INSTITUTO POLITÉCNICO DE BRAGANÇA
Escola Superior de Tecnologia e Gestão

Procedimentos de Resposta a Incidentes de Cibersegurança no GRA

Rui Pedro Afonso Barata

Relatório de Projeto apresentado à Escola Superior de Tecnologia e Gestão para obtenção do Grau de Mestre em Informática

Trabalho realizado sob a orientação de:

Professor Tiago Pedrosa

Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança

Bragança

Maio de 2023

Dedicatória

A ti meu Pai, meu Herói e exemplo, que partiste cedo demais…

Agradecimentos

Depois de um longo percurso de trabalho e dedicação, seria bastante ingrato deixar de parte este especial agradecimento a todos os que me deram apoio para alcançar esta conquista.

Em primeiro lugar, e como não poderia deixar de ser, agradeço aos meus pais, tia, esposa, filho, irmã, cunhado e sobrinho pelo amor e apoio incondicional durante todo este caminho.

Ao meu orientador, o Professor Tiago Pedrosa, pela orientação prestada, pelo seu incentivo, disponibilidade, apoio, compreensão e amizade que sempre demonstrou.

À Presidência do Governo Regional dos Açores, nas pessoas dos Assessores Dr. º Luís Ramos Freitas e Dr. º Carlos Borges, assim como ao Diretor Regional da DRCTD, Eng.º Pedro Batista e ao Diretor de Serviços da Direção de Serviços Técnicos e de Cibersegurança, Eng.º Fernando Reis, que possibilitaram a realização do trabalho.

Ao Eng. Pedro Freitas, Dr. º Bruno Veríssimo e Dr.ª Isabel Carvalho, que me apoiaram durante os Exercícios de Cibersegurança e ajudaram na concretização dos mesmos.

Resumo

A evolução tecnológica, principalmente o aparecimento da Internet e a generalização do seu uso, veio alterar por completo as sociedades e o seu funcionamento.

Esta evolução tecnológica tem impactado todos os sectores de atividade e com ela surgiram enormes desafios para as organizações, dos quais salientamos a mobilidade e a segurança dos dados, assim como a literacia informática dos colaboradores, desafios que também o Governo Regional dos Açores enfrenta.

O GRA, através do seu Programa de Governo, assumiu a Cibersegurança como um dos pilares de desenvolvimento do seu território e procura consolidar o seu posicionamento de vanguarda ao nível da Inovação e Desenvolvimento Tecnológico.

Este documento traduz a preparação e a análise que foi desenvolvida, nomeadamente no que se refere ao levantamento de constrangimentos e de requisitos do Ecossistema GRA, bem como, a participação do GRA em Exercícios de Cibersegurança, e ainda uma reflexão sobre o que já foi realizado.

Com a Participação nos Exercícios de Cibersegurança (ExNCS2022 e CyP2022), o GRA pretendeu testar e melhorar os seus procedimentos, e assim promover uma cultura de segurança, relativa à utilização dos meios informáticos, contribuindo para a sensibilização e aumento da ciber-maturidade regional, assente em políticas adequadas, em articulação com um conjunto de entidades nacionais com competências em matéria de Cibersegurança, para uma proteção eficaz contra as ameaças com origem no ciberespaço.

Foi proposta a determinação de políticas e de normas de utilização de meios informáticos e a definição de um modelo de governança que permita a gestão e capacidade de resposta adequadas no âmbito da Cibersegurança, que se pretende que seja implementada, primeiramente, nos serviços da Presidência do GRA e, posteriormente, seja replicada a todas as Secretarias e Direções Gerais do GRA, contribuindo assim para uma cultura de Segurança e potenciando o aumento da resiliência e redundância da Região.

Palavras-Chave: Cibersegurança, GRA, Resposta a Incidentes de Segurança, Cultura de Segurança

Abstract

Technological evolution, mainly the appearance of the Internet and the generalization of its use, completely changed societies and their functioning.

This technological evolution has impacted all sectors of activity and with it, enormous challenges have arisen for organizations, of which we highlight data mobility and security, as well as the IT literacy of employees, challenges that the Regional Government of the Azores also faces.

GRA, through its Government Program, has assumed Cybersecurity as one of the pillars of development in its territory and seeks to consolidate its vanguard position in terms of Innovation and Technological Development.

This document translates the preparation and analysis that was carried out, namely regarding the survey of constraints and requirements of the GRA Ecosystem, as well as the participation of the GRA in Cybersecurity Exercises, and a reflection on what has already been done.

With the participation in the Cybersecurity Exercises (ExNCS2022 and CyP2022), the GRA intended to test and improve its procedures, and thus promote a culture of security, regarding the use of computer resources, contributing to raising awareness and increasing regional cyber-maturity, based on appropriate policies, in conjunction with a set of national entities with competences in the field of cybersecurity, for effective protection against threats originating in cyberspace.

It was proposed to determine policies and standards for the use of IT resources and the definition of a governance model that allows for adequate management and response capacity in the context of Cybersecurity, which is intended to be implemented, firstly, in the services of the Presidency of the GRA and, subsequently, be replicated to all the Secretariats and General Directorates of the GRA, thus contributing to a culture of Safety and enhancing the Region's increased resilience and redundancy.

Índice Geral

Lista de Siglas/Abreviaturas

APR – Administração Pública Regional

B&C – *Bain & Company*

BEC– *Business E-mail Compromise*

CCEJ – GR - Centro de Consulta e Estudos Jurídicos do Governo Regional

CEO - *Chief Executive Officer* - Diretor Executivo

CERT - *Computer Emergency Response Team*

CERT.PT - Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei 46/2018)

CISO – *Chief Information Security Officer*

CNCS - Centro Nacional de Cibersegurança

CNPD - Comissão Nacional de Proteção de Dados

CSI - *Computer Security Institute*

CSIRT - *Computer Security Incident Response Team*

CUF - Companhia União Fabril

CyP2022 – Exercício CIBER PERSEU 2022

DDoS – *Distributed Denial of Service*

DGPJ - Direção-Geral da Política de Justiça

DoS - *Denial of Service*

DPO - *Data Protection Officer* – Encarregado de Proteção de Dados

DRCom – Direção Regional de Comunicações

DRCTD – Direção Regional das Comunicações e da Transição Digital

DRS – Direção Regional de Saúde

EAC – *E-mail Account Compromise*

EC3 - *European Cybercrime Centre*

ENISA - *European Union Agency for Cybersecurity* - Agência Europeia para a Segurança das Redes e da Informação

ENSC - Estratégia Nacional para a Segurança do Ciberespaço

ESTIG – Escola Superior de Tecnologia e Gestão

EU - *European Union* – União Europeia

EUROPOL - Agência da União Europeia para a Cooperação Policial

ExNCS 2022 – Exercício Nacional de Cibersegurança 2022

FBI - *Federal Bureau of Investigation*

FPC – *Final Planning Conference*

GRA – Governo Regional dos Açores

HDES – Hospital do Divino Espírito Santo de Ponta Delgada

HH – Hospital da Horta na Ilha do Faial

HSEIT – Hospital do Santo Espírito da Ilha Terceira de Angra do Heroísmo

IC3 – *Internet Crime Complaint Center*

IoT – *Internet of Things* – Internet das Coisas

IPB – Instituto Politécnico de Bragança

IPC – *Initial Planning Conference*

IPS - *Intrusion Prevention System*

ISO - *International Standard Organization*

IT – *Information Technology*

LIR - *Local Internet Registry*

MOOC - *Massive Open Online Course* - Curso Online Aberto e Massivo

MPC – *Main Planning Conference*

NATO ou OTAN - *North Atlantic Treaty Organization* ou Organização do Tratado do Atlântico Norte

OCS – Órgãos de Comunicação Social

ONU – Organização das Nações Unidas

PGR – Procuradoria-Geral da República

PGRA – Presidência do Governo Regional dos Açores

POC – Ponto de Contato

QNRCS - Quadro Nacional de Referência para a Cibersegurança

RAA - Região Autónoma dos Açores

RASI – Relatório Anual de Segurança Interna

RCMCS - Roteiro de Capacidades Mínimas de Cibersegurança

RDP – *Remote Desktop Protocol*

RGPD - Regulamento Geral sobre a Proteção de Dados

RNCSIRT – Rede Nacional de CSIRT

RSIT WG – *Reference Security Incident Taxonomy Working Group* da ENISA

SIEM – *Security Information and Event Management*

SINP - Sistema Interno de Normas e Políticas

SOC – *Security Operations Center* – Centro de Operações de Segurança

TI – Tecnologia da Informação

TIC – Tecnologias da Informação e Comunicação

USB - *Universal Serial Bus*

USB IF - *Universal Serial Bus Implementers Forum*

WWW – *World Wide Web*

Índice de Figuras

Índice de Tabelas

Capítulo 1 Introdução

Este Capítulo pretende apresentar a evolução tecnológica e o que, por consequência, surgiu, a cibercriminalidade e as suas consequências, quer ao nível económico como de impacto nas organizações. A necessidade da Cibersegurança e das políticas, medidas e mecanismos que a podem regular.

1.1. Introdução

A evolução tecnológica, especialmente o surgimento da Internet e sua ampla adoção, transformou as sociedades, levando-nos das Sociedades Industriais para a Sociedade da Informação. Nesta nova sociedade globalizada, há um ênfase na partilha e no fácil acesso a diferentes tipos de informação. Estados, indivíduos e organizações passaram a depender do uso das TIC, especialmente da Internet, para realizar as suas tarefas diárias.

As organizações foram afetadas pela Sociedade da Informação, resultando em novas formas de relacionamento e paradigmas organizacionais. Algumas organizações existem virtualmente, com uma presença predominantemente online, enquanto outras adotaram modelos de descentralização, permitindo que diferentes partes da produção estejam localizadas em qualquer lugar do mundo. Mesmo com esta dispersão geográfica, elas ainda são capazes de produzir bens e fornecer serviços a clientes noutros locais, muitas vezes simultaneamente. Um exemplo disso é a indústria automobilística e o setor de desenvolvimento tecnológico.

Neste ambiente, começaram a surgir ataques a este sistema global de informação, onde a informação já não se encontra armazenada num espaço específico e restrito, passando a estar num local - ciberespaço - que, devido à sua amplitude, torna mais difícil o controlo

do acesso à informação, podendo torná-la mais acessível a indivíduos mal-intencionados, dotados de determinadas competências informáticas - *hackers*. Portanto, este sistema pode deixar os Estados, as organizações e os cidadãos mais vulneráveis a ciberataques, geralmente realizados com o intuito de proporcionar benefícios económicos ao atacante, a disrupção e desestabilização de Estados e/ou indivíduos, etc. (Mamede, 2006)

Segundo informação já referida no Relatório de Cibercrime de 2012 da Norton, o cibercrime está a aumentar rapidamente, representando um desafio considerável para as agências de aplicação da lei e um custo significativo para a sociedade no geral: um relatório recente sugere que, todos os anos, no mundo inteiro, as vítimas perdem cerca de 290 mil milhões de euros (somando tempo e dinheiro), como resultado do cibercrime, tornando-o mais rentável que o comércio mundial de marijuana, cocaína e heroína, juntas (custo estimado em 215 mil milhões), a estes custos temos de acrescentar os custos relativos à perda de credibilidade, que não são facilmente mensuráveis. (Norton, 2013)

Tendo por base os dados do IC3, no seu *2021 Internet Crime Report*, nos últimos 5 anos (2017 - 2021), estes registaram um total de 2,76 Milhões de queixas e uma perda monetária de 18,7 Biliões de dólares, o que corresponde a uma média de 552,000 queixas por ano, mais de 2,300 queixas diárias, e representaram uma perda monetária de 3,74 Biliões de dólares anuais. (IC3, 2022)

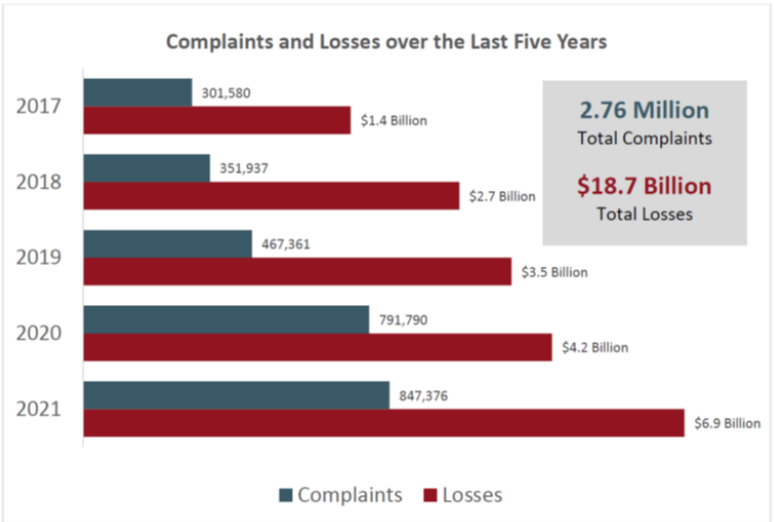


Figura 1 - Queixas e Perdas Monetárias nos últimos 5 anos (2017-2021) – Dados IC3 FBI

Os dados mais recentes mostram que, as ameaças digitais estão a evoluir rapidamente e que o público considera a cibercriminalidade como uma ameaça importante: alguns

estudos, levados a cabo pela UE, sugerem que, tendo-se verificado um aumento de 300% dos ataques com recurso a software de sequestro desde 2015, o impacto económico da cibercriminalidade aumentou cinco vezes entre 2013 e 2017, quadruplicando até 2019. Oitenta e sete por cento dos europeus consideram a cibercriminalidade como um desafio importante para a segurança interna da UE. (Commission, 2017)

A temática da Segurança Informática é tão antiga como a temática de Utilização de Meios Automáticos para o tratamento e o Armazenamento de Informação. (Mamede, 2006)

Os sistemas informáticos são maioritariamente utilizados para o processamento e o armazenamento de informação em formato digital, pelo que a abordagem à segurança desses sistemas estará intimamente relacionada com a segurança de dados e de informação.

Se considerarmos que os dados são observações individuais, medidas e primitivas de mensagens, estando na base da comunicação humana, das mensagens textuais, das interrogações eletrónicas e nos instrumentos científicos de medição de fenómenos, conforme definiu *Edward Waltz*, em 1998; e a Informação não é mais do que um conjunto organizado de dados, através de classificação, indexação ou do estabelecimento de relações, que permita posterior pesquisa e análise. Podemos concluir que o conhecimento não é mais do que informação analisada e compreendida. (Carvalho, 2009)

A Segurança Informática para além de outras questões e dificuldades depara-se com um "grande Dilema: os utilizadores que possuem requisitos de segurança, mas que não têm qualquer sensibilidade para as questões de segurança". É partindo deste dilema que os profissionais de segurança têm de procurar dar resposta, projetando soluções que respondam aos requisitos das Organizações e aos seus utilizadores.

A utilização destes mecanismos de proteção para atingir os objetivos pretendidos, podem ser implementados sob diversas formas, sendo da responsabilidade do Técnico / Organização que as projeta escolher a sua incidência, se sob os dados, as operações, os recursos ou sobre os utilizadores.

Inicialmente, a Segurança Informática estava endereçada para a garantia de disponibilidade de dados e a proteção do ambiente de computação da altura, fortemente centralizados. Neste sentido, foram desenvolvidos mecanismos para a proteção de dados,

através de *Backup* e outros conceitos, de modo a garantir que em caso de avaria de hardware, a informação contida nos dispositivos fosse recuperável. Com estas medidas surgiram os sistemas de cópia de segurança, que apesar de permitirem recuperar os dados, apenas o garantiam para um período anterior, o que originava a perda dos dados tratados e alterados mais recentemente. No seguimento deste processo, as questões levantadas com a prevenção de incêndios, inundações e outras questões de âmbito ambiental foram também apreciadas. (Monteiro, 2003)

O processo ideal será aquele que consiga dar o mesmo nível de atenção a todos os aspetos referidos, no entanto, isso poderá criar vulnerabilidades de segurança, pelo que o seu grau de incidência deve ser cuidadosamente ponderado.

Após estas preocupações estarem resolvidas, novas surgiram relativamente ao controlo de acesso ao sistema e aos dados, o que trouxe a evolução dos sistemas computacionais e consigo as redes de computadores e os problemas associados a estas.

Com a interligação destas redes e a constituição da Internet, os problemas existentes multiplicaram-se exponencialmente, com a banalização da utilização da Internet diariamente, e não apenas no local de trabalho, os problemas de segurança contemplaram também os computadores de utilização doméstica.

Do ponto de vista da Segurança Informática, partimos de uma altura em que os ambientes empresariais eram estanques, sem contacto com o exterior em que os componentes internos desses ambientes eram baseados em sistemas com linhas privadas e onde as possíveis variáveis exógenas eram facilmente controladas.

Com a evolução ao nível informático, das redes e dos equipamentos, com todas as funcionalidades, acessibilidades com e sem fios e a comunicação a ser maioritariamente suportada pela Internet, o ambiente Empresarial é hoje cheio de fragilidades e vulnerabilidades através de vírus informáticos, roubo de dados, interceção de comunicações, negação de serviço, ataques a redes sem fios e a servidores. Mas os problemas não se situam apenas do lado de fora das organizações, pois no interior das mesmas existem diversos comportamentos e atitudes que podem facilitar o desenvolvimento de ataques.

Estes comportamentos e atitudes proporcionam um dos vetores de ataque mais difíceis de gerir por parte dos responsáveis de segurança, visto, ser impossível prever as reações dos colaboradores com os quais as empresas interagem. Podemos exemplificar estes comportamentos pela forma como muitas vezes, dentro da organização, se partilha informação e documentos de modo não seguro, seja através de dispositivos móveis (*USB drives*, discos externos, etc.) ou o acesso aos diversos sistemas da organização através de equipamentos tablets ou telemóveis não protegidos e fora do perímetro físico da empresa.

Esta situação, de acordo com o CSI – *Computer Security Institute*, tem levado a que os crimes relacionados com a informática e sistemas tenham vindo a aumentar de forma muito sustentada, bem como os custos associados aos mesmos, tendo como exemplo o aumento verificado nos Estados Unidos da América entre 1997 e 2001 a situar-se nos 1460 milhões de dólares. (CSI, 2022)

A que se deve o aumento de custos associados com os problemas de segurança? Este aumento deve-se, principalmente, ao facto de as Organizações não acompanharem a evolução tecnológica, tomando atitudes pró-ativas de modo a melhorar as questões de Segurança.

Se formos verificar as principais causas de falhas de Segurança nas Organizações, constatamos que, estas se devem à exploração por parte dos "*Hackers*" de vulnerabilidades públicas e que apesar de terem sido comunicadas há bastante tempo, não foram implementadas as correções e as atualizações necessárias para as debelar. Outro dos grandes problemas é o de estereotipar os "*Hackers*" como sendo alguém que ataca os sistemas por divertimento, sendo que, existem estudos, como o realizado por Richard Power, em 2000, que comprova que a maioria dos crimes informáticos provêm de "*Hackers*" profissionais. (Power, 2000)

Partindo da análise destes dados, verificamos que a ameaça é real e que se as Organizações não começarem a considerá-la de uma forma séria, os ataques vão crescer, quer em custos quer em volume. Nesse sentido, como ponto de partida, as Organizações devem pugnar para que os seus Sistemas estejam atualizados, o que representa um esforço mínimo, mas que ao nível da segurança representa benefícios significativos. (Mamede, 2006)

Um estudo realizado pela *Bain & Company* revelou que, em média, as empresas demoram 210 dias para descobrir que sofreram uma invasão de *Hackers* e outros 24 dias para solucionar totalmente o problema. (Company, 2018)

De acordo com o mesmo estudo, as empresas possuem, em média, 5,3 mil áreas vulneráveis a ataques em toda a sua estrutura de tecnologia da informação, 27 por cento mais do que possuíam no ano anterior. O aumento das áreas vulneráveis está relacionado com a distribuição de dados em diferentes centros de informações, bem como, a adoção de mais aplicações e programas que não são controlados pela equipa de TI das empresas, e ao aumento do uso de dispositivos móveis de uso pessoal nas companhias.

Nesse ambiente, detetar as ameaças e combatê-las tornou-se uma tarefa mais demorada. O resultado é que os Cibercriminosos têm mais tempo para roubar informações e cometer fraudes, até que as falhas de segurança sejam solucionadas pelas organizações. De acordo com o estudo da *Bain & Company*, o prejuízo médio por invasão para cada organização é de 9 milhões de dólares.

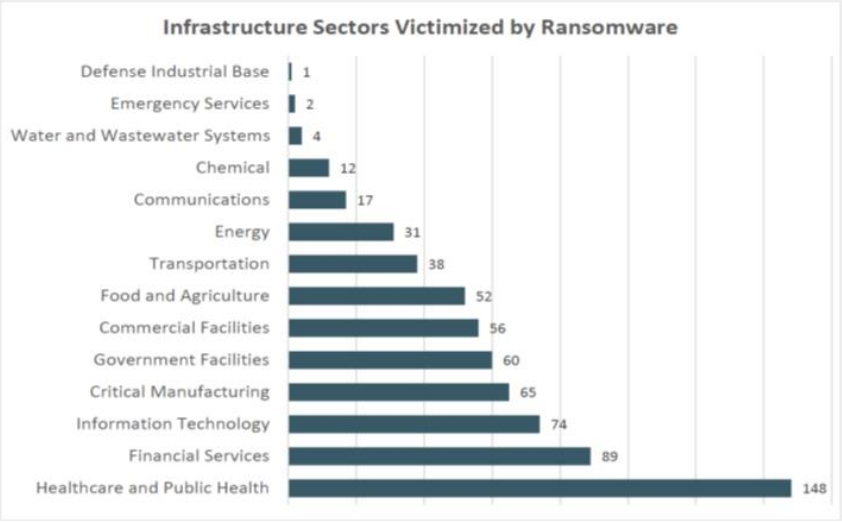


Figura 2 - Sectores Infraestruturais vítimas de Ransomware em 2021 – Dados IC3 FBI

No ano de 2021 o IC3 recebeu 649 queixas que indicavam que organizações pertencentes ao setor das infraestruturas críticas foram vítimas de um ataque de *ransomware*. Dos 16 setores de infraestruturas críticas, o IC3 reportou que 14 setores tiveram pelo menos 1 membro que foi vítima de um ataque de *ransomware* em 2021. (IC3, 2022)

Assim, a Cibersegurança e a Ciberdefesa posicionam-se, atualmente, como fatores determinantes para a garantia do sucesso e da resiliência das sociedades, assim como, das

organizações e dos indivíduos que as integram. Com o desenvolvimento ubíquo das iniciativas e soluções que tornam a nossa vivência cada vez mais digital, importa estabelecer estratégias e mobilizar recursos capazes de dar resposta adequada às ameaças e aos riscos crescentes.

O Regulamento Cibersegurança da União Europeia define a Cibersegurança como "as atividades necessárias para proteger a rede e os sistemas de informação, os utilizadores desses sistemas e outras pessoas afetadas pelas ciberameaças". (Europeia, 2019) No relatório do *The Global Risks Report 2021* do Fórum Económico Mundial, no top 10 de riscos por probabilidade de ocorrência, as falhas de Cibersegurança ocupam a 9ª posição, demonstrando a preocupação crescente com este tipo de ameaças. (Forum, 2021)

Atendendo ao número crescente de ciberataques de forma transversal em todos os setores, públicos ou privados, importa estabelecer políticas, medidas e mecanismos adequados para que as entidades se protejam e alcancem um patamar de preparação e maturidade cibernética proporcional às ameaças. Neste domínio, deve ter-se em consideração, também, os normativos legais que dispõem sobre a matéria de Cibersegurança e a *compliance* com os mesmos, bem como as diretrizes e recomendações de entidades com competência na matéria, como o Centro Nacional de Cibersegurança (CNCS).

De acordo com o supracitado, e se, por um lado, a digitalização trouxe, também, novos riscos e potenciou o aumento dos ciberataques, por outro lado, existe uma maior conscientização da necessidade de implementar medidas e boas práticas que protejam as entidades no seu todo, incluindo informação, dados, sistemas e recursos e, por conseguinte, a continuidade do seu negócio. (Mamede, 2006)

Ainda, e atendendo às próprias interligações entre organizações públicas e privadas, as fragilidades de uma no domínio da Cibersegurança podem expor várias outras organizações a ciberameaças devendo posicionar-se a Cibersegurança como vetor determinante da resiliência das sociedades e organizações como um todo.

A definição de boas práticas fundamentais em matéria de Cibersegurança constitui-se como a base de partida para uma estratégia robusta. De igual modo, uma boa gestão de Cibersegurança é essencial para a segurança da informação e dos sistemas informáticos.

Em Portugal, a perceção de risco de alguma entidade sofrer um Incidente de Cibersegurança aumentou em 2021 para 98% dos inquiridos no inquérito anual à comunidade de entidades com protocolo com o CNCS - mais 4% do que em 2020, mas, apesar do incremento da perceção de risco, uma grande parte dos inquiridos (48%) considera que o ciberespaço de interesse nacional está mais capacitado em 2021.

De acordo com o conjunto de dados do Relatório de Riscos & Conflitos (junho de 2022), a tipologia de ciberameaças, efetivamente, mais relevantes em Portugal em 2021 eram o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla online, o comprometimento de contas ou tentativa e a exploração de vulnerabilidades, segundo o CNCS. (CNCS, Relatório de Cibersegurança em Portugal - Riscos & Conflitos 2021, 2022)

A tendência de aumento no volume de incidentes e de indicadores de cibercrime em 2021 não foi apenas nacional, mas também internacional de acordo com dados do ENISA (ENISA, 2021) e da Europol (EC3, 2021).

Identificavam-se as seguintes prospetivas para o ciberespaço de interesse nacional em 2022 e 2023: o contexto internacional propenso à ação de atores estatais; a persistência da exploração das fragilidades do fator humano; os casos de ransomware; as violações de dados para uso de credenciais de acesso; a exploração de vulnerabilidades; e a relevância das tecnologias móveis e da Internet das Coisas como potenciais superfícies de ataque. (CNCS, 2022)

1.2. Enquadramento

Considerando, que há ciberataques em Portugal, todos os dias e a todas as horas, todos com consequências distintas e muitos deles sem êxito, pelo que não são notícia. De referir, que no ano de 2022 já houve, em território nacional, oito grandes ciberataques, tendo dois deles provocado a destruição de toda a informação das organizações visadas.

Salientamos ainda que, alguns destes ciberataques tiveram como alvo o sector da saúde nacional (Hospital Garcia da Orta, Hospital de Almada, etc.), e que a Região Autónoma dos Açores sofreu, recentemente, dois grandes ataques (Hospital do Divino Espírito Santo de Ponta Delgada – HDES e a Empresa Eletricidade dos Açores – EDA).

O Governo Regional dos Açores (GRA) participou, pela primeira vez no Exercício Nacional de Cibersegurança 2022 – ExNCS2022, através da Presidência do GRA e da DRCTD - Direção Regional de Comunicações e Transição Digital. Tendo este Exercício Nacional de Cibersegurança sido vocacionado para testar a resiliência do sector da Saúde, participaram, conjuntamente, as entidades de Saúde Regional dos Açores (DRS - Direção Regional de Saúde dos Açores, HDES - Hospital do Divino Espírito Santo de Ponta Delgada, HSEIT - Hospital do Santo Espírito da Ilha Terceira em Angra do Heroísmo e HH - Hospital da Horta).

O Exercício serviu como ponto de partida e análise sobre a capacidade de resposta do GRA a um Incidente de Cibersegurança, permitindo obter uma imagem clara sobre o que já foi feito e o que é premente realizar. Para isso muito contribuiu a "experiência" ganha aquando do incidente ocorrido no HDES, em julho de 2021 e que empenhou inúmeros elementos do GRA (DRCTD).

Neste sentido e considerando as minhas funções no GRA, trabalhando na Presidência do GRA, mais concretamente no Gabinete de Segurança da Presidência do GRA, com incidência nas Áreas de Segurança Interna, Defesa Nacional e *Security* & *Safety*, e no Órgão de Segurança Sub-Registo da Presidência do Governo Regional dos Açores como substituto do Encarregado de Segurança e Administrador CRESO, e tendo sido nomeado como POC do GRA no ExNCS2022 e como POC e *Planner* no CyP2022, e fazendo parte do grupo de trabalho que tem participado ativamente na discussão e na implementação do CJCS no GRA, encontro-me numa posição privilegiada para a prossecução deste trabalho, onde poderei contribuir para a criação e implementação de procedimentos de resposta em caso de incidentes de Cibersegurança no Ecossistema GRA, assim como na obtenção, do GRA, de capacidades mínimas de resposta a esse tipo de incidentes.

1.3. O Problema

As organizações são cada vez mais confrontadas com ataques ou tentativas de ataques que, se bem-sucedidos, acarretam enormes prejuízos diretos e indiretos.

Os custos com a Segurança Informática têm vindo a aumentar de forma exponencial, sendo que a grande maioria das organizações não possui capacidade de resposta, quer a

nível financeiro, quer a nível de recursos humanos, que lhes permita acompanhar a evolução dos ataques e das vulnerabilidades a que se encontram expostos.

No caso do GRA, apesar do enorme esforço na implementação de medidas de Cibersegurança, foi possível verificar que não existe, neste momento, um Manual de Procedimentos e/ou de resposta a Incidentes de Cibersegurança para que as entidades que constituem o Governo Regional dos Açores – GRA, possam seguir e ter uma linha condutora, que as auxilie, no caso de sofrerem um incidente de Cibersegurança.

1.4. Objetivos

Pretende-se, com este trabalho, contribuir para o aumento da capacidade do GRA na prevenção, na análise e na resposta a Incidentes de Cibersegurança.

Nesse sentido, pretende-se criar uma proposta de Manual de Procedimentos e de Resposta a Incidentes de Cibersegurança, melhorando assim os procedimentos e procurando implementar alguns processos mais eficientes, junto das entidades ligadas ao GRA, neste tipo de situações, e testar os mesmos em contexto de exercícios nacionais de Cibersegurança (ExNCS2022 e CyP2022).

1.5. Estrutura do Documento

Este documento está organizado em 6 Capítulos.

O Capítulo 2 pretende desenvolver a questão da Cibersegurança como Política Pública assim como apresentar a ocorrência da Criminalidade Informática a nível Nacional e depois com maior incidência na RAA.

O Capítulo 3 apresenta as normas e metodologias existentes para a resposta a incidentes de segurança, que servirão de base para a proposta.

O Capítulo 4 é a descrição da Proposta que será aplicada na resposta a incidentes de segurança no GRA.

O Capítulo 5 descreve a participação do GRA nos Exercícios de Cibersegurança (ExNCS2022 e CyP2022), onde foi testada a proposta de resposta a incidentes de segurança, assim como uma análise à participação do GRA.

No Capítulo 6 são apresentadas as conclusões acerca do que foi feito e apresentadas propostas para trabalho futuro.

Capítulo 2 Cibersegurança

Neste Capítulo vamos abordar a questão da Cibersegurança, o que é, como evoluiu, e a forma como deve ser encarada, através de Política Pública, analisando ainda a questão da Cibercriminalidade e do seu impacto em Portugal e ainda na Região Autónoma dos Açores.

2.1. A evolução da Cibersegurança

Se pensarmos o quanto o mundo evoluiu nos últimos 30 anos, o que mais se destaca é a nossa relação com a tecnologia. Em 1994 a internet já era acessível a pessoas e empresas, mas de forma muito mais simples e limitada do que nos dias de hoje. Mas mesmo nessa altura já existia a preocupação com a questão da Cibersegurança. As empresas tecnológicas já compreendiam a importância de se contruírem plataformas de redes seguras e a importância que isso teria num futuro próximo. (Leite, 2016)

Mas mesmo estas empresas não poderiam imaginar a evolução que se veio a verificar, com os negócios e a sociedade a estruturarem-se em torno da internet, de tal forma que não podem existir mais fora desta. O mundo todo conectou-se à Internet e com a chegada da Internet das Coisas (IoT) surgiu uma questão que há 30 anos não podia ser feita – Como nos podemos preparar para uma realidade Hiper conectada?

Com os avanços realizados nas últimas três décadas, o problema da segurança digital, tornou-se mais crítico que nunca. Com o aumento das “coisas” conectadas, também as ameaças cresceram e diversificaram-se, pois, cada dispositivo conectado é também uma potencial brecha de segurança. Além disso, também evoluíram os hábitos de utilização das pessoas, o que abriu novas portas a serem utilizadas pelos criminosos. (Leite, 2016)

O dinheiro existente nas redes informáticas, alvo prioritário há 30 anos, não é, agora, o bem mais precioso que os Cibercriminosos podem obter, mas sim os dados e a privacidade das empresas. Com o crescimento exponencial do tráfego de dados, que transitam por biliões de dispositivos, as possibilidades de ataque tornaram-se infinitas, variando do clássico *malware* até a práticas modernas como a violação de dados bem-sucedidas e casos de *ransomware* com pagamento do resgate.

Com este novo cenário, se há 30 anos as ameaças digitais eram pensadas para atacar as infraestruturas das empresas, hoje elas são pensadas para terem como alvo as pessoas e os seus hábitos de consumo. Exemplo disso são os e-mails e mensagens de *phising*, empregando *links* de sites muito utilizados pelos utilizadores, arquivos falsos de fotos e vídeos, ficheiros *word* ou *pdf* que executam programas sem conhecimento dos utilizadores ou correntes no *WhatsApp* utilizando temas do momento.

Deste modo, a mesma ameaça, desenvolvida com os mesmos recursos, pode vitimar desde o CEO de uma grande empresa, um político influente ou qualquer outra pessoa, podendo causar danos devastadores aos dados e à privacidade, com impactos inimagináveis no mundo real, tanto a nível social como económico.

Estes ataques existem, e conseguem cumprir os seus objetivos porque não estamos preparamos para proteger as pessoas e as empresas digitalmente, pois as pessoas, ainda não se consideram bem informadas sobre estes incidentes de segurança.

Um claro exemplo disso foi a multiplicação de cibercrimes durante o período de confinamento adotado devido à pandemia causada pelo novo coronavírus – CoVID 19.

Com o aumento do número de utilizadores da internet, de forma dramática, devido à implementação do ensino à distância e ao teletrabalho, os Cibercriminosos aproveitaram o facto de as redes de internet domésticas não possuírem as mesmas configurações de segurança que as redes empresariais.

