Universidade Europeia
LAUREATE INTERNATIONAL UNIVERSITIES

Deception Technology: A Strategic Decision for Information Security

António Jorge Palminha Pinto (50033580)

Sistemas de Informação para a Gestão (M-SIG)

Dissertation Supervisor:
Professora Doutora Carla Manuela Carvalho Marques Pereira

June 2017

Acknowledgements

"Try not to become a man of success, but rather try to become a man of value." (Miller, 1955, p. 64), I humbly agree with the renowned physicist and Nobel Laureate Albert Einstein quote and would like to acknowledge everyone that contributed to "my value."

Love value comes from my dearest wife, Olga Pinto, that took this Master Degree endeavor as his one, facilitating all the time and availability possible, supporting me all the way. On our toughest moments, she gave me the strength to keep on going.

Family value comes from my daughter, Silvia Pinto, and my two granddaughters, Princess Mara and Ninja Matilde, they gave the support and love to feel like the "world's luckiest man" by having them in my life.

Professional and friendship value from my leader Paul Haywood that believed in me and made this Master Degree enrollment a reality.

Friendship value from of all my friends, that listened to my challenges as their own and gave a true meaning of, "Friends Are The Family You Choose."

Resilience value from my sister-in-law, let's just call her my sister, Sónia Rodrigues that, from inside the biggest fight of his life, always had the love to encourage me and gave me the final push to finish this dissertation.

Collaboration value of the SPMS Management, Drº Rui Gomes e Drº Bruno Soares, my gratitude for the sympathy, knowledge sharing and by investing the required time on this dissertation.

The educational value of the Laureate International Universities, Liverpool and Lisbon campus, and all the teachers that had the skills and techniques to share their knowledge successfully.

Friendship and guidance value from my dissertation supervisor, Carla Pereira, my gratitude for his patient and all the assistance, I hope she feels proud with this dissertation.

To everyone that contributed to my value as a father, grandfather, husband, a person, a professional, a friend and an academic, I truly appreciated, please have my deepest gratitude.

General Index

List of Figures

List of Tables

List of Acronyms

APT	Advanced Persistent Threats
AR	Action Research
EDR	Endpoint Detection and Response
CISO	Chief Information Security Officers
DBA	Database Administrator
DCT	Deception Technology (as the main topic)
DS	Design Science
DSR	Design Science Research
DSR	Design Science Research
ENF	Enterprise Network Firewall
IDS	Intrusion Detection Systems
IFM	Infrastructure Manager
IPS	Intrusion Prevention Systems
IS	Information Security
ISOC	Intelligence-driven Security Operations Centers
IT	Information Technology
MSSP	Managed Security Service Providers
NTM	Network Manager
URL	Uniform Resource Locator
SOC	Security Operation Center
SA	Systems Architect
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SPMS	Serviços Partilhados do Ministério da Saúde, EPE
SR	Survey Research
VLAN	Virtual Local Area Network
WHH	White Hat Hacker

Resumo

A utilização de recursos informáticos é a estratégia mais comum à maioria das organizações para gerirem os seus ativos e propriedade intelectual. Esta decisão estratégica implica a sua exposição ao exterior através de canais de comunicação (infraestrutura de dados).

McDermott e Redish (1999), descrevem a terceira lei de Newton como o princípio da ação - reação, as organizações ao exporem a sua infraestrutura ao exterior despoletaram, como reação, estranhos quererem aceder à sua infraestrutura para diversos fins, seja como puro divertimento, detetarem fragilidades ou, mais relevante para este trabalho, roubarem ativos/propriedade intelectual e criarem uma disrupção no serviços.

As organizações sentem necessidade de se protegerem contra estes estranhos/ataques ao implementarem estratégias de segurança, mas a realidade é que as linhas de defesa da rede são permeáveis e as arquiteturas de segurança não são suficientemente dinâmicas para travar as ameaças existentes.

Uma estratégia de segurança informática baseada na tecnologia "Deception" poderá permitir de uma forma rápida detetar, analisar e defender as redes organizacionais contra-ataques em tempo real. Esta tecnologia "Deception" poderá oferecer informações precisas sobre "malware" e atividades maliciosas não detetadas por outros tipos de defesa cibernética.

Este trabalho pretende explorar esta estratégia recente baseada em "Deception", que pretende ser diferenciadora face à panóplia de dispositivos/software de segurança informática existentes.

Como resultados, pretende-se elaborar uma análise onde as organizações possam perceber a tecnologia "Deception" nas suas vertentes da eficácia, eficiência e o seu valor estratégico para que, eventualmente, a possam utilizar para suportar/adicionar valor a uma decisão de estratégia de segurança informática.

Palavras Chave: Information Security, Deception, Cyber-threat, Cyber-crime, Cyber-Incident

Abstract

The use of Information Technology (IT) resources are the common approach for most organizations so they assets and intellectual property are properly managed. This strategic decision implies its exposure to the outside world through the data infrastructure.

McDermott and Redish (1999), described the third Newton's law as the principle of action-reaction, when organizations expose their infrastructure to the outside world and, as a response, strangers want to access their infrastructure for various purposes, either as pure fun, detect weaknesses or, more relevant for this work, steal assets/intellectual property.

Organizations feel the need to protect themselves against these strangers/attacks by implementing security strategies, but truly, the network's first defense lines are permeable, and the security architectures are not dynamic enough to face existing or future threats.

A Deception-based technology could enable the organizations to quickly detect, analyze and defend organizational networks against real-time attacks. Deception technology may provide accurate information on malware and malicious activity not detected by other types of cyber defense.

