fim de difundir a conscientização sobre boas práticas em segurança cibernética**.**

RESP: 1.3- O CSIRT-Defesa tem tido um impacto muito oportuno e positivo na implementação de boas práticas com cursos e workshops de sensibilização para a utilização de dispositivos tecnológicos, tanto na área da tecnologia como noutras áreas que podem prevenir ataques cibernéticos.

RESP: 1.4- O impacto foi significativo, uma vez que foram relatados XX número de descobertas que se traduzem em vulnerabilidades e/ou políticas de segurança fracas na implementação. Da mesma forma, eles foram conscientizados sobre a importância de se estabelecer uma área de cibersegurança dentro da instituição, além do fato de que as oficinas ministradas pelo CSIRT-Defesa aumentaram a conscientização sobre a importância das boas práticas de cibersegurança tanto para o pessoal técnico da Informação A área de tecnologia, bem como todos os usuários que compõem o quadro de funcionários da referida instituição, pois pela experiência que tivemos e coincidindo com empresas internacionais de cibersegurança, a maior ameaça vem de dentro.

2- Como resultado da criação do CSIRT-Defesa, qual o impacto que as oficinas de cibersegurança tiveram no FARD?

RESP: 2.1- Graças às oficinas ministradas pelo CSIRT-Defesa, tais como:

• Phishing! Ser hackeado nunca foi tão fácil.

• Ransomware: Workshop teórico/prático.

• Importância do Backup de Dados.

• Gestão de identidade digital como é construída?

Os membros do FARD podem e serão capazes de aprender conceitos-chave de segurança cibernética, proteção da informação e prevenção de ameaças. Onde o CSIRT-Defesa oferece informações teóricas e práticas para garantir conteúdo de qualidade a todos os integrantes das Forças Armadas. FF. AA.

RESP: 2.2- O CSIRT-Defesa tem ministrado vários workshops sobre cibersegurança, para reforçar as capacidades e/ou competências técnicas dos membros das Forças Armadas.

Workshops ministrados:

- Phishing, Ransomware, Importância do Backup de Dados, Gerenciamento de Identidade Digital.

Note-se que se criou um interesse progressivo nos membros das Forças Armadas. Pelas oficinas ministradas. Estes têm uma duração mínima de 2 horas e uma média de 80-90 membros mensais.

RESP: 2.3- O impacto que teve é a conscientização da equipe que navega no vasto mundo da Internet, ajudando a analisar qualquer site enganoso que possa plagiar nossa identidade, pois muitas vezes esses sites são idênticos aos sites originais. Graças a isso, podemos analisar de onde vem qualquer link ou informação e confirmar que é confiável.

RESP:2.4- O impacto tem sido significativo, pois cada vez que o pessoal é convocado para as oficinas, é maior o número de integrantes da Força Aérea da República Dominicana (FARD), que se reúnem para conhecer diversos temas relacionados à segurança cibernética. Além disso, deve-se notar que, em princípio, quando os relatórios de vulnerabilidade foram enviados ao departamento de Tecnologia da Informação da FARD, a equipe não sabia como mitigar algumas das vulnerabilidades relatadas, pois quando se trata de segurança cibernética nas Forças Armadas do Na República Dominicana, o Centro de Comando, Controle, Comunicações, Informática, Cibersegurança e Inteligência (C5i) das Forças Armadas (dependência onde está localizada a CSIRT-Defesa) foi a primeira dependência do Ministério da Defesa a estabelecer e tratar novas ameaças exibidas no ciberespaço.

3- Quais são as ameaças cibernéticas de maior risco no ciberespaço da FARD? E como eles os gerenciaram junto com o CSIRT-Defesa?

RESP: 3.1- O FARD, possuindo uma infraestrutura tecnológica de importância para a nação, é um ponto de interesse no ciberespaço; por ter um portal web, ele pode ser vítima de ataques cibernéticos, como: Negação de Serviço Distribuída, Defacement (Distorção do portal web), SQL Injection e Cross Site Scripting. É por isso que o CSIRT-Defesa mantém o monitoramento contínuo do seu portal, com a implementação de um Web Application Firewall (WAF) qualquer ameaça que possa afetar a disponibilidade e integridade do site é exibida.

RESP:3.2

- Botnet.

- IIS vulnerável.
- SSL/TLS.

Essas são apenas algumas das ameaças mais relatadas no ciberespaço da FARD, que foram resolvidas em colaboração com analistas da CSIRT-Defesa e gerentes de tecnologia da FARD

RESP: 3.3- Nosso portal é o mais vulnerável a ataques cibernéticos, pois é o que é encontrado ou o que é exposto ao público, cuja url é https://fard.mil.do, quanto ao CSIRT-Defesa, nós gerenciamos as vulnerabilidades e ameaças que nossa página teve por meio de relatórios e e-mails, conseguindo evitar ataques.