Verificou-se uma multiplicação de esquemas de fraudes eletrónicas para a obtenção de senhas e dados financeiros pessoais e empresariais, ataques de ransomware e a disseminação de notícias falsas.

Durante a primeira vaga da pandemia da CoVID-19, um dos alvos preferenciais dos Cibercriminosos, foi o Sector da Saúde visto, os hospitais dependerem da tecnologia digital. O tipo preferencial de ataque foram os ataques de *ramsonware*, pois na situação

em que o Sector da Saúde se encontrava, no combate à pandemia, iriam pagar os resgates pedidos sem hesitar, após terem o seu sistema informático infetado e os seus dados encriptados.

2.2. A Cibersegurança

A Cibersegurança é a prática que permite proteger computadores, servidores, dispositivos móveis, sistemas eletrónicos, redes e dados de ataques maliciosos. A Cibersegurança é também conhecida como sendo a segurança da Tecnologia da Informação ou a Segurança de Informações Eletrónicas. (Kaspersky, 2023)

O termo Cibersegurança pode ser aplicável a uma grande variedade de contextos, que vão desde negócios até a computação móvel, pode ser dividido em algumas categorias comuns (Kaspersky, 2023):

Segurança de Rede – engloba os procedimentos que protegem uma rede de computadores contra intrusos, sejam eles invasores direcionados ou *malware* oportunista.

Segurança de Aplicações - focada em manter o *software* e os dispositivos livres de ameaças. Uma aplicação comprometida pode fornecer acesso aos dados que se pretende proteger. O sucesso da segurança começa na fase de projeto, bem antes de um programa ou dispositivo ser inserido no sistema.

Segurança de Informação – pretende proteger a integridade e a privacidade dos dados, tanto no armazenamento como em trânsito entre os elementos da entidade.

Segurança Operacional - inclui os processos e decisões para tratamento e proteção dos arquivos com dados. As permissões que os utilizadores têm ao aceder a uma rede e os procedimentos que determinam como e onde os dados podem ser armazenados ou compartilhados enquadram-se nesta categoria.

A Recuperação de desastres e continuidade dos negócios - definem como uma organização responde a um incidente de Cibersegurança ou qualquer outro evento que cause a perda de operações ou dados. As políticas de recuperação de desastres determinam como a organização restaura as suas operações e informações para voltar à mesma capacidade operacional anterior ao evento. A continuidade dos negócios é o plano

ao qual a organização recorre para tentar trabalhar sem determinados recursos, isto é, a sua capacidade de resiliência.

Educação do utilizador final - aborda o fator de Cibersegurança mais imprevisível: as pessoas. Qualquer pessoa pode introduzir acidentalmente um vírus num sistema seguro se deixar de seguir as práticas recomendadas de segurança. Ensinar/alertar os utilizadores a excluir anexos suspeitos de e-mail, não conectar unidades USB não identificadas e várias outras lições importantes é vital para a segurança de qualquer organização.

2.3. A Cibersegurança como Política Pública

A Cibersegurança é uma política pública transversal que abrange diversas áreas setoriais e está cada vez mais presente devido à aceleração do processo de transição digital. Os riscos e ameaças à segurança das redes e sistemas de informação aumentam, apresentando desafios significativos para as entidades que dependem desses recursos para suas atividades. (CNCS, Relatório de Cibersegurança em Portugal - Políticas Públicas, 2021)

Em Portugal, as estratégias, programas e ações de Cibersegurança são fundamentadas num conjunto de dispositivos legais e regulamentares que estabelecem o quadro normativo para o desenvolvimento e implementação de políticas de segurança cibernética. Além disso, há uma componente institucional responsável pelo planeamento, execução, monitorização e fiscalização do cumprimento desse quadro normativo.

A participação de Portugal na União Europeia, bem como em organizações internacionais como a NATO e a OSCE, influencia o panorama jurídico-político nacional em Cibersegurança, uma vez que, medidas adotadas e compromissos assumidos nessas organizações têm impacto direto nas políticas internas. A estrutura institucional também procura a colaboração com atores externos, reconhecendo a importância das interações transnacionais diante de uma realidade que ultrapassa as fronteiras nacionais. As ameaças cibernéticas transnacionais e a alta interdependência das economias nacionais exigem ações coordenadas e cooperativas entre os Estados. A cooperação internacional é essencial para a prevenção e resolução de incidentes, bem como para a construção de um ciberespaço mais seguro numa sociedade cada vez mais digital. (CNCS, Relatório de Cibersegurança em Portugal - Políticas Públicas, 2021)

Desta forma, a Cibersegurança é abordada como uma questão de interesse público, que requer ações conjuntas e coordenação tanto no âmbito nacional quanto internacional, com o intuito de proteger a infraestrutura digital, os dados e os cidadãos contra ameaças cibernéticas em constante evolução.

2.4. Ciberataques em Portugal

O relatório de Cibersegurança em Portugal referente a 2021, publicado em maio de 2022 pelo Centro Nacional de Cibersegurança, aponta os setores da banca e da saúde como potenciais alvos. No documento é referido que "É expectável que ocorram ataques oportunistas ao trabalho remoto, às cadeias de fornecimento, aos setores da banca e saúde e às tecnologias emergentes".(CNCS, 2022)

Também o norte-americano Centro para a Queixa de Crimes na Internet (IC3, na sigla inglesa) identifica o setor da saúde pública como uma das 16 áreas críticas no que aos ataques informáticos diz respeito. Dentro desta lista de áreas críticas, o setor dos cuidados de saúde e saúde pública foi o mais atacado durante o ano de 2021, registando 148 incidências. (IC3, 2022)

Os dados pessoais, incluídos nas bases de dados das instituições de saúde, têm valor comercial, principalmente os de contacto e identificação do utente, e a ameaça da divulgação dos dados atua como um elemento de pressão muito elevado sobre a entidade, devido aos riscos legais, ao comprometimento dos dados e à reputação da empresa. No entanto, a venda e divulgação não serão a principal atividade dos hackers que optam, principalmente, por ataques de *ransomware*.

Em Portugal já ocorreram alguns ataques informáticos ao Sector da Saúde, dos quais se salientam:

- Ataque ao Hospital Garcia de Orta – últimos meses de 2016 – Ataque informático que atingiu o sistema onde são guardadas imagens obtidas em exames médicos como radiografias ou TAC, mas a unidade garantiu, na altura, que não foram roubados registos de utentes. Este ataque acabou por significar uma mudança do paradigma da Cibersegurança em Portugal. (Reis, 2017)

- Ataque ao Serviço Regional de Saúde dos Açores (SRSA) – MAR2017 - Os dados pessoais de 230 mil utentes do SRSA, quase todos os habitantes do Arquipélago dos Açores, foram publicamente expostos na Internet, no site da ARS Alentejo. O ficheiro tinha o nome 'Exportação Utentes SRSA para Reembolsos' e, numa grelha *Excel* estavam os dados discriminados dos utentes, incluindo nomes completos, número fiscal, número de utente dos serviços de saúde regionais, moradas, datas de nascimento e números de telefone e/ou telemóveis. (LUSA, Dados de 230 mil utentes dos Açores foram divulgados na Internet, 2017)
- Ataque à CUF – 03AGO2018 – Ataque cibernético aos sistemas informáticos, através do vírus *SamSam*, que bloqueou os dados desta rede privada de saúde pertencente ao Grupo José de Mello Saúde. Os responsáveis informáticos do Grupo Mello Saúde e os peritos da Polícia Judiciária (PJ) acabaram por constatar que o ataque não tinha começado nesse dia, mas sim vários meses antes. A normalidade da CUF apenas foi retomada cerca de uma semana depois da identificação do ataque. (Ferro, 2018)
- Ataque à Fundação Champalimaud – 01JUL2019 – Ataque cibernético aos sistemas informáticos, através de *ramsonware*, que bloqueou os dados da Fundação, tendo sido pedido um resgate para libertar o sistema, a que a Fundação não cedeu. Com o apoio da Altice Portugal, os responsáveis informáticos da Fundação conseguiram repor os sistemas, praticamente na sua plenitude, 44 Horas após a identificação do ataque. (DN/LUSA, Fundação Champalimaud sofre "ataque informático sem precedentes", 2019)
- Ataque Informático ao HDES – 16JUN2021 – Ataque informático através de um *crypto-ransomware*, que afeta o sistema operativo *Microsoft Windows*, denominado *WannaCry*, um tipo de ciberataque difundido em 2017 após afetar várias instituições em todo o mundo, como o Serviço Nacional de Saúde Britânico. A equipa da DRCTD optou por desligar todas as comunicações do hospital. Esta ação levou a constrangimentos na atividade assistencial daquela unidade hospitalar. Foram detetadas diversas falhas de segurança, pela equipa da Microsoft que foi contratada para intervir no Hospital. A normalização de todos os sistemas demorou vários meses a ser obtida. (LUSA, 2021)
- Ataque informático aos Laboratórios Germano de Sousa – 10FEV2022 - O ataque, através de um vírus que entrou no sistema informático, afetou principalmente a

comunicação informática entre postos de colheita e hospitais. A entidade referiu que os dados dos clientes não foram comprometidos. A resolução dos efeitos deste ataque demorou cerca de uma semana. (DN, 2022)

- Novo Ataque informático ao Hospital Garcia de Orta - 25ABR2022 – Ataque informático, de *Ramsonware* que afetou todos os serviços do Hospital, levando a que este ativasse o protocolo de segurança. Os Serviços Partilhados do Ministério da Saúde (SPMS) e o CNCS avaliaram a situação, tendo sido um processo moroso de normalização e reposição de todos os sistemas do Hospital. (DN/LUSA, 2022)

2.5. A Criminalidade Informática

O campo de atuação do cibercrime não se reduz a ações diretas sobre potenciais vítimas por parte de Cibercriminosos que, desenvolvam instrumentos técnicos maliciosos, mas é também constituído por um mercado de produtos e serviços que estes mesmos Cibercriminosos vendem a outros Cibercriminosos com menos competências técnicas ou que não investem em desenvolvimento. A esta atividade chama-se "cibercrime-como-serviço".

Verifica-se uma importância crescente do cibercrime-como-serviço e de agentes de ameaça, os *Hackers-for-Hire*, que alimentam uma segunda esfera, eventualmente menos especializada, de outros agentes de ameaça que atuam no ciberespaço. Segundo a ENISA, os *Hackers-for-Hire* tornaram-se um dos principais agentes de ameaça em 2021 e tendem a especializar-se em *Access-as-a-Service* e em práticas da família da espionagem. (ENISA, 2021)

O cibercrime-como-serviço provoca várias dificuldades ao combate ao cibercrime e à investigação criminal: facilita a entrada na cibercriminalidade de atores que não têm competências técnicas (ex. *script kiddies*), democratizando o cibercrime; dificulta a captura de toda a cadeia de cibercriminalidade, na medida em que, o vendedor/prestador do serviço deixa menos pegada; e propicia uma maior massificação do número de incidentes de Cibersegurança.

Os tipos de produtos e serviços mais relevantes comercializados nos mercados típicos do cibercrime-como-serviço, de acordo com relatórios da ENISA (ENISA, 2021) e da Europol (EC3, 2021), são:

- ***Access-as-a-Service:*** serviço de intrusão prestado em geral por organizações, com frequência a Estados, mas também a empresas e indivíduos, com o fim de aceder a sistemas alheios e recolher informação sensível;
- ***DDoS-For-Hire-Services:*** ações contratadas de negação de serviço distribuída, dirigidas a alvos específicos, muitas vezes utilizando a infraestrutura IoT e realizando um pedido de resgate;
- ***Disinformation-as-a-Service:*** campanhas de desinformação para manipular a opinião pública, disponibilizadas sobretudo a governos, partidos políticos e empresas de relações públicas;
- ***Phishing-as-a-Service:*** ataques de *phishing* vendidos por um operador que desenvolve uma campanha completa, podendo incluir, por exemplo, uma página falsa para realização de credenciação, alojamento de website e análise e redistribuição de credenciais;
- ***Ransomware-as-a-Service:*** venda de serviços de ransomware, frequentemente através de uma plataforma que fornece os instrumentos para a realização da encriptação e para a receção do resgate, ficando o provedor da plataforma com uma parte do valor extorquido. O comprador do serviço fica responsável pela interação com a vítima.

Houve um aumento na perceção de risco de se sofrer um incidente de Cibersegurança no ciberespaço de interesse nacional, em 2020 e em 2021. (CNCS, 2022)

O *phishing/smishing*, o sistema infetado por *malware*, o *ransomware*, algumas formas de intrusão, variados tipos de fraude/burla, a *sextortion* e a desinformação digital tendem a manter a sua relevância no panorama de ciberameaças. É expectável ainda que ocorram ataques oportunistas ao trabalho remoto, às cadeias de fornecimento, aos setores da banca e saúde e às tecnologias emergentes. Os Cibercriminosos e os Agentes Estatais tenderão a manter níveis elevados de atividade em 2021 no ciberespaço de interesse nacional. (CNCS, Relatório de Cibersegurança em Portugal - Riscos & Conflitos 2021, 2022)

Em 2022 observaram-se vários focos de operações cibernéticas ofensivas contra alvos nacionais, com origem num leque alargado de agentes de ameaça. Podemos destacar 4

focos de insegurança: ciberespionagem, desinformação, Cibercriminalidade e *hacktivismo*.

Principais Crimes que integram a criminalidade Informática:

- Acesso indevido ou ilegítimo, interceção ilegítima;
- Falsidade informática;
- Sabotagem informática;
- Viciação ou destruição de dados, dano relativo a dados de programas.

Como foi verificado em termos de ameaças, nos anos de 2021 e 2022, verificou-se, um aumento no número de incidentes e cibercrimes. Contudo, a mitigação progressiva da pandemia e o surgimento de uma guerra na Ucrânia fizeram emergir novos fatores de ameaça.

O contexto de pandemia favoreceu as burlas online, o comprometimento de sistemas próprios do trabalho remoto (RDP, VPN) e o *phishing*, verificando-se como temáticas dominantes de *phishing* as ligadas à banca, aos transportes e logística e à captura de credenciais de e-mail. Por outro lado, com o emergir da guerra na Ucrânia, já em 2022, surgem com um reforço na sua relevância a ciberespionagem, o comprometimento de cadeias de fornecimento, o *DDoS* e o *phishing* dirigido a pessoas específicas (*spear phishing*), entre outros, com tendência para afetar a Administração Pública e os operadores de serviços essenciais. Em ambos os cenários, algumas ameaças são constantes, como, por exemplo, o *ransomware*. (Interna, 2022)

Em 2021, em particular, persistiram como ameaças importantes o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla online, o comprometimento de contas e a exploração de vulnerabilidades. (CNCS, 2022) Em qualquer dos casos, as fragilidades do fator humano são recorrentemente exploradas como vetores de ataque.

As atitudes, os comportamentos, a sensibilização e a educação são tópicos fundamentais para promover o reforço do fator humano.

Considerando as ameaças mais relevantes de 2021 e a análise dos eventos registados em 2022, verifica-se a existência de algumas circunstâncias que têm um contributo negativo para a mitigação das ameaças:

- o aumento da utilização da Internet e serviços digitais;

- a diminuição do número de estratégias de segurança de informação e a falta de profissionais da área na Administração Pública;
- a existência de poucas ações de sensibilização nas PME e, as que se realizam na Administração Pública, serem sobretudo voluntárias;
- a diminuição do número de diplomados em cursos especializados;
- os desequilíbrios sociodemográficos relativamente aos conhecimentos, práticas e ações de sensibilização em Cibersegurança.

Com um contributo em geral positivo, encontram-se as seguintes situações:

- a razoável gestão dos dados pessoais online por parte dos indivíduos e a sua preocupação com as compras online;
- a elevada preocupação das PME com os riscos de cibercrime e a significativa tendência para reportarem incidentes;
- os aumentos na aplicação de medidas de segurança das TIC e no reforço de recomendações deste âmbito na Administração Pública;
- o alcance generalizado das ações de sensibilização em Cibersegurança em termos temáticos e de público-alvo;
- o crescimento do número de cursos e alunos especializados em Cibersegurança e segurança de informação.

Algumas ameaças afetam alvos e exigem competências e práticas mais individuais, como a fraude/burla *online*; outras, mais organizacionais, como o *ransomware*; outras ainda, têm um caráter mais técnico, como a exploração de vulnerabilidades; enquanto o *phishing*, por exemplo, depende muito do fator humano. Estas diferenças interferem na relevância de cada boa prática em relação a cada ameaça.

Entre as notificações enviadas à CNPD em 2021, a origem mais frequente para os incidentes em causa é a falha humana (24% das notificações), o *ransomware* (22%) e as ações fraudulentas (13%). O princípio da informação mais comprometido é o da confidencialidade (62%). (CNCS, 2022)

Relativamente à "Criminalidade Informática", o RASI 2022 mostra que os crimes informáticos apresentaram um aumento de 723 casos (+48,3%). Concorreram para este resultado o aumento verificado nos crimes de "acesso/interceção ilegítima" (+60,1%), de "falsidade informática" (+54,3%), de "sabotagem informática" (+31,7%) e "viciação ou destruição de dados, dano relativo a dados programas" (+14,3%).

Segundo a Polícia Judiciária, durante 2022 foram constituídos 1.197 arguidos (+61,1%), realizaram-se 54 detenções (-38,6%) e 12 indivíduos foram colocados em prisão preventiva (+9,1%). (Interna, 2022)

2.6. Dados sobre o Cibercrime no Ano de 2022 e primeiro Trimestre de 2023

O CERT.PT (Equipa de Resposta a Incidentes de Segurança Informática Nacional), no ano de 2022, recebeu e processou 8.971 notificações, mais 48,7% que no ano anterior, em que cerca de 22,6% dessas notificações resultaram na abertura de incidentes de Cibersegurança analisados e resolvidos (2.023 incidentes, +13,6%). Destes incidentes, 33,2% afetaram entidades da Administração Pública, verificando-se um aumento em relação ao ano anterior. (Interna, 2022)

À semelhança dos relatórios anteriores, dentro da classe Fraude, os ataques de *Phishing* e de *Smishing* este último com um forte crescimento em 2022 – continuam a dominar. As marcas utilizadas nestas campanhas afetam entidades do setor bancário e serviços financeiros, entidades do setor de transporte e logística e entidades fornecedoras de serviços de e-mail eletrónico. Estas campanhas têm como objetivo principal a recolha de credenciais de acesso do serviço *homebanking* e recolha de dados de cartões de crédito ou débito. Adicionalmente, registaram-se várias campanhas com o intuito de recolha de credenciais de acesso, que são posteriormente usadas como vetor inicial de ataques de *ransomware*.

As classes Código Malicioso e Recolha de Informação registaram o mesmo número de incidentes no ano 2022. Ambas assinalam um aumento em relação ao ano anterior. Em linha com o ano passado, na classe Código Malicioso destacam-se com 214 e 84 incidentes, respetivamente, a Distribuição de Malware e os Sistemas Infetados, ambos associados a várias famílias de códigos maliciosos (*Agent Tesla, FormBook, Hidden Macro 4.0, SystemBC, Emotet,* entre outros).

Relativamente à classe de Recolha de Informação, tal como no ano transato, são predominantes os ataques de Engenharia Social. Dentro destes ataques, destacam-se os casos de *vishing* (principalmente chamadas telefónicas simulando um técnico de uma

empresa tecnológica, com o intuito de ter acesso ao dispositivo da vítima; e também chamadas de um suposto trabalhador de uma instituição bancária ludibriando a vítima para que esta lhe forneça detalhes de acesso à sua conta bancária e, por fim, realizar dano monetário), *CEO fraud* (mensagens de texto ou de e-mail personificando indivíduos de posições hierárquicas superiores a pedir cartões-oferta que mais tarde seriam pagos pela entidade ou personificando fornecedores que indicariam uma nova conta de destino de pagamento das faturas emitidas, ambas situações com o intuito de dano monetário) e *sextortion* (essencialmente receção de mensagens de e-mail que implicam coação moral).

Importa referir que, os ataques pertencentes à classe Segurança de Informação tiveram elevada relevância no ano de 2022, com um aumento de 40 incidentes em relação ao período homólogo. Dos 78 incidentes registados neste ano, 69 foram ataques de ransomware.

O CERT.PT registou, em 2022, a abertura de 2.023 incidentes de Cibersegurança.

Classes de Incidentes mais reportados ao CERT.PT em 2022 (8.971 notificações - +48,7%), dados nacionais:

- Fraude – 871 (+68) – ataques de *phising* e de *smishing*
- Código Malicioso – 300 (+25) – Sistemas infetados e *Malware*
- Recolha de Informação – 300 (+39) – ataques de Engenharia Social – *Sextortion*, *vishing* e *CEO Fraud*
- Intrusão – 202 (+48)
- Restantes classes – 350 (+62).

No primeiro Trimestre de 2023, a média global de ataques semanais aumentou 7% face ao mesmo período em 2022, com cada organização a enfrentar uma média de 1248 ataques por semana, de acordo com as estatísticas e tendências dos ciberataques a nível global da *Check Point Research.* (Research, 2023)

No primeiro trimestre do ano, o sector da Educação/Investigação foi o mais atingido com o maior número de ataques, com uma média de 2507 ataques por organização por semana, o que representa um aumento de15% em relação ao primeiro trimestre de 2022.

O sector Administração Pública/Defesa foi o segundo mais visado, com uma média de 1725 ataques por semana, o que indica um incremento de 3% em relação ao ano anterior.

O sector da Saúde registou um aumento significativo de ataques, com uma média de 1684 ataques por semana, o que representa um aumento substancial de 22% em relação ao ano anterior. No entanto, a mudança mais significativa ocorreu no sector do Retalho, que registou o maior aumento, de 49%, em relação ao ano anterior, com uma média de 1079 ataques por semana.

Em Portugal, os dados da *Check Point Research* revelam que houve uma média semanal de 1065 ataques por organização, valor acima da média europeia, o que representa um aumento de 2% face ao primeiro trimestre de 2022.

2.7. Evolução da Criminalidade Informática na RAA entre 2012 e 2022

O volume de incidentes de Cibersegurança e os indicadores de cibercrime continuam a apresentar uma tendência crescente.

Contudo, é uma tendência negativa quanto ao impacto da ENSC que deve ser considerada, nomeadamente tendo em conta a capacidade das atividades previstas no Plano de Ação da ENSC fazerem face ao número de incidentes e de cibercrimes registados.

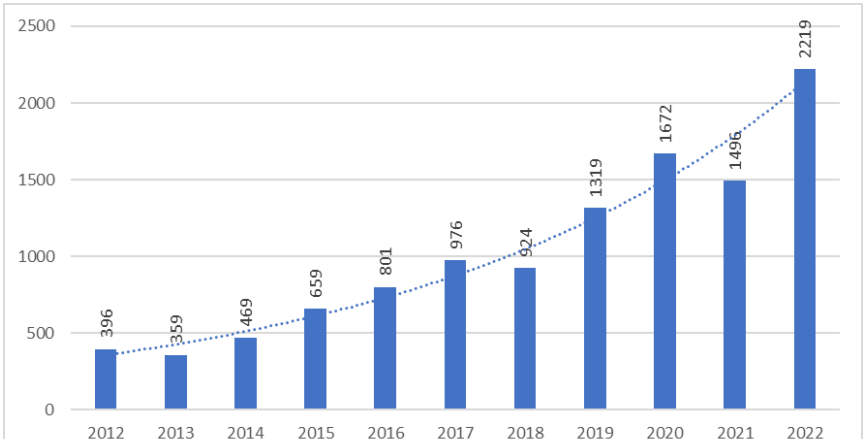
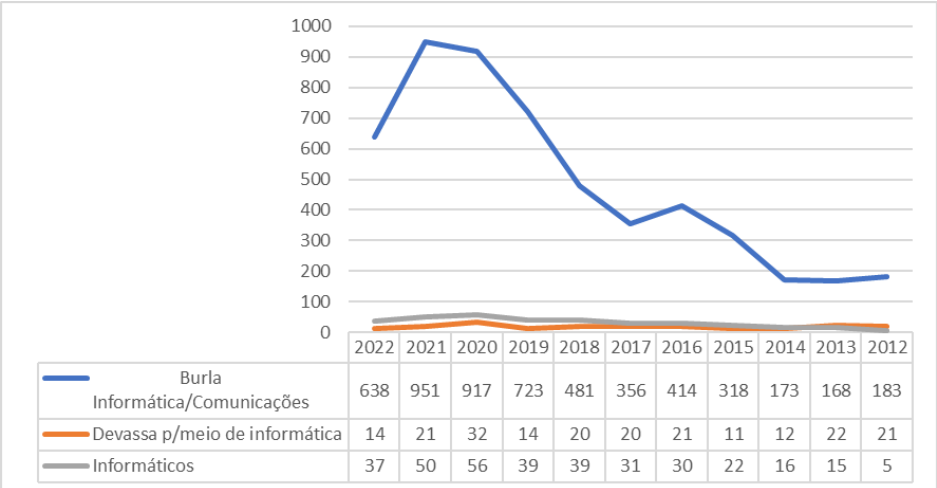


Figura 3 - Evolução da Cibercriminalidade Informática na RAA entre 2012 e 2022

Pelo exposto, é importante reforçar, cada vez mais, os processos no sentido de prevenir com mais eficácia os incidentes de Cibersegurança.



	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012
Burla Informática/Comunicações	638	951	917	723	481	356	414	318	173	168	183
Devassa p/meio de informática	14	21	32	14	20	20	21	11	12	22	21
Informáticos	37	50	56	39	39	31	30	22	16	15	5

Figura 4 - Evolução dos principais tipos de Crimes Informáticos na RAA entre 2012 e 2022

Capítulo 3 Boas Práticas e Regulamentação Nacional

Neste capítulo iremos abordar algumas normas e metodologias existentes para a resposta a Incidentes de Segurança, que vamos analisar, de modo a servir de base para a proposta que foi apresentada para o GRA.

3.1. O Governo Regional dos Açores

O Arquipélago dos Açores constitui uma Região Autónoma da República Portuguesa, criada pela Lei n.º 39/80, de 05 de agosto. (República, 1980)

O estatuto político-administrativo foi consagrado na Constituição da República de 1976 (artigo 229º). Trata-se de uma entidade jurídica de direito público dotada de poderes legislativos e executivos. (Constituinte, 1976)

Constituem-se Órgãos de Governo próprio a Assembleia Legislativa Regional, composta por 57 deputados eleitos por sufrágio universal e direto a cada quatro anos, sediada na cidade da Horta, e o Governo Regional, de legitimidade parlamentar, composto, no caso do XIII Governo Regional dos Açores, por um Presidente do Governo (José Manuel Bolieiro), um vice-presidente (Artur Lima), e por 8 secretários regionais com departamentos nas cidades de Ponta Delgada, Angra do Heroísmo e Horta.

A República Portuguesa é representada nos Açores por um Representante da República, nomeado pelo Presidente da República.

O Presidente do Governo é nomeado por Decreto do Representante da República (antes de 2004, pelo Ministro da República), ouvidos os partidos políticos com assento parlamentar e tendo em conta a composição do parlamento regional. Cabe ao Presidente do Governo propor ao Representante da República a nomeação e a exoneração dos restantes membros do Governo, os quais são nomeados por decreto. O Governo apenas assume a plenitude dos seus poderes após investidura parlamentar, o que acontece com a aprovação na Assembleia Legislativa do seu Programa de Governo.

Em relação à Administração Local, existem 19 concelhos e 150 freguesias.

3.2. Organograma do GRA

Organograma com a indicação da Presidência, Vice-presidência e Secretarias Regionais, e que pretende dar a conhecer, de uma forma simples a Organização GRA. (Açores, 2023)

O XIII Governo Regional dos Açores é constituído por:

- Presidência do Governo Regional - José Manuel Bolieiro
    - Comissão Coordenadora para os Arquivos da Região Autónoma dos Açores
    - Direção Regional das Comunidades
    - Fundo Regional de Apoio à Coesão e ao Desenvolvimento Económico
    - Secretaria-Geral da Presidência
    - Centro de Consulta e Estudos Jurídicos do Governo Regional
    - Centro Histórico e Documental da Autonomia Regional
    - Direção Regional da Cooperação com o Poder Local
    - Direção Regional das Comunicações e da Transição Digital
    - Subsecretário Regional da Presidência - Pedro Chaves de Faria e Castro
        - Direção Regional dos Assuntos Europeus e Cooperação Externa
        - Gabinete de Representação da Região Autónoma dos Açores em Bruxelas
        - Estrutura de Missão dos Açores para o Espaço
- Vice-Presidência do Governo Regional - Artur Lima
    - Direção Regional da Ciência e Tecnologia
    - Fundo Regional para a Ciência e Tecnologia
    - Direção Regional para a Promoção da Igualdade e Inclusão Social

    - Direção Regional da Habitação
    - Direção Regional da Solidariedade Social
    - Instituto da Segurança Social dos Açores
    - Aerogare Civil das Lajes
- Secretaria Regional das Finanças, Planeamento e Administração Pública - Duarte Freitas
    - Direção Regional da Organização, Planeamento e Emprego Público
    - Direção Regional do Empreendedorismo e Competitividade
    - Direção Regional do Orçamento e Tesouro
    - Direção Regional do Planeamento e Fundos Estruturais
    - Inspeção Administrativa, da Transparência e do Combate à Corrupção
    - RIAC – Agência para a Modernização e Qualidade do Serviço ao Cidadão, IP.
    - Serviço Regional de Estatística dos Açores
- Secretaria Regional da Educação e dos Assuntos Culturais - Sofia Ribeiro
    - Direção Regional da Educação e Administração Educativa
    - Inspeção Regional da Educação
    - Fundos Escolares
    - Direção Regional dos Assuntos Culturais
    - Inspeção Regional das Atividades Culturais
- Secretaria Regional da Saúde e Desporto – Mónica Seidi
    - Direção Regional da Saúde
    - Centro de Oncologia dos Açores
    - Inspeção Regional da Saúde
    - Provedor do Utente da Saúde
    - Direção Regional de Prevenção e Combate às Dependências
    - Direção Regional do Desporto
    - Serviço Regional de Proteção Civil e Bombeiros dos Açores
- Secretaria Regional da Agricultura e do Desenvolvimento Rural - António Ventura
    - Direção Regional da Agricultura
    - Instituto de Alimentação e Mercados Agrícolas
    - Instituto da Vinha e do Vinho dos Açores

    - Direção Regional do Desenvolvimento Rural
    - Direção Regional dos Recursos Florestais
    - Instituto Regional de Ordenamento Agrário
- Secretaria Regional do Mar e das Pescas - Manuel São João
    - Direção Regional das Pescas
    - FUNDOPESCA
    - Inspeção Regional das Pescas
    - Direção Regional de Políticas Marítimas
- Secretaria Regional do Ambiente e Alterações Climáticas - Alonso Miguel
    - Direção Regional do Ambiente e Alterações Climáticas
    - Inspeção Regional do Ambiente
    - Direção Regional do Ordenamento do Território e dos Recursos Hídricos
    - Entidade Reguladora dos Serviços de Águas e Resíduos dos Açores
- Secretaria Regional do Turismo, Mobilidade e Infraestruturas - Berta Cabral
    - Direção Regional da Energia
    - Direção Regional da Mobilidade
    - Fundo Regional dos Transportes Terrestres
    - Direção Regional das Obras Públicas
    - Laboratório Regional de Engenharia Civil
    - Direção Regional do Turismo
    - Inspeção Regional do Turismo
- Secretaria Regional da Juventude, Qualificação Profissional e Emprego - Maria João Carreiro
    - Centro de Artesanato e Design dos Açores
    - Direção Regional da juventude
    - Direção Regional de Qualificação Profissional e Emprego
    - Fundo Regional do Emprego
    - Inspeção Regional das Atividades Económicas
    - Inspeção Regional do Trabalho
    - Observatório do Emprego e Qualificação Profissional

3.3. Organograma dos Serviços da Presidência do GRA

O Organograma dos Serviços e Direções Regionais sob a alçada da Presidência do GRA, e onde será proposta a implementação de um Manual de Procedimentos de resposta a incidentes de Cibersegurança, assim como a adoção de um Manual de Resposta a cada tipologia de incidentes de Cibersegurança, tendo como base a taxonomia da rede nacional de CSIRT. (Açores, Presidência do Governo Regional, 2023)

A Presidência do Governo Regional dos Açores é composta por:

- Gabinete do Presidente do Governo Regional
- Gabinete de Edição do Jornal Oficial
- Comissão Coordenadora para os Arquivos da Região Autónoma dos Açores e do Núcleo Operacional
- Direção Regional das Comunidades
- Fundo Regional de Apoio à Coesão e ao Desenvolvimento Económico
- Secretaria-Geral da Presidência
    - Divisão de Recursos Humanos, Financeiros e do Património
        - Secção de Recursos Humanos
        - Secção de Contabilidade e Património
        - Serviço de Manutenção e Conservação dos Palácios da Presidência
        - Serviço de Conservação e Manutenção de Jardins
    - Centro de Informação e Documentação da Presidência do Governo
    - Centro Multimeios do Governo Regional
        - Delegação em Angra do Heroísmo e na Horta
    - Centro do Protocolo e Relações Públicas do Governo Regional
- Delegação de Lisboa do Governo Regional dos Açores
- Centro de Consulta e Estudos Jurídicos do Governo Regional
- Centro Histórico e Documental da Autonomia Regional
- Direção Regional da Cooperação com o Poder Local
- Direção Regional das Comunicações e da Transição Digital
- Subsecretário Regional da Presidência
    - Direção Regional dos Assuntos Europeus e Cooperação Externa
    - Gabinete de Representação da Região Autónoma dos Açores em Bruxelas
    - Estrutura de Missão dos Açores para o Espaço

3.4. Quadro Legal da Estrutura Nacional de Cibersegurança

A Lei n.º 46/2018, de 13 de agosto, estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), transpondo para a ordem jurídica interna a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016 (Diretiva SRI). A Diretiva SRI constitui a primeira medida legislativa ao nível da EU, destinada a reforçar a cooperação entre Estados-Membros no que respeita à Cibersegurança, estabelecendo nomeadamente obrigações de segurança a cumprir pelos operadores de serviços essenciais em setores críticos como transportes, energia, saúde, finanças, assim como, pelos prestadores de serviços digitais. Desde maio de 2019, existe também no âmbito do Conselho da UE um quadro de sanções aplicáveis a pessoas ou entidades associadas a casos específicos de ciberataques com origem no exterior da UE que constituam uma ameaça à União ou aos seus Estados-Membros.