This work intends to explore a new technology, Deception, that claims a differentiation when compared with the range of existing information security suite. The types of cyber-threats and their materialization could be relevant to the information technology and risk analysis.

Thus, the intent is to elaborate an analysis where organizations can understand the Deception technology, his effectiveness, and strategic value so they can, eventually, use it to support/add value to a decision regarding information security strategy.

Key Words: Information Security, Deception, Cyber-threat, Cyber-crime, Cyber-Incident

1. Introduction

1.1 Motivation

Dinicu (2014) stated that the cyber-attack is the “Achilles heel” of the modern state security, highly technologized and well developed, whose biggest problem is, in this matter, the proper and precise identification of the source, and the problem becomes more complicated as the attack is becoming more sophisticated.”

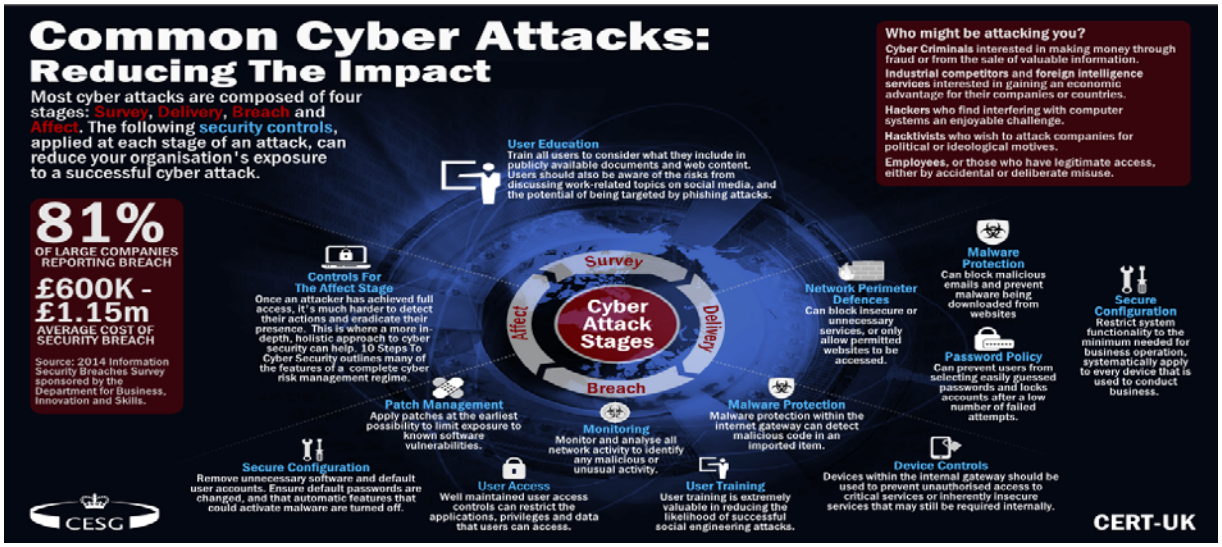


Figure 1. Common Cyber Attacks (Source GOV.UK)

Kopp (2000) states that Information Warfare is particularly impacting the world order in the sense that intellectual/military property is being used to target nations and organizations in such a way that business advantage and military dominance are just two clicks away from being destroyed.

The cyber-crime trend is increasing in the sense that more and more attacks are occurring. Additionally, the cyber-threats are increasing, the number of “zero-day” vulnerabilities reported exposes how vulnerable the network perimeter is even with an aggressive patching policy.

All the available information lead to the assumption that the organization's first line of defense is not performing as expected, allowing the attackers continuous access to assets and intellectual property impacting the organizations at a brand and financial levels.

1.2 Problem

The cyberspace attackers techniques are dynamic as they are supported by a large community of experts and by continuous research that not bound to formal software development so can be used very quickly, the information security architectures are not. The lead time between an attack and the detection of that attack, by the organization's security teams, are immense, if ever. The disruption provoked by the cyber-incidents affects everyone from financial organizations to life support devices.

1.3 Objective

Identify the Deception Technology (DCT) main features and the applicability to the problem statement. Identify an organization to test the concept and derive the results. Add testimonial, Use Case and Proof of Concept to strength the arguments.

1.4 Proposed Solution

Deception technology was considered as a proposed solution by questioning the status quo regarding the information security suite of tools that are not performing as expected. Based on the number of cyber-incidents, and change the paradigm from protecting the network and stop an attacker from penetrating the environment too, also, assume that all the attacks cannot be stopped, and an intrusion will occur eventually.

A Deception technology based solution that reduces the intrusion detection time performs better than a human-based solution and exposes quality information to prevent future attacks.

Deception technology pairs with the information security suite of tools adding a layer of protection reveal the attacker when they are already inside the network.