RESP: 3.4- As ameaças com maior impacto na infraestrutura tecnológica da Força Aérea da República Dominicana têm sido o erro humano, digamos: programas desatualizados, falta de manutenção nos códigos que automatizam alguns processos, ou seja, falta de higiene digital; Da mesma forma, a ausência de ferramentas que lhes permitam proteger os serviços que oferecem online de ataques cibernéticos, como negação de serviços distribuída (DDoS), spam, visitas a países bloqueados, injeção de SQL, entre outros. No que diz respeito à gestão de incidentes comunicados, foi estabelecido na FARD um ponto de contato oficial que pode responder aos alertas emitidos pela CSIRT-Defesa 24 horas por dia, 7 dias por semana, de forma a promover uma comunicação eficaz e, claro, um responsável por ser assim. As formas de gerenciar os incidentes relatados são diversas, como: e-mail, aplicativos de mensagens instantâneas e por telefone.

4- Como essas ameaças cibernéticas podem afetar as missões realizadas pelas FARD?

RESP: 4.1- Essas ameaças podem significar que quem quiser acessar o portal da FARD não terá acesso, verá informações errôneas ou poderá se tornar vítima de malware se as medidas apropriadas não forem tomadas. Mas, até o momento, nenhuma dessas ameaças ocorreu.

RESP: 4.2- Estes podem afetar diretamente as operações realizadas pela FARD. Podem ter impato nos ativos digitais e/ou nas informações dos membros desta instituição.

RESP: 4.3- Eles podem afetar tanto nosso prestígio como instituição militar à qual pertencemos, quanto nossos dados cujas informações podem ser encontradas nas mãos de cibercriminosos e usar essas informações para lucrar, seja financeiramente ou moralmente.

RESP: 4.4- Negar a disponibilidade dos serviços que oferecem online; violar a disponibilidade, integridade e confidencialidade de informações confidenciais encontradas online nas plataformas FARD, contendo dados e informações sobre contratos temporários, militares assimilados, praças, oficiais subalternos e oficiais superiores da Força Aérea da República Dominicana; contaminar a rede da instituição com códigos maliciosos, podendo se tornar vítimas de Ransomware, aqueles ataques cibernéticos que criptografam as informações pedindo indenização em troca da devolução do que foi roubado, cuidado, pagar esses resgates não garante que esses dados e informações obtidas por terceiros, não autorizados, não será compartilhado em mídia clandestina, mas pelo contrário, os cibercriminosos irão compartilhá-lo e a instituição não deixará de ser atacada, pois os ciberataques sabem que a instituição é vulnerável e perdem dinheiro facilmente. Da mesma forma, o impacto reputacional que a instituição teria se as informações sobre ataques cibernéticos perpetrados na infraestrutura tecnológica da FARD seriam negativos e poderiam ter um grande impacto tanto na mídia nacional e internacional, como nas redes sociais.

5- Que projetos tem o FARD sobre aspectos cibernéticos como resultado da campanha de conscientização sobre segurança cibernética realizada pelo CSIRT-Defesa?

RESP: 5.1- Graças às campanhas realizadas pela CSIRT-Defense, a FARD poderá desenvolver as suas competências em cibersegurança através do exercício Capture the Flag (CTF) realizado pela equipa CSIRT-Defense; bem como o projeto de implantação da ferramenta Wazuh para monitoramento da infraestrutura crítica do FARD.

RESP: 5.2- Perante a necessidade de proteger o seu ciberespaço, o FARD optou pela criação de uma direção de cibersegurança dentro da instituição.

RESP: 5.3- Os projetos em conjunto com o CSIRT-Defesa visam recolher as necessidades das instituições ao nível da Defesa Cibernética, tanto ao nível do licenciamento como da formação de pessoal, para sensibilizar os utilizadores para a utilização das novas tecnologias.

RESP: 5.4- Estabelecer uma área de cibersegurança que assegure a implementação de boas práticas de cibersegurança, análises de vulnerabilidade recorrentes de todas as plataformas que entram online, bem como a inclusão de questões de cibersegurança nas formações da academia.

Entrevistados

1- Operações Cibernéticas da CSIRT-Defesa, Francis Segura.

2- Operações Cibernéticas da CSIRT-Defesa, Mark Benítez.

3- Departamento de Tecnologia da Informação da Força Aérea Dominicana

4- Diretora de Cibersegurança e Ciberdefesa do Centro de Comando e Controle, Comunicação, Informática, Cibersegurança e Inteligência, C5i das Forças Armadas, A/M Elsa Encarnación, MIDE.