Encontra-se atualmente em preparação uma nova diretiva – Diretiva SRI 2 – para responder à evolução do cenário de ciberameaças. Entre outras medidas, prevê-se que a nova Diretiva SRI 2 venha reforçar o regime de obrigações das empresas em matéria de segurança, intensificar a partilha de informação e a cooperação entre Estados-Membros, e tornar mais rigorosa a supervisão das autoridades nacionais.

A Lei nº 46/2018 define as bases jurídicas e institucionais da Cibersegurança em Portugal, mas somente para o âmbito civil. Esta lei é aplicável à Administração Pública (AP), aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais e a todas as entidades que utilizem redes e sistemas de informação, nomeadamente no âmbito da notificação voluntária de incidentes. De fora ficam as entidades que operam as redes e sistemas de informação militares (diretamente relacionados com o EMGFA e com qualquer ramo das Forças Armadas) e de informação classificada (art.º 2º da Lei n.º 46/2018).

O diploma apresenta um elenco de conceitos e noções próprios do ciberespaço (por exemplo, “incidente”, “infraestrutura crítica”, “norma”, “prestador de serviços digitais”, “segurança das redes e dos sistemas de informação”, entre outros), que delimitam as responsabilidades e obrigações dos diferentes atores e entidades nele envolvidos (art.º 3.º).

Confere ao Governo a competência para elaborar e aprovar a Estratégia Nacional de Segurança do Ciberespaço (ENSC), a qual, define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional (art.º 4º). A Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, aprovou a ENSC 2019-2023, sucedendo à Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, que aprovou a primeira ENSC.

3.5. Estratégia Nacional De Segurança Do Ciberespaço

Portugal tem uma Estratégia Nacional de Cibersegurança desde 2015. Esta estratégia foi revista em 2019 dando origem à Estratégia Nacional para a Segurança do Ciberespaço 2019-2023. (Ministros, 2019)

O CNCS é a Autoridade Nacional de Cibersegurança. O CERT.PT é o CSIRT nacional e é um serviço integrado no CNCS Português.

O CNCS está também encarregue de coordenar a elaboração, o acompanhamento da execução e a revisão do Plano de Ação da Estratégia Nacional para a Segurança do Ciberespaço 2019-2023 em articulação e estreita cooperação com todas as entidades responsáveis pela segurança do ciberespaço.

A execução desta estratégia tem como objetivo primordial tornar Portugal num país mais seguro e próspero, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade.

Com a aprovação da Estratégia Nacional para a Segurança do Ciberespaço foram definidos os seguintes objetivos estratégicos:

- Maximização da Resiliência: Fortalecer e garantir a resiliência digital nacional potenciando a inclusão e a colaboração em rede, de forma a salvaguardar a segurança do ciberespaço de interesse nacional face às ameaças que possam comprometer ou provocar a disrupção das redes e sistemas de informações essenciais á sociedade;

- Promover a Inovação: Fomentar e potenciar a capacidade nacional de inovação afirmando o ciberespaço como um domínio de desenvolvimento económico, social, cultural e de prosperidade;
- Gerar e garantir recursos: Contribuir para obter e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço.

Considerando as necessidades associadas a cada um dos objetivos estratégicos, foram considerados seis eixos de intervenção, onde se enquadram as ações a executar no âmbito do Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço.

Os seis eixos de intervenção são:

1. Estrutura de Segurança do Ciberespaço

Estrutura nacional constante da Lei n. º46/2018, de 13 de agosto, que assegura a envolvência de recursos, conhecimentos e competências necessárias para lidar com a complexidade e a abrangência dos desafios da segurança do ciberespaço, da qual destacamos:

- O Conselho Superior de Segurança do Ciberespaço, como órgão específico de consulta do Primeiro-Ministro, com representantes de todas as partes interessadas, que assegura a coordenação político-estratégica para a segurança do ciberespaço;
- O CNCS, como Autoridade Nacional de Cibersegurança e ponto de contacto único nacional para efeitos de cooperação internacional em matéria de Cibersegurança.

2. Prevenção, educação e sensibilização

- Antecipar a emergência, evolução e mutação das ameaças.
- Estimular nos cidadãos o desenvolvimento de competências digitais a vários níveis.
- Reforçar as medidas de sensibilização da sociedade civil para o uso seguro e responsável das tecnologias digitais, dando particular importância à capacitação e conhecimento obtidos por crianças, adolescentes, população sénior e outros grupos de risco.

3. Proteção do ciberespaço e das infraestruturas

- Promover o contínuo desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço.
- Promover estruturas de cooperação nacional e setorial de proteção do ciberespaço, incluindo o setor público e privado.
- Garantir o desenvolvimento e a aplicação de quadros de referência nacionais e internacionais de gestão da segurança do ciberespaço.

4. Resposta às ameaças e combate ao cibercrime

- Desenvolver e consolidar a capacidade de Ciberdefesa.
- Avaliar as necessidades de revisão e atualização da legislação.
- Promover ao nível setorial e do tecido empresarial, a criação de fóruns de partilha de informação operacional e técnica, de resposta coordenada a incidentes de segurança.

5. Investigação, desenvolvimento e inovação

- Propiciar a produção científica, o desenvolvimento e a inovação nos vários domínios da segurança do ciberespaço, afirmando a independência nacional neste domínio.
- Potenciar as capacidades científicas, técnicas e industriais do país, com especial ênfase nos domínios críticos e nas tecnologias emergentes.
- Apoiar a participação dos intervenientes em investigação, desenvolvimento e inovação em projetos internacionais.

6. Cooperação nacional e internacional

- Contribuir para a regulação e universalização do ciberespaço promovendo o respeito do direito internacional aplicável.
- Fomentar sinergias nacionais e internacionais, nomeadamente, no âmbito da UE (*pooling & sharing*), da ONU e da NATO (*smart defence*).
- Integrar organismos internacionais de Cibersegurança e de Ciberdefesa tendo em vista a cooperação internacional e a afirmação de Portugal neste domínio.

3.6. O Regime Jurídico da Segurança do Ciberespaço

Foi publicado, a 30 de julho de 2021, o Decreto-Lei n.º 65/2021, que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da Cibersegurança, em execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019. (República, Diário da República - Lei n.º 46/2018, 2018)

Na sua generalidade, este Decreto-Lei visa promover um ciberespaço mais seguro, considerando, desde logo, três pressupostos:

- o papel cada vez mais decisivo que as tecnologias de informação assumem no desenvolvimento da vida em sociedade;
- o desafio da transição digital;
- a emergência de novas tecnologias disruptivas (ex. a inteligência artificial, a realidade virtual e aumentada e a Internet das Coisas).

Por um lado, o diploma ora em apreço vem regulamentar dois aspetos que a Lei n.º 46/2018, de 13 de agosto - que aprovou o RJSC, transpondo, deste modo, a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União – remetia para legislação complementar, a saber:

- Definição dos requisitos de segurança das redes e sistemas de informação;
- Definição das regras para a notificação de incidentes.

Estes devem ser cumpridos pela Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

Refira-se que os requisitos de segurança ora previstos não se aplicam:

(a) Às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, as quais se encontram sujeitas aos requisitos previstos na Lei das Comunicações Eletrónicas (Lei n.º 5/2004, de 10 de fevereiro);

(b) Aos prestadores de serviços de confiança (serviços eletrónicos que consistem na criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico, certificados relacionados com estes serviços, certificados para a autenticação de sítios web ou na

preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços), os quais se encontram sujeitos aos requisitos previstos no Regulamento (UE) n.º 910/2014, de 23 de Julho, do Parlamento Europeu e do Conselho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

Por seu turno, as regras de notificação de incidentes não se aplicam às entidades referidas em (a) e (b), mas também aos prestadores de serviços digitais que sejam microempresas ou pequenas empresas, tal como definidas pelo Decreto-Lei n.º 372/2007, de 6 de novembro.

Acresce que, os requisitos previstos no Decreto-Lei n.º 65/2021 são requisitos mínimos a assegurar pelas entidades abrangidas pelo RJSC, podendo, assim, vir a ser estabelecidas regras adicionais por parte de outras entidades (ex. Ministério Público, Autoridade Nacional de Comunicações, CNPD, demais autoridades sectoriais), em função da natureza das entidades abrangidas, de aspetos específicos da atividade desenvolvida ou do contexto em que esta se desenvolva.

Reconhecendo a necessidade de articular a aplicação destas novas disposições legais com normativos complementares sectoriais já existentes, consagra-se a possibilidade do CNCS, na qualidade de Autoridade Nacional de Cibersegurança, proceder a uma avaliação de equivalência dos requisitos constantes de legislação sectorial, quando considere que tal é necessário e em articulação com as entidades reguladoras e de supervisão sectorial.

Por outro lado, considerando que a certificação de produtos, serviços e processos de tecnologia de informação e comunicação é complementar para a promoção de um ciberespaço mais seguro, o diploma em apreço:

(i) consagra o CNCS como Autoridade Nacional de Certificação da Cibersegurança, definindo igualmente as respetivas competências;
(ii) implementa na ordem jurídica nacional um quadro nacional de certificação da Cibersegurança, denominado Quadro Nacional de Referência para a Cibersegurança, o qual se assume como referencial de análise de risco para o fortalecimento da resiliência de cada organização face às ameaças que afetam o ciberespaço.

No âmbito das disposições finais, determina-se que o regime sancionatório previsto no RJSC seja aplicável às infrações ao disposto neste Decreto-Lei, isto é, o não cumprimento das regras estabelecidas neste diploma constituirão contraordenação, podendo as entidades ser punidas pelo CNCS com coima até €50.000,00. Além disso, constitui contraordenação punível com coima de €1.000,00 a €3.740, 98, no caso de pessoa singular, ou de €5.000,00 a €44.891,81, no caso de pessoa coletiva, a prática de infrações relativas à certificação da Cibersegurança.

O presente Decreto-Lei entrou em vigor 10 dias após a sua publicação, isto é, a 10 de agosto de 2021, sem prejuízo de determinadas disposições só produzirem efeitos 90 dias após a sua entrada em vigor (*inter alia*, as relativas à indicação de um ponto de contacto permanente com o CNCS, à designação de um responsável de segurança, à elaboração e manutenção de um plano de segurança e o capítulo referente às notificações de incidentes) e de certas disposições só produzirem efeitos no prazo de 1 ano após a sua entrada em vigor (i.e., o capítulo atinente à segurança das redes e dos sistemas de informação).

3.7. Quadro Nacional de Referência para a Cibersegurança

O CNCS publicou a 26 de julho de 2019 o Quadro Nacional de Referência para a Cibersegurança, que pretende ser uma ferramenta de apoio às Organizações no cumprimento dos requisitos mínimos de segurança da informação recomendados, na gestão do risco de segurança dos sistemas de informação e no tratamento eficiente de incidentes. (CNCS, Quadro Nacional de Referência para a Cibersegurança, 2022)

O contexto da ameaça de Cibersegurança deve ser encarado através de uma abordagem sistematizada que tenha por objetivo a sensibilização das organizações públicas e privadas.

Neste processo coletivo de crescente sensibilização, é fundamental uma mudança de paradigma materializada por via da definição de linhas orientadoras de um sistema de processos e procedimentos, nem sempre de caráter tecnológico, que possa constituir uma linguagem comum, transversal aos diversos setores de atividade e que promova a convergência de práticas conducentes a uma melhor Cibersegurança das organizações.

O QNRCS consubstancia-se numa visão homogénea e inclusiva da realidade organizacional (pública e privada) portuguesa, no que diz respeito à necessidade de implementação de medidas de identificação, proteção, deteção, resposta e recuperação contra as ameaças que possam colocar em causa a segurança das suas redes e sistemas de informação e, desta forma, da sua informação.

A elaboração do QNRCS teve em consideração, enquanto documento enquadrador legislativo no ordenamento jurídico nacional, o exposto na Lei nº 46/2018, de 13 de agosto, que definia, na altura, o regime jurídico da segurança do ciberespaço.

O QNRCS não pretendeu constituir-se como uma norma de Cibersegurança, mas sim, como uma referência que permita identificar as normas, padrões e boas práticas existentes em vários domínios da segurança da informação. A sua aplicação nas organizações é voluntária e passível de ser adaptada, por forma a melhor endereçar necessidades específicas inerentes ao seu setor, dimensão ou qualquer outro aspeto distintivo que caracterize a organização.

A estrutura central do QNRCS foi definida numa perspetiva de ciclo de vida da gestão da Cibersegurança de uma organização, tendo em atenção os aspetos humanos, tecnológicos e processuais, com especial enfoque nos processos e procedimentos da gestão do risco.

Uma característica intrínseca do risco é o facto de este não poder ser totalmente eliminado, tornando-se fundamental a concretização de uma estratégia global da organização, para garantir a implementação de um processo eficaz de gestão do risco.

Este é um processo contínuo de identificação, diagnóstico e resposta, sendo que, para que seja possível gerir o risco, as organizações devem compreender a probabilidade de um determinado evento ocorrer, bem como, os seus potenciais impactos adversos e vulnerabilidades existentes. Conhecendo esta informação, qualquer organização pode determinar o seu nível aceitável do risco e, desta forma, promover a resiliência da sua atividade enquanto prestador de bens ou serviços. A esta informação corresponde a perceção de tolerância ao risco, condição *sine qua non* para a priorização das atividades realizadas no âmbito da Cibersegurança.

Deste modo, o QNRCS deve ser implementado pelas Organizações ou, pelo menos, integrado nos programas de *compliance* internos para a segurança dos sistemas de informação, no que concerne, nomeadamente, à conformidade com a legislação em vigor

e à adoção de um processo de gestão do risco e mitigação do impacto dos incidentes nas Organizações.

3.8. Capacidades Mínimas para reação a Incidentes de Cibersegurança

Independentemente da quantidade e qualidade dos mecanismos de prevenção instalados, os incidentes de Cibersegurança têm-se mostrado mais frequentes e complexos. Neste cenário, interessa mitigar o impacto e reduzir os danos decorrentes de incidentes desta natureza. (CNCS, Roteiro para Capacidades Mínimas de Cibersegurança, 2019)

É com este objetivo, de apoiar o desenvolvimento de valências mínimas em Cibersegurança na generalidade das organizações do panorama nacional, que o CNCS definiu um conjunto de capacidades, técnicas, humanas e processuais, constituindo uma base harmonizada e desejável nesta matéria.

O CNCS proporcionou assim, um instrumento que aumente o nível da organização no domínio da governação de segurança de informação, focado nas competências e capacidades, incluindo ao nível de recursos humanos, para identificar ameaças, percebê-las e reagir face aos riscos do ciberespaço e das atividades em Rede, através do "Roteiro para Capacidades Mínimas em Cibersegurança".

O Roteiro é constituído por cinco fases que permitem, às organizações, integrar o ecossistema nacional de Cibersegurança e criar as condições para uma melhoria sustentada e coerente dessas capacidades. Este Roteiro, deve ser utilizado como um instrumento complementar ao Quadro Nacional de Referência para a Cibersegurança (QNRCS), já abordado anteriormente.

O GRA deverá assim, apoiado por este documento, desenvolver gradualmente o nível de Cibersegurança dentro da organização e as suas capacidades fundamentais para a reação a incidentes de Cibersegurança.

3.9. Roteiro para Capacidades Mínimas em Cibersegurança

O processo de desenvolvimento de capacidades mínimas para a Cibersegurança, apoiado no Roteiro, permite um desenvolvimento progressivo relativamente ao seu grau de capacitação, através do percurso de um conjunto de fases numeradas de um a cinco.

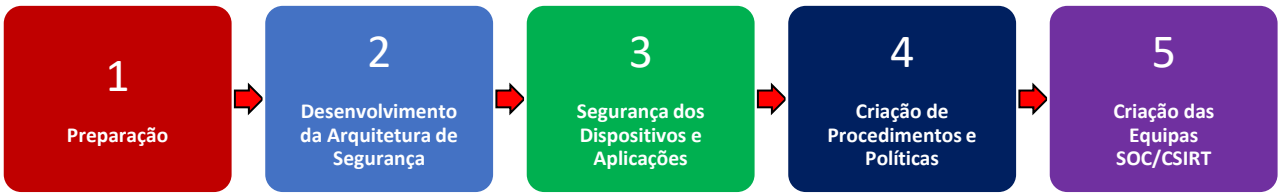


Figura 5 - Fluxo das Fases do Roteiro de Capacidades Mínimas do CNCS

A primeira fase é preparatória e o seu objetivo é estabelecer os alicerces para a cooperação entre o GRA e o CNCS. Nesta fase, o GRA deverá trabalhar para definir um ponto de contacto a articular com o CNCS (poderá ser considerado o Ponto de Contato já identificado para as situações de incidentes de Cibersegurança). Deve ser igualmente identificado o quadro de ameaças que impende sobre o GRA, calculando o valor relativo dos seus ativos (bem como o grau de risco a que estão sujeitos), definindo as áreas de segurança distintas, conforme o valor dos respetivos ativos e definindo ainda as respetivas regras de acesso. Deverá ainda identificar as dependências funcionais entre sistemas internos e entre estes e sistemas geridos por terceiros, levando sempre em linha de conta a importância do conjunto para o negócio. De referir que, todas estas questões já são solicitadas no âmbito da implementação do RJSC no GRA, isto é, o estabelecimento de um Ponto de Contacto permanente, a elaboração de um inventário de todos os ativos

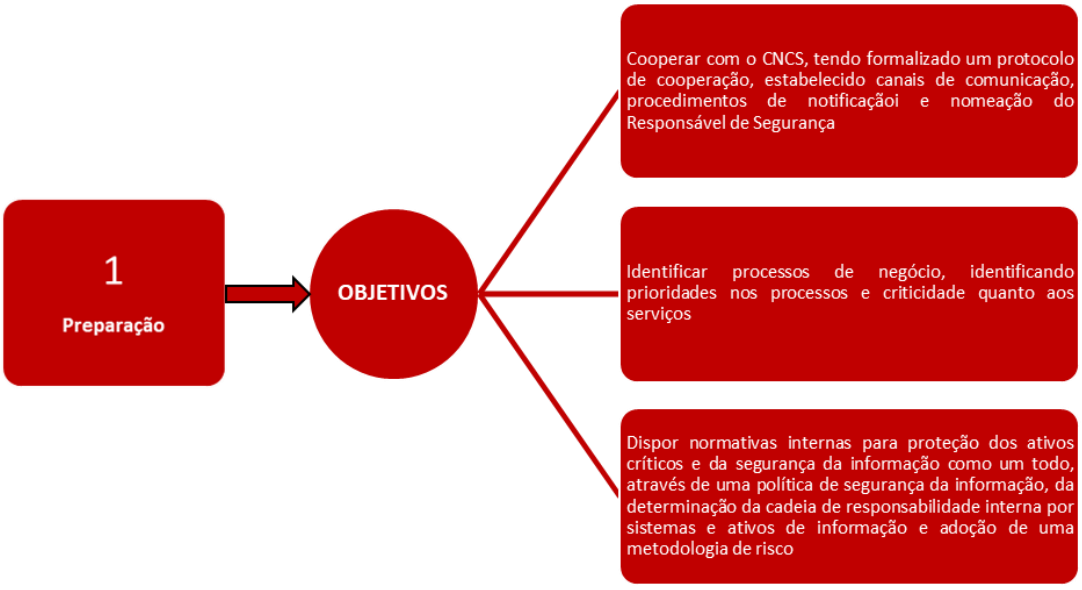


Figura 6 - Fase 1 RCMCS - Objetivos esperados

essenciais para a prestação de serviços e a realização de uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados.

Tabela 1 - Fase 1 - Roteiro de Capacidades Mínimas de Cibersegurança (Reproduzido do Roteiro de Capacidades Mínimas de Cibersegurança)

AÇÕES DA FASE 1	
A 1.1	Formalização de Protocolo de Colaboração e Adenda
A 1.2	Identificação de RESPONSÁVEL DE SEGURANÇA
A 1.3	Identificação de funções ou atividades críticas
A 1.4	Estabelecimento de canais de comunicação
A 1.5	Registo de endereços de IP no LIR (*Local Internet Registry*)
A 1.6	Estabelecimento de metodologia de Análise de Risco
A 1.7	Cadeia de responsabilidade: preparação
A 1.8	Definição de política de segurança de informação
A 1.9	Procedimentos de notificação de incidentes

A segunda fase serve para desenvolver a arquitetura de segurança, focando-se em delimitar as várias áreas de segurança e aplicar regras de controlo de acessos que permitam, por exemplo, detetar tentativas de intrusão em cada uma das zonas de segurança. Ainda nesta fase, o GRA deverá agregar num repositório central e correlacionar os eventos de segurança detetados nos diversos elementos de segurança ativa e passiva, bem como agregar, nesse mesmo repositório central, a informação de *metadados* de comunicações eletrónicas e registos de sistema e aplicações. Em casos

Figura 7 - Fase 2 RCMCS - Objetivos esperados

específicos, os eventos de segurança relevantes poderão ser comunicados em tempo real ao CNCS para enriquecimento do Quadro Situacional Nacional de Cibersegurança.

Tabela 2 - Fase 2 - Roteiro de Capacidades Mínimas de Cibersegurança (Reproduzido do Roteiro de Capacidades Mínimas de Cibersegurança)

AÇÕES DA FASE 2	
A 2.1	Desenho e implementação da arquitetura e segurança perimétrica
A 2.2	Implementação de sistema de recolha e armazenamento do fluxo de tráfego
A 2.3	Comunicação com o CNCS
A 2.4	Inventariação de ativos / produção de um mapa de rede
A 2.5	Recolha centralizada de registos (*logs*)
A 2.6	Criação de instrumentos de correção ou mitigação de incidentes
A 2.7	Estabelecimento de conformidade com a legislação aplicável
A 2.8	Estabelecimento de conformidade com normas aplicáveis à área de atividade
A 2.9	Criação de política de uso aceitável
A 2.10	Manutenção de infraestruturas de cópias de segurança e reposição (*Backup/Restore*)
A 2.11	Mapa de competências e planos de formação
A 2.12	Treino e sensibilização interna: geral
A 2.13	Treino e sensibilização interna: gestão

A terceira fase deverá versar a segurança de dispositivos e aplicações, desenvolvendo no GRA mecanismos de deteção e prevenção de ameaças nos dispositivos que tratam os ativos informativos mais valiosos, incluindo a capacidade de detetar movimentos laterais dos atacantes dentro da mesma zona de segurança. Ainda nesta fase, devem ser definidas capacidades para a criação de mecanismos de auditoria e alerta de acessos indevidos a bases de dados e outros ativos de elevado valor, mecanismos de alerta para falhas de desempenho e disponibilidade de serviços e mecanismos de controlo e auditoria de acessos a sites de Internet.

Tabela 3 - Fase 3 - Roteiro de Capacidades Mínimas de Cibersegurança (Reproduzido do Roteiro de Capacidades Mínimas de Cibersegurança)

AÇÕES DA FASE 3	
A 3.1	Definição de procedimentos de operação
A 3.2	Instalação e configuração de sensores em dispositivos
A 3.3	Auditoria de segurança e Bases de Dados
A 3.4	Instalação e configuração de controlo de acessos web – (ex. *serviços proxy*)
A 3.5	Proteção e gestão de equipamentos
A 3.6	Instalação e configuração de mecanismos de monitorização

A 3.7 *Hardening* das configurações

A 3.8 Instalação e configuração de um *Security Information and Event Management* (SIEM)

A 3.9 Definição de planos de continuidade de negócio

A 3.10 Aquisição de competências técnicas

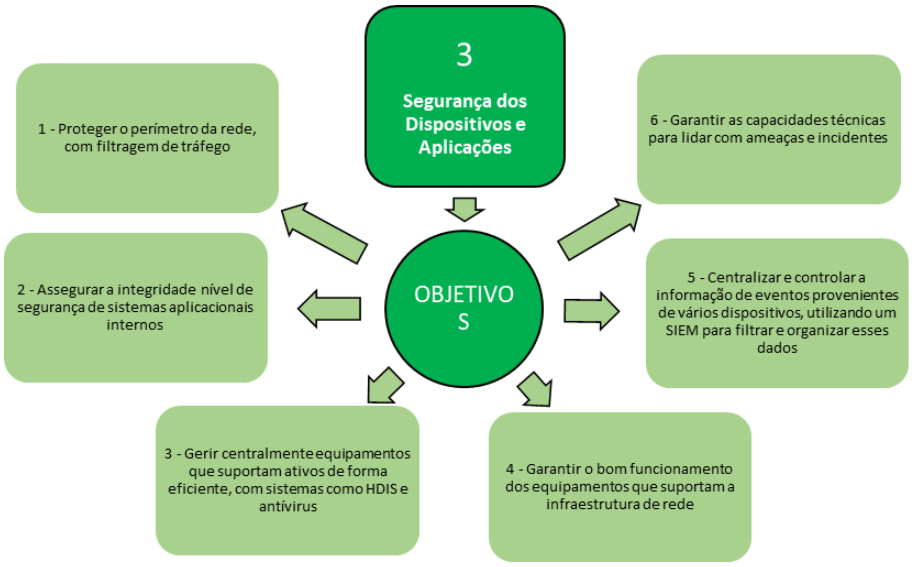


Figura 8 - Fase 3 RCMCS - Objetivos esperados

A quarta fase deve consistir em criar procedimentos e políticas que definam e otimizem as capacidades da equipa que estará encarregue da Cibersegurança interna do GRA, formalizar os procedimentos para operações de Cibersegurança, definir as

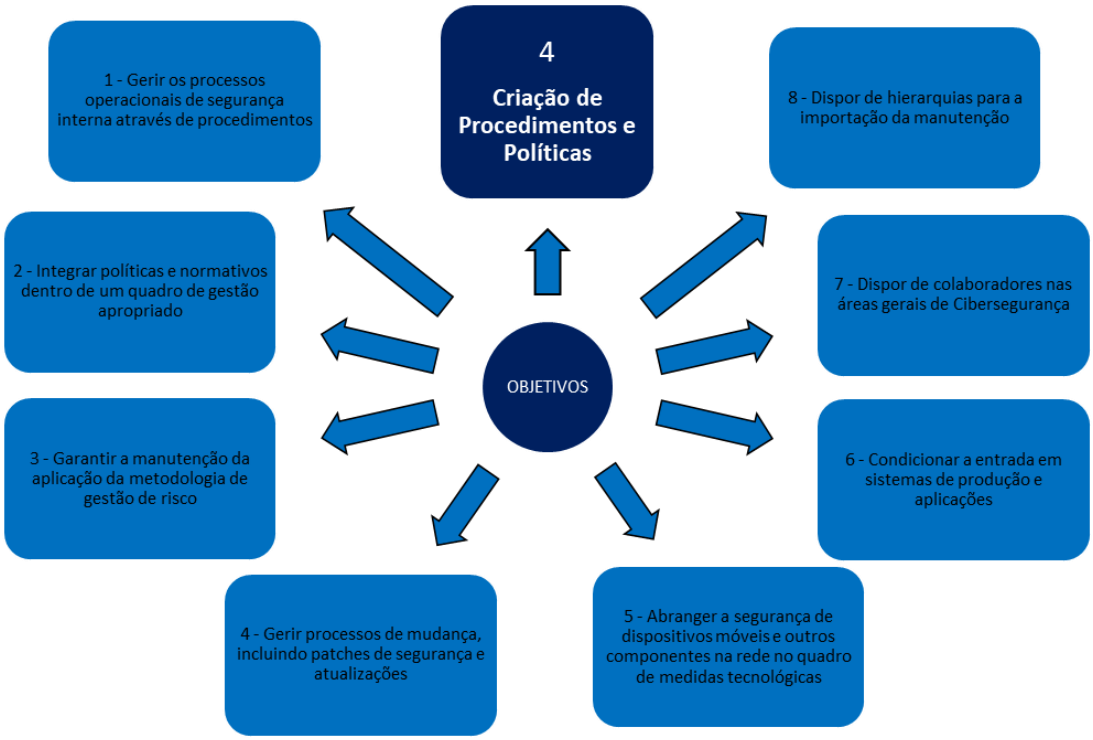


Figura 9- Fase 4 RCMCS - Objetivos esperados

responsabilidades pelas operações de Cibersegurança e elaborar um plano de formação individual para os colaboradores envolvidos, desta forma construindo uma estrutura de Cibersegurança em todo o GRA.

Tabela 4 - Fase 4 - Roteiro de Capacidades Mínimas de Cibersegurança (Reproduzido do Roteiro de Capacidades Mínimas de Cibersegurança)

AÇÕES DA FASE 4	
A 4.1	Cadeia de responsabilidades: formalização
A 4.2	Definição do Sistema Interno de Normas e Políticas (SINP)
A 4.3	Análise de risco - reavaliação
A 4.4	Simulacro
A 4.5	Definição de procedimentos de reação a incidentes
A 4.6	Treino e sensibilização interna: SINP
A 4.7	Testes de aceitação de serviços
A 4.8	Mecanismos de engodo (*honeypots*)
A 4.9	Gestão de mudanças e atualizações

Por último, a quinta fase, que se aplica ao GRA pela sua dimensão, criticidade ou complexidade que o justifique, consiste na formalização de equipa(s) dedicada(s) à deteção e resposta de incidentes, com as seguintes capacidades: monitorização e alerta de incidentes de Cibersegurança – *Security Operations Centre* (SOC) e/ou *Computer Security Incident Response Team* (CSIRT). O GRA deve ainda procurar colaborar em projetos de desenvolvimento e partilha de informação de Cibersegurança de uma forma regular dentro do sector de atividade e, se necessário, com a comunidade de Cibersegurança, devendo ainda participar em exercícios nacionais e internacionais de Cibersegurança, de modo a poder testar, em ambiente simulado, os procedimentos e a sua capacidade de resposta a incidentes de Cibersegurança.

Tabela 5 - Fase 5 - Roteiro de Capacidades Mínimas de Cibersegurança (Reproduzido do Roteiro de Capacidades Mínimas de Cibersegurança)

AÇÕES DA FASE 5	
A 5.1	Nomear um CISO
A 5.2	Estabelecer um serviço de gestão de vulnerabilidades
A 5.3	Estabelecer e implementar um plano de auditorias
A 5.4	Definir a missão, a comunidade servida e o portfólio de serviços do SOC ou CSIRT
A 5.5	Elaborar e fazer aprovar o plano e o orçamento para o SOC ou CSIRT
A 5.6	Montar e anunciar o SOC ou CSIRT

A 5.7 Estabelecer um sistema de gestão de Crise

A 5.8 Afiliação nas comunidades nacionais e internacionais de CSIRT

A 5.9 Participação num Exercício Nacional de Cibersegurança

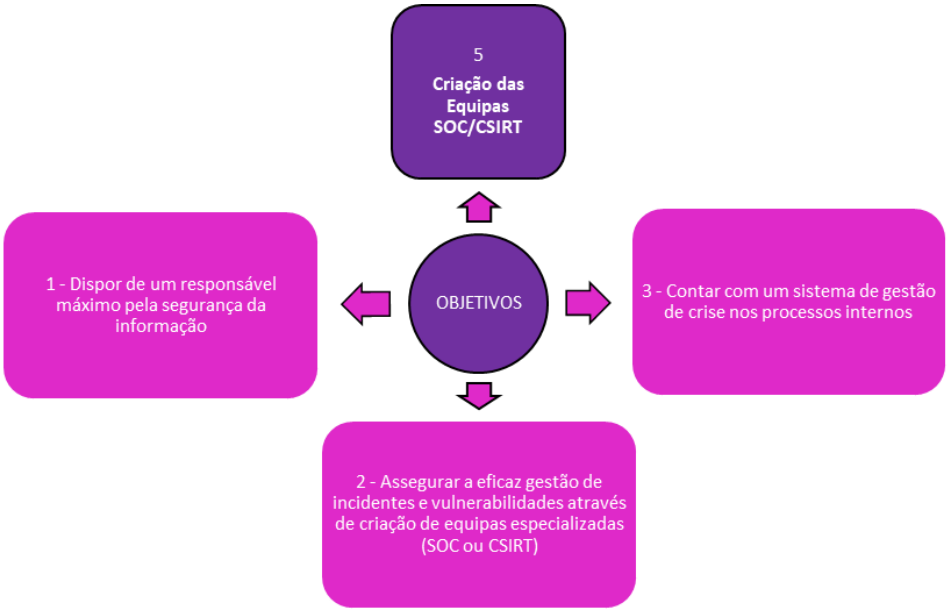


Figura 10 - Fase 5 RCMCS - Objetivos esperados

O cumprimento destas ações, no percurso destas cinco Fases, vai permitir a criação de capacidades mínimas, no domínio da Cibersegurança, no GRA, dotando-o de recursos próprios para a reação a incidentes de Cibersegurança.

Em resumo, podemos dizer que o GRA deve ter as seguintes capacidades/funcionalidades desenvolvidas:

- Definição de um ponto de contato e articulação com o CNCS a reação a incidentes de Cibersegurança;
- Identificação das áreas de atividade e serviços considerados críticos e realização da gestão de ativos para as mesmas;
- Recolha e armazenamento de *metadados* de comunicações eletrónicas e outros registos de serviços informáticos necessários para a análise de incidentes;
- Possua um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos ciberataques mais comuns;
- Constitua os recursos humanos com as competências necessárias para a realização de grande parte das investigações forenses necessárias e que articulem com eficácia com o CNCS;

- Aprove e implemente procedimentos internos de resposta a incidentes de Cibersegurança;
- Definida a estrutura e a cadeia de responsabilidade nesta matéria e realize, periodicamente, simulacros de Cibersegurança.

O GRA, pela sua dimensão e importância estratégica regional, assim como por executar funções críticas deve, ainda, ter a sua função de resposta a incidentes assegurada por uma equipa dedicada, vulgarmente designada de CSIRT. Assim sendo, o GRA deve possuir ainda as seguintes capacidades:

- Uma equipa dedicada à reação a incidentes de Cibersegurança – CSIRT;
- Colaboração em projetos de desenvolvimento e partilha de informação de Cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT;
- Participação em exercícios nacionais e internacionais de Cibersegurança.