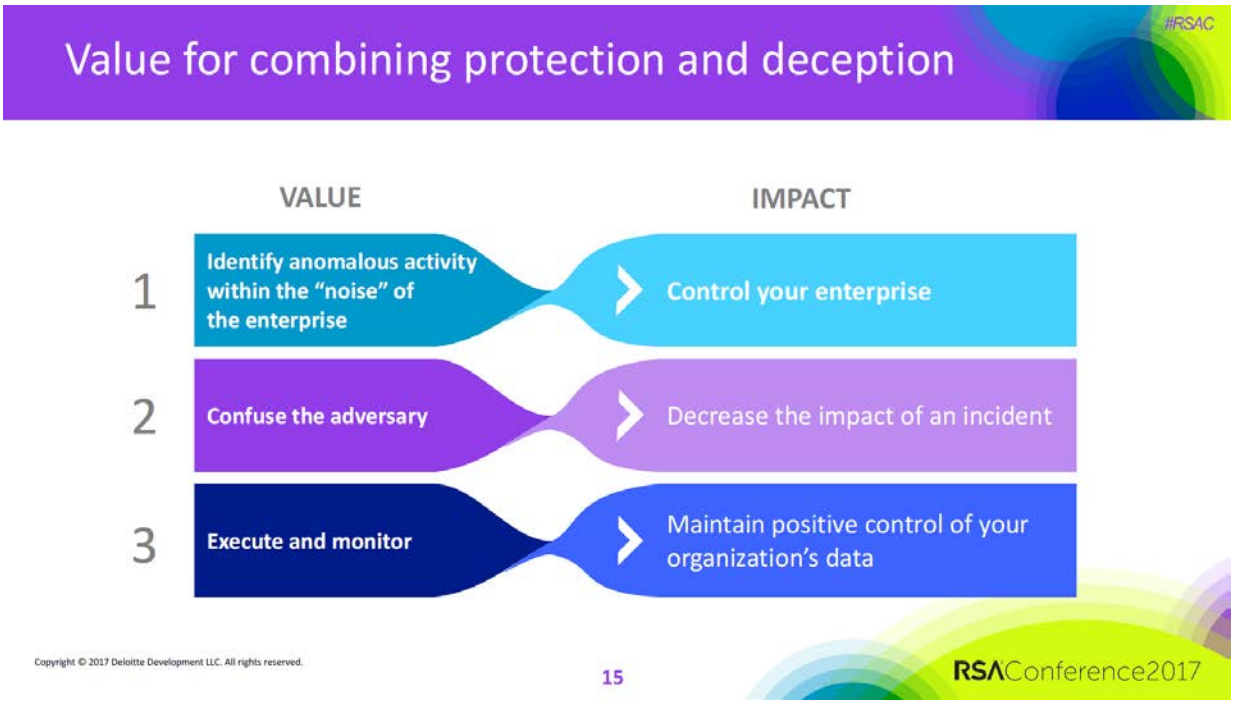


Figure 2. Deception Value (Source RSA Security Conference 2017)

1.5 Document Structure

This work is a structure of seven(7) chapters. First, the **Introduction,** where the motivation to write this work is highlighted, followed by the problem statement and solution proposal, finished by the projected goals.

The next chapter is the **Literature Overview;** the domain is put into a context to induce the correct mindset for this work. The relevant, for this work, knowledge areas are also referred to understand the top IS technologies, actors, threats and the Deception technology.

On the **Methodology** chapter, the method is referred along with the theoretical map, assumptions and the path to reach the goals.

After the Methodology chapter, the **Results** chapter describe what was achieved by describing the artifacts and expectations.

The **Conclusions and Future Work** chapter describe the insights and wrap up this work, ended by a projection on what could be logical next investigation steps.

The references list can be found in the **Bibliography** chapter;

Inside the **Appendix** chapter holds mainly the SPMS supporting documents and some tables used but more readable.

2. Literature Overview

2.1 Research Methodology

2.1.1 Building on Prior Research

The body of the investigation, both within the Information Security and Network Security literature and in the neighborhood disciplines, did not provide the traditional support for this work. The technological component Deception, part of the proposed solution, is a recent evolution of a more old concept, Honeypot, but only at a conceptual level. The intention is to adopt a research strategy that will address the objectives but also the challenges of this work, so an analysis touching research methodologies are mandatory to leverage any relevant for this work methods, techniques.

2.1.2 Methodology Landscape

The scientific method is based, in part, on the ability to replicate a particular research. Specifically, in order to fully replicate a research, other researchers must know the Who, What, Where, When, and How. In short, a methodology provides a blueprint for conducting research based on other using the same framework of procedures and techniques by setting a shared understanding across the community. By reaching this baseline, researchers can infer the results using a common background.

A methodologic approach is defined by a logical and systematic mindset that focuses on the content, mainly on the techniques and methods used.

Research is scientific when it employs the scientific method. The key to the scientific method is replicability. A method is scientific to the extent that procedures are described objectively and in detail so that another investigator may repeat and independently verify results. A method to be scientific must be valid and reliable. Validity is the degree to which scientific observations actually measure or record what they purport to measure, and reliability is the repeatability, including interpersonal replicability of scientific observations, (Reswick, 1994).

2.1.3 Quantitative and Qualitative Methodologies

Pickard (2007) echoes a fairly basic standpoint that there are only two basic methodologies: quantitative and qualitative. The choice between these two is the highest level methodological decision. The metatheoretical assumptions discussed in the previous chapter have a strong influence on this methodological choice.

2.1.3.1 Quantitative vs. qualitative

It is true that quantitative research is usually associated with the physical and biomedical sciences while qualitative research is found mostly in the social sciences. But neither is exclusive of the other. In fact, a great deal of social science research is highly quantitative involving, as it does, advanced statistical methods (Reswick, 1994).

Quantitative and qualitative research differ in at least three major ways:

1. The processes are different
2. The tools are different
3. The outcomes differ

Characteristic	Quantitative	Qualitative
Metatheory	Positivist, Postpositivist	Interpretive
Nature of reality	Singular, stable, independent of observer; external reality	Multifarious, culturally determined, socially constructed; holistic reality,
Relation of investigator to what is studied	External, observing from outside; in artificial setting	In the study setting, observing from within; in real-life setting
Relation to social phenomenon	Neutral Empirical	Engaged Normative
Research aim	Nomothetic; hypothesis testing; generalizing	Idiographic; hypothesis generating; contextualizing
Strategies	Structured, theory-derived variables identified beforehand; controls; operationalization & measurement	Unstructured, open-ended, theory developed during research; concepts that are rich in meaning
Typical methods	Experiments, surveys	Participant observation, case studies
Criteria for judging research	Validity & Reliability; objectivity	Credibility, transferability, dependability; authenticity

Table 1. Quantitative Research vs. Qualitative Research (Reswick, 1994)

As shown in *Table 1*, the quantitative research process is linear and unidirectional. In automatic control theory, it would be termed "open loop." The quantitative researcher is able to isolate the experimental or study system, define the parameters, and select and measure relevant variables with precision and accuracy; The thinking process is essentially deductive following a creative act of hypothesis formulation, (Reswick, 1994).

As shown in *Table 1*, the inductive character of qualitative research and its interactive or closed-loop feedback nature. The qualitative researcher cannot define the system and its variables with the relevancy and accuracy of the quantitative researcher. Therefore, creates an original theory (based perhaps on intuition and experience), and proceeds to organize the study, apply tools, and gather data. As data accumulate and are reduced, the researcher may well redefine the model and alter the study design employing a refining method called comparative analysis, (Reswick, 1994).

The quantitative researcher may work in the laboratory with instruments that measure quantities with precision and accuracy. Statistical methods provide tools to measure reliability and validity of results.

The qualitative researcher is likely to include questionnaires, focus groups, interviews, and personal participation and observation.

The outcome of quantitative research is usually a true test of an a priori stated hypothesis.

The results of qualitative research is a grounded theory. The process starts with a theory based on experience and intuition. It ends with a theory that is grounded in data. If the data are reliable and valid and the study can be replicated by others, then the theory is credible, and the process is scientific (Reswick, 1994).

2.1.4 Main Research Methodologies under Analysis

The approach for the analysis is a tabular format for each of the methodologies for a more easy identification of the key aspects, the naming, characterization with reference authors and applicability will be part of the analysis.

Here, the Behavioral science methodology was not considered due to his focus on psychology, social neuroscience, and cognitive aspects, not aligned with the scope of this work.

A final table with the key dimensions of each methodology will drive the approach for this work, either a pure or a mixed approach as defended by (Nabukenya 2012).

Figure 3. Research Methodologies under Analysis

2.1.4.1 Design Science (DS)

Summary Table of Research Methods: Characterization and Applicability		
Research Method	**Characterization**	**Applicability**
Design Science (DS)	Systematic way of designing or designing things **(Fuller and McHale 1965)**	Predominance in the area of information systems because is an agregator of people, organisations and technology
	Create knowledge about the design process, general or specific, particularly relevant to design tasks, and aims to develop artefacts that originate satisfactory solutions for practical problems **(Gregory 1966)**	
	Use of artifacts that are "artificial objects that can be characterized in terms of goals, functions and adaptations. They are usually discussed, particularly during the concession, both in imperative terms and descriptives... "thereby giving"... fulfillment of a purpose, or adaptation to a goal. Involves a relationship of three elements: the purpose or purpose, the character of the artifact and the environment in which it works... "IE"... an artifact can be regarded as a meeting point-interface-between an internal environment, the substance and organisation of the artifact itself, and an external environment, this is the conditions under which the artifact works... **(Simon 1996)**	

Table 2. Design Science (DS) Summary

The DS process clearly defines the path, from the identification of the situation, the definition of the problem. Ahead, the loop until the present state is defined, retro-feed the problem definition moving to a preferred system design, with inputs from the inventory alternatives and evaluation criteria. After developing the implementation strategies, the process is documented, the artifacts developed, and the plan is communication. Finally, a larger planning process is initiated.

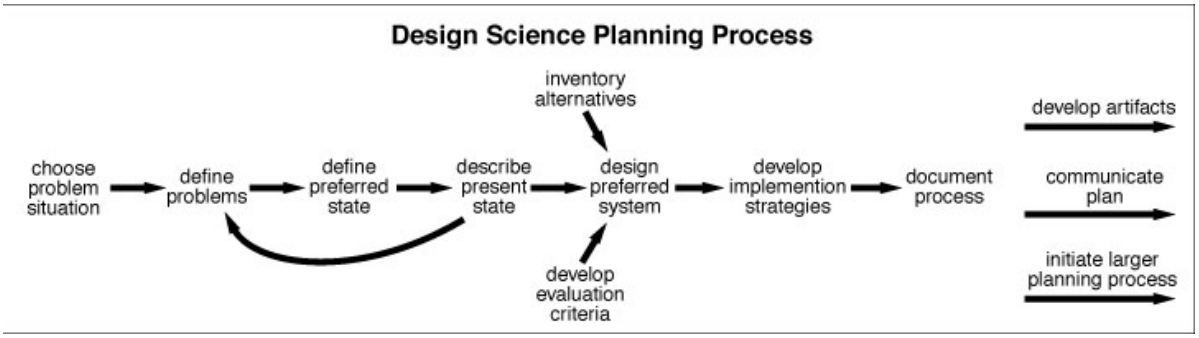


Figure 4. Design Science Planning Process (Simon, 1996)