Pode ser considerado, no decurso da análise de risco e na eficiência a nível de custos, que resultados equivalentes podem ser obtidos recorrendo à subcontratação de serviços, equipamentos ou mesmo de recursos humanos, no entanto, somos da opinião que se deve priorizar a dotação de recursos próprios, colocando-os não só ao serviço do GRA, mas também de outras entidades na RAA.

3.10. Políticas de Segurança

Uma Política de Segurança define a segurança para um sistema ou para uma localização específica, podendo incluir questões físicas e administrativas e com políticas implícitas. Esta pode ser formal ou informal e pode ainda conter justificações de correção em termos de consistência ou técnicas. (Mamede, 2006)

Uma Política de Segurança deve transformar-se num conjunto de requisitos e operações que caracterizam os estados de proteção aprovados.

Uma Política de Segurança é definida tendo em consideração um conjunto de fatores internos e externos à própria organização. Como fatores internos podemos enunciar os objetivos de segurança da organização, os riscos e as ameaças, os serviços necessários, o respetivo nível de criticidade e os custos associados a todo o ambiente computacional. Como fatores externos devemos considerar as questões legais, os riscos e os custos, entre

outros. Para esboçar corretamente uma política de segurança devemos ter em consideração e refletir sobre todos estes fatores. (Mamede, 2006)

Como exemplos de uma política típica podemos referir: a política geral da instituição, com os constrangimentos genéricos e tendo uma visão global. Isto é, a política a ter com o e-mail constituirá uma de um conjunto de políticas auxiliares, subordinadas à política geral de segurança da organização.

A política de segurança deve ser escrita de modo informal e deve ser orientada à comunidade de utilizadores a que se destina, endereçando os constrangimentos relativos ao uso geral e não a questões como os tipos de controlo de acesso.

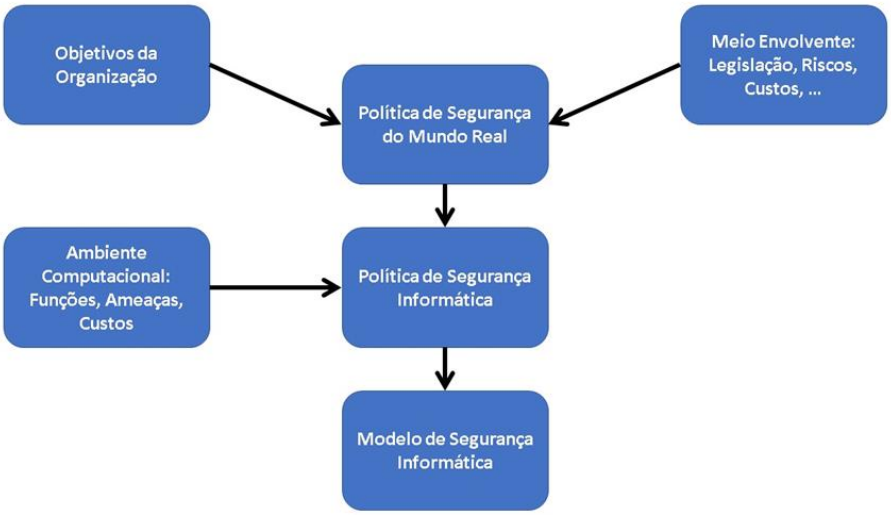


Figura 11 - Fontes para uma Política de Segurança (reproduzido de (Mamede, 2006))

Uma política definida desta forma irá apresentar vantagens e desvantagens. Como vantagem principal podemos apontar o facto de que qualquer colaborador da organização conseguirá ler e entender o documento. Como desvantagens podemos apontar a imprecisão por se recorrer à utilização de linguagem natural; a falta de definições exatas pode levar à existência de ambiguidades na interpretação do documento; as apresentações de requisitos genéricos podem ser difíceis de entender em distintos departamentos, por terem realidades diferentes; e por último devemos ter em consideração o facto de ser baseada em técnicas de remediação de situações ao invés de ser baseada em ameaças.

As políticas de segurança devem, deste modo, constituir-se como procedimentos, processos e métodos dinâmicos e complexos, sendo utilizados para incrementar a segurança de uma organização, devendo ter em consideração que a sua criação não constituirá um ato isolado, mas algo renovável ao longo do tempo, de modo a poder

ajustar novos requisitos que a organização terá com o decorrer da sua evolução e do seu negócio. Assim sendo, as características fundamentais que qualquer política de segurança deverá ter serão a abrangência e a flexibilidade.

3.11. Políticas e Procedimentos

Numa Organização, o desenvolvimento de uma política de segurança deve envolver quatro atividades distintas: (Hartley, 2001)

- Avaliação e entendimento das necessidades de segurança;
- Revisão das políticas e procedimentos em vigor, caso existam;
- Definição dos requisitos de proteção;
- Formalização da Política de Segurança.

As duas primeiras atividades exigem conhecimentos técnicos de segurança, de análise e de gestão do risco de modo a recolherem informação. A terceira atividade exige conhecimentos de análise e técnicos, e um entendimento razoável dos princípios de gestão do risco, visto ser puramente analítica. A quarta atividade consistirá na elaboração do documento que irá formalizar a política de segurança da Organização, sendo claramente administrativa, sendo habitualmente executada de forma interativa, isto é, envolvendo várias áreas da Organização (Recursos Humanos, Área Jurídica, Informática, Financeira, etc.) e origina diversas revisões do documento. (Mamede, 2006)

Quando definimos políticas e procedimentos de segurança, devemos ter em consideração diversos aspetos e várias perspetivas tão diferenciadas como a segurança das instalações e infraestruturas, procedimentos para os utilizadores, acessos físicos, questões administrativas, graus de uso aceitáveis, autenticações, respostas a incidentes e recuperação.

Uma política de segurança apenas fará sentido de existir numa Organização se a mesma for aplicada e seguida. Se a sua aplicação não for garantida por nenhum método, durante um determinado e breve período de tempo, após a sua entrada em vigor, os procedimentos irão ser seguidos, para rapidamente entrarem num estado de não cumprimento.

Os objetivos globais de uma Política de Segurança instanciam um conjunto de processos e métodos que aumentam a segurança da Organização e ao mesmo tempo criam um estado

de perceção e sensibilização de segurança na mente de todos os colaboradores. Desta forma os processos e os procedimentos vão constituir os meios para a implementação da segurança na Organização, enquanto a sensibilização dos colaboradores irá permitir que esta seja continuada no tempo. (Anonymous, 2003)

De forma a envolver os colaboradores na Política de Segurança de uma Organização devemos procurar que cada colaborador leia, concorde e assine um documento escrito onde esta esteja plasmada. Deste modo, o colaborador irá estar envolvido de duas formas, se por um lado teremos um documento escrito onde o colaborador se compromete com o cumprimento do estipulado, por outro lado, do aspeto psicológico associado à assinatura, que levará a um maior comprometimento e envolvimento, do colaborador, com a aplicação da Política de Segurança.

É no início do processo de criação dos procedimentos que constituirão a Política de Segurança que devem ser definidos o âmbito e os objetivos globais da mesma. Deve ser também decidido o nível de especificidade dos procedimentos, encontrando um meio termo, evitando um elevado nível de detalhe e também um nível de detalhe muito vago, permitindo um correto entendimento dos mesmos. Devem evitar-se os factos técnicos pois estes tendem a mudar com relativa frequência com o passar do tempo, pelo que, não devem ser incluídos.

As políticas devem ser passiveis de ser implementadas e com a capacidade de validar essa mesma implementação, devem ser precisas, concisas, facilmente percetíveis e não serem um bloqueio à produtividade individual. As políticas devem ainda explicar o porquê de serem necessárias, o que contemplam, os responsáveis pelas mesmas e as sanções que podem advir do seu incumprimento e, eventualmente, como serão aplicadas.

Um Procedimento é, tipicamente, dividido nas seguintes partes (Mamede, 2006):

- **Objetivo –** onde é apresentada a razão da existência do procedimento;
- **Descrição –** onde todas as questões relacionadas com o procedimento em questão são detalhadas;
- **Responsabilidades –** onde são declarados todos os responsáveis pelo procedimento;
- **Validade –** onde se indica a data de entrada em vigor do procedimento e quando será efetuada a revisão do procedimento;

- **Aprovação –** onde se especifica o circuito de aprovações do procedimento e respetivas assinaturas que confirmam o mesmo.

Para verificar e validar a aplicação e o cumprimento da Política de Segurança, pelos colaboradores da Organização, deve ser efetuada uma Auditoria de Segurança.

Esta Auditoria de Segurança pode ser calendarizada ou aleatória. A primeira é anunciada e permite um tempo de preparação dos colaboradores para enfrentar o processo e que estes assegurem estar a cumprir o estipulado. A auditoria aleatória ocorre por surpresa e são importantes para manter a segurança na operação diária da Organização, assumindo formas de ataques simulados ou tentativas de penetração de sistemas ou de instalações.

Os procedimentos devem se concisos e precisos, de modo a serem efetivos, pois ninguém lê documentos muito grandes, sendo que um documento com cerca de 10 páginas deverá ser suficiente. Como podem mudar ao longo do tempo, os detalhes técnicos de implementação não devem ser incluídos no documento.

Cada Organização desenvolverá um conjunto de procedimentos específico para a sua realidade, não sendo possível criar uma lista e afirmar que terão de existir procedimentos que cubram todos os tópicos da mesma, pois poderão não fazer sentido para Organização, como poderão existir outros que, não fazendo parte da lista, são muito importantes.

Os mais comuns numa Política de Segurança são os seguintes (Mamede, 2006):

- Autenticação e Controlo de Acessos;
- Criação e Gestão de Senhas;
- Níveis de Serviço;
- Cópias de Segurança e Recuperação de desastre;
- Gestão do Perímetro de Segurança;
- Formação e Treino em Segurança informática;
- Aquisição de produtos e de Sistemas Informáticos;
- Segurança na transmissão de dados, ligações e acessos remotos;
- Informação aos novos utilizadores;
- Segurança na externalização de serviços;
- Contratação e Saída de Recursos Humanos;
- Acesso físico às instalações;
- Acesso físico à infraestrutura e sistemas computacionais;

- Configuração e gestão de equipamentos clientes;
- Uso aceitável;
- Proteção contra vírus;
- Utilização da Internet;
- E-mail;
- Ligações e acessos remotos.

É muito importante a criação de documentos que definam a visão da Organização relativamente ao que é o processo de segurança e como se pretende manter o funcionamento deste.

As políticas são a pedra basilar de qualquer prática de segurança de informação e devem ser vistas como a constituição que governa a operação segura do Ambiente operativo. Constituem, em muitas ocasiões, a última linha de defesa.

A política de segurança deve endereçar vários itens, nomeadamente, a utilização aceitável, a classificação do valor dos dados, o ciclo de vida dos dados, os papeis e responsabilidades, o controlo de alterações e o *disaster recovery*. Em situações, muito usuais, de multiplataformas, devem ser criados standards de configuração e implementação dos Sistemas Operativos, tomando atenção às atualizações, procurando, para o efeito, um consenso entre os administradores dos diferentes sistemas, recordando que nenhum sistema operativo é seguro na sua forma de instalação básica.

A resposta a incidentes irá obrigar-nos a uma reflexão profunda, onde iremos procurar as respostas para questões aparentemente simples, como por exemplo, que incidentes são possíveis? Que resposta devemos assumir em cada possível incidente?

Devemos, deste modo, criar um tipo de capacidade de resposta a incidentes, assim como, desenvolver uma série de atividades, como a monitorização dos bens chave e a utilização de um método de deteção de intrusão. Devemos, também, determinar quem será o responsável pela resposta a ameaças de segurança, quais os procedimentos a seguir em cada situação e a lista de chamada para a tomada de decisão em situações críticas para o negócio. (Mamede, 2006)

Sendo a Segurança uma questão transversal a todas as pessoas da Organização e não apenas aos técnicos de segurança, devemos:

- Garantir que todas as Políticas de Segurança de caracter geral são distribuídas a todos os colaboradores da Organização;
- Definir uma campanha de sensibilização junto dos colaboradores da organização;
- Identificar um executivo interno disposto a criar memorandos para o resto da Organização;
- Reforçar a importância de práticas de forte segurança e construir matrizes de responsabilidade que identifiquem claramente responsabilidades de segurança no seio da organização.

Devemos realizar todos os esforços em conjunto, em prol da eficácia, sendo o segredo conseguir fazê-lo de forma eficaz.

3.12. Normas e Metodologias para Resposta a Incidentes

Têm surgido vários regulamentos recomendando as melhores práticas, especialmente dedicados aos procedimentos e às políticas a adotar ao nível das tecnologias de informação e comunicação, com o objetivo de contribuir para a Segurança da Informação, nomeadamente no esforço de garantir a qualidade da informação através das premissas confidencialidade, integridade, autenticidade e disponibilidade, em sistemas cada vez mais abertos e complexos.

As normas existentes são muito abrangentes e acompanham em detalhe todos os processos nas várias fases do desenho da arquitetura de um Sistema de Informação. Considerando o âmbito deste trabalho, começaremos por abordar a norma da série 27000 da ISO/TEC, mais concretamente a ISO 27035.

Os Estados Unidos e a Europa possuem organizações que produzem regulamentos relativos à Segurança da Informação, assim, será analisado o documento SP 800-61 *do National Institute of Standards and Technology* (NIST) dos EUA, um guia para a gestão de incidentes de segurança de computadores e também um guia de boas práticas para a Gestão de Incidentes, da *European Union Agency for Network and Information Security* (ENISA).

3.13. Norma ISO/IEC 27035

A norma ISO/IEC 27035 foi publicada em 2011 e revista em 2016 (encontrando-se neste momento em fase de aprovação a nova versão que irá substituir a versão de 2016), substituindo a ISO 18044 de 2004, com o título de "Tecnologia de Informação – Técnicas de Segurança – Gestão de Incidentes de Segurança da Informação". Apresenta-se como um guia para a gestão de Incidentes de Segurança da Informação para organizações de média e grande dimensão, ou para organizações externas que forneçam esse serviço. (ISO, 2016)

Conforme publicado no site da *International Standard Organization* (ISO), a norma fornece uma aproximação estruturada e planeada para:

- Detetar, reportar e avaliar incidentes de segurança da informação;
- Responder e gerir incidentes de segurança da informação;
- Detetar, avaliar e gerir vulnerabilidades na segurança da informação;
- Melhorar continuamente a gestão dos incidentes de segurança da informação como resultado da gestão dos incidentes da segurança da informação e vulnerabilidades.

A norma disponibiliza as orientações necessárias às organizações que pretendem preencher os requisitos definidos na ISO/IEC 27001 (ISO, ISO/IEC 27001, 2013) e como um complemento à gestão de incidentes abordada na norma ISO/IEC 27002 (ISO, ISO/IEC 27002, 2022).

A norma aborda a definição de eventos de segurança da informação como ocorrências em sistemas, serviços ou redes que indicam possíveis falhas nos controlos ou políticas de segurança, ou situações desconhecidas que possam ser relevantes para a segurança. Ela também define incidentes de segurança como eventos inesperados ou indesejados que têm uma alta probabilidade de comprometer o negócio da organização ou ameaçar a segurança da informação.

É de ressaltar, que a ocorrência de um evento de segurança não implica necessariamente numa tentativa bem-sucedida de comprometimento, nem tem implicações imediatas na confidencialidade, integridade e disponibilidade da informação. A implementação de controlos por si só não garantem a ausência de vulnerabilidades que possam comprometer a segurança da informação e, portanto, a ocorrência de possíveis incidentes de segurança.

A norma destaca os potenciais impactos diretos/indiretos nos negócios da organização causados pelos incidentes de segurança. Portanto, é necessário adotar uma abordagem estruturada e planeada pela organização em relação à sua segurança da informação.

Em resumo, a norma enfatiza a importância de identificar e gerir eventos de segurança, bem como de adotar medidas adequadas para proteger a informação e mitigar os riscos associados a possíveis incidentes de segurança da informação. Para atingir o objetivo de implementação de uma efetiva gestão de incidentes de segurança da informação, a norma ISO 27035 apresenta cinco fases que se articulam entre si (ver figura 12):

Figura 12 - Fases da gestão de incidentes de segurança da informação

3.13.1.1. Fase de preparação e planeamento

Para operacionalizar uma efetiva capacidade de gestão de incidentes de segurança da informação, a organização tem de realizar uma preparação e um planeamento apropriado, identificando as suas vulnerabilidades, alocando os recursos necessários e esquematizando a sua resposta. A norma aponta um conjunto de atividades a serem concluidas para atingir este objetivo.

A primeira atividade é a definição de uma política de gestão de incidentes, com o compromisso da gestão de topo da organização. É importante que os colaboradores sejam capazes de reconhecer eventos de segurança, saibam o que fazer e compreendam a importância de uma política de gestão. Além disso, a gestão da organização deve apoiar

fortemente a construção dessa capacidade, fornecendo os recursos necessários para responder a incidentes de segurança da informação.

Uma atividade importante é a atualização contínua das políticas de gestão de risco, levando em consideração a gestão de eventos, incidentes e vulnerabilidades de segurança da informação, tanto em redes quanto em serviços.

Também é crucial estabelecer um processo detalhado de gestão de incidentes de segurança da informação, documentado por meio de formulários, procedimentos e ferramentas de deteção e relato. Este processo deve incluir mecanismos de avaliação para auxiliar na tomada de decisões, apontando as medidas a serem adotadas perante um incidente, além de, consolidar aprendizagens com ocorrências anteriores e a mitigação dos incidentes.

A criação de uma equipa de resposta a incidentes de segurança da informação, devidamente capacitada e treinada, é apresentada como uma das atividades fulcrais. A equipa deve ser organizada e estruturada de acordo com as necessidades operacionais da organização, podendo ser composta por membros dedicados, membros virtuais que desempenham outras funções na organização ou uma combinação dessas abordagens. É essencial garantir a existência de canais de comunicação tanto internos quanto externos relacionados à gestão de incidentes de segurança da informação.

A norma também recomenda o desenvolvimento de programas de treino e consciencialização não apenas para a equipa de resposta a incidentes, mas para todos os utilizadores dos sistemas da organização. É importante que todos tenham conhecimento da existência de incidentes de segurança da informação e que a organização possua políticas e procedimentos para lidar com eles. O envolvimento de todos os membros da organização é fundamental para o sucesso na gestão de incidentes.

Por fim, destaca-se que a gestão de incidentes de segurança da informação é um processo dinâmico, sendo necessário testar as políticas existentes e a participação da organização em exercícios que simulem situações reais, submetendo a equipa de resposta a incidentes a cenários de pressão o mais próximos possíveis da realidade.

3.13.1.2. Fase de deteção e registo

A segunda fase de uma operação de gestão de incidentes envolve a deteção dos incidentes, a coleta de informações, o relato de eventos de segurança e a identificação de vulnerabilidades, mesmo que ainda não tenham sido exploradas. Toda a informação relacionada com um incidente deve ser armazenada num banco de dados operado pela equipa de gestão de incidentes.

Para garantir a deteção, é necessário armazenar e analisar os registos de eventos de diversos dispositivos de segurança, como *firewalls*, sistemas de prevenção de intrusões

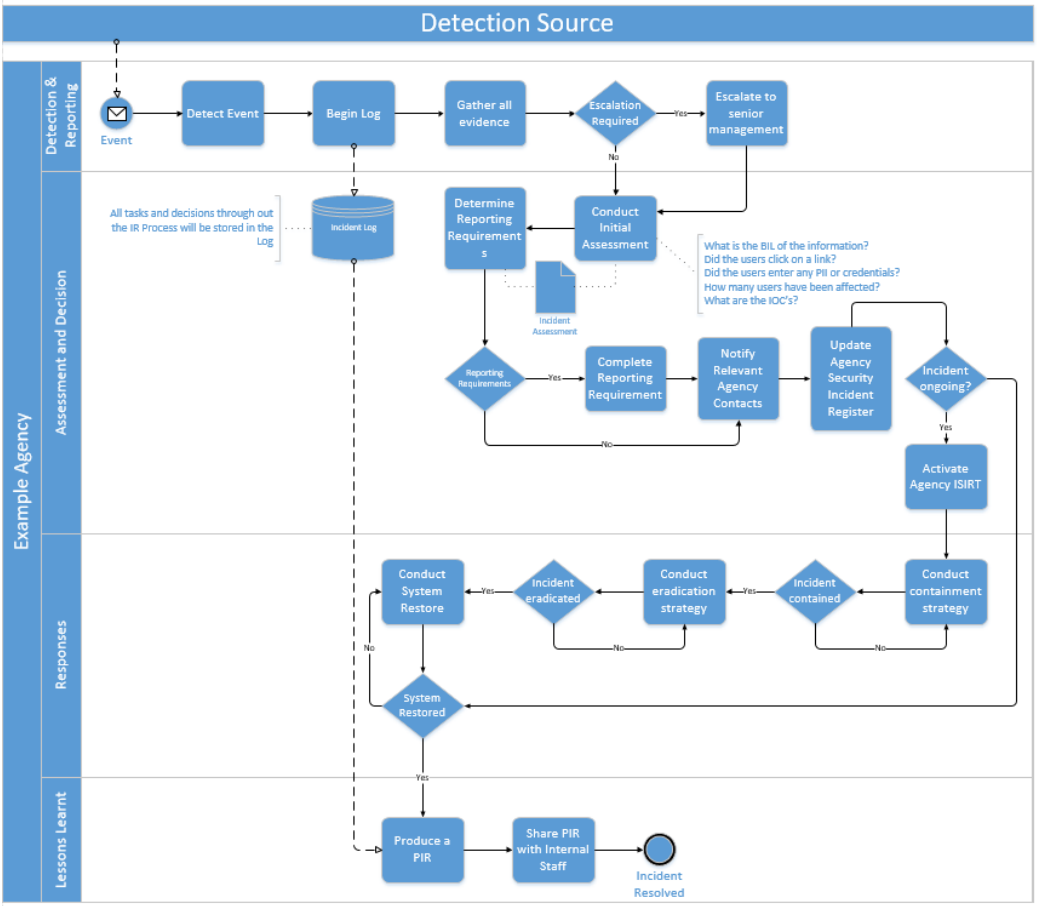


Figura 13 - Fluxo da Informação de um Incidente de Segurança (adaptado de (ISO, ISO/IEC 27035-1, 2016))

(IPS), antivírus e outros, a fim de integrar um sistema de acompanhamento dos incidentes.

A responsabilidade de notificar um evento de segurança recai sobre aquele que o detetou pela primeira vez. Portanto, é essencial que todos os colaboradores conheçam os procedimentos a serem adotados ao depararem-se com um evento de segurança da informação, preferencialmente seguindo um guia de ações e sabendo a quem reportar o evento. A equipa de resposta a incidentes deve ter um membro designado para receber e

analisar os eventos comunicados ou detetados, decidindo qual a ação a ser tomada. Mesmo os eventos que não sejam considerados incidentes devem ser registados de acordo com um formulário preestabelecido para manter a consistência das informações coletadas. Na figura 13 está representado o esquema proposto pela norma ISO 27035 para o fluxo de informação de um evento ou Incidente de Segurança da Informação.

3.13.1.3. Avaliação e decisão

Nesta fase, a norma identifica as atividades referentes à avaliação dos eventos de segurança da informação que permitem escolher os que deverão ser tratados como incidentes.

O membro da equipa de resposta a incidentes de segurança que recebe a notificação do evento, deve avaliar os eventos comunicados de acordo com uma análise de risco feita com base nas vulnerabilidades conhecidas dos sistemas e num conjunto de ações predefinidas. Com base na avaliação feita, o evento deve ser classificado de acordo com o impacto que este evento pode ter sobre os sistemas e com a forma como pode afetar o modelo de negócio da organização, sendo assim, definida qual a prioridade a atribuir à sua resolução ou acompanhamento. Para esta fase, a norma indica que todos os eventos devem ser avaliados de acordo com os seguintes elementos:

- Impacto na estrutura física e lógica da organização;
- Os equipamentos, infraestruturas, processos, serviços e aplicações afetados;
- Possíveis efeitos nos serviços nucleares da organização.

Todas as ações relacionadas com o evento e a sua eventual evolução para o incidente, devem ser registadas numa plataforma de registo de incidentes que permita o acompanhamento das várias ações executadas e a sua posterior consulta como histórico.

3.13.1.4. Resposta

Nesta etapa, são apresentadas as atividades necessárias para responder aos incidentes de acordo com as decisões tomadas na fase anterior. Após a resolução de um incidente, a resposta envolve a restauração dos serviços afetados, a documentação do incidente e a comunicação às partes envolvidas. No entanto, pode ser necessário escalar o incidente para um nível técnico superior ou envolver entidades externas à organização. Essa

avaliação é realizada pela equipa de resposta a incidentes de segurança da informação, que deve garantir a reposição dos sistemas afetados e o registo de todas as ações realizadas, para preservar a integridade das informações como prova.

Ao responder ao incidente, a equipa deve assegurar que todos os sistemas estejam operacionais e que a vulnerabilidade que causou o incidente tenha sido mitigada, não apenas no sistema ou equipamento afetado, mas em todos os sistemas semelhantes ou que, possam ser afetados pela mesma vulnerabilidade. Após a conclusão de todo o processo, o evento/incidente deve ser formalmente encerrado na plataforma de registo mencionada anteriormente.

3.13.1.5. Lições aprendidas

A última fase refere-se ao que fazer quando o evento/incidente se encontra formalmente encerrado. A primeira coisa a considerar será a avaliação da adequação dos procedimentos estabelecidos para o tratamento do evento/incidente, desde a sua deteção até à reposição dos serviços e mitigação da vulnerabilidade. As conclusões obtidas a partir desta avaliação, com eventuais melhorias a introduzir nos processos e as recomendações para a revisão ou implementação de novos controlos de segurança, devem ser incorporadas na política de segurança da informação da organização e no planeamento das futuras ações de resposta a incidentes.

As lições aprendidas devem ser partilhadas com a comunidade de entidades parceiras da segurança da informação. Esta partilha de informação com outras equipas de resposta a incidentes de segurança de informação, com as quais existam relações de confiança, devem ser realizadas de forma regular, pois são importantes para a criação de uma consciência global e de um conhecimento situacional da Cibersegurança.

A norma ISO 27035 reforça a ideia de que o processo de resposta a incidentes de segurança da informação é um processo iterativo, para o qual a organização deverá estar atenta, procurando introduzir melhorias nas suas diversas fases. Para isso os processos devem ser revistos com base nos eventos/incidentes ocorridos, com base nas tendências detetadas.

3.14. National Institute of Standards and Technology (NIST)

O NIST é uma agência federal norte americana do Departamento do Comércio que tem por missão promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, as normas e a tecnologia de forma a melhorar a segurança económica e a qualidade de vida. (NIST, 2023)

De acordo com a lei federal norte americana publicada em 2002 (FISMA – *Federal Information Security Management Act*) as agências federais devem reportar formalmente todos os incidentes de segurança ao *United States Computer Emergency Readiness Team* (US-CERT).

O NIST publicou o NIST SP 800-61, um guia para a gestão de Incidentes de Segurança de Computadores, com o objetivo de apoiar as organizações e as agências federais na mitigação do risco associado aos incidentes de segurança de computadores, disponibilizando orientações sobre como responder a estes incidentes de modo eficiente e efetivo. (Cichonki, 2012)

No SP 800-61 o NIST identifica quais as principais ações a realizar para a edificação de uma capacidade de resposta a incidentes:

- Criar um plano e uma política de resposta a incidentes;
- Desenvolver procedimentos para realizar a gestão de incidentes e o seu registo baseado na política de reposta a incidentes;
- Definir as linhas orientadoras para comunicarem com as entidades parceiras sobre os incidentes;
- Escolher um modelo de constituição e operação da equipa de resposta a incidentes;
- Estabelecer relações entre a equipa de resposta a incidentes e outros órgãos internos (ex. o departamento jurídico) e externos (ex. forças policiais, órgãos de investigação criminal);
- Selecionar quais os serviços de resposta a incidentes serão disponibilizados;
- Aprovisionar e treinar a equipa de reposta a incidentes.

O documento apresenta recomendações e boas práticas para a construção da capacidade de resposta a incidentes nas organizações. Essa capacidade, visa prevenir problemas que possam evoluir para incidentes, aumentando assim a segurança das redes, sistemas e

aplicações. É destacada a importância da documentação e comunicação formal dos incidentes com outras entidades, facilitando a interação e evitando erros de interpretação. Detetar o incidente o mais cedo possível é crucial, utilizando mecanismos de correlação para automatizar o processo.

A classificação e priorização dos incidentes são essenciais, uma vez que nem todos têm o mesmo impacto na organização. Linhas orientadoras devem ser estabelecidas para ajudar na classificação e processos devem ser implementados para ajustar os conhecimentos na resolução de incidentes.

No caso de incidentes de larga-escala, que podem ser complexos e não facilmente percebidos pelos colaboradores da organização, é necessário um plano de comunicação para alertar todos os colaboradores e permitir que contribuam com informações relevantes para uma resposta rápida da equipa. A partilha de informações com outras entidades afetadas pelo mesmo incidente possibilita a tomada de decisões com base em toda a informação disponível.

O documento do NIST também define os termos "eventos" e "incidentes". Eventos referem-se a acontecimentos observados em sistemas ou redes, enquanto eventos adversos são aqueles que têm consequências negativas para os sistemas ou informações. Excetuando-se os incidentes relacionados a causas naturais ou falhas de hardware, os eventos com consequências negativas são considerados incidentes de segurança, resultantes de violações ou ameaças às políticas e práticas de segurança estabelecidas. O documento apresenta como exemplo de incidentes vários casos (ver tabela 6).

Tabela 6 - Exemplo de Incidentes de Segurança (adaptado de NIST SP 800-61)

Incidente	**Descrição**
Negação de serviço	Um atacante envia pacotes especialmente adulterados para um servidor ligado em rede (na Intranet ou Internet) de modo que este bloqueie. Um atacante dirige centenas de máquinas comprometidas para gerarem tráfego de modo a comprometer o normal funcionamento da rede.
Código malicioso	Um *worm* acede aos ficheiros partilhados da organização de modo a infetá-los. Aviso por parte do fabricante de software de um novo vírus ou *worm* com capacidade de explorar vulnerabilidades existentes na nossa rede.
Acesso não autorizado	Um atacante consegue correr uma ferramenta de exploração de vulnerabilidades conseguindo aceder ao ficheiro de *passwords*. O atacante consegue aceder a informação sensível para a organização.

Uso inadequado	Um utilizador disponibiliza *software* ilegal através de sistemas de partilha de ficheiros. Um utilizador ameaça outro através de e-mail.

O documento do NIST aborda os vários aspetos envolvidos na construção de uma capacidade de resposta a incidentes de segurança. Isso inclui a elaboração de políticas, a organização da capacidade, os recursos humanos envolvidos e os serviços que a equipa de resposta a incidentes pode fornecer à organização. O documento apresenta recomendações, enfatizando a necessidade de formalizar a capacidade de resposta a incidentes por meio de políticas e procedimentos bem definidos, adaptados à realidade específica da organização.

É destacada a importância de estabelecer modelos de comunicação e registo de incidentes que facilitem a comunicação interna e a interação com entidades externas. Além disso, é essencial selecionar as pessoas certas, com a devida formação e treino, para ocuparem posições adequadas dentro da equipa de resposta a incidentes, abrangendo áreas como gestão da capacidade, deteção e análise técnica, capacidade forense e apoio jurídico.

O conhecimento do quadro legal aplicável a estas situações é considerado fundamental para lidar com possíveis consequências disciplinares e para validar a adoção de medidas de monitorização e análise que possam envolver questões legais. O documento fornece uma visão abrangente e diretrizes para a construção de uma capacidade eficaz de resposta a incidentes de segurança, considerando a complexidade e os desafios associados a esta área.

3.14.1.1. Gestão de Incidentes

O documento editado pelo NIST detalha o processo de gestão de incidentes em 4 fases distintas, a Preparação, a Deteção e Análise, a Contenção, Irradicação e Recuperação e finalmente a Atividade Pós-Incidente. As várias fases, bem como a relação existente entre elas, são apresentadas na figura 14 no chamado “Ciclo de Vida do Incidente”.

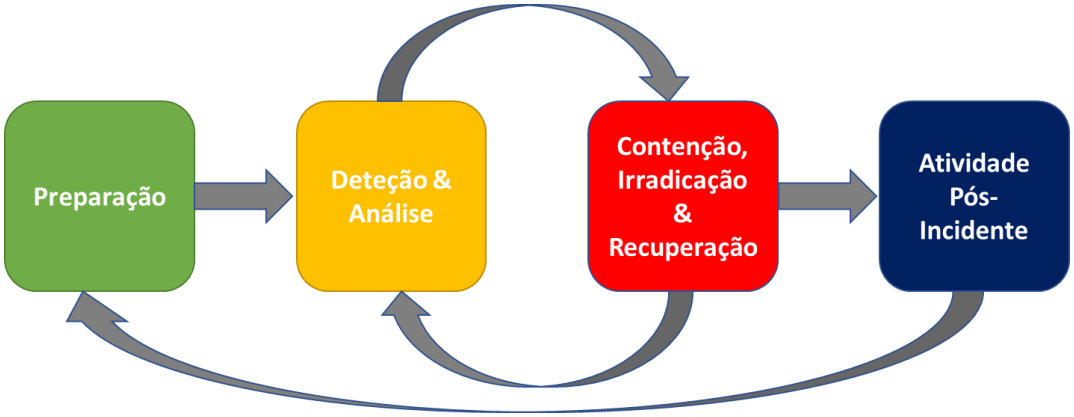


Figura 14 - Ciclo de vida do Incidente (adaptado de (Cichonki, 2012))

A fase de Preparação tem como objetivos principais a construção de uma equipa de resposta a incidentes devidamente treinada, equipada e a implementação de controlos de segurança adequados para limitar o número de incidentes. A equipa de resposta a incidentes deve ter um *kit* portátil que inclua um computador com *software* apropriado, ferramentas para captura e análise de tráfego de rede, realização de *backups* e equipamento básico de rede. Isso permite uma rápida mobilização para fornecer suporte ou realizar investigações forenses. Embora a prevenção de incidentes normalmente não seja de responsabilidade direta da equipa de resposta a incidentes, a sua perceção das ameaças e a sua evolução permitem uma análise de risco dinâmica que deve ser considerada na definição dos controlos de segurança a serem implementados na organização.

A fase seguinte é a Deteção e Análise de incidentes. Devido à variedade de tipos de incidentes e as suas formas de afetar a organização, não é possível estabelecer um procedimento específico para cada tipo de incidente. O NIST propõe a criação de categorias de incidentes e sua categorização com base no modo de transmissão. Por exemplo, um vírus que cria uma *backdoor* para obter acesso ilegítimo deve ser categorizado como "Código malicioso" em vez de "Acesso não autorizado".

A deteção de incidentes pode ser desafiadora devido ao grande número de fontes de eventos, que fornecem informações sobre potenciais incidentes com diferentes níveis de detalhes e credibilidade. Além disso, requer experiência e conhecimento técnico avançado para uma análise eficiente de todas as informações disponíveis. O NIST introduz o conceito de "sinais do incidente", dividindo-o em duas categorias: "Indicações", que são sinais de que um incidente ocorreu ou está a ocorrer, e "Indícios",

que são sinais de um incidente que pode ocorrer no futuro. Sempre que um indício for detetado, a organização deve tomar medidas para prevenir o incidente, embora existam ataques que não apresentem indícios.

A análise de incidentes é frequentemente desafiadora. Muitos dos sinais recebidos pela equipa de resposta a incidentes podem ser falsos positivos, erros operacionais ou falhas de hardware. Os sinais podem ser ambíguos, contraditórios ou não fornecer toda a informação necessária para categorizar um incidente. Por isso, é fundamental ter uma equipa experiente, bem treinada e capacitada para evitar ineficiências na deteção e análise de incidentes, pois, erros de decisão podem ter custos significativos para a organização. Na tabela 7 apresentam-se as recomendações do NIST para uma análise de incidentes mais efetiva.

Tabela 7 - Análise de Incidentes (adaptado das recomendações NIST)

Recomendação	**Descrição**
Perfis de rede e sistemas	Criação de perfis de utilização ao nível das máquinas e dos sistemas, nomeadamente ao nível da integridade dos ficheiros críticos. Perfil de utilização da infraestrutura, nomeadamente os valores médios e de pico.
Compreender os comportamentos normais	Análise frequente de registos de desempenho e de operação que permitam detetar desvios e tendências.
Política de *Logging*	Consolidação dos "*log*" das diversas plataformas numa plataforma centralizadora. Definição de uma política de retenção de "*log*".
Correlação de eventos	Capacidade de correlacionar os "*log*" de diferentes equipamentos (*firewall*, IDPS, outros) detetando assim indícios de incidentes.
Sincronização de relógios	Utilização do protocolo NTP permite uma efetiva correlação de eventos ocorridos em várias máquinas da organização.
Base de dados conhecimento e informação	Documentação sobre a infraestrutura e vulnerabilidades conhecidas. Informação relativa a *software* malicioso. Informação de domínios maliciosos.

Na fase de Preparação, é importante registar rapidamente todos os elementos disponíveis quando um incidente é detetado, bem como todos os eventos relacionados com ele. A informação recolhida durante a investigação também deve ser armazenada, registada e

assinada pelo responsável pela investigação, pois a validade da utilização dessas informações em tribunal ou em processos disciplinares internos depende do cumprimento correto dos procedimentos. É recomendado o uso de uma base de dados de registos de incidentes, que deve incluir, entre outras coisas, informações sobre o "estado do incidente", um resumo do incidente, registo de todas as ações realizadas, contatos dos envolvidos (utilizadores e gestores), lista de evidências recolhidas e comentários dos gestores do incidente.

Além disso, nessa fase, é necessário considerar a classificação do incidente. Essa classificação é uma das ações mais importantes, pois os incidentes não são todos iguais e afetam a organização de maneiras diferentes. Uma correta classificação é essencial para abordar o incidente com a prioridade adequada. A priorização do incidente está intimamente relacionada com o negócio da organização e com o impacto que o incidente pode ter em termos de funcionalidade e segurança da informação. Essa priorização pode ser expressa por um valor numérico que reflita a severidade e o impacto que o incidente tem para a organização. No caso específico do NIST, que se refere às agências federais americanas, existe uma tabela que permite definir com precisão o grau de criticidade do incidente, e essa informação deve ser compartilhada com o US-CERT.

A fase de Contenção, Irradicação e Recuperação está fortemente relacionada à fase anterior, pois muitas das ações de contenção ou erradicação dependem das informações reunidas na fase de deteção e análise. A contenção é extremamente importante, pois após a deteção de um incidente em andamento ou já ocorrido, é necessário responder de maneira a limitar ao máximo seus efeitos. Para isso, é necessário ter estratégias e procedimentos de contenção previamente estabelecidos para os diferentes tipos de incidentes. Após a contenção, vem a erradicação do incidente, que muitas vezes está associada à recuperação. Isso é comum em casos de incidentes de *malware*, onde a eliminação de arquivos infetados requer a restauração dos arquivos afetados. O mesmo se aplica quando há comprometimento de credenciais de utilizadores, onde inicialmente pode ser necessário eliminar a conta do utilizador nos sistemas e, posteriormente, criar novas contas. Essa relação é particularmente importante quando os sistemas operacionais são afetados, podendo exigir uma nova instalação do sistema, mas recuperando as informações de customização anteriores.

A Atividade Pós-Incidente desempenha um papel importante no registo das "lições aprendidas" e na identificação de oportunidades de melhoria nas políticas, controlos e procedimentos. Após o encerramento de um incidente significativo, toda a equipa deve reunir-se e reavaliar todo o processo para investigar o que aconteceu, como aconteceu e por que aconteceu. Também é importante verificar se todos os procedimentos foram seguidos e se os processos de comunicação foram respeitados, procurando valor e aprendizagem para melhorar a preparação da organização para futuras ocorrências. Na ausência de incidentes significativos, a equipa deve reunir-se periodicamente com o intuito de analisar vários incidentes, com o objetivo de identificar melhorias e propô-las para serem incorporadas na fase de preparação. No final, deve ser elaborado um relatório do incidente, contendo todas as informações relevantes, as conclusões da equipa e as sugestões de melhoria. As informações reunidas nesta fase contribuirão para uma nova análise de risco, avaliação do desempenho da equipa de resposta a incidentes e auditoria da capacidade de resposta a incidentes da organização.

3.15. Guia de boas práticas para a gestão de incidentes da ENISA

A ENISA, como agência europeia para a segurança da informação e redes, apoia os estados-membros da União Europeia e as agências europeias, funcionando como um Centro de Excelência que produz avisos e recomendações para os assuntos relativos à segurança da informação e das redes, nomeadamente das infraestruturas críticas europeias (ENISA, Threat Landscape - Responding to the Evolving Threat Environment, 2012). Em 2010 a ENISA publicou um guia para apoio à constituição de um serviço de tratamento de incidentes, considerando-o como o núcleo da capacidade de gestão de incidentes. (ENISA, Good Pratice Guide For Incident Management, 2010)

Neste guia de boas práticas, a ENISA apresenta a Gestão de Incidentes como um conjunto de serviços mais alargados de segurança a munir à organização, como sejam a capacidade de tratamento de incidentes, a análise e mitigação de vulnerabilidades, comunicados e alertas de segurança, entre outros serviços de gestão de incidentes. A figura 15 apresenta a visão da ENISA sobre o serviço de resposta a incidentes, de acordo com uma capacidade de gestão dos mesmos. Nela, estão representadas as quatro fases principais do tratamento de um incidente, a Deteção, a Triagem, a Análise e a Resposta ao Incidente.

Figura 15 - Gestão de Incidentes e tratamento de Incidentes (adaptado de (ENISA, Good Pratice Guide For Incident Management, 2010))

Para o desempenho das várias fases do tratamento dos incidentes, a organização da gestão de incidentes tem obrigatoriamente de prever a existência de uma equipa com pessoal técnico preparado para desempenhar essas funções. A ENISA identifica como funções obrigatórias as seguintes que passo a descrever.

O *Duty Officer* é o responsável por receber relatos de incidentes e registá-los, garantindo que cada incidente tenha um responsável. O *Triage Officer* recebe o incidente, realiza uma triagem inicial e decide o encaminhamento para a equipa de resposta apropriada. O *Incident Handler* é responsável por analisar e responder aos incidentes, enquanto o *Incident Manager* supervisiona todas as atividades de tratamento de incidentes e atua como representante da equipa. Existem outras funções relacionadas com o tratamento dos incidentes, mas estas, não requerem a existência de um membro permanente, podendo ser requerida a sua participação de acordo com a necessidade, são disso exemplo os elementos de apoio jurídico ou de relações públicas.

3.15.1.1. Tratamento de incidentes

Sobre o tratamento de incidentes a ENISA propõe um conjunto de fases organizadas de acordo com um *workflow* (ver figura 16) que pode e deve ser ajustado com maior ou menor detalhe às especificidades da organização.

Fazendo a ligação deste *workflow* com as fases do tratamento de incidentes anteriormente enumeradas, as tarefas de relato de incidente e o seu registo fazem parte da fase de Deteção. A deteção do incidente envolve o relato e registo do incidente, seja através de relatos recebidos por e-mail, telefone ou formulários eletrônicos, bem como a monitorização preventiva dos sistemas de segurança.

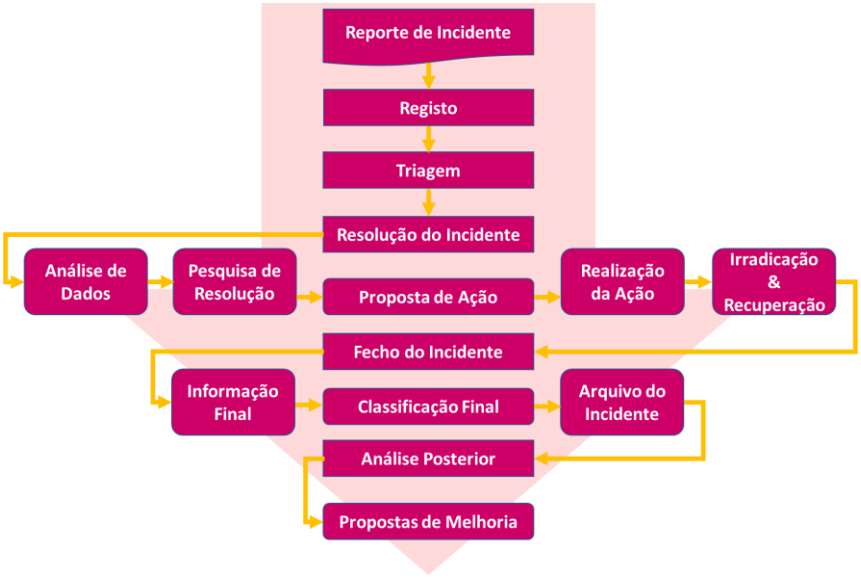


Figura 16 - *Workflow* para o tratamento de incidentes (adaptado de (ENISA, Good Pratice Guide For Incident Management, 2010))

A fase de triagem envolve a verificação se o incidente é de segurança, a sua relevância para a organização, o impacto e a quantidade de pessoas necessárias para tratar o incidente.

A ENISA indica várias questões que devem ser colocadas nesta fase, das quais destacamos:

- Estamos perante um incidente de segurança?
- É referente aos nossos sistemas?
- Qual o seu impacto?
- Quais os danos colaterais?
- Quantas e quais as pessoas necessárias para tratar deste incidente?

As fases de Análise e de Resposta ao Incidente são apresentadas como um ciclo de resolução (ver figura 17), que inclui a análise de informações, notificação de afetados, pesquisa de solução, definição e comunicação de ações propostas, verificação das ações realizadas, irradicação do problema e recuperação dos sistemas afetados. Após a resolução, o incidente é encerrado com a comunicação de encerramento a todas as partes envolvidas e o armazenamento seguro das informações relevantes.

Figura 17 - Ciclo de resolução do Incidente (adaptado de (ENISA, Good Pratice Guide For Incident Management, 2010))

Além disso, a ENISA recomenda a realização de análises posteriores para identificar lições aprendidas com incidentes complexos ou novos. Essas lições podem contribuir para a revisão de políticas de segurança, processos operacionais e monitoramento, melhorando as condições de segurança dos sistemas e serviços. Essa abordagem reativa da gestão de incidentes também pode ter um efeito preventivo, ao melhorar as políticas de segurança e contribuir para a prevenção de futuros incidentes. É importante destacar que a gestão de incidentes é um processo contínuo e interativo, sujeito a ajustes e melhorias com base nas experiências e conhecimentos adquiridos ao longo do tempo.

Capítulo 4 Proposta de Implantação

Este Capítulo pretende apresentar a Proposta que se pretende implementar, assim como, o trabalho que já foi desenvolvido neste âmbito, de acordo com os objetivos propostos para este projeto.

4.1. Resposta a Incidentes

Tendo como ponto de partida o documento do NIST, sobre o processo de gestão de incidentes, vulgo "Ciclo de Vida do Incidente", vamos dividir a proposta e o trabalho já realizado em 4 fases distintas, a Preparação, a Deteção e Análise, a Contenção, Irradicação e Recuperação e finalmente a Atividade Pós-Incidente.

4.2. Preparação

Nesta Fase pretendeu-se a criação de um Plano de Segurança e Resposta a Incidentes no GRA, apoiado na Plataforma Azores Cyber 360º (SOC do GRA), apoiado pela criação de uma Cyber Academia, Campanhas de Sensibilização e Manuais de Boas Práticas que permitam aumentar a Cultura de Segurança no GRA.

4.2.1.1. O Plano de Segurança e o Plano de Resposta a Incidentes no GRA

A capacitação em Cibersegurança tem três componentes fundamentais: a prevenção, que atua numa vertente de proteção da organização; a deteção, que pretende detetar eventos e incidentes o mais rápido possível; e finalmente a reação, que pretende mitigar o incidente e recuperar dos possíveis danos. Transversalmente, às três componentes consta uma fase

de preparação, onde se identificam os serviços vitais, onde é realizada uma análise de risco, onde se capacita a organização em *cyber threat intelligence*; e onde é realizada uma constante monitorização e implementação de ações de melhoria contínua.

Para a criação do Plano de Segurança do GRA, deverá ser realizada uma avaliação ao ecossistema GRA, identificando potenciais lacunas na capacitação, seguindo-se uma priorização das ações a tomar e finalmente o desenho e a implementação do Plano. Como após a implementação do Plano os objetivos mudam, assim como, o ambiente de risco evolui, o Plano deve ser revisto e ajustado com uma periodicidade anual, permitindo uma maior maturidade, adaptações ao ecossistema GRA e à constante evolução tecnológica.

A estratégia de capacitação da deteção de incidentes de Cibersegurança deve estar alinhada com o *core business* da entidade GRA, através da gestão de risco. Deste modo, todas as ações propostas devem surgir após a identificação, mapeamento e quantificação dos riscos de segurança da informação; só posteriormente é traçado um plano de deteção, com base nos riscos identificados. De acordo com o quadro global de ameaça identificado, são propostas ações a realizar no GRA para desenvolver métodos de deteção das ameaças identificadas. A forma como uma ação deve ser implementada não é detalhada neste Plano, mas são identificadas normas de referência para servir de guia de implementação das ações propostas.

Devemos considerar quatros grandes dimensões no desenvolvimento das capacidades mínimas de deteção de incidentes: técnica, humana, processual e organizacional.

- A dimensão técnica envolve ações mais direcionadas às equipas técnicas, tais como, a definição de uma arquitetura segura e a identificação de ferramentas a adquirir;
- A dimensão humana pretende dotar os recursos humanos do GRA, com ações de formação customizadas às funções desempenhadas e com a garantia que todos os colaboradores adquirem os conhecimentos mínimos necessários;
- A dimensão processual define procedimentos, políticas e boas práticas, não só operacionais, mas no âmbito de todo o GRA;
- A dimensão organizacional vai garantir a definição de uma estratégia para criar uma cultura de Cibersegurança em todo o GRA.

A estratégia de Defesa em Profundidade deverá ser a adotada, garantindo a deteção nas múltiplas camadas funcionais e tecnológicas do GRA. Pretende-se assim, proteger os

ativos críticos do GRA e detetar os ataques antes que o agente malicioso produza um impacto significativo nos sistemas do ecossistema GRA.

Deve ser estabelecido um plano de desenvolvimento de capacidades mínimas, constituído por cinco níveis, para que as entidades GRA sejam integradas no ecossistema nacional de Cibersegurança e criem condições para uma melhoria sustentada das mesmas. No primeiro nível de preparação, é realizada uma análise de risco e é desenhado o panorama inicial do GRA. Segue-se o projeto de uma arquitetura segura no segundo nível; a segurança dos dispositivos e aplicações no terceiro nível; a definição dos procedimentos de Cibersegurança no quarto nível; e por fim, no quinto nível, a criação formal de uma equipa dedicada à deteção de incidentes. Cada nível é constituído por uma série de capacidades e ações associadas e, se uma entidade demonstrar que tem todas as capacidades dentro de um nível (e dos níveis anteriores), então será certificada para esse mesmo nível.

Os cinco Níveis, baseados no RCMCS, são:

- Nível 1 – Preparação;
- Nível 2 – Arquitetura;
- Nível 3 – Dispositivos e Aplicações;
- Nível 4 – Procedimentos de Cibersegurança;
- Nível 5 – *Security Operations Center* – SOC.

O Plano deverá considerar, ainda, a criação de uma equipa CSIRT do GRA, que irá proteger o interesse legítimo da sua comunidade particular, o ecossistema GRA, através da coordenação de resposta a incidentes de segurança informática, o que pressupõe a prevenção, tratamento e resposta de incidentes.

Esta equipa deverá usar uma taxonomia comum e mecanismos automáticos para partilha de informação operacional, conforme desenvolveremos adiante.

4.2.1.2. Desenvolvimento e consolidação de manuais de boas práticas de utilização de meios informáticos e de Cibersegurança do GRA

Atendendo ao número crescente de ciberataques de forma transversal em todos os setores, públicos ou privados, importa estabelecer políticas, medidas e mecanismos adequados para que as entidades se protejam e alcancem um patamar de preparação e maturidade

cibernética proporcional às ameaças. Neste domínio, deve ter-se em consideração, também, os normativos legais que dispõem sobre a matéria de Cibersegurança e a *compliance* com os mesmos, bem como, as diretrizes e recomendações de entidades com competência na matéria, como o CNCS.

Porem, e se, por um lado, a digitalização trouxe, também, novos riscos e potenciou o aumento dos ciberataques, por outro lado, existe uma maior conscientização da necessidade de implementar medidas e boas práticas que protejam as entidades no seu todo, incluindo informação, dados, sistemas e recursos e, por conseguinte, a continuidade do seu negócio.

Ainda, e atendendo às próprias interligações entre organizações públicas e privadas, as fragilidades de uma no domínio da Cibersegurança podem expor várias outras organizações a ciberameaças, devendo-se, pois, posicionar a Cibersegurança como vetor determinante da resiliência das sociedades e organizações como um todo.

A definição de boas práticas fundamentais em matéria de Cibersegurança constitui-se como a base de partida para uma estratégia robusta. De igual modo, uma boa governação de Cibersegurança é essencial para a segurança da informação e dos sistemas informáticos.

Naturalmente, entre as diversas entidades do setor público e privado existem diferentes níveis de maturidade em matéria de Cibersegurança. Assim, foi proposto o desenvolvimento e consolidação de quatro manuais de boas práticas no que concerne à utilização de meios informáticos e de Cibersegurança, adaptados, ainda que de forma transversal, às especificidades das entidades.

- Manual de governança, de exploração de Sistemas de Informação e de Cibersegurança da Administração Pública Regional;
- Manual do utilizador da Administração Pública Regional de meios informáticos e de Cibersegurança;
- Manual de boas práticas de Cibersegurança para PMEs;
- Manual de boas práticas de Cibersegurança para Freguesias e Municípios.

Os manuais destinados à APR visam, entre outros, a determinação de políticas e normas de utilização de meios informáticos e a definição de um modelo de governança que permita a gestão e capacidade de resposta adequadas no âmbito da Cibersegurança.

Enquanto os manuais a serem disponibilizados a entidades terceiras, designadamente PMEs e entidades do poder local, visam contribuir para o reforço da maturidade digital e de Cibersegurança destas entidades, potenciando o acréscimo da sua resiliência a incidentes e ameaças.

4.2.1.3. Plataforma Azores Cyber 360º - SOC

O Governo Regional dos Açores, através da DRCTD encontra-se a criar um centro de operações de Cibersegurança (SOC) que visa responder aos crescentes ataques informáticos.

O SOC deve ser um ponto de contacto único, disponível 24x7, para a monitorização (permanente) e reação a incidentes de segurança (em regime de ativação" on *call*").

Para a operacionalização mínima, a equipa do SOC, deverá ser composta por 14 elementos com conhecimentos de Cibersegurança (Um Coordenador do SOC, dois Analistas Forenses, três Gestores de Incidentes e oito Monitores de Incidentes), sendo expectável que o recrutamento de pessoal com as qualificações necessárias seja um processo moroso (3 a 4 anos), pelo que durante a fase inicial de operacionalização, deve ser garantido o funcionamento durante as horas normais de serviço, sem prejuízo de serem chamados perante um Incidente.

O SOC é o componente responsável pela monitorização constante e acompanhamento de incidentes em tempo real. Entre as tarefas mais comuns do SOC, encontram-se a reação rápida a incidentes, gestão de crises, coordenação com a equipa de IT do GRA, coordenação com autoridades e arquivo de *logs* relevantes para as equipas de análise forense procederem à recolha de informação.

Características de um SOC:

- *Security Response Team* responsável pelas ações de contenção de ataques, 24x7;
- Isolamento dos sistemas afetados e mitigação dos efeitos do ataque nos componentes da infraestrutura do GRA;
- Acompanhamento e coordenação de incidentes no GRA;
- Utilização de ferramentas de SIEM;
- Análise em tempo real dos *logs* dos vários sistemas sob vigilância do GRA: *network firewalls, web application firewalls, servidores web, routers*,

balanceadores de carga, servidores de cache, sondas de deteção de intrusões, servidores de e-mail, filtros de *antispam*, antivírus e ferramentas de análise de reputação.

4.2.1.4. A Criação de uma Cyber Academy

Com o desenvolvimento ubíquo das iniciativas e soluções que tornam a nossa vivência cada vez mais digital, importa estabelecer estratégias e mobilizar recursos capazes de dar resposta adequada às ameaças e aos riscos crescentes.

Este domínio de atuação caracteriza-se por uma elevada complexidade técnica e requer a alocação de recursos humanos altamente qualificados e escassos, que necessitam de estar sujeitos a ações de formação e atualização frequentes, pelo que importa apostar e promover a formação e o desenvolvimento de competências adequadas, inclusive através da requalificação profissional, com o intuito de reforçar a oferta profissional, altamente qualificada, na RAA. Deverão ser criadas sinergias no sentido de alavancar a dinamização, no âmbito da cooperação com o SOC do GRA – DRCTD, criando uma academia de formação em Cibersegurança, reforçando-se, assim, a dinâmica de atuação e estimulando-se a criação de uma cultura centrada no desenvolvimento e renovação contínua do conhecimento.

O modelo de operacionalização e funcionamento desta cyber academia deverá visar a promoção da formação, teórica e prática, da investigação e da inovação, fomentando e desenvolvendo o ecossistema regional, nacional e internacional na área da Cibersegurança e consolidando o *know-how* e as competências em contexto profissional, e, em última análise, contribuindo para o desenvolvimento de capacidades de Ciberdefesa e Cibersegurança na RAA.

Espera-se a sua dinamização, através da interligação com universidades e outros centros de formação e científicos/de investigação, bem como, com outras entidades do setor público e privado.

4.2.1.5. Realização de uma Campanha de Sensibilização à população açoriana, inserida no mês Europeu da Cibersegurança

Outubro é designado o mês Europeu da Cibersegurança, tratando-se de uma iniciativa anual de sensibilização, que tem lugar em toda a União Europeia, e que visa sensibilizar para as ameaças do ciberespaço e promover a Cibersegurança entre cidadãos e organizações e a partilha de boas práticas.

O GRA, através da DRCTD, realizou uma campanha de divulgação de conselhos e sugestões, aos cidadãos e organizações, para que possam melhorar a sua Ciberhigiene, adotando práticas essenciais de Cibersegurança, e ajudar na aquisição de competências e métodos para estarem mais seguros no mundo em linha. A campanha teve a sua divulgação através de um site de internet - *http://www.ativaatuaseguranca.azores.gov.pt/*, assim com, a publicação, nas redes sociais e nos órgãos de comunicação regionais, de spots sobre a temática da Cibersegurança.

4.2.1.6. Formalização da Equipa Multidisciplinar na PGRA

Deve ser formalizada a equipa multidisciplinar na Presidência do Governo Regional dos Açores para que possa acompanhar os assuntos relativos às questões da Cibersegurança (Participação do GRA em Exercícios de Cibersegurança, informar o Gabinete do Presidente sobre esta temática, apoiar a tomada de decisões relativas à Cibersegurança no ecossistema GRA, etc.).

Esta equipa deve ficar sob a coordenação do Assessor para a Comunicação Institucional, Modernização e Transição Digital, Ciência e Tecnologia, e deve ser constituída por:

- O Diretor Regional da DRCTD;
- O Diretor de Serviços da Direção de Serviços Técnicos e de Cibersegurança;
- 2 Elementos do CCEJ (com conhecimentos jurídicos e que acompanhe as questões jurídicas relacionadas com a Cibersegurança, o RJPD e o RJSC);
- O Técnico Especialista na Área de Gestão de Sistemas Informáticos do Gabinete do Presidente;
- O Assessor de Comunicação do PGRA e um elemento do Centro Multimeios;
- O Responsável pelo RJPD da Presidência do GRA;
- Outros elementos que sejam considerados importantes para esta temática.

Esta Equipa terá como principais atribuições, em apoio e coordenação com a DRCTD e outras entidades GRA na área da Cibersegurança:

- Organização e Planeamento da participação do GRA em Exercícios de Cibersegurança (Nacionais e Internacionais);
- Funcionar como interlocutor entre a PGRA, a DRCTD e todos os outros Departamentos do GRA;
- Apoiar a DRCTD na prossecução da sua Missão e atribuições, nomeadamente:
    - Criação e Organização de Exercícios de Cibersegurança Regionais;
    - Implementação de um Plano Anual sobre a Cibersegurança (Reuniões e Encontros Regionais, Seminários, Ações de Sensibilização, Objetivos a atingir, divulgação, Formação, etc.);
    - Apoio ao Gabinete da Presidência e a outros Departamentos em situações de incidentes de Cibersegurança no GRA (comunicação, procedimentos, contactos, etc.);
    - Elaboração de listas de contactos (Pontos de Contacto Permanentes em cada Secretaria Regional e Direção Regional, apoio jurídico em cada Direção Regional, responsáveis pelos diversos Serviços GRA, responsáveis do RGPD nos diversos Departamentos do GRA, etc.) a serem utilizadas em caso de incidentes de Cibersegurança;
    - Criar uma plataforma de Gestão de Incidentes de Cibersegurança do GRA;
    - Ajudar na Definição de uma estratégia para criar uma cultura de Cibersegurança no GRA;
    - Divulgação e fomentação do cumprimento dos Procedimentos em matéria de Cibersegurança;
    - Ajudar na criação de orientações e procedimentos que permitam, em situações de incidentes ou de vulnerabilidades, a DRCTD intervir nas diversas Secretarias Gerais e entidades do ecossistema GRA, em articulação com os meios de IT existentes no organismo para mitigar os incidentes;
    - Propor superiormente, relativamente aos riscos e ameaças de Cibersegurança a que o GRA está sujeito, a alteração dos níveis de prontidão no GRA;

- Elaborar uma proposta de Estratégia de Comunicação com o Exterior, em caso da ocorrência de incidentes no GRA, definindo quem, como e o que é dito;
- Outras questões relacionadas com a temática da Cibersegurança.

4.2.1.7. O RJSC e a sua implementação no GRA

É necessário "formar" as chefias das organizações GRA em vários aspetos ligados à Cibersegurança, em particular para a importância do RJSC e respetiva regulamentação.

O Ponto de Contato Permanente do GRA é a DRCT, que assegurará os fluxos de informação de nível operacional e técnico com o CNCS.

O Ponto de Contato do GRA com o CNCS apenas funciona de fora para dentro, devendo, preferencialmente, ser criada uma rede interna, com "SubPOC's" nas diversas entidades do GRA, por Direção Regional por exemplo, de modo a poderem funcionar como fonte de informação para o POC Permanente GRA na comunicação com o exterior (CNCS), em caso de incidente ou na necessidade de obtenção de mais dados (esta rede interna já se encontra a ser operacionalizada em muitas Direções Regionais mas deve ser alargada a todo o Ecossistema GRA).

Relativamente à necessidade de elaboração do Relatório Anual relativo à lista de ativos, assinado pelo Responsável de Segurança (Informática) do GRA (Eng.º Fernando Reis da DRCTD), foi verificado que o CNCS pretende que o GRA apenas entregue um relatório relativo a todas as entidades que o compõem, pelo que o ideal seria cada Direção Regional fazer o seu e submeter à DRCTD, que os compilará e submeterá apenas num único documento ao CNCS (pela informação obtida o mesmo já se encontra pronto e foi enviado para o CNCS).

Existe a necessidade de elaboração de um Plano de Segurança, devidamente documentado e fundamentado, com os procedimentos, medidas de mitigação e plano de resiliência relativamente à existência de um incidente no GRA, sendo da responsabilidade do Responsável de Segurança do GRA a sua manutenção e atualização (foi recolhida a informação que o mesmo se encontra em execução, pelo que se aguarda a sua divulgação/difusão pelos elementos da Presidência do GRA).

4.2.1.8. Formação e Sensibilização sobre Cibersegurança no GRA

Criar uma cultura de segurança no GRA significa equipar todos os colaboradores com os conhecimentos e ferramentas necessários para se tornarem participantes ativos nos diálogos contínuos de segurança dentro do GRA.

a) Verifica-se uma grande necessidade de formação na área da Cibersegurança para os colaboradores GRA que trabalham nesta área, devido à constante evolução e necessidade de atualização e obtenção de novas competências.
b) Realização de ações de Formação com entidades externas (PJ, CNCS, Universidades, etc.) sobre esta temática, fornecendo aos técnicos do GRA novas "ferramentas" e mais *Know-how*. Algumas destas formações deveriam ser vocacionadas para as chefias de topo, como forma de uma maior sensibilização para as questões da Cibersegurança e a sua importância.
c) Apoiar e fomentar a participação, dos profissionais de IT do GRA, em formação especializada em Cibersegurança fornecida pela C-Academy, através da Universidade dos Açores ou outra instituição do Ensino Superior.
d) Realização de Encontros Regionais dos profissionais de IT para partilha de experiências, conhecimentos e novas metodologias. Estes encontros serviriam também para afinar estratégias e procedimentos existentes no GRA.
e) Deveria ser introduzida, a obrigatoriedade de realização, de uma Formação Inicial de Sensibilização a todos os Colaboradores do GRA, relativamente às questões, cada dia mais prementes, relacionadas com a Cibersegurança. Poderia ser utilizada a disponibilização, de forma gratuita, pelo CNCS de Cursos MOOC, na plataforma NAU, que abordam vários temas, como as principais ameaças no ciberespaço, os cuidados a ter na utilização das tecnologias, o problema da desinformação ou o que fazer para consumir online de forma segura, entre outros. Exemplos de Cursos disponibilizados:
    - Cidadão Ciberseguro - é um curso de e-learning curto, simples e acessível ao cidadão/colaborador em geral, com o intuito de o dotar de conhecimentos que permitam proteger-se e adotar boas práticas de ciberhigiene em diferentes contextos diários, incluindo no local de trabalho.
    - Cidadão Ciberinformado - destina-se a qualquer cidadão que procure aprender a identificar notícias falsas e a verificar a veracidade da

informação consultada online, evitando a partilha de desinformação e contribuindo para um ciberespaço verdadeiramente democrático.

- Consumidor Ciberseguro - os formandos poderão obter conhecimentos que lhes permitam proteger-se e adotar boas práticas quando realizam compras online, evitando de modo mais eficaz a burla e o roubo de credenciais de cartões de crédito, por exemplo. Com este curso cada um poderá fazer compras online com mais segurança.
- Cidadão Cibersocial - é uma iniciativa do Centro Internet Segura, coordenado pelo CNCS. Trata-se de um curso interativo, que procura ser apelativo para todas as pessoas que queiram saber como utilizar as redes sociais de um modo mais seguro e protegendo a sua privacidade.
- RGPD para Cidadãos Atentos - O RGPD introduziu novos conceitos, procedimentos, direitos e obrigações relativos aos dados pessoais, que determinam alterações no funcionamento das organizações, nomeadamente da Administração Pública Portuguesa, com impacto direto na vida de todos os cidadãos.
- RGPD para Implementadores na Administração Pública - Este curso visa facilitar os processos de implementação do RGPD, promover o conhecimento generalizado das exigências deste processo, o reconhecimento do impacto e investimento que se espera de cada organização e a necessidade de investir na constituição e formação das equipas de implementação.

f) O GRA deveria promover parcerias/contatos com instituições do ensino superior, que possuam cursos e especializações no âmbito da Cibersegurança, fazendo um levantamento dos estudantes açorianos, para através da oferta de estágios, ações de divulgação, possibilitar aos alunos dessas instituições, oriundos ou não dos Açores, a possibilidade de virem trabalhar para os Açores, mitigando assim a falta de profissionais na Área da Cibersegurança/IT do GRA.

4.2.1.9. O papel da DRCTD

A DRCTD é o serviço executivo da Presidência do GRA que tem por missão concretizar a política regional nos domínios das comunicações, dos sistemas e tecnologia de

informação e da Cibersegurança, assim como nos domínios da transição digital e desenvolvimento e promoção da sociedade da informação.

A DRCTD exerce as suas competências no âmbito da coordenação e do desenvolvimento das ações conducentes à concretização da politica regional nos domínios das comunicações, dos sistemas e tecnologias de informação, das infraestruturas que os suportam e da Cibersegurança, por forma a assegurar um importante salto tecnológico, quer ao nível da resiliência e da redundância, quer das condições de eficiência, performance, segurança e gestão do licenciamento de *software*, dos utilizadores e das aplicações em exploração.