2.1.4.2 Design Science Research (DSR)

Summary Table of Research Methods: Characterization and Applicability		
Research Method	**Characterization**	**Applicability**
Design Science Research (DSR) **DS Evolution**	Evolution of activities through the DSR methodology, in the construction phase and after defining the problem, leads us to the definition of the objective seeking the development of the best artifact, then we have the evaluation phase with the use of the artifact for the solution of the problem By evaluating the effectiveness/efficiency and ending with the communication of its outcome, it can be done or back to the construction phase. **(Vidgen et al. 2012)**	Main purpose of creating artifacts, ensuring rigour and transparency so that the knowledge obtained in addition to technological, scientific and aims to respond to the questions formulated in the search for the expected outcome.
	Implements three research cycles: • The review cycle begins research in an application context by providing the requirements for research and defines the criteria for acceptance of the evaluation of the research results; • The rigor cycle provides scientific knowledge for the research project in order to ensure its innovation; • Design cycle iterates through the main activities of the construction and evaluation of design artifacts and research processes. **(Hevner et al. 2004)**	
	New look or a set of analytical techniques that allow the development of research in the various areas, particularly in engineering. The DSR aims to study, research and investigate the artifact and its behaviour, both from academic and organisational perspective. Accordingly, the DSR is a rigorous process of designing artifacts to resolve problems, assessing what was designed or what is functioning and communicating the results obtained **(Kuechler and Vaishnavi 2011)**	

Table 3. Design Science Research (DSR) Summary

The DSR cycle uses the domains Environment and Knowledge Base as inputs, in a loop where the organizations and scientific knowledge come together to produce artifacts and processes.

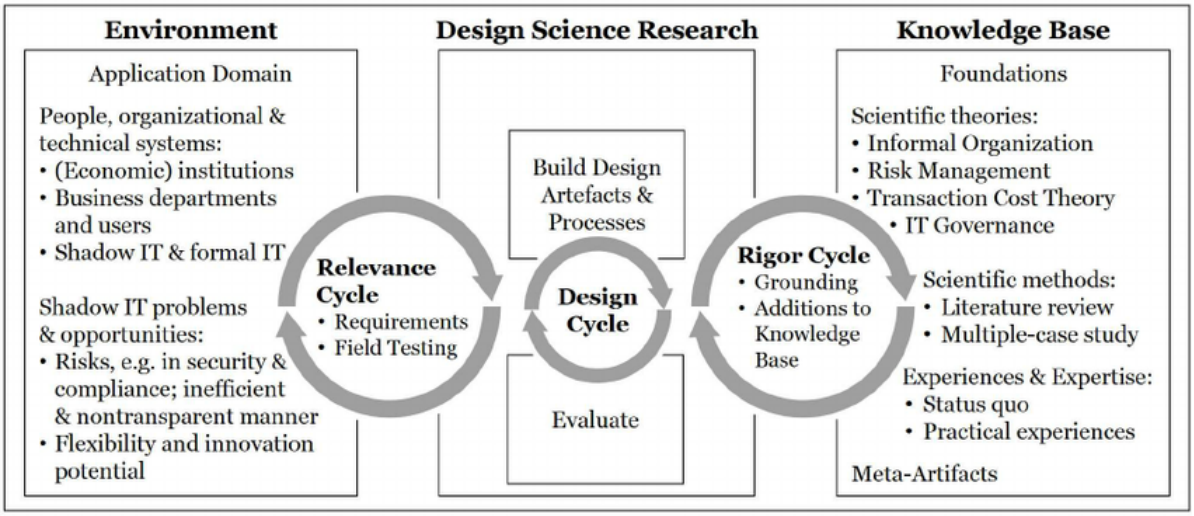


Figure 5. Design Science Research Cycle (Hevner et al. 2004)

2.1.4.3 Case Study Research (CSR)

Summary Table of Research Methods: Characterization and Applicability		
Research Method	**Characterization**	**Applicability**
Case Study Research (CSR)	• Phenomenon observed in its natural environment; • Data collected using various means (direct and indirect observations, interviews, questionnaires, audio and video logs, journals, letters, among others); • One or more entities (person, group, organisation) are analyzed; • The complexity of the unit is studied thoroughly; • Research directed at the stages of exploration, classification and development of assumptions of the knowledge building process; • Experimental forms of control or manipulation are not used; • The investigator does not need to specify the set of dependent and independent variables in advance; • The results strongly depend on the power of integration of the investigator; • Changes may be made to the selection of the case or data collection methods as the investigator develops new hypothesis; • Research involved with issues "how?" and "Why?" unlike "What?" and "How many?" **(Benbasat, I., Goldstein, DK and Mead 1987)**	Uunderstand, explore or describe **complex events and contexts** with the involvement of **several factors** being widely used in the **studies of an interpretative/qualitative nature**, but also in quantitative and qualitative studies
	Empirical research that investigates a contemporary phenomenon within its real life context, especially when the boundaries between phenomenon and context are not so evident., and may be classified as predominantly qualitative and observatory, **(Nabukenya 2012**).	
	Look at social reality through a range of techniques, as interviews, observations, investigations and data gathering, constituting a "... means of organizing the social data by preserving the unitary character of the studied social object... an approach that considers any social unity as a whole [...] [E] includes the development of this unit, which can be a person, a family or a social group, a set of relationships or processes (such as family crises, adjustment to illness, friendship formation, ethnic invasion of a neighbourhood etc.) or even a culture [...], **(Goode and Hatt 1958)**	

Table 4. Case Study (CSR) Research Summary

The CSR defines himself by stages where on the first four(4) can be considered preparation and the final two(2) the data collection, analysis and final considerations and reporting.

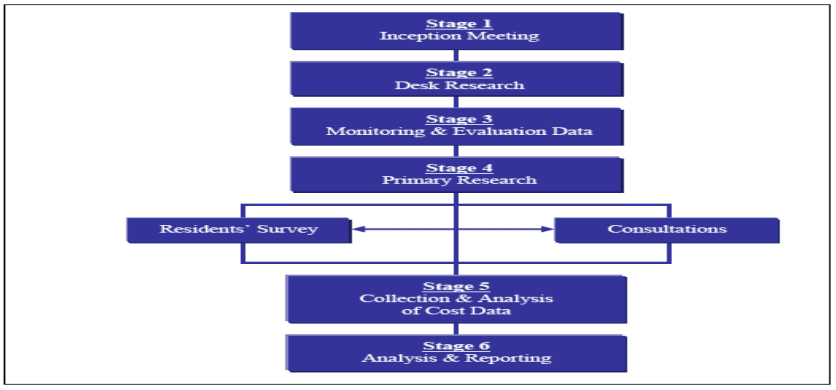


Figure 6. Case Study Research (Nabukenya 2012)

2.1.4.4 Action Research (AR)

Summary Table of Research Methods: Characterization and Applicability		
Research Method	**Characterization**	**Applicability**
Action Research (AR)	Process in which participants examine their own educational practice systematically and carefully, using the techniques of research. It is based on the following assumptions: • Teachers and principals work best on problems they have identified for themselves • Teachers and principals become more effective when encouraged to examine and assess their own work and then consider ways of working differently • Teachers and principals help each other by working collaboratively • Working with colleagues helps teachers and principals in their professional development **(Watts, 1985, p. 118)**	Action research happens at the place where these questions arise, it happens where the real action is taking place and it allows for immediate action.
	Work that did not separate the investigation from the action needed to solve the problem. **(McFarland & Stansell, 1993, p. 14).**	
	Cyclical process involving a "non-linear pattern of planning, acting, observing, and reflecting on the changes in the social situations" **(Noffke & Stevenson, 1995, p. 2).**	

Table 5. Action Research (AR) Research Summary

Looking at AR cycle, we see an endless improvement loop that starts with the problem identification and ends with results evaluation and next steps.

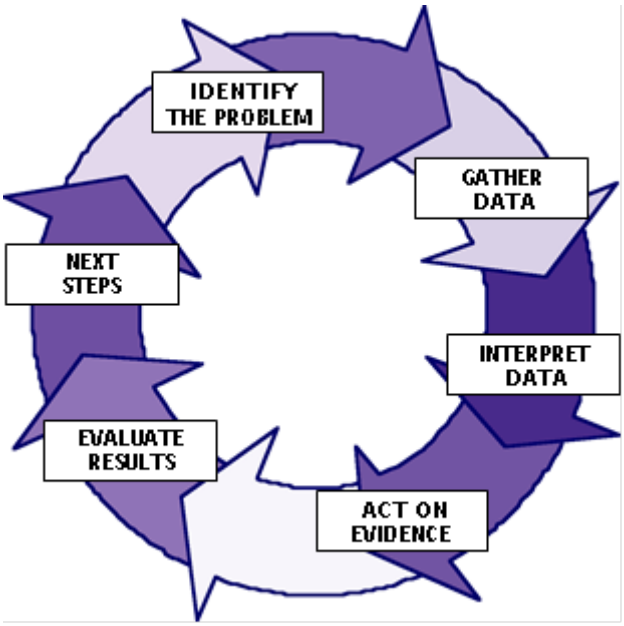


Figure 7. Action Research (AR) Cycle (Noffke & Stevenson, 1995, p. 2)

2.1.4.5 Comparison Analysis

Based on (Nabukenya 2012) and (Hevner et al. 2004), The comparison of the main research methodologies, previously considered, enables the distinction between them based on the following criteria:

- Knowledge Base
- Empirical Knowledge
- Researcher Role
- Researcher / Object of Study Collaboration
- Objectives
- Main Tasks
- Results
- Results Evaluation
- Methods
- Deployment

Research Methologies - Comparison Table				
Components / Research Method	Design Science (DS)	Design Science Research (DSR)	Case Study Research (CSR)	Action Research (AR)
Knowledge Base	- How things should be	- Operates how things should be	- How things are or how they behave	- How things are or how they behave
Empirical Knowledge	- Not required	- Not required	- Required	- Required
Researcher Role	- Artifact Builder and Constructor	- Artifact Builder and Constructor	- Observer	- Multiple, depending on the type of Action Research
Researcher / Object of Study Collaboration	- Not required	- Not required	- Not required	- Required
Objectives	- Develop artifacts that allow satisfactory solutions to practical problems	- Develop artifacts that allow satisfactory solutions to practical problems	- Assist in understanding Complex social phenomena	- Solve or explain problems of a given System giving rise to knowledge
	- Prescribe	- Prescribe	- Explore	- Outputs practice and theory
	- Design	- Design	- Describe	- Explore, describe and explain
		- Operationalization	- Explain	
Main Tasks	- Raise awareness	- Raise awareness	- Define conceptual structure	- To plan
	- Suggest	- Suggest	- Plan	- Collect data
	- Develop	- Develop	- Pilot project	- Analyze data
	- Evaluate	- Evaluate	- Analyze the data	- Implement
	- Conclude	- Conclude	- Final report	- Evaluate
				- Continuous monitoring
Results	- Artifacts	- Artifacts	- Constructors	- Constructors
	- Constructors	- Constructors	- Hypotheses	- Hypotheses
	- Models	- Models	- Descriptions	- Descriptions
	- Methods	- Methods	- Explanations	- Explanations
	- Instantiations	- Instantiations		- Actions
Results Evaluatioon	- Applications	- Applications	- Confronting the theory	- Confronting the theory
	- Simulations	- Simulations		
	- Proof of Concept	- Proof of Concept		
Methods	- Qualitative and / or Quantitative	- Qualitative and / or Quantitative	- Qualitative	- Qualitative
Deployment	- Not required	- Not required	- Not applicable	- Required

Table 6. Research Methodologies - Comparison

The main differences can be identified in the knowledge base, objectives, results in the evaluation, in the role of the researcher and the necessity of an empirical basis (based on experience). Design Science and Design Science research are very identical, but the second operational as things should be. The case study aims to assist the understanding of phenomena and action research focuses on solving a particular problem arising from knowledge.