Na prossecução das suas competências e atribuições, a DRCTD procura pautar a sua atuação pelos princípios éticos com integridade, tendo sempre subjacente que prossegue uma atividade de interesse público. Enquanto serviço de interesse público geral, a prossecução desta missão exige que a mesma seja pautada pelo rigor e transparência, conferindo a todos os que nela trabalham ou que com ela se relacionam, uma responsabilidade acrescida no que respeita à sua conduta e ao seu desempenho.

A intervenção da DRCTD

Deve ser criada uma orientação de serviço (Orientação Interna do GRA ou Decreto Legislativo Regional), por parte da Presidência do GRA, que permita, em situações de incidentes ou de vulnerabilidades, a DRCTD intervir nas diversas Secretarias Gerais e entidades do ecossistema GRA, em articulação com os meios de IT existentes no organismo para mitigar os incidentes.

A Orientação deverá permitir uma facilitação da parte burocrática, evitando assim a perda de segundos que podem ser cruciais para a intervenção atempada, devendo a mesma, ser comunicada, via e-mail, para as chefias, dando-lhes conhecimento da mesma.

Definir, de forma simples, a possibilidade de efetuar contratação pública, de meios e serviços, sem ser pelos canais habituais, de forma quase instantânea e menos burocrática. Esta, deve ser comunicada e fundamentada superiormente, de modo que a mesma seja conhecida.

4.2.1.10. Procedimentos

A responsabilidade de notificação de um evento de segurança é pertença de quem o detetou em primeiro lugar. Deste modo, é importante que todos os colaboradores conheçam os procedimentos a adotar quando confrontados com um evento de segurança da informação, de preferência, seguindo um guião de procedimentos, conhecendo o ponto de contato para comunicarem esse evento. A equipa de resposta a incidentes deve ter alguém escalado para receber e analisar os eventos comunicados ou detetados, decidindo então qual a ação subsequente. O registo dos eventos, mesmo que não escalem para incidente, devem ser registados de acordo com um formulário previamente estabelecido de modo a manterem a informação recolhida consistente. No Fluxograma de Procedimento após deteção de Incidente de Segurança, na página 122, está representado o esquema proposto pela norma ISO 27035 para o fluxo de informação de um evento ou incidente de segurança da informação.

Este esquema foi o utilizado/proposto durante o Exercício CyP2022, sendo que pensamos que este deve servir de modelo para que os diferentes Departamentos do GRA, em colaboração com a DRCTD, possam definir os seus procedimentos em caso de Incidente de Cibersegurança.

4.2.1.11. Listas de Contactos

Devem ser criadas e disponibilizadas, por todos os serviços GRA, uma listagem de contactos dos responsáveis e pessoas de contacto de todas as plataformas e serviços, para serem utilizados em caso de um incidente de Cibersegurança. Estas listagens poderiam ser depois compiladas pela DRCTD, gerando uma única listagem GRA.

Seria um dos pontos a ser disponibilizado na plataforma de Gestão e Registo de incidentes de Cibersegurança no ecossistema GRA, pois facilitaria o contacto e a comunicação com os responsáveis.

Não existindo esta plataforma devia ser pensado um local para o acesso (simples e rápido) a estas listagens, num caso de incidente ou urgência.

4.2.1.12. Exercícios Regionais de Cibersegurança

Após a implementação de procedimentos e orientações técnicas, no GRA, dever-se-á implementar a realização, com periodicidade anual (inicialmente), de Exercícios Regionais de Cibersegurança, coordenados pela DRCTD, que permitam testar os meios da RAA, técnicos e operacionais, assim como os procedimentos, medidas de mitigação e a política de comunicação.

Os exercícios poderão ser realizados em simultâneo com o ExNCS e o CyP, testando o sector e o cenário do exercício, ou ser escolhida outra altura e testar sectores e cenários ajustados à realidade regional.

Estes exercícios permitiriam afinar os procedimentos existentes, complementados por encontros entre os profissionais de IT, potenciando o conhecimento das infraestruturas regionais, as infraestruturas críticas e elaborar planos de resiliência da região aquando da ocorrência de um incidente.

4.2.1.13. Serviços de aconselhamento

Deverá ser criado, preferencialmente na DRCTD, um serviço que permita ajudar as diversas entidades do GRA, antes de qualquer procedimento concursal ou de aquisição, dar o seu parecer sobre:

- Validação de Fornecedores – Listagem de fornecedores pré-acreditados para fornecimento de equipamento e *software* para o GRA, assim como a monitorização constante das práticas de segurança destes;
- Aquisição de equipamentos – listagem com equipamentos pré-aprovados, fornecedores e valores de referência;
- Software recomendado, com fornecedores e valores de referência;
- Reportório de aplicações e *software* – garantir a fiabilidade e veracidade das aplicações, assim como indicação das que podem ser instaladas na rede GRA e evitando o *download* das mesmas de fontes não fiáveis;
- Requisitos de segurança e de *compliance* dos sites a serem criados e implementados no ecossistema GRA.

4.3. Fase de Deteção e Análise

Nesta Fase pretende-se criar um Plano de Resposta a Incidentes do GRA, permitindo categorizar os incidentes, através da sua deteção e análise, fornecendo informação importante para que, na próxima fase seja possível a sua Contenção, Irradicação e Recuperação.

4.3.1.1. Comunicação de Incidentes de Cibersegurança no GRA

Deve ser criado/delineado um Plano de Resposta a Incidentes do GRA, que possa servir como modelo ou guia para as entidades do ecossistema GRA.

A comunicação, por parte de qualquer IT de uma entidade GRA, de um incidente ao CNCS, deverá ter simultaneamente a comunicação do incidente à DRCTD e ao POC da entidade e do GRA.

Deve ser criada uma *shared mailbox* da DRCTD, para a comunicação destes incidentes, possibilitando o acesso a estas comunicações com a maior brevidade pela equipa da DRCTD e assim acionar as medidas de mitigação do GRA e verificar se o mesmo, é localizado ou se se encontra replicado noutras entidades.

Se o incidente ou vulnerabilidade é identificado pela DRCTD, esta comunica aos IT's das entidades GRA, com o conhecimento dos seus superiores, sendo que os IT's devem proceder, de modo a implementar os procedimentos de mitigação indicados pela DRCTD.

4.3.1.2. Sala de Controlo de Operações do Projeto AzoresCloud

A implementação de uma Sala de Controlo de Operações do Projeto AzoresCloud com a qual se pretende a implementação de uma solução de monitorização para uma sala de controlo de operações.

O Projeto AzoresCloud visa promover a centralização das infraestruturas computacionais e de suporte de dados do Governo Regional dos Açores, balanceada em dois *'data centers'* gémeos, localizados em ilhas distintas (São Miguel e Terceira), cooperantes e que garantam a continuidade de funcionamento em caso de catástrofe, a autonomia das entidades na exploração das suas aplicações e uma maior competitividade a nível tecnológico, desempenho e segurança.

Com a implementação deste projeto será possível ao Governo dos Açores criar uma plataforma computacional de serviços da Administração Pública Regional, de forma a aumentar a eficiência na gestão e níveis de desempenho dos sistemas de armazenamento de dados, fomentando a utilização de serviços em rede na administração pública e melhorar a segurança desses sistemas.

4.3.1.3. Solução de anti-DDoS, WAF e CDN para o GRA

Procedeu-se à aquisição de uma solução *Cloud* de *anti-DDoS*, *WAF* e *CDN* para o Governo Regional dos Açores.

A solução cumpre as seguintes especificações técnicas:

- Solução de *Content Delivery Network* (CDN) que permita a configuração de 3 domínios (mínimo), incluir 500 milhões de pedidos HTTP/s por mês (mínimo) e, no mínimo, 10 TB de tráfego mês;
- Solução de *Domain Name System* (DNS) que deve ser do tipo *Anycast*, permitindo configurar/implementar DNSSEC, incluir, no mínimo, 300 milhões de pedidos por mês e permitir a configuração, no mínimo de 3 zonas diretas e 12 zonas inversas.

4.4. Contenção, Irradicação e Recuperação

Esta Fase encontra-se ligada à anterior, sendo que se pretende a criação de uma CSIRT no GRA que permita ter uma capacidade de resposta aos Incidentes de Cibersegurança identificados na Fase de Deteção e Análise. Nesta Fase seria importante a criação, a médio prazo, de uma CSIRT do GRA, que permitiria a realização das ações de contenção ou mesmo de irradicação dos Incidentes detetados e analisados na Fase anterior, pela Equipa do SOC.

4.4.1.1. Criação de uma CSIRT do GRA

Deve ser delineada a criação de uma CSIRT no GRA, permitindo assim ter uma maior capacidade de resposta a Incidentes de Cibersegurança. A criação desta equipa iria necessitar de algum investimento em meios humanos, com conhecimentos de Cibersegurança e Análise Técnica e Forense de Incidentes. Esta equipa, após a deteção e

monitorização dos Incidentes de Segurança, identificados pelo SOC GRA, irá responder de forma célere com medidas de contenção, irradicação e recuperação, minimizando os danos provocados pelo Incidente.

Esta equipa seria responsável por realizar:

- A triagem de notificações de incidentes no GRA, a sua análise técnica e forense;
- A articulação do GRA com as entidades nacionais e internacionais envolvidas;
- A produção de recomendações de mitigação e/ou de resolução do incidente;
- A coordenação da resposta a incidentes pode partir da iniciativa do CNCS, por exemplo numa situação de incidente de larga escala, ou ser-lhe solicitada pelos canais designados para o efeito. Em caso de necessidade ou de força maior, o CNCS coordena as suas ações com as restantes autoridades nacionais.

Permitiria ainda que, fossem prestados estes "serviços" a outras entidades da RAA, fomentando uma maior política de Cibersegurança nas entidades e empresas da RAA.

A CSIRT do GRA deve utilizar uma taxonomia comum e mecanismos automáticos para partilha de informação operacional, devendo ser usada a taxonomia aprovada em 2012 e revista, pela última vez, em 2019 pela RN CSIRT. Esta taxonomia também tem sido utilizada como diretriz a nível internacional, o *European Cybercrime Centre* (EC3) de onde é parte integrante a Polícia Judiciária.

4.4.1.2. Plataforma de Gestão de Incidentes de Cibersegurança

O GRA deve equacionar a criação de uma Plataforma Web que possibilite a Gestão e Registo de Incidentes de Cibersegurança no ecossistema GRA.

Esta Plataforma iria possibilitar a parametrização do fluxo correto da comunicação/informação relativa a um incidente de Cibersegurança (o que acorreu, onde, a quem comunicar, que dados/elementos fornecer, etc.), possibilitando um correto fluir da informação e uma maior gestão destes incidentes, possibilitando saber o ponto de situação em qualquer momento (onde está, o que se está a fazer, ações necessárias, etc.), possibilitando ainda aos *Points Of Contact's* (POC's) uma melhor noção de quem comunicou e acedendo com maior facilidade aos dados a fornecer na comunicação com o POC GRA (DRCTD) ou com o CNCS.

A parametrização permitiria controlar o correto fluxo da informação sobre os incidentes, e identificar possíveis constrangimentos e procedimentos a melhorar.

De referir que, durante a participação nos Exercícios de Cibersegurança foi possível observar que já existem outras entidades que desenvolveram uma plataforma deste tipo (ex. Região Autónoma da Madeira, Município de Oeiras, etc.).

4.4.1.3. Níveis de prontidão no GRA

Devem ser criados e implementados quatro níveis de prontidão, relativamente aos riscos e ameaças de Cibersegurança a que o GRA está sujeito, devendo ser analisado diariamente e comunicado aos meios de IT do GRA, pela DRCTD (seja através de e-mail, plataforma interna ou intranet).

Exemplo de uma política de categorização dos níveis de prontidão ou de risco e ameaça no GRA:

I. **Alpha –** Nível inicial – indica o nível de prontidão diário – Baixo nível de risco e ameaça;
II. **Beta –** Nível de Prontidão Inicial – Equipas de Prevenção - Identificados incidentes e vulnerabilidades no exterior, com reportes de ciberataques e aumento do nível de risco e de ameaça sobre as infraestruturas do GRA;
III. **Charlie –** Nível de Prontidão imediato – Equipas em Intervenção - Identificados incidentes e ameaças na infraestrutura GRA, empenhamento de meios de análise e apoio;
IV. **Delta** – Nível mais alto – *lockdown* das infraestruturas GRA e empenhamento de todos os meios do GRA para mitigação e resiliência.

4.4.1.4. Comunicação com o Exterior em Incidentes de Cibersegurança

Deve ser elaborada uma Estratégia de Comunicação com o Exterior, em caso de ocorrência de incidentes no GRA, definindo quem, como e o que é dito.

Deve ser melhorado o plano de comunicação e proceder-se à elaboração de um plano de circulação de informação interna na PGR, prevendo todos os casos possíveis.

Quando ocorre um incidente, e após informação deste, deverá ser ativada uma equipa (Responsável pela Comunicação do GRA, responsável pela equipa Técnica e Jurista

Especializado) que acompanha a situação e que de forma centralizada coordena a comunicação e o que é divulgado para os OCS. Servirá de apoio aos Órgãos de Comunicação da entidade alvo do incidente, se existirem, na elaboração e planeamento da Informação divulgada, evitando assim uma comunicação desorganizada e que "colida" com o que se pretende comunicar para o exterior (comunicações contraditórias entre diferentes órgãos).

4.4.1.5. Gabinete Jurídico de Apoio à Cibersegurança

Considerou-se essencial a existência de uma ou duas pessoas, no Centro de Consulta e Estudos Jurídicos do Governo Regional, com especialização na área da Informática/Cibersegurança, de modo a poderem dar um apoio jurídico aquando de um incidente, isto é, dar respostas sobre como e se é possível fazer certas ações, salvaguardando sempre o cumprimento das leis e a atuação dos profissionais.

Serviria também de suporte e apoio aos diversos serviços jurídicos dos Departamentos, em caso de necessidade de clarificação e padronização de procedimentos jurídicos, assim como ajuda clarificar algumas das inúmeras questões que se levantam durante um Incidente de Cibersegurança.

Estas pessoas estarão sempre disponíveis e em ligação/contato com os responsáveis pelas intervenções relacionadas com Cibersegurança em todas as entidades do GRA.

4.5. Atividade Pós-Incidente

Nesta Fase pretende-se que seja realizado uma análise ao Incidente ocorrido, registando as lições aprendidas, assim como a identificação das oportunidades de melhoria das políticas, dos controlos e dos procedimentos. Esta análise permitirá a elaboração de relatório que irá contribuir para uma nova análise de risco, para avaliar o desempenho da equipa de resposta a incidentes e auditar a capacidade de resposta a incidentes do GRA.

4.6. Taxonomia Comum da Rede Nacional de CSIRT

Para possibilitar uma melhor forma de comunicação entre os CSIRTs (Nacionais e Internacionais) foi adotada uma Taxonomia de Classificação de Incidentes de Cibersegurança (encontra-se na sua versão 3 e teve em consideração a Taxonomia de referência do *Working Group* – RSIT WG), que se entendeu, dever ser, comum a todos, facilitando assim, a comunicação e a troca de informações e ajuda entre os diversos atores.

A classificação de incidentes deverá ser feita de acordo com 2 vetores – "Tipo de Incidente" e "Tipo de Evento". No modelo de classificação de incidentes adotado foi ainda decidida uma divisão dos vários Tipos específicos de incidentes por Classes genéricas que agrupam conjuntos de incidentes com resultados ou objetivos semelhantes. Para além das Classes e Tipos de incidentes, foi ainda identificado um conjunto de eventos associados a cada Tipo de incidente.

Tendo em conta que, poderá ser necessário aplicar mecanismos de classificação automática de incidentes, sugere-se como referência o seguinte modelo relacional entre "Tipo de Evento" e "Tipo de Incidente". Importa, no entanto, salvaguardar que esta associação não é estrita, podendo um determinado Tipo de Evento estar associado a qualquer Tipo de Incidente.

Na RAA deve, também, ser adotada esta mesma Taxonomia Comum para a Classificação de Incidentes de Segurança Informática, que se apresenta na tabela nos anexos (pág. 120). (RNCSIRT, 2020)

4.7. Comportamento Individual e Organizacional perante as principais Ciberameaças

Este ponto pode ser englobado na Fase de Preparação, no entanto, entendo que o mesmo deve ser explanado de forma individual, visto ser de extrema importância, como ponto de partida para a capacitação da componente humana do GRA. Deste modo o GRA deve:

- Formar os profissionais com responsabilidades a nível técnico para a necessidade de ativarem a conservação de registos (*logs*) de serviços na Internet para análise após a eventual ocorrência de incidentes, por um período mínimo de 6 meses, preferencialmente um ano;

- Formar as chefias em vários aspetos ligados à Cibersegurança, em particular para a importância do Regime Jurídico da Segurança do Ciberespaço e respetiva regulamentação;
- Promover junto dos indivíduos em geral a denúncia de incidentes e cibercrimes por forma a melhor monitorizar estas atividades e contribuir para a realização de investigações.

Tabela 8 - Recomendação de comportamento, individual e organizacional, perante as principais Ciberameaças

Ciberameaças principais	**RECOMENDAÇÕES POR CIBERAMEAÇA**	
	Comportamento Individual	**Comportamento Organizacional/GRA**
Phishing / *Smishing*	Não clicar em *links* ou anexos de e-mails ou SMS suspeitos, verificar a origem dos e-mails, não partilhar dados sensíveis solicitados por e-mail, confirmar noutras fontes os pedidos de transferências bancárias	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores, realizar simulações de *phishing* e aplicar as melhores práticas e standards de segurança ao nível da configuração do e-mail organizacional, no âmbito de políticas de segurança definidas
Ransomware	Aplicar as recomendações relativas ao *phishing*, salvaguardar cópias de segurança em localização secundária e desconectada da rede, manter o antivírus atualizado, evitar navegar em websites sem garantias de segurança, não utilizar dispositivos USB de origem desconhecida	Formar os colaboradores relativamente às recomendações relativas ao *phishing* e e-mail, salvaguardar cópias de segurança em localização secundária e desconectada da rede, manter o antivírus atualizado, evitar navegar em *websites* sem garantias de segurança, não utilizar dispositivos USB de origem desconhecida, ações monitorizadas por políticas de segurança definidas
Malware	Manter o antivírus atualizado, não clicar em *links* ou anexos suspeitos, evitar navegar em *websites* sem garantias de segurança, não utilizar dispositivos USB de origem desconhecida	Garantir que os dispositivos da organização possuem antivírus atualizados através de políticas de segurança definidas, sensibilizar os colaboradores em relação à navegação insegura, *phishing* e dispositivos USB de origem desconhecida
Fraude/Burla online	Desconfiar de ofertas demasiado boas para serem verdade, não partilhar dados sensíveis em plataformas não reconhecidas, não transferir dinheiro sem verificar noutras fontes o destino e essa necessidade, desconfiar de solicitações por parte de terceiros de alterações das configurações de aplicações como a *MBway*, utilizar carteiras virtuais ou cartões temporários nos pagamentos online, verificar a veracidade dos *websites* de vendas e privilegiar aqueles que utilizam HTTPS	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores, garantir que os colaboradores confirmam o destino e a necessidade das transferências bancárias solicitadas, utilizar carteiras virtuais ou cartões temporários nos pagamentos online a fornecedores, verificar a veracidade dos *websites* de fornecedores e privilegiar aqueles que utilizam HTTPS
Comprometimento de contas ou tentativa	Utilizar palavras-passe fortes e alterá-las sempre que se suspeite de comprometimento, aplicar as recomendações relativas ao *phishing*, aplicar o múltiplo fator de autenticação	Aplicar de forma contínua as políticas de segurança definidas quanto às palavras-passe em particular, promovendo o cumprimento de requisitos mínimos de dimensão e complexidade, monitorizar e bloquear ataques

		de força-bruta, registar os eventos, aplicar o múltiplo fator de autenticação
Vulnerabilidades e sua exploração	Manter os sistemas e as aplicações atualizadas com as últimas atualizações de segurança	Manter os sistemas e as aplicações atualizadas com as últimas atualizações de segurança de forma regular, ação monitorizada por políticas de segurança definidas
Sextortion	Não pagar pedidos de resgate que ameaçam a publicação de imagens comprometedoras, não partilhar imagens de teor sexual online	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores
Desinformação digital	Não partilhar notícias falsas online, confirmar a veracidade das notícias através de outras fontes, apenas partilhar notícias de fontes reconhecidas, verificar a atualidade das notícias partilhadas	Desenvolver ações de sensibilização contra a desinformação digital junto dos colaboradores

4.8. O RGPD no GRA

O XIII Governo Regional dos Açores já iniciou a implementação de medidas que visam eliminar práticas e riscos associados a esta problemática, estando a decorrer a implementação do Sistema Integrado de Gestão da Proteção de Dados do Governo Regional dos Açores (SIGPD-GRA).

A APR dos Açores e os seus colaboradores, sem exceção, devem continuar a abraçar e a serem consciencializados da importância da proteção dos dados pessoais.

- Verifica-se que o processo de implementação do RGPD no GRA se encontra estagnado.
- Deveria existir um EPD por cada Secretaria Regional, que não é obrigatório, mas é recomendado em todas as organizações que tratem dados pessoais ou sensíveis, em conformidade com a legislação nacional, previsto nos Artigos 37º, 38º e 39º do RGPD, ficando sujeito ao dever e sigilo ou confidencialidade bem como ao dever de incompatibilidade, não podendo exercer quaisquer funções e atribuições que resultem de um conflito de interesses para o exercício das funções.

  A designação do EPD deve ser realizada em função das competências profissionais em especial dos conhecimentos avançados de proteção de dados e que seja capaz de cumprir as tarefas atribuídas no Artigo 39º, relacionadas com a segurança e proteção de dados, por exemplo deve ter as seguintes funções:

  i. Sensibilização e informar todos os que tratem dados pessoais;

ii. Assegurar o comprimento das políticas de privacidade e proteção de dados;
iii. Controlar e regular a conformidade do RGPD;
iv. Recolher informação para identificar atividades de tratamento;
v. Controlar e acompanhar a produção da AIPD – Avaliação de Impacto sobre Proteção de Dados;
vi. Promover as abordagens de Privacidade por Desenho e por Padrão;
vii. Realizar a avaliação na exposição aos riscos de violações de privacidade e mitigados com ações de melhoramento;
viii. Recolher informação para identificar atividades de tratamento;
ix. Manter atualizado os registos das atividades de tratamento de dados;
x. Controlar o cumprimento de contratos escritos subcontratante;
xi. Promover formações de boas práticas para a proteção de dados;
xii. Ser o ponto de contacto com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados;
xiii. Ser o ponto de contacto com as autoridades de controlo;

Percebe-se que idealmente deveria ser alguém capaz de conciliar conhecimentos de, pelo menos, as seguintes áreas: tecnológica, gestão e legal.

O EPD assume, assim, a responsabilidade na aplicação da estratégia para proteção dos dados e conformidade do RGPD. Todo o descuido em eventuais não conformidades e incidentes ou violações serão imputadas ao responsável pelo tratamento, em última instância à administração.

O EPD não decide, não ordena. O EPD aconselha, recomenda. O EPD dá o seu parecer, pronuncia-se, verifica, alerta, audita, sensibiliza.

- Neste momento verifica-se a falta de capacidade, no GRA, de executar auditoria de dados, isto é, quem acedeu ao que, se tinha necessidade de aceder e para que fins foram acedidos os dados.

Para a implementação do RGPD na sua plenitude, propomos um plano de ação com 5 fases, onde indicamos também as condições a serem verificadas em cada fase, de uma forma muito simplificada:

- 1ª Fase - Designar um Encarregado de proteção de Dados;
    - Nomear um EPD com as funções de apoiar a implementação e a conformidade com o RGPD;

  - Publicar os seus contactos no site institucional;
  - Comunicar a designação e os contactos do EPD à CNPD;
  - Assegurar as condições necessárias para o EPD poder desenvolver de forma independente e eficaz as tarefas que lhe incumbem.
- 2ª Fase - Mapear os dados pessoais objeto de tratamento;
  - Identificar todos os serviços e entidades que processam dados pessoais;
  - Identificar os tipos de dados pessoais objeto de tratamento, incluindo os dados sensíveis (quando seja o caso);
  - Estabelecer a listagem dos principais processos de tratamento e da(s) finalidade(s) a que se destinam;
  - Identificar eventuais fluxos de dados, indicando a sua origem e o destino;
  - Identificar todos os locais onde os dados pessoais se encontram arquivados;
  - Estabelecer por quanto tempo esses mesmos dados devem ser mantidos.
- 3ª Fase - Priorizar as Ações a desenvolver;
  - Identificar o(s) fundamento(s) de licitude que legitimam cada operação de tratamento;
  - Verificar a conformidade das declarações de consentimento pré-existentes com o RGPD;
  - Verificar que nenhum dado é tratado de forma incompatível com a finalidade para que foi recolhido;
  - Verificar que a recolha e tratamento de dados se limita ao estritamente necessário;
  - Verificar a conformidade dos contratos de tratamento de dados pré-existentes com o RGPD.
- 4ª Fase - Organizar os Processos Internos;
  - Verificar que os princípios de tratamento de dados pessoais são tidos em conta na conceção de todas as ferramentas, procedimentos e sistemas de recolha, tratamento e conservação dos dados;
  - Verificar que os principais riscos de segurança foram identificados e devidamente acautelados;
  - Verificar que foram elaborados planos de contingência que permitem saber o que fazer e quem contatar em caso de incidente de segurança;

  - Verificar que a informação sobre o tratamento de dados é disponibilizada de forma clara e concisa;
  - Verificar que estão instaladas plataformas/canais de comunicação que permitem aos titulares dos dados exercer os seus direitos;
  - Verificar que foi elaborado um plano de formação e sensibilização dos colaboradores.
- 5ª Fase - Documentar a conformidade com o RGPD;
  - Garantir que a entidade documenta de forma sistemática as atividades de tratamento desenvolvidas;
  - Garantir que as informações incluídas no registo permitem demonstrar o cumprimento das obrigações estabelecidas no RGPD;
  - Garantir que o registo é regularmente atualizado;
  - Garantir que a segurança e integridade do registo está assegurada.

Relativamente a um Incidente de Cibersegurança com violação de dados pessoais, foi elaborado um Fluxograma (Fluxograma do Procedimento de Violação de Dados Pessoais – página 123) para ajudar no procedimento de intervenção e comunicação do Incidente, assim como a explicação, resumida, das etapas e o que fazer durante o mesmo incidente (Etapas após deteção de Incidente de Segurança com Violação de Dados Pessoais – página 124) que consideramos que podem servir como ponto de partida para a divulgação e implementação nos diversos Departamentos do GRA.

Capítulo 5 Análise e Discussão de Resultados

Este Capítulo pretende descrever a participação do GRA nos Exercícios de Cibersegurança (ExNCS2022 e CyP2022), exercícios nos quais foi testada a proposta de resposta a Incidentes de Segurança e após os quais foi realizada uma análise e avaliação à participação do GRA.

5.1. Metodologia Utilizada

A participação nos dois Exercícios de Cibersegurança foi essencial para o desenvolvimento deste trabalho, tendo sido possível, deste modo testar, em contexto simulado e controlado, as propostas por mim apresentadas, assim como a articulação entre as diversas equipas do GRA.

No Primeiro Exercício, o ExNCS2022, as equipas GRA foram confrontadas com Injeções gerais e direcionados para o setor da Saúde, mas que serviu para testar, quer o plano de resposta a incidentes, quer as capacidades técnicas e operacionais, das equipas GRA.

No Segundo Exercício, o CyP2022, as equipas GRA foram confrontadas com Injeções direcionados e planeados para a realidade regional, bem como, serviu para testar procedimentos e capacidade de resposta a Incidentes, assim como, a tomada de Decisão num Incidente de Segurança no GRA.

5.2. O ExNCS2022

O ExNCS é promovido pelo Centro Nacional de Cibersegurança (CNCS) e pretende promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da Cibersegurança e desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de Cibersegurança e Ciberataques.

O ExNCS2022 foi orientado para o Sector da Saúde, assim como para potenciais impactos noutros sectores da economia.

O ExCNC2022 esteve englobado no *Cyber Europe* 2022 que decorreu em simultâneo.

O *Cyber Europe* é um exercício bi-anual, lançado em 2010, coordenado pela ENISA – *European Union Agency For Cybersecurity*, que está na sua sexta edição, e que simula cenários de incidente em tempo real e serve para avaliar o grau de preparação e de cooperação dos Estados-Membros relativamente à segurança das redes e dos sistemas de informação.

O *Cyber Europe* 2022 também foi orientado para o sector da Saúde e, tal como o ExCNS2022 engloba entidades do sector público e do sector privado.

No *Cyber Europe* 2022 participam os membros da União Europeia e os membros da EFTA – *European Free Trade Association* (Islândia, Liechtenstein, Noruega e Suíça).

5.3. A participação do GRA no Exercício ExNCS2022

O Planeamento da Participação do GRA no ExNCS2022 iniciou-se a 22 de março de 2022, com o convite realizado, pelo CNCS, para participar na Reunião Inicial de Planeamento do ExNCS2022 que decorreu a 06 de abril de 2022.

Foram realizadas diversas reuniões com o CNCS, assim como, entre os elementos participantes do GRA, de forma a preparar a participação do GRA no ExNCS2022.

O GRA participou no ExNCS2022 com os seguintes elementos:

- Presencialmente na sala de situação existente no Centro de Congressos do Estoril:
    - POC e *Planner*;
- De forma remota:

- Equipas de IT dos 3 Hospitais da RAA (HDES, HSEIT e HH);
- Conselhos de Administração dos 3 Hospitais da RAA (HDES, HSEIT e HH);
- Apoio Jurídico de um elemento do CCEJ do GR;
- Equipas de IT da DRS e da DRCTD;
- Assessor de Imprensa da Presidência do GRA;
- Equipas de Imprensa dos 3 Hospitais da RAA (HDES, HSEIT e HH).

Durante o ExNCS2022, os participantes foram confrontados com as seguintes Injeções a que foi necessário dar resposta:

- *2022 Olympics anti-doping hack;*
- *Data exposure blackmail;*
- *VIP data leak;*
- *Robocall DoS;*
- *Drug & medical supplies shortage;*
- *Implantable device vulnerability;*
- *Data exfiltration campaign.*

De realçar que foi solicitado, pelo CNCS, a apresentação do GRA e da forma como este se articulou para participar neste Exercício aos observadores do Instituto Nacional de Tecnologias de Informação e Comunicação de Moçambique. Foi solicitada esta apresentação ao GRA, pois participou como um todo e era a Entidade, em sala, mais próxima da realidade de presença de um País neste exercício.

Foi ainda feita a simulação, em sala, de uma reunião do Gabinete Coordenador de Segurança, visto ter sido declarado o Estado de Segurança Bravo no País, assim como posteriormente o Estado de Segurança Charlie.

Na simulação, da reunião, participaram as seguintes entidades:

- Ministério dos Negócios Estrangeiros – em representação do Governo da República;
- Sistema de Segurança Interna;
- Sistema de Informações da República Portuguesa;
- Governo Regional dos Açores e da Madeira – os POC's em representação dos seus Presidentes;

- Polícia Judiciária;
- Serviço de Informações de Segurança;
- Centro Nacional de Cibersegurança;
- Infraestruturas de Portugal;
- INEM;
- SPMS.

Por último, referir que o Inspetor Paulo Abalada da Polícia Judiciária, deu os parabéns, aos elementos presentes na sala de situação, pelos relatórios e comunicações recebidas pela PJ das entidades do GRA, pois eram claras, diretas e com a informação necessária para estes conseguirem compreender e dar resposta ao incidente reportado.

5.4. Análise da participação do GRA no ExNCS2022

No seguimento da participação do GRA no ExNCS2022, foi realizado um balanço relativo à participação no exercício e através deste fazer uma reflexão sobre o ponto de situação, na resposta a incidentes de segurança, por parte do GRA.

Assim, os elementos que participaram no ExNCS2022, quer presencialmente, quer remotamente, realizaram no dia 17JUN2022 uma reunião de *Debriefing*, com o intuito de fazer um balanço e recolher as impressões sobre a participação do GRA neste exercício.

Sendo o ExNCS2022 um exercício que testou o plano de resposta a incidentes, quer as capacidades técnicas quer as operativas, uma das primeiras lacunas identificadas foi a ausência de um Plano de Segurança e de um Plano de Resposta a Incidentes transversal ao GRA, assim como, a "gestão" da Comunicação com o exterior. Identificou-se ainda a necessidade de identificação dos ativos críticos no GRA/RAA.

Da parte do CNCS e da ENISA faltou o envio de mais informação de forma a poder fazer um melhor enquadramento do ecossistema em que o exercício iria decorrer, assim como alguma desadequação do exercício à realidade e ao contexto regional.

Foi ainda verificada uma grande cadência de Injeções, em curtos espaços de tempo, o que impossibilitou, da parte das equipas regionais de IT, resposta em tempo real aos mesmos e capacidade de acompanhamento das solicitações. De salientar que a equipa nacional de

CSIRT do CNCS também não conseguiu dar resposta, em tempo real, às inúmeras solicitações de que foi alvo.

Foram ainda verificados alguns problemas com a plataforma de envio de e-mails e de inserção de Injeções durante o exercício, o que originou que alguns destes e-mails e Injeções tivessem sido comunicados e recebidos fora do horário e mesmo no final do exercício.

A plataforma *Cyber Exercise Platform*, da ENISA, foi pouco utilizada durante o exercício, sendo apenas utilizada como uma simulação de redes sociais e de partilha de informação dos Órgãos de Comunicação Social. Poderia ter sido pensada uma maior interação e utilização desta.

Como já tinha sido vinculado anteriormente nas reuniões de preparação, o exercício serviu para confirmar que a região não possui, neste momento, capacidade de análise de artefactos, de análise e recolha forense, na dimensão exigida neste tipo de cenários, pelo que é sempre necessário solicitar a intervenção de equipas e especialistas externos em caso de incidentes.

Foi ainda decidido, elaborar um documento, Relatório sobre a participação do GRA no ExNCS2022, que possa apresentar não só um balanço da participação no exercício, mas também algumas ideias para o futuro que todos pensam serem relevantes para a melhoria da cultura de Cibersegurança dentro do ecossistema GRA, e para o qual todos contribuíram. O Referido Relatório foi concluído e enviado para a Presidência do GRA no dia 01 de agosto de 2022.