2.1.4.6 Main Research Methodologies Analysis Conclusion

The analysis of the four(4) main methodologies highlights:

- Case Study Research(CSR) or Action Research(AR) can be used for descriptive, explanatory or predictive research objectives;
- For prescriptive objectives or technology artifacts development, Design Science Research(DSR) is a more appropriate strategy;
- Case Study Research(CSR) could be used for prescriptive or objective development to enable the comprehension of existing artifacts;

Design Science Research targets investigation questions related to the rigor and the body of knowledge for which the research project contributes. As the main objective, overcome the limitations of both human and organizational capacities, creating new artifacts or developing existing artifacts.

Due to the nature of the present work, technological domain, the most applicable research methodology is Design Science Research(DSR), that validates the work against the scientific research criteria. On the variation Qualitative, Design Science Research(DSR) reveal himself to be more adaptable to the environment and nature of the investigation.

2.2 Domain Contextualization:

In this chapter, a contextualization of the domain, expressed by several authors, will add the necessary supporting knowledge base to enable different technical backgrounds to access to the contents of the work. Additionally, a general overview of literature that is contextual to this work aims a background vision about information security and dominant strategies concerning the first line of defense against cyber-attacks.

Main Artifacts:

- Relevant actors
- Cyber-Threats Types
- Advanced Persistent Threat (ATP)

2.2.1 Relevant actors

2.2.1.1 Information Security (IS) Team

Playing the role of the perimeter defender, implementing the IS security strategy, defined and approved by the management. The IS Team as two main skill sets and subdivided into two main teams, the Blue and the Red Teams.

From the military, the Blue Team is the “regular” forces, Database Administrator (DBA), Systems Architect (SA), Infrastructure Manager (IFM), Network Manager (NTM) and other peer roles. On the other side, the highly skilled and organized Red Team, which adopts an attacker’s mindset. (Mirkovic et al., 2008).

2.2.1.2 Attackers

2.2.1.2.1 Black hat hacker

Black hat hackers, or simply “black hats,” are characterized by an intrusive attitude aiming to break the IS protective layer for personal or organization gain (credit card numbers, intellectual property or personal data for sale). Another goal is the attacks against websites for real service disruption. The black hat hacker's goal is to find a new, “zero-day” security vulnerability that would be attractive for the criminal organizations or to use to compromise computer systems (Bratus, 2007).

2.2.1.2.2 White hat hacker(WHH)

White hat hackers are experts in IS systems, use their abilities for good, ethical, and legal purposes rather than wrong, unethical, and criminal purposes.

IS Teams include on his Red Team white-hat hackers responsible for testing the perimeter just as a black hat hacker would. This approach is known as “penetration testing.”

A white hat hacker who finds “zero-day” security vulnerability would disclose it to the organization, allowing them to apply the necessary patch (Bratus, 2007).

2.2.1.2.3 Gray hat hacker

The definition point us to someone that mixes a black and white profiles, they perform with a white hat mindset, but they may, technically, commit crimes and do arguably unethical things.

A gray hat hacker might attempt to compromise a computer system, without permission, informing the organization after the fact and allowing them to patch the system. The gray hat tries to compromise an IS without permission, which is illegal (Bratus, 2007).

2.2.2 Cyber-Threats

Based on the State of Cyber Security: Emerging Threats Landscape Paper, (Ahmad, Yunos, Sahib, & Yusoff, 2015).

2.2.2.1 Phishing and email Spamming

Phishing and email Spamming defines a type of threat through the internet, or flooding of the Internet or any unwanted online correspondences. The requests gather client’s credentials using a deception technique. Phishing is an Internet fraud in such a way that the attacker will acquire details like stealing passwords, credit card numbers, bank account details, and other private information. In recent times, law enforcement agencies and the judiciary appear to be taking cybercrime more seriously.

2.2.2.2 Botnet

A Botnet is a guard of compromised Systems, sometimes called “zombies,” that are under the command and control of a solitary “Botmaster.”. A botnet is an accumulation of computers networked together that are no doubt regulated by Cyber-criminals for malicious and unlawful purposes. Botnets are currently turning into a key threat for the cyber-crime since they are designed deliberately to disturb targeted computer systems. Many infected computers can figure out how to disturb and disseminate malicious code, virus, and spam.

2.2.2.3 Malware and Spyware

These are a malicious program designed to gather computer information without the awareness of the client. Malware is one of the key threats to Businesses, Governments, and people. For instance, in 2009 the number of new malware signatures was accounted to be just under 2.9 million, a 71 percent increase over 2008, yet Symantec discovered more than 286 million new malware variants in 2010.

2.2.2.4 Keyloggers

Keyloggers are programs that can screen and record the client keyboard information while typing in Computer System for later access. Key loggers store the data or send the information secretly to the other programs. They can record user names, messages and secret key for remote systems and computer application. Some key loggers oblige the right to gain access to the criminal invader or attacker to get the data from the machine while other forcefully transfers the data to different machines using email; file transfers and so forth. Sagiroglu and his Colleagues further find out that the personal use of keyloggers can be beneficial, because the use of culture may assist private computer owner to enhance his daily routine with much privacy. By using a keylogger is possible to recuperate content wrote into word processors, spreadsheets, and computer programming environment after an application or system crash.