5.5. O CIBER PERSEU 2022

O GRA participou no Exercício CIBER PERSEU 2022, que decorreu entre os dias 14 e 18 de novembro de 2022.

Esta participação serviu para testar, de forma controlada, alguns procedimentos e tomadas de decisão numa situação de ciberataque ao Ecossistema GRA.

5.6. Visão Geral

O exercício CIBER PERSEU é um exercício promovido pelo Exército, incluído no Plano Integrado de Formação Operacional 2022 (PITOP22), programado pelo Chefe do Estado-Maior do Exército e realizado pelo Comandante da Força Terrestre, focado na capacidade de testar e avaliar a resposta do Exército às ameaças cibernéticas e na resolução de incidentes ciberespaço.

5.7. Objetivos do Exercício CyP22

- EO1 – Exercitar o processo de tomada de decisão para garantir um Exército coordenado na resposta a um ataque cibernético.
- EO2 – Exercitar a defesa cibernética em nível tático, a fim de contribuir para a superioridade das informações e garantir a continuidade das operações.
- EO3 - Validar as Técnicas, Táticas e Procedimentos do Exército na área de Defesa Cibernética.
- EO4 - Promover a partilha de conhecimentos técnicos com forças militares estrangeiras e outros "militares e civis" nacionais no domínio do ciberespaço.

5.8. Princípios do Exercício CyP22

O Exercício procura a Segurança do Ciberespaço; a Integração; e a Autoavaliação (não externa) das Entidades participantes, contribuindo para uma relação de confiança entre as mesmas e para a construção de sinergias entre estas. De referir que, todas as Organizações, Instituições e Entidades participam de uma forma voluntária no Exercício.

O Exercício CyP2022 teve como princípios:

- O foco principal do CIBER PERSEU é a colaboração;
- O CIBER PERSEU considera diferentes enredos e desafios técnicos para alcançar a coordenação e colaboração entre todas as entidades participantes;
- O CIBER PERSEU segue o princípio "treine enquanto luta", utilizando canais normais de comunicação, bem como um banco de testes para novos/inovadores procedimentos de interação;
- O CIBER PERSEU é considerado um ambiente NÃO CLASSIFICADO, portanto, a partilha de informações deve ser feita de acordo com este Princípio;

- Todos os participantes do CIBER PERSEU foram convidados a contribuir com o cenário para que ele corresponda aos seus objetivos e expectativas de treino.

5.9. Missões do Cyp22

- MS01 - Ciberataque à infraestrutura de CSI do Exército – Missão Militar e de Teor Processual/Procedimentos;
- MS02 - Ciberataques a uma rede de missão da componente terrestre (meios táticos) – Missão Militar e de Teor Tático;
- MS03 - Resposta, análise e investigação de ciber-incidentes (plataforma *cyber range*) – Missão aberta a todos os participantes e de Teor Técnico;
- MS04 - Ciberataque ao sector público e privado - Missão aberta a todos os participantes e de Teor Processual/Procedimentos;
- MS05 - Competição *Capture The Flag* – Missão aberta a equipas de 5 elementos, sendo uma competição para testar a componente Técnica.

5.10. Ameaças Possíveis no Cenário

- Usar a engenharia social para atingir indivíduos vulneráveis ou de alto perfil com e-mails de *Spearphishing* cuidadosamente elaborados;
- Usar "*poison the well*" para comprometer sites estratégicos, usando-os para servir software malicioso aos seus visitantes – e "*snaring*" as suas vítimas ao fazê-lo;
- Também pode "suavizar" o seu alvo por meio de engenharia social adicional, como a criação de perfis falsos em redes sociais, ou comprometendo primeiro a cadeia de suprimentos da organização alvo;
- Pode realizar ataques complexos contra *hardware* específico;
- Pode envolver ações contra Governos específicos;
- Pode ser encarregue de rastrear, interromper e perseguir dissidentes ou ativistas;
- Outros grupos de atores do Estado-Nação especializados em propaganda e desinformação no ciberespaço, que formam exércitos de *Trols* que contra-atacam contra fontes de mídia desfavoráveis, controladas ou tendenciosas para tentar elevar a reputação de seu empregador.

5.11. A participação GRA no Exercício CyP2022

O GRA participou neste exercício em duas vertentes:

- uma equipa da DRCTD participou na Missão MS03 - Resposta, análise e investigação de ciber-incidentes (plataforma *cyber range*) – Missão aberta a todos os participantes e de Teor Técnico, que irá possibilitar aos intervenientes ganhar mais conhecimentos e capacidades técnicas na análise de artefactos e de análise e recolha forense em incidentes de Cibersegurança;
- uma equipa, composta por diversos elementos de várias entidades GRA, participou na Missão MS04 - Ciberataque ao sector público e privado - Missão aberta a todos os participantes e de Teor Processual/Procedimentos, servindo esta para testar, de forma controlada, alguns procedimentos e tomadas de decisão numa situação de ciberataque ao Ecossistema GRA.

Esta participação teve como objetivos principais:

- Construir Sinergias, partilha de conhecimento e experiências com as outras Entidades e Organizações participantes;
- Criar uma rede de contactos, na Área da Cibersegurança, ao mais alto nível;
- Testar a capacidade de resposta do GRA a um Incidente de Cibersegurança, nomeadamente procedimentos e tomadas de decisão;
- Interação e cooperação entre diversos elementos de entidades GRA.

O GRA participou no CyP2022 com os seguintes elementos:

- Presencialmente na sala de situação existente na Academia Militar – Destacamento da Amadora:
    - POC e *Planner* GRA;
- De forma remota:
    - *Planner* GSRFPAP-GRA;
    - Assessores do Presidente (Comunicação Institucional, Modernização e Transição Digital, Ciência e Tecnologia e de Imprensa)
    - Elementos da DROPEP:
        - Diretor Regional da Organização, Planeamento e Emprego Público;
        - Diretor de Serviços da Organização, Planeamento e Emprego Público;

- Chefe de Divisão de Gestão de Recursos Humanos e Planeamento Organizacional;
- Encarregado de Proteção de Dados da SRFPAP;
- Ponto Focal da DROPEP;
- Ponto de Contato da Secretaria Regional das Finanças e Administração Pública;
- Jurista DROPEP – RGPD.

- Elementos da DRCTD:
  - Diretor Regional das Comunicações e da Transição Digital;
  - Diretor de Serviços Técnicos e de Cibersegurança;
  - Elementos da Equipa de IT;
- Apoio Jurídico de um elemento do CCEJ do GR;
- Encarregada de Proteção de Dados da PGRA;
- Elemento do Centro Multimeios do Governo Regional.

5.12. O Cenário Do Exercício CyP2022

5.12.1.1. Cenário Geopolítico

O Cenário Geopolítico do CyP2022, que serviu de base para todo o desenvolvimento do exercício e das suas interações, foi composto por duas regiões, OTHERLAND (conjunto de países que constitui a Otherland Alliance) e a TUGLAND (representa o país do qual os participantes vão fazer parte).

É a interação entre estas duas regiões e os seus "partidários" que serviu como cenário do exercício, sendo que o GRA participou como TugAzoGRA (Governo Regional de AZO). A apresentação de todo o cenário, com as características detalhadas das duas regiões, de modo a poder dar uma melhor compreensão, pode ser encontrado nos Anexos.

5.12.1.2. Cenário no Ciberespaço

A OTA desenvolve várias atividades no campo da Guerra Cibernética, em parte devido aos seus custos mais baixos, um cluster de Tecnologia da Informação e Comunicação e o fato de que as atividades cibernéticas não dependem da localização geográfica.

O grupo hacktivista conhecido como Pinkworm, que apoiou os objetivos da OTA ao longo dos anos, ainda está ativo. Um relatório da Tugland Intelligence divulgado recentemente identifica que o grupo Pinkworm está a planear realizar ataques cibernéticos contra Tugland.

5.12.1.3. Evolução do CYP2022 – Injeções e Informação

Acontecimentos prévios

01NOV2022 – Diversos Sites da Internet de diversas entidades administrativas sofreram ataques informáticos (maioritariamente ataques DDoS), ficando *offline* por várias horas.

Na Região Azo, foram afetados os portais do Governo Regional, o Portal SIGRHARA, o Site do Parlamento ONLINE e o Portal do Jornal Oficial de AZO, e após a intervenção das equipas da DRCTD, foram mitigados, encontrando-se o ecossistema GRA em pleno funcionamento.

08NOV2022 – Inicia-se o importante evento mundial de tecnologia, o '*Tugland Tech Summit*' (TTS), em LIS. Estando a ameaça cibernética contra este evento classificada como "Grave".

Acontecimentos CYP2022

De seguida apresento, de forma resumida (a descrição integral dos acontecimentos pode ser consultada nos Anexos deste documento – pág. 120), os principais acontecimentos do Exercício CyP2022, nomeadamente o momento dos envios das Injeções.

14NOV2022 – 1.º Dia

14:00 – STARTEX CyP2022

16:30 – Lançamento da Primeiro Injeção GRA - possível exfiltração de dados dos trabalhadores GRA da Plataforma SIGRHARA.

15NOV2022 – 2.º Dia

12:00 – Lançamento da Segunda Injeção GRA - ataque, através de *SQL Injection*, a uma distribuição do SGC, com a alteração de um documento referente a um despacho do Presidente do GRA.

16NOV2022 – 3.º Dia

10:00 – Lançamento da Terceira Injeção GRA - ataque de engenharia social "*Spear Phishing*" direcionado aos técnicos de IT da DRCTD.

17NOV2022 – 4.º Dia

15:00 – Comunicação oficial a informar que todos os incidentes foram solucionados. Solicitação, às equipas intervenientes, de Relatórios sobre os incidentes, causas, formas de mitigação e propostas de melhoria.

17:00 – ENDEX CIBER PERSEU 2022

5.13. Análise à Participação do GRA no CYP2022

O GRA participou em 2 das Missões do CIBER PERSEU 2022, a MS03 - Resposta, análise e investigação de ciber-incidentes em plataforma *cyber range* (Missão Técnica onde entraram apenas os Técnicos da DRCTD) e a MS04 - Ciberataque ao sector público e privado (Missão de Teor Processual/Procedimentos).

Na MS03 a equipa GRA, composta por apenas dois elementos, procurou, dentro dos desafios apresentados na plataforma de *cyber range*, dar uma resposta técnica, resolvendo os vários problemas apresentados. Salientamos que, em próximas participações deveria ser equacionada a participação de uma equipa mais numerosa, visto que, as outras equipas participantes eram constituídas por cinco ou mais elementos, o que possibilitou, em alguns casos, uma resposta mais célere. Foi ainda identificada, pelos participantes, alguma falta de informação, na plataforma, que possibilitasse ajuda durante a realização dos desafios.

Para a participação na MS04 foram idealizadas 3 Injeções para serem "tratadas" pelos participantes GRA durante o CyP2022. Foram idealizadas para serem respondidos de acordo com os procedimentos identificados nos Anexos (Fluxograma de procedimento após deteção de Incidente de Segurança; Fluxograma do procedimento de Violação de Dados Pessoais; Etapas após deteção de Incidente de Segurança com Violação de Dados Pessoais; páginas 122 a 124) e que foram pensados para responder a este tipo de Incidentes de Cibersegurança.

A primeira Injeção - referente a uma possível exfiltração de dados dos trabalhadores GRA da Plataforma SIGRHARA.

Com a primeira Injeção pretendeu-se testar o procedimento referente a uma exfiltração de dados, multi departamental e que exigisse a solicitação da intervenção, pela DROPEP, da DRCTD à Presidência do GRA e o consequente procedimento para o mesmo.

A DROPEP possui uma estrutura identificada e com uma "cadeia de comando" bem definida, tendo o procedimento sido seguido desde a identificação e comunicação do incidente de Cibersegurança, até ao restabelecimento do serviço afetado. Realçamos a participação das várias chefias da DROPEP neste Exercício.

Foram identificados alguns constrangimentos, principalmente referentes a algumas questões jurídicas, que devem ser clarificadas, nomeadamente quem possui competência ou autoridade para encerrar um servidor ou serviço, quem deve comunicar (serviço ou o GRA), etc.

Deve ser melhorada a Comunicação com o Exterior (a Política de Comunicação deve ser afinada, havendo uma maior participação do Centro de Multimeios na elaboração desta, e sempre em cooperação com a DRCTD e com o Assessor de Imprensa da PGRA) e o feedback referente a algumas solicitações, possibilitando um melhor seguimento do procedimento e do ponto em que este se encontra (a existência de uma plataforma Gestão de Incidentes de Cibersegurança do GRA otimizaria este ponto).

Foi interessante verificar que, numa situação em que o Presidente do GRA (visita ao Estrangeiro e em Reuniões), o Chefe de Gabinete do Presidente (em viagem e sem comunicação), foi possível fazer uma reunião, com a participação dos Assessores do Presidente, de modo a poder ultrapassar uma situação de urgência. Consideramos de extrema importância a envolvência das chefias de Topo nestes "simulacros" de incidentes de Cibersegurança, e onde se podem identificar entropias e constrangimentos que podem ocorrer numa "situação real".

Numa próxima participação será fundamental recriar uma ocorrência real de exfiltração de dados para testar o procedimento de comunicação à CNPD, assim como por quem esta comunicação deve ser feita.

A Segunda Injeção - referente a um ataque, através de *SQL Injection*, a uma distribuição do SGC, com a alteração de um documento referente a um despacho do Presidente do GRA.

Com a segunda Injeção pretendeu-se testar a comunicação institucional do GRA para o exterior, assim como, o procedimento de identificação e reporte de um incidente de Cibersegurança.

Sendo esta uma Injeção mais institucional, pretendeu-se obter comunicações em resposta a pedidos de esclarecimento de jornalistas baseados em *fake news*, à Presidência do GRA.

Será importante um maior envolvimento do Centro de Multimeios (deverá, em nossa opinião, estar presente em todas próximas participações em Exercícios de Cibersegurança) de forma a poder auxiliar o Assessor de Imprensa, na sua ausência ou impossibilidade de contato, e os Departamentos do GRA, aquando das solicitações de informação ou comunicados para o Exterior aquando da existência de Incidentes de Cibersegurança.

A Terceira Injeção - referente a um ataque de engenharia social "*Spear Phishing*" direcionado aos técnicos de IT da DRCTD.

Com a terceira Injeção pretendeu-se testar o procedimento de identificação e comunicação de um incidente de Cibersegurança.

Após a mensagem de *Spear Phishing*, os elementos da DRCTD conseguiram identificar o ataque e, de forma correta, efetuar a comunicação do mesmo ao CNCS e agir de forma correta internamente, "neutralizando" a ameaça.

Em conclusão podemos referir que a participação do GRA neste Exercício de Cibersegurança foi muito positiva, relembrando que este ainda se encontra no início de um longo e trabalhoso caminho para dotar o Ecossistema GRA de uma capacidade robusta de resposta e resiliência perante um Incidente de Cibersegurança.

5.14. Inquérito à participação no CyP2022

Foi elaborado um questionário, através dos *Google Forms*, que pretendeu obter, junto dos participantes GRA no Exercício CyP2022, um feedback sobre o exercício e sobre a participação do GRA neste tipo de exercícios.

O questionário era composto por 12 questões, sendo 8 de resposta múltipla, 3 de resposta quantitativa e uma de resposta livre. O questionário foi disponibilizado online, tendo sido obtidas 12 respostas ao mesmo.

O Questionário, assim como as respostas e gráficos correspondentes podem ser consultadas nos Anexos deste documento na página 126.

5.15. Análise ao questionário CyP2022

5.15.1.1. Resumo

Fazendo uma análise do feedback dos participantes GRA no CyP2022 podemos dizer que a totalidade considera importante a participação do GRA em Exercícios de Cibersegurança, devendo estes ser executados a nível Regional, Nacional e Internacional, e deverão englobar a Componente Procedimental e Técnica.

A Participação nestes Exercícios de Cibersegurança deverá ser semestral numa primeira fase, evoluindo para uma periodicidade anual como consolidação de procedimentos e conhecimentos.

É considerado ainda que, o Exercício cumpriu as expectativas, cumprindo maioritariamente ou na totalidade os objetivos iniciais, sendo que a participação no mesmo irá trazer mais valias para a Organização.

Os participantes consideram que a organização foi Boa/Muito Boa, assim como a informação recebida antes do evento, sendo que o apoio que recebeu durante a realização do evento é classificado como Muito Bom/Bom.

5.15.1.2. Participação em Exercícios

- 100% considera importante a participação do GRA neste tipo de exercícios de Cibersegurança;
- 91,7% considera que o GRA deve participar em Exercícios Procedimentais e Técnicos, enquanto 8,3% apenas considera que deve participar em Exercícios Técnicos;

- 75% considera que o GRA deve participar em Exercícios a nível Regional, Nacional e Internacional, 16,7% apenas a nível Regional e 8,3% a nível Regional e Nacional;
- 91,7% considera participar noutro exercício de Cibersegurança, enquanto 8,3% não considera essa participação.

5.15.1.3. Periodicidade dos Exercícios

- 41,7% considera que devem ser anuais;
- 25% considera que devem ser bianuais;
- 16,7% considera que devem ser semestrais;
- 8,3% considera que devem ser bianuais numa primeira fase e depois anuais para consolidação;
- 8,3% considera que se deve considerar a mais adequada.

5.15.1.4. Objetivos

- 66,7% considera que os objetivos foram maioritariamente atingidos;
- 16,7% considera que os objetivos foram totalmente atingidos;
- 8,3% considera que os objetivos foram apenas parcialmente atingidos ou não foram atingidos.

5.15.1.5. Organização

- 50% classifica a organização do Exercício como Boa (4), 33,3% classifica a organização como Muito Boa (5) e 16,7% classifica a organização como. Razoável (2);
- 41,7% classifica como Boa (4) a informação recebida antes do evento, 33,3% como Muito Boa (5), 8,3% como Suficiente (3), 8,3% como Razoável (2) e 8,3% como Má (1);
- 50% considera como Muito Bom (5) o apoio que recebeu durante a realização do exercício, 25% como Bom (4), 8,3% como Suficiente (3), 8,3% como Razoável (2) e 8,3% como Mau (1);

5.15.1.6. Considerações

- 91,7% considera que a participação no exercício irá trazer "mais valias" para a organização e 8,3% considera que o exercício não explorou as potencialidades relativamente à organização;
- 81,8% considera que o exercício cumpriu as expectativas, sendo que 9,1% refere que não tinha expectativas e que entende que ficou aquém do objetivo transmitido superiormente e 9,1% indica que o exercício não cumpriu as expectativas.

5.15.1.7. Propostas de melhorias para próximos Exercícios

As propostas de melhoria referem que em próximos eventos o GRA deve ter em consideração:

- Informação de participação com uma maior antecedência, permitindo uma preparação mais profunda;
- Utilização/criação de uma plataforma que permita o seguimento e a gestão dos registos de incidentes (com fluxos corretos de comunicação e acompanhamento dos incidentes);
- Melhorias no Plano de Comunicação Interno e para o Exterior;
- Um maior acompanhamento na realização das componentes técnicas;
- Uma maior presença de elementos do GRA no local (*BackOffice*) do exercício;
- Uma maior "personalização" dos incidentes a "enfrentar", permitindo testar com maior veracidade a capacidade de resposta a incidentes reais.

Capítulo 6 Conclusões

Neste Capítulo pretende-se apresentar as conclusões e uma reflexão sobre o trabalho realizado, assim como algumas ideias de trabalho para o Futuro.

6.1. Conclusão

A Participação do GRA nos dois Exercícios de Cibersegurança (ExNCS e CyP), no ano de 2022, permitiram, de uma forma muito concreta avaliar o estado de maturação do Ecossistema GRA, mais propriamente o relacionado com a Presidência do GRA e com a Secretaria Regional das Finanças, relativamente aos Procedimentos a realizar em caso de deteção de Incidente de Segurança.

Durante estes foram testados os procedimentos, baseados na Metodologia de Gestão de Incidentes do NIST e no Fluxo de Informação para resposta a Incidentes da Norma ISO 27035, que nos pareceu a que melhor se enquadra no Ecossistema GRA, possibilitando assim uma melhor e mais eficaz resposta.

Neste documento foi elaborada uma introdução à temática da Cibersegurança, assim como o levantamento do cenário de risco. Foi produzida uma análise do estado da arte relativamente às boas práticas, normas e legislação aplicável. Procedeu-se, também, a um levantamento dos constrangimentos e requisitos do Ecossistema GRA.

De referir que, no âmbito do trabalho desenvolvido, houve várias atividades/propostas, por mim elencadas e no seguimento da participação do GRA nos Exercícios de Cibersegurança, que durante o ano de 2022 e início de 2023, foram desenvolvidas ou que pela participação ganharam “mais força”. Destas saliento:

- Criação do SOC GRA – Azores Cyber 360º;

- Desenvolvimento e consolidação de manuais de boas práticas de utilização de meios informáticos e de Cibersegurança no GRA;
- Estudo para a criação de uma Cyber Academy GRA;
- Realização de Campanha de Sensibilização;
- Implementação do NOC do Projeto Azores Cloud;
- Aquisição de solução anti-DDoS, WAF e CDN para o GRA;
- A equipa Multidisciplinar na PGRA;
- O cumprimento do RJSC;
- A implementação do RGPD;
- Elencar de juristas do CCEJ do Governo Regional para acompanhar os aspetos jurídicos da Cibersegurança.

Mas ainda há muito trabalho para fazer e concretizar, visto o GRA ainda se encontrar a "dar os primeiros passos" na sua capacitação e capacidade de prevenção e análise de Incidentes, assim como a resposta a Incidentes de Cibersegurança.

Assim, é essencial pensar uma Estratégia do GRA para a Cibersegurança.

A implementação do RJSC permitirá que, com a elaboração dos Relatórios de Ativos Anuais, se conheça as infraestruturas que compõem o GRA, os seus ativos e assim saber o que é necessário proteger e assim definir, de uma forma mais clara, como proteger essas mesmas infraestruturas.

Deve ser aplicada a política de *Zero Trust* na rede GRA, com a implementação de mais procedimentos de segurança que permitam práticas recomendadas de defesa em profundidade e implementar um modelo de defesa em camadas que garanta que as tecnologias certas sejam aplicadas nas camadas apropriadas da arquitetura de rede do GRA.

Deve ser criado o Plano de Segurança do GRA e o Plano de Resposta a Incidentes no GRA, que possam servir de modelo e replicados por todas as entidades do GRA, de forma a estruturar a atuação em incidentes de Cibersegurança.

O investimento em Cibersegurança e em meios humanos, de *hardware* e de *software* deve ser tido em conta, antes de um incidente ocorrer e como medida preventiva, e não apenas depois deste ocorrer, como meio paliativo ou de resposta/reação.

Neste sentido é necessário o investimento em Formação, quer das chefias de topo (ao nível da sensibilização e implementação, com capacidade de decisão) quer dos colaboradores e dos técnicos de IT, assim como a criação de condições para uma maior capacidade de atuação do GRA em situações ou na prevenção de incidentes de Cibersegurança, com a criação de um SOC e de uma CSIRT do GRA, prestando apoio não apenas no ecossistema GRA, mas também a entidades e empresas da RAA.

Como reflexão final considero que os objetivos a que me propus, no início deste projeto, foram atingidos, tendo contribuído para que o GRA pudesse aumentar a sua capacitação ao nível da prevenção, análise e resposta a Incidentes de Cibersegurança, potenciando assim o aumento da resiliência da Região.

Contribuí, com a realização deste projeto, a participação nos Exercícios de Cibersegurança e a elaboração de relatórios de análise aos mesmos, que entreguei à Presidência do Governo Regional dos Açores, para a promoção uma cultura de segurança, relativa à utilização dos meios informáticos e colaborando para a sensibilização e aumento da ciber-maturidade no GRA.

Bibliografia

Açores, G. d. (Maio de 2023). *Presidência do Governo Regional*. Obtido de Portal dos Açores: https://portal.azores.gov.pt/web/prgra

Açores, G. d. (Maio de 2023). *XIII Governo Regional dos Açores*. Obtido de Portal dos Açores: https://portal.azores.gov.pt/web/xiii-gra

Anonymous, G. (2003). *Maximun Security, A Hacker's Guide to protecting Your Computer Systems and Network.* SAMS.

Carvalho, N. (2009). *Organizações e Segurança Informática.* Lugar da Palavra.

Cichonki, P. M. (2012). *Computer Security Incident Handling Guide- Recomendations of the National Intitute os Standards and Technology*.

CNCS. (2019). *Roteiro para Capacidades Mínimas de Cibersegurança.*

CNCS. (2022). *Quadro Nacional de Referência para a Cibersegurança*.

CNCS. (2022). *Relatório de Cibersegurança em Portugal - Riscos & Conflitos 2021*.

Commission, T. E. (2017). *Resilience, deterrence and defence: Building strong cybersecurity in Europe.*

Constituinte, A. (10 de Abril de 1976). *Diário da República- Decreto de Aprovação da Constituição da República Portuguesa.* Obtido de Diário da República eletrónico: https://dre.pt/dre/legislacao-consolidada/decreto-aprovacao-constituicao/1976-34520775

DN. (2022). Laboratórios Germano de Sousa alvo de ciberataque. CUF cancela testes à covid-19. *Diário de Notícias*.

DN/LUSA. (2019). Fundação Champalimaud sofre "ataque informático sem precedentes". *Diário de Notícias*.

DN/LUSA. (2022). Hospital Garcia de Orta foi alvo de ataque informático e ativou protocolo de segurança. *Diário de Notícias*.

EC3, E. (2021). *Europol Internet Organized Crime Threat Assessment 2021*.

ENISA. (2010). *Good Pratice Guide For Incident Management.*

ENISA. (2012). *Threat Landscape - Responding to the Evolving Threat Environment.*

ENISA. (2021). *ENISA Threat Landscape 2021*.

Ferro, C. (2018). Hospitais da CUF alvo de ataque informático. *Diário de Notícias*.

Hartley, B. &. (2001). *The Process of Security.* In Business Security Advisor.

IC3, F. (2022). *Internet Crime Report 2021*.

ISO. (2013). *ISO/IEC 27001*.

ISO. (2016). *ISO/IEC 27035-1*.

ISO. (2022). *ISO/IEC 27002*.

LUSA. (2017). Dados de 230 mil utentes dos Açores foram divulgados na Internet. *Diário de Notícias*.

LUSA. (2021). Hospital de Ponta Delgada diz que "ataque informático" de que foi alvo a maior unidade de Saúde dos Açores está "em investigação". *Observador*.

Mamede, H. S. (2006). *Segurança Informática nas Organizações.* FCA.

Ministros, C. d. (05 de Junho de 2019). *Diário da República- Estratégia Nacional de Segurança do Ciberespaço - Resolução do Conselho de Ministros N. 92/2019*. Obtido de Diário da República Eletrónico: https://dre.pt/ dre/detalhe/resolucao-conselho-ministros/92-2019-122498962

Monteiro, F. (2003). *Engenharia de Redes Informáticas.* FCA.

NIST. (10 de Janeiro de 2023). *NIST General Information*. Obtido de NIST: http://www.nist.gov/public_affairs/general_information.cfm

Norton. (2013). *2012 Norton Cybercrime Report.*

Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace.* Que Corporation.

Reis, M. F. (2017). Piratas informáticos atacam hospital Garcia de Orta. *Nascer do Sol*.

República, A. d. (5 de agosto de 1980). *Diário da República - Estatuto político Administrativo da RAA.* Obtido de Diário da República Eletrónico: https://dre.pt/application/file/a/470150

República, A. d. (13 de Agosto de 2018). *Diário da República - Lei n.º 46/2018*. Obtido de Diário da República Eletrónico: https://dre.pt/dre/detalhe/lei/46-2018-116029384

Research, C. P. (2023). *The Check Point Research 2022.*

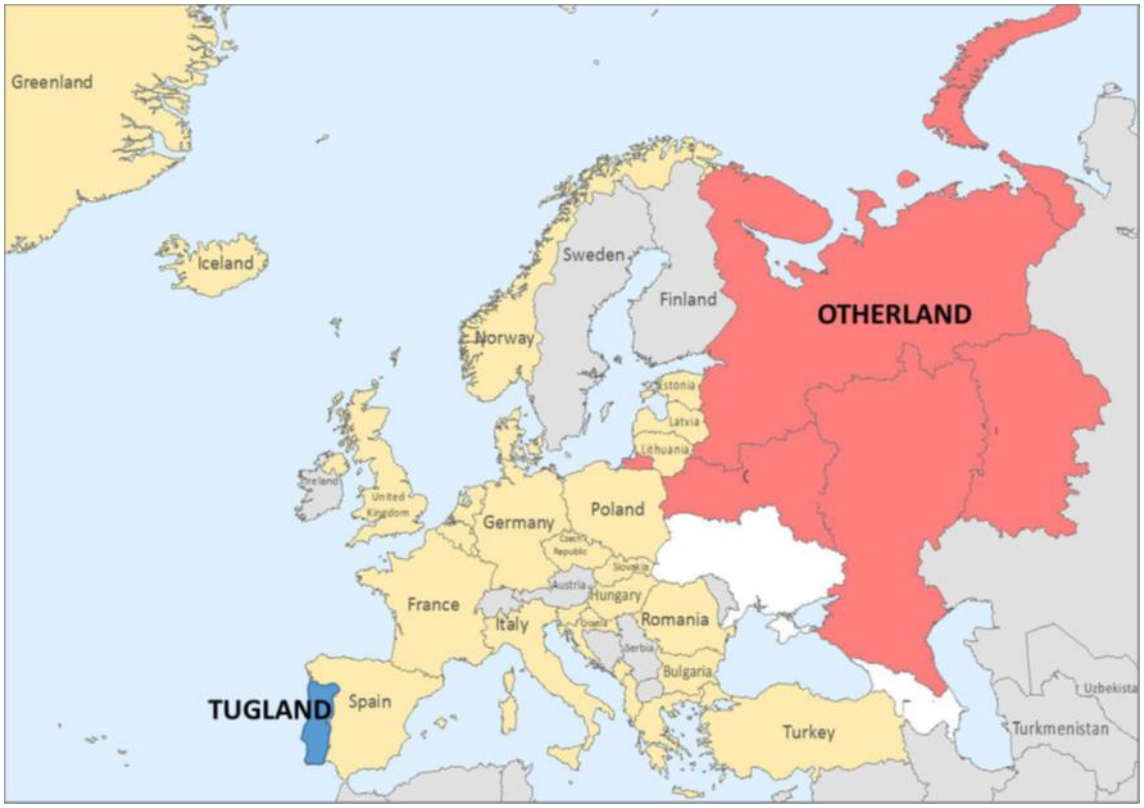
RNCSIRT. (2020). *Taxonomia Comum da Rede Nacional de CSIRT.*

Anexos

EXERCÍCIO CIBER PERSEU 2022 – CyP2022

Cenário no "*The Regional Government of Azo*" - TugAzoGRA

Cenário Geopolítico



A Região de OTHERLAND

Os aliados OTHERLAND são um conjunto de países que têm raízes culturais, idioma, perspetivas históricas, perspetivas de desenvolvimento e objetivos comuns. Eles assinaram um tratado de defesa e assistência mútua garantindo a defesa na Região de Otherland, conhecido como OTherland Alliance (OTA). Eles concordaram em mostrar posições semelhantes e coordenar a votação em assuntos internacionais. Cada país se beneficia do acordo de defesa e assistência mútua, contando com o apoio político, diplomático e militar dos outros três.

As Forças Militares da OTA estão bem equipadas e em processo de modernização. Sua maior força é a receita que obtém das exportações de gás, petróleo, metais e indústria de defesa. Possui uma forte capacidade nuclear e de armas de destruição em massa (WMDs). O principal objetivo da OTA é dominar a região do Alto Norte e a região dos Estados Bálticos e alterar o equilíbrio de poder na Europa, a fim de recuperar a influência regional e global e garantir a segurança e a prosperidade econômica.

A OTA também foi identificada como envolvendo-se em "guerra híbrida" disruptiva. Táticas de guerra assimétrica, como ataques cibernéticos e espionagem industrial, estão a ser empregues pela OTA noutras nações, particularmente em Tugland.

Nos últimos anos a Tugland tem feito um esforço para participar ativamente na segurança global, enquanto procura aumentar a sua resiliência na segurança interna e proteção civil. Atualmente, há uma operação ativa na região de Otherland em que Tugland participa com Forças do Exército Tugland (TugArmy). A OTA está a lançar uma grande campanha de desinformação para desacreditar esta operação.

TUGLAND

Tugland é um pequeno país situado na ponta oeste da Península Ibérica com uma área que abrange cerca de 92.000 km² com uma população de 10.000.000. O território de Tugland inclui dois arquipélagos no Oceano Atlântico: os arquipélagos de Mad e Azo. A sua localização geográfica é estrategicamente importante devido à proximidade com o Atlântico.

Tugland é membro das Nações Unidas (ONU) e de outras organizações internacionais.

Tugland tem feito um esforço para participar ativamente da segurança global, ao mesmo tempo em que busca aumentar sua resiliência na segurança interna e proteção civil.

Um importante evento mundial de tecnologia, o 'Tugland Tech Summit' (TTS) está planeado para realizar-se em Lis no dia 8 de novembro.

As organizações de inteligência envolvidas, incluindo a inteligência militar nacional, alertam que a ameaça cibernética contra o TTS é considerada "grave".

Acontecimentos CYP2022 - Detalhados

14NOV2022 – 1.º Dia

14:00 – STARTEX CyP2022

16:30 – Técnico da área de processamento de salários da SRFinanças comunica à equipa de IT da SRF que foi identificado um problema com o Portal SIGRHARA, não sendo possível o processamento dos salários dos Funcionários GRA relativos a este mês.

17:00 – Equipa de IT da SRF informa que a anomalia estará relacionada com os ataques do dia 01NOV2022. Foi identificado um acesso de um ex-trabalhador, através da análise dos *logs*, que terá executado um programa, sem autorização, que afetou o Portal.

17:00 – A DRCT faz comunicação ao PGRA que identificou diversas tentativas de ataques e acessos aos diversos portais do Ecossistema GRA, pelo que solicita a elevação do nível de *awareness* e "política" a adotar.

17:15 – O Ex-Trabalhador, informou a equipa de IT da SRF que sofreu um ciberataque ao seu computador pessoal, que utilizava para aceder ao Ecossistema GRA desde casa. As credenciais deste ex-trabalhador (nível administrador) foram roubadas e utilizadas no ataque.

15NOV2022 – 2.º Dia

09:00 – A equipa de IT informa o Gabinete do SRF que, apesar de já ter identificado o *modus operandi* do ciberataque, não possui não possui capacidade técnica para a resolução do mesmo, pelo que é necessária a intervenção da DRCTD para o restabelecimento do sistema.

09:00 – É verificada a existência, na *Dark Web*, de dados dos funcionários GRA. É possível ter havido uma exfiltração dos mesmos da Plataforma SIGRHARA.

09:15 – As equipas da DRCTD encontram-se a verificar se os dados são reais.

09:20 – O SRF solicita a intervenção "externa" da equipa da DRCTD.

09:25 – É necessária comunicação (interna e externa) sobre estes ataques.

10:00 – Convocada reunião de emergência dos órgãos da PGRA, com a presença do Presidente do GRA, para ponto de situação e tomada de decisão sobre a estratégia a adotar perante os ataques.

10:30 - Reunião dos órgãos da PGRA, com a presença do Presidente do GRA, para ponto de situação e tomada de decisão sobre a estratégia a adotar perante os ataques.

É ativada a "*task force*" de resposta à crise de Cibersegurança (com os diversos elementos de vários departamentos da PGRA) e autorizada a intervenção das equipas da DRCTD em apoio das equipas de IT da SRFinanças.

É solicitado, à Encarregada de Proteção de Dados, para tomar conhecimento de uma possível violação de dados pessoais (deve efetuar uma avaliação do risco).

A EPD do GRA deve contactar o Gabinete da Presidência do GRA, informando sobre a situação e indicando a avaliação de risco (sem risco, com risco ou com risco elevado), solicitando o iniciar da investigação da eventual violação de dados pessoais, e informando as primeiras medidas de contenção, em colaboração com as equipas da DRCTD.

O Chefe de Gabinete/PGRA deve solicitar a colaboração do Departamento Jurídico, da DRCTD e da Assessoria da Comunicação, para em conjunto com a responsável verificarem as implicações legais relevantes, em função dos factos apurados.

Deve ser Notificada a CNPD, caso a violação de dados pessoais seja suscetível de resultar num risco parra os direitos e liberdades das pessoas singulares. Esta informação, à CNPD, pode ser feita de acordo com os dados que forem sendo verificados.

Proposta de medidas a adotar para a reparação da violação dos dados pessoais, inclusive medidas para atenuar os seus eventuais efeitos negativos.

Verificar ainda a necessidade de notificação dos titulares dos dados.

O PGRA/CG toma a decisão sobre a estratégia de Comunicação a ser implementada pelo GRA (comunicação com o exterior, comunicação com o interior e qual o nível de informação facultado).

O PGRA/CG, sob proposta da DRCTD e do responsável de Informática da PGRA, deve propor a utilização, em paralelo, da Plataforma *Signal* para troca de comunicações entre os decisores de topo, agilizando assim alguns procedimentos, intervenções e autorizações.

11:00 – Foi verificado um acesso estranho, com as credenciais do ex-funcionário à Plataforma SGC. O Acesso foi identificado pelas equipas da DRCTD ao analisar o tráfego da rede GRA, desde o dia 01NOV2022, no seguimento dos ataques já identificados.

12:00 – A Agência noticiosa ONews informa, apresentando um documento oficial, que uma Organização conotada com a OTA, teve, no passado dia 03NOV2022, despacho favorável, do GRA, para a instalação de uma infraestrutura de comunicações e novas tecnologias, na Ilha Terceira, mais precisamente junto à Base Aérea N. º4. Tal posição levantou várias questões e alertas da Comunicação social de TugNews, questionando o GRA sobre o referido despacho.

12:30 – Comunicação Oficial a refutar a informação sobre o despacho para a instalação da referida infraestrutura. Mais informações em breve.

14:00 – O Secretariado do PGRA identifica que o documento, referido pela ONews, se encontra adulterado no Sistema SGC. Solicita a intervenção da DRCTD para verificar a situação.

15:00 – Após cuidadosa análise, foi verificado que os dados possivelmente exfiltrados, não proveem do SIGRHARA, e não apresentam dados sensíveis, identificados como sendo dados de residentes na RAA, mas sendo dados exfiltrados no ataque já reportado, a uma companhia aérea, não apresentando, desta forma problema.

15:30 – A DRCTD identifica um ataque por *SQL Injection* com a intensão de alterar diversos documentos para despachos favoráveis à Organização de OTA.

16NOV2022 – 3.º Dia

10:00 – Através de um e-mail é solicitada, com urgência, um acesso, com privilégios de administrador, para uma entidade externa (para ontem). E-mail enviado com o Alias "Pedro Batista". Solicitado acesso a máquina sensível dentro do ecossistema GRA.

12:00 – DRCTD informa que o problema com o processamento de salários se encontra resolvido.

16:00 – Solicitação, por parte do CG, de informação sobre os procedimentos para a mitigação/resolução dos problemas.

17NOV2022 – 4.º Dia

10:00 – Envio de "relatórios" com a informação sobre o ponto de situação

15:00 – Comunicação oficial a informar que todos os incidentes foram solucionados.

16:00 – Comunicação a informar que o grau de ameaça cibernética é revisto para normal.

16:30 – o GRA comunica às equipas de Cibersegurança o novo grau de ameaça.

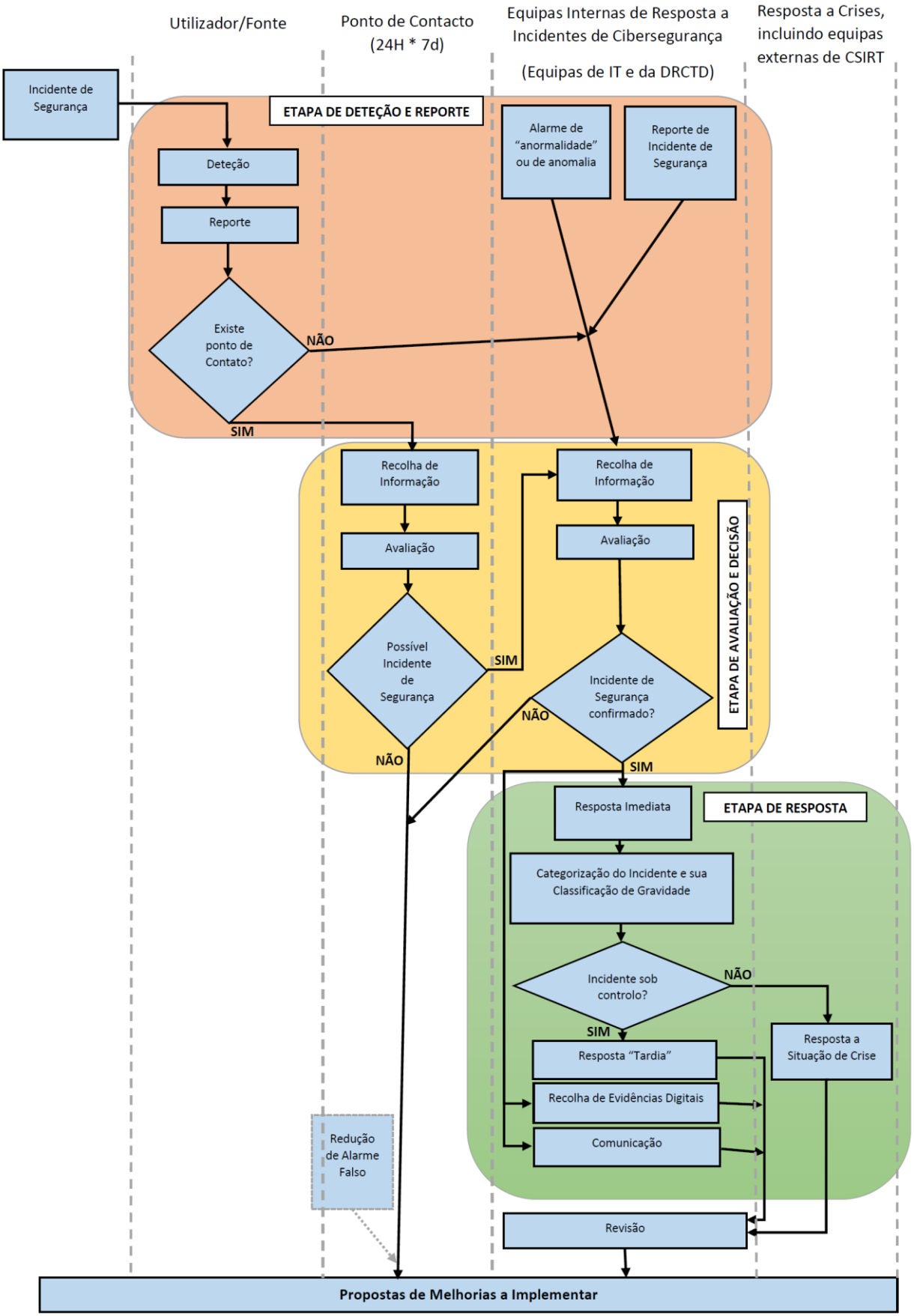
17:00 – ENDEX CIBER PERSEU 2022

Taxonomia Comum para a Classificação de Incidentes de Segurança Informática

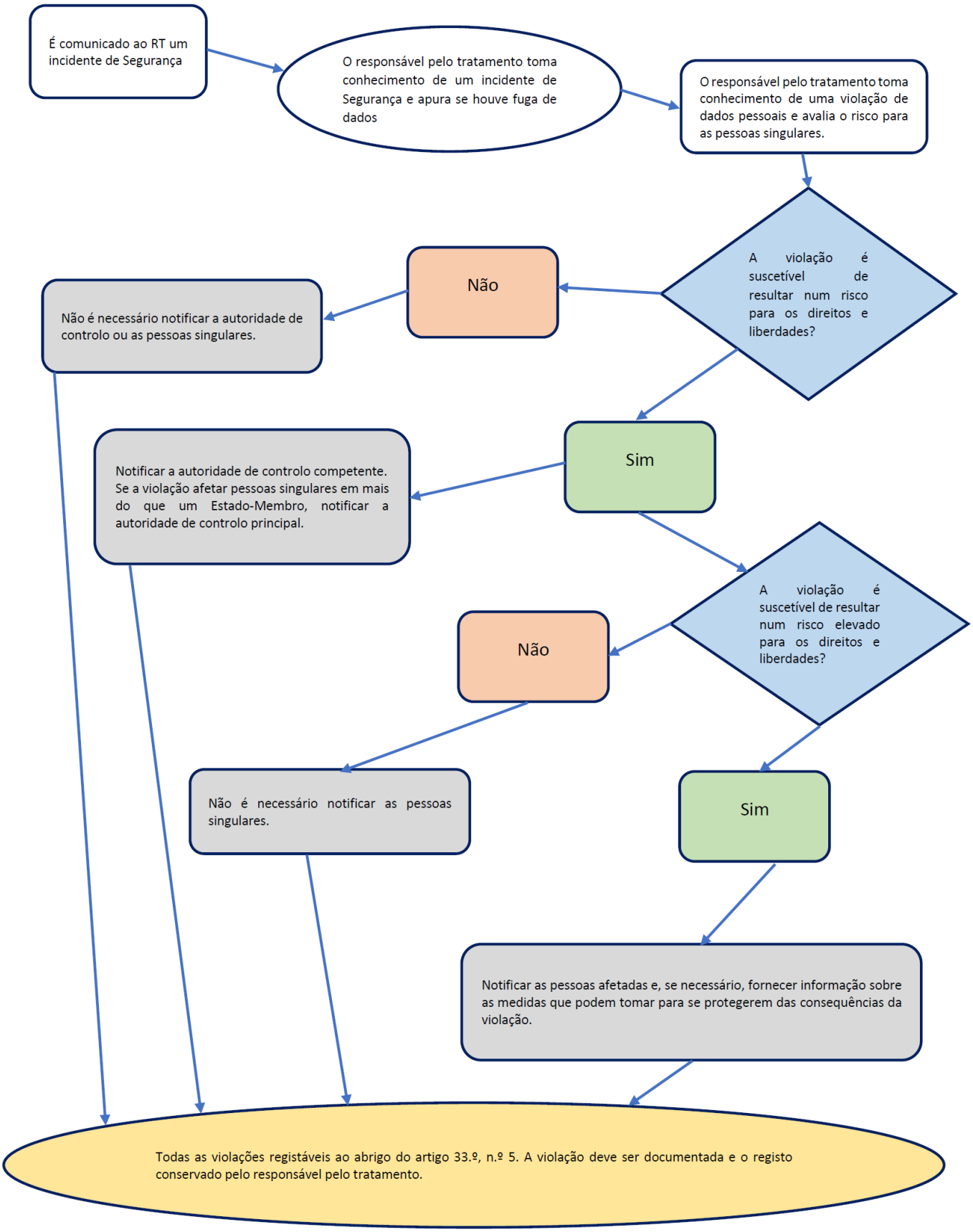
Tipo de Evento	Tipo de Incidente	Classe de Incidente
Flood de e-mails	*SPAM*	Conteúdo Abusivo
Envio de mensagem não solicitada		
Publicação de informação com o objetivo de intimidar ou coagir outrem	Discurso Nocivo	
Disseminação de conteúdos proibidos por lei (crimes públicos)	Exploração sexual de menores, racismo e apologia da violência	
Sistema(s) ou software(s) infetado(s) com *malware* permitindo acesso remoto, *monitorização* de atividades do sistema e recolha de informações	Sistema Infetado	Código Malicioso
Alojamento de servidor C2	Servidor C2	
Disseminação de *malware* através de vários canais de comunicação	Distribuição de *Malware*	
Probe a sistema	*Scanning*	Recolha de Informação
Scan de rede		
Transferência zona DNS		
Wiretapping	*Sniffing*	
Informação obtida através de meios não técnicos passível de ser usada em ataques futuros	Engenharia Social	
Tentativa de utilização de *exploit*	Exploração de Vulnerabilidade	Tentativa de Intrusão
Tentativa de SQL *Injection*		
Tentativa de XSS		
Tentativa de *File Inclusion*		
Tentativa de *Brute-force*	Tentativa de *login*	
Tentativa de password *cracking*		
Tentativa de Ataque Dicionário		
Furto de credenciais de acesso privilegiado	Compromisso de Conta Privilegiada	Intrusão
Furto de credenciais de acesso	Compromisso de Conta Não Privilegiada	
Entrada não autorizada em instalações físicas	Arrombamento	
Exploit ou ferramenta para esgotamento de recursos (rede, capacidade processamento, sessões, etc…)	Negação de Serviço	Disponibilidade
Flood de pedidos		
Flood distribuído de pedidos	Negação de Serviço Distribuída	
Exploit ou ferramenta distribuídos para esgotamento de recursos		

Vandalismo	Sabotagem	
Disrupção intencional de mecanismos de transmissão e tratamento de dados		
Disrupção não intencional de mecanismos de transmissão e tratamento de dados	Interrupção	
Acesso indevido a sistema	Acesso não autorizado	Segurança da Informação
Acesso indevido à informação		
Exfiltração de dados		
Modificação de informação	Modificação não autorizada	
Eliminação de informação	Perda de dados	
Utilização indevida ou não autorizada de recursos	Utilização indevida ou não autorizada de recursos	Fraude
Distribuição ou partilha de conteúdos protegidos por direitos de autor	Direitos de autor	
Utilização ilegítima de nome da instituição ou de terceiros	Utilização ilegítima de nome de terceiros	
Disseminação de e-mails de *phishing*	*Phishing*	
Alojamento de sites de *phishing*		
Agregação de informação recolhida em esquemas de *phishing*		
Utilização de mecanismos de cifra considerados inseguros	Criptografia fraca	Vulnerabilidade
Servidor NTP configurado com *monlist*	Amplificador DDoS	
RDP exposto	Serviços acessíveis potencialmente indesejados	
Documentos internos acessíveis em partilha pública	Revelação de Informação	
Sistema sem atualizações e/ou correções de segurança.	Sistema vulnerável	

Fluxograma de Procedimento após Deteção de Incidente de Segurança



Fluxograma do Procedimento de Violação de Dados Pessoais



Etapas a Realizar após deteção de Incidente de Segurança com Violação de Dados Pessoais

Passo	Ação Recomendada	Comentários
1	**Informar o Responsável pelo Tratamento dos Dados (Plataforma)**	Os utilizadores GRA devem ter uma lista de contactos para situações de incidentes de segurança da Informação. Esta lista deve estar sempre atualizada, deve ser divulgada e estar disponível on-line e off-line.
2	**O RT deve contactar o EPD e as Equipas de IT** Deve contactar rapidamente, via telefone ou e-mail os seguintes Departamentos: • EPD (Encarregado de Proteção de Dados) • Equipas de IT ou DRCTD	O Responsável de Tratamento deve ter uma lista de contactos para situações de incidentes de segurança da Informação. Esta lista deve estar sempre atualizada, deve ser divulgada e estar disponível *online* e *offline*.
3	**Iniciar a investigação da eventual violação de dados pessoais e tomar as primeiras medidas de contenção**	Se dispuser de meios para tal ou com o apoio das equipas de IT.
4	**O EPD deve contactar o Departamento Jurídico para identificar as obrigações legais** O Departamento Jurídico, em conjunto com o EPD, identifica as obrigações legais relevantes, em função dos dados apurados	Devem ser avaliados os riscos para as pessoas singulares (sem risco, com risco ou com elevado risco) e devem ser informadas as funções / pessoas relevantes do GRA. Deve ser tida em conta a probabilidade e a gravidade do risco, assim como ter em conta os considerandos 75 e 76 do RGPD.
5	**Notificar a CNPD (se aplicável)** A notificação deve ser efetuada sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da violação de dados pessoais. A notificação deve, pelo menos: a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa; b) Comunicar o nome e os contactos do encarregado da proteção de dados ou outro ponto de contacto onde possam ser obtidas mais informações; c) Descrever as consequências prováveis da violação de dados pessoais; d) Descrever as medidas adotadas ou propostas para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.	A entidade não está obrigada a notificar a CNPD caso a violação de dados pessoais são seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas à CNPD por fases, sem demora injustificada. Se a entidade não tiver já comunicado a violação de dados pessoais ao titular dos dados (nos casos em que esta comunicação é obrigatória), a CNPD pode exigir que proceda a essa notificação ou dispensá-la, nos casos previstos no artigo 35.º n.º 3.
6	**Notificar os titulares de dados (se aplicável)** Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica também a violação de dados pessoais ao titular dos dados, sem demora injustificada.	Uma das finalidades da comunicação aos titulares é limitar os danos que estes possam sofrer. A comunicação não é exigida se for preenchida uma das seguintes condições: a) A entidade tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados

	Esta comunicação deve descrever em linguagem clara e simples a natureza da violação dos dados pessoais e fornecer, pelo menos, as seguintes informações e medidas: a) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; b) Descrever as consequências prováveis da violação de dados pessoais; c) Descrever as medidas adotadas ou propostas pelo responsável de tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.	pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem; b) O responsável de tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares já não é suscetível de se concretizar; c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.
7	**Documentar a violação de dados pessoais** Este registo deve conter os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada.	Esta documentação deve permitir à CNPD verificar o cumprimento do disposto no art.º 33.º do RGPD. No seu ponto n.º 5 indica que devem ficar documentados: • Factos relacionados; • Respetivos efeitos; • Medida(s) de reparação adotada(s).
8	**Melhorar os processos internos**	Implementar, de acordo com a informação obtida, melhoria nos processos internos de modo a mitigar futuras violações de dados pessoais

Questionário sobre o Exercício CIBER PERSEU 2022

EXERCÍCIO CIBER PERSEU 2022

Com este breve questionário pretende-se obter feedback dos participantes GRA no Exercício CIBER PERSEU 2022 que decorreu de 14 a 17 de novembro de 2022.

Considera importante a participação do GRA neste tipo de exercícios?

- ◯ Sim
- ◯ Não

Acha que os objetivos iniciais foram atingidos durante o Exercício?

- ◯ Totalmente atingidos
- ◯ Maioritáriamente atingidos
- ◯ Parcialmente atingidos
- ◯ Não foram atingidos

Qual periodicidade que considera ótima para a participação neste tipo de exercícios?

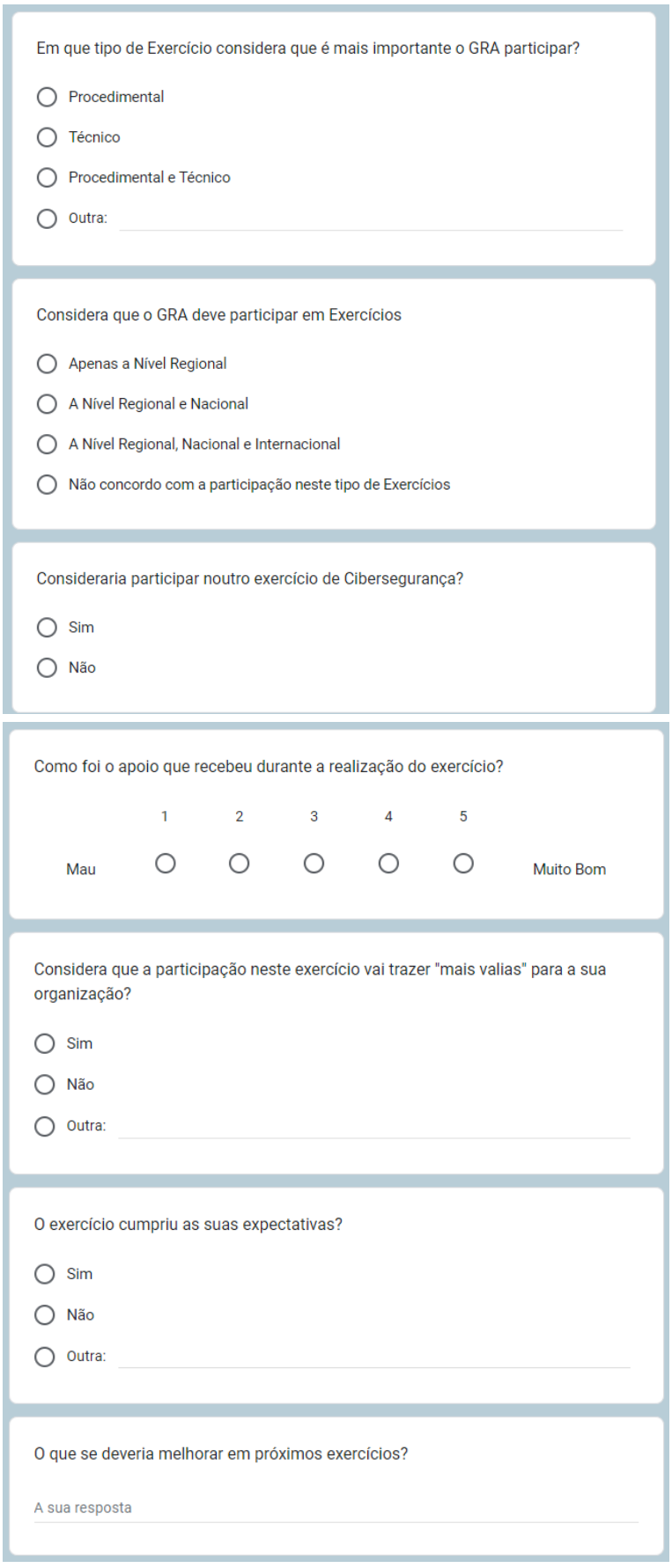
- ◯ Nunca
- ◯ Bi-anual
- ◯ Anual
- ◯ Semestralmente
- ◯ Trimestralmente
- ◯ Outra: _____

Como classificaria a organização do evento?

	1	2	3	4	5	
Mau	◯	◯	◯	◯	◯	Muito Bom

Como classifica informação recebida antes do evento?

	1	2	3	4	5	
Má	◯	◯	◯	◯	◯	Muito Boa



Em que tipo de Exercício considera que é mais importante o GRA participar?

- ○ Procedimental
- ○ Técnico
- ○ Procedimental e Técnico
- ○ Outra: _____

Considera que o GRA deve participar em Exercícios

- ○ Apenas a Nível Regional
- ○ A Nível Regional e Nacional
- ○ A Nível Regional, Nacional e Internacional
- ○ Não concordo com a participação neste tipo de Exercícios

Consideraria participar noutro exercício de Cibersegurança?

- ○ Sim
- ○ Não

Como foi o apoio que recebeu durante a realização do exercício?

	1	2	3	4	5	
Mau	○	○	○	○	○	Muito Bom

Considera que a participação neste exercício vai trazer "mais valias" para a sua organização?

- ○ Sim
- ○ Não
- ○ Outra: _____

O exercício cumpriu as suas expectativas?

- ○ Sim
- ○ Não
- ○ Outra: _____

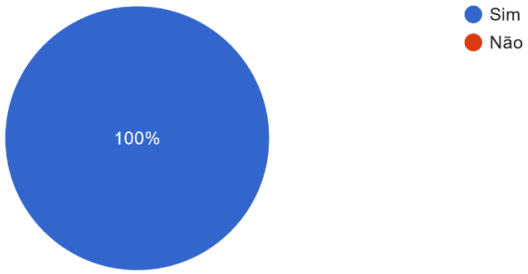
O que se deveria melhorar em próximos exercícios?

A sua resposta

Gráficos Respostas Questionário

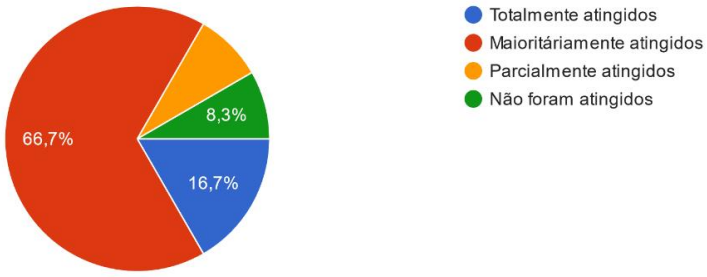
Considera importante a participação do GRA neste tipo de exercícios?

12 respostas



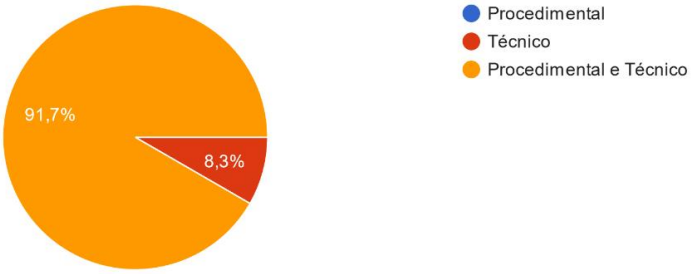
Acha que os objetivos iniciais foram atingidos durante o Exercício?

12 respostas



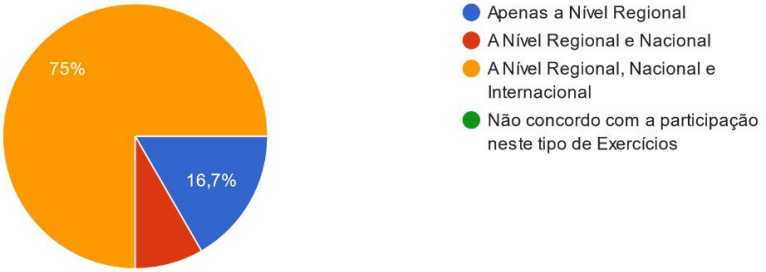
Em que tipo de Exercício considera que é mais importante o GRA participar?

12 respostas



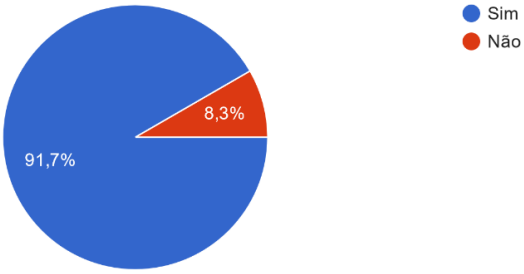
Considera que o GRA deve participar em Exercícios

12 respostas



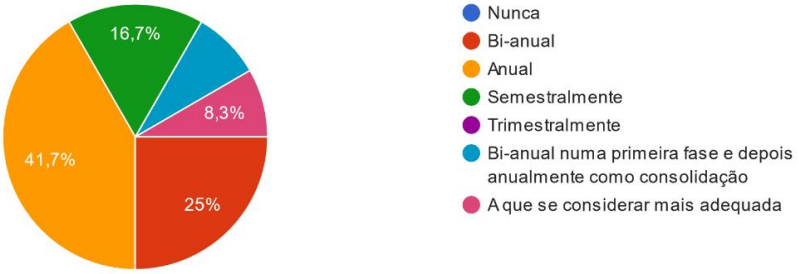
Consideraria participar noutro exercício de Cibersegurança?

12 respostas



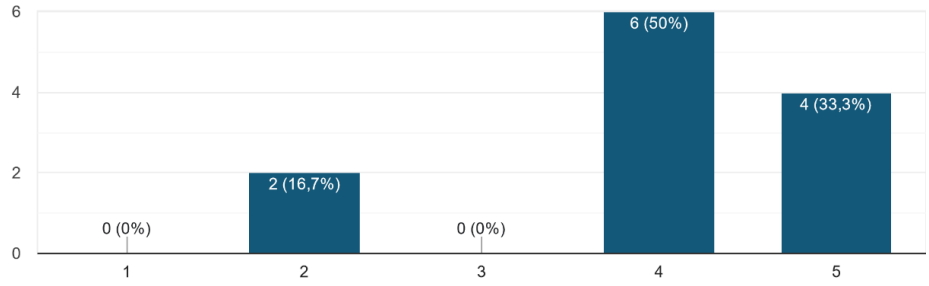
Qual periodicidade que considera ótima para a participação neste tipo de exercícios?

12 respostas



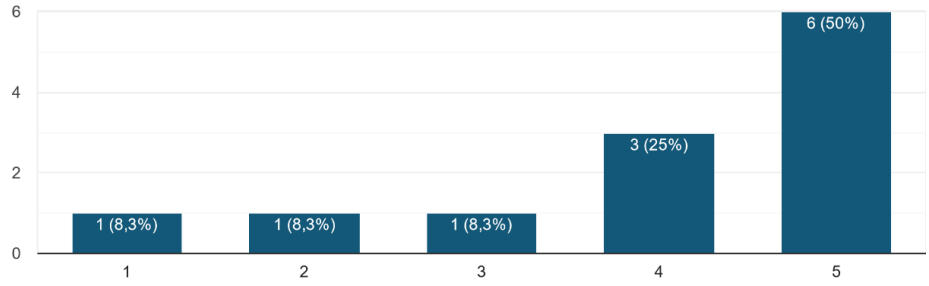
Como classificaria a organização do evento?

12 respostas



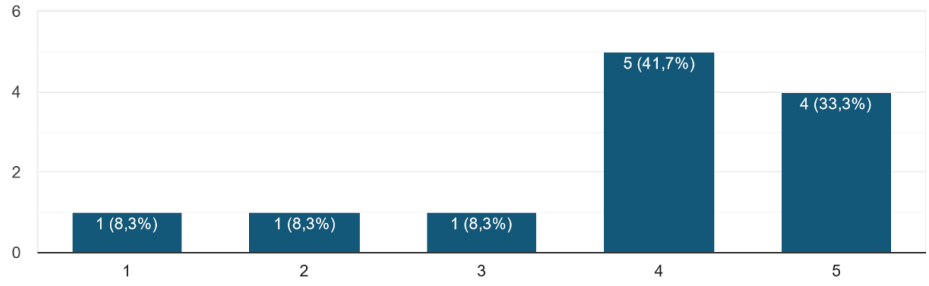
Como foi o apoio que recebeu durante a realização do exercício?

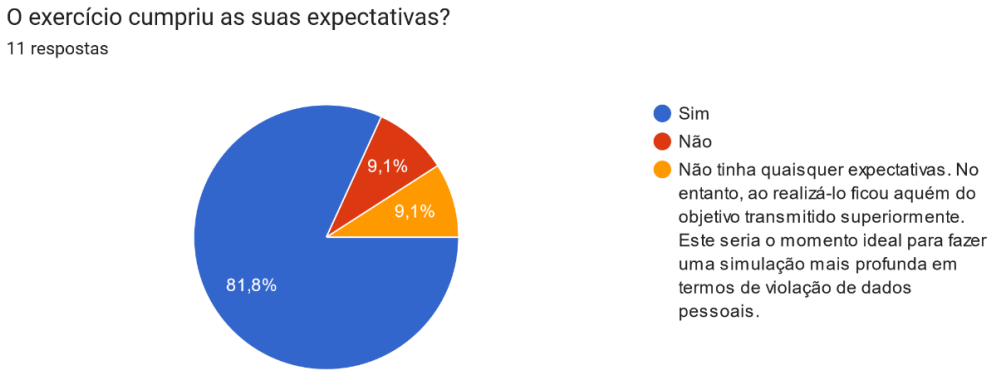
12 respostas



Como classifica informação recebida antes do evento?

12 respostas





Sugestões de melhoria propostas no questionário - 7 respostas

"Maior acompanhamento na realização dos exercícios técnicos."

"Mais presenças no local (*backoffice*) do exercício."

"A comunicação entre os participantes, a envolvência das equipas participantes, e, em especial, a utilização de incidentes diretamente relacionados com a atividade da organização, permitindo-se dessa forma que esta se coloque à prova, testando assim a forma como se encontra, ou não, preparada para responder a ataques reais."

"Melhorar o plano de comunicação e proceder-se à elaboração de um plano de circulação de informação interna na PGR, prevendo todos os casos possíveis."

"Informação atempada sobre o evento; Demasiados organismos na participação do evento; Simulação de uma situação de violação de dados pessoais até à entidade final (CNPD)."

"O Exercício foi bem organizado. Nas próximas iniciativas o serviço escolhido pelo GRA deve ser informado pelo menos 2 a 3 meses antes do exercício para efetuar toda a preparação possível. Deveria ser equacionado pelo GRA a criação de uma plataforma que concentre a gestão do registo de incidente e que possibilite a parametrização do fluxo correto de comunicação para os intervenientes e partes interessadas. O reporte e comunicação via email leva a erros de comunicação e de fluxo."

"Os exercícios técnicos, apesar de terem sido interessantes e realistas, deviam ter mais informação. As "dicas" que a plataforma dava eram inúteis na maioria das vezes."