2.2.2.5 Social Engineering

Social engineering is a kind of technique in which it traps or tricks the client to reveal valuable information. The user will think the reason is honest to goodness yet the aim is truly criminal. “SE relies on the trusting nature of individuals as it depends on getting unapproved secret information through mimicking people using Nontechnical means; Consequently, the SE is viewed as the human side of breaking into a corporate network.” (Okenyi & Owens, 2007).

2.2.2.6 Denial of Service

Denial of Service is an attack that upsets the normal function of the computer system and thus prevents access to authorized users. DoS is an incident in which a Client or organization is deprived of the services of a resource they would regularly expect to have. DOS is legitimately a resource overloading attack that may have the likelihood of either smashing the host such that it cannot communicate properly with the rest of the System, in this way the services may remain inaccessible to customer clients.

2.2.2.7 Virus

A virus is a program that spreads itself from one computer to another computer without the users’ authorization to do so, and they distribute themselves to the infected files or programs on a PC. Viruses cause a negative and unforeseen event when the machine runs. Different kind of viruses has a distinctive purpose. Some are designed to trap clients, and some are designed to destruct Machine programs. They can harm computer programs, and they activate himself through email attachments. Consequently, computer viruses can additionally spread by connecting itself to executable files of systems areas, to external storage devices such as USB drives.

2.2.2.8 Worm

A worm is usually a computer Program that moves from one machine environment, then onto the next machine environment often keeping a record of the last environment, it has entered. Worms are self-duplicating programs towards oneself, which essentially implies that they do not require a host program to attack a victim. When a worm moves to another environment, it can do whatever it needs as per the obligatory access controls. In the case of Virus, it requires human intervention, but worms do not, and it moves around via the internet connection.”.

2.2.3 Advanced Persistent Threat (ATP)

An APT is characterized as continuous computer hacking that is actively supported by several people that usually targets one specific entity. They are engineering their attack to breach the perimeter defense successfully.

Their goal is to place malware (spyware) on one or more computer elements for an extended period, to utilize these items to seek out valuable information for compromise actively, and then to extract (exfiltrate) that information. Persistent means that they almost always have a specific target in mind and they are continually working to move their objectives forward. ATP is an attack targeted from the very beginning.

The cyber-defense teams still don’t have new tools that enable them to discover APTs or zero-day events before the severe damage occurs.

APTs move silently through the organization and steal data which they target and discover.

APTs only need one entry point to get past the perimeter defense.

Once inside, most of the legacy technology will not detect their movement in areas such as the Virtual Local Area Network (VLAN).

APTs can move silently within the corporate network and can remain undetected for months or even years.

2.3 Knowledge Areas:

- Cyberspace
- Information Warfare
- Cyber Attack
- Cyber Event
- Cyber Terrorism
- Network Security and Cyber Security Differences
- Tactical Deception

2.3.1 Cyberspace

The cyberspace as becoming the area where all organizations need to be to do business, additionally, social media, email, and other technologies are also being used by many. This reality opens opportunities for attackers to strike effectively, inexpensively with little risk. Also, states and non-state actors turn to cyberspace to conduct warfare with greater frequency (Gervais, 2012).

Kuehl, (n.d.) collected and analyzed the various definitions leading him to conclude that cyberspace is more than just computers and digital information and that there are several aspects of cyberspace:

- Operational
  Organizations use cyberspace to do business and drive behavior
- Information based
  Cyberspace is used to create, store, modify and exchange information
- Networking
  The existence of networks enables information and assets communication

Figure 8. Cyberspace is everything out there (Source Shutterstock)

A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies."

2.3.2 Information Warfare

"The strategic, operational, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives." (Libicki, 1995).

Figure 9. Information Warfare, different forms (Source Radiantskies)

Denning (1999) argues that information warfare can occur in some domains such as crime, individual rights, and national security.

Kopp (2000) states that the aim of information warfare is to, "corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity, and availability of one's information." Information warfare is particularly impacting the world order in the sense that intellectual/military property is being used to target nations and organizations in such a way that business advantage and military dominance are just two clicks away from being destroyed.

2.3.3 Cyber Attack

Based on (Okenyi & Owens, 2007)

A cyber attack is the core building block that is common to all hostile cyber situations. The cyber attack is defined as follows:

- An act in cyberspace that could reasonably be expected to cause harm.
    - Harm is defined in its broadest sense: economic, psychological, physical, reputational, strategic and so on

Intent

The intent behind that attack is characterized as follows:

- Warfare; Achieving military objectives
- Crime; Personal gain through illegal means
- Bullying; Causing psychological distress to another individual
- Espionage; Obtaining political or military information
- Terrorism; Influence a nation's policies and decisions through violence and fear

Actor

The entity that carried out the cyber-attack must also be considered alongside the intent. Consideration of the actor improves the chances of coming to a correct conclusion on their intent. If the actor is a state, a conclusion of warfare-like intent would arguably be easier to reach than if the actor was an individual. If the actor is a known terrorist group, findings of terrorism-like intent are arguably more feasible.

2.3.4 Cyber Event

Having considered the actor and the intent, we can define a cyber situation by comparing it to a non-cyber situation. For example, if a cyber attack was launched by a nation state with the intent of achieving a military objective, this cyber situation is defined as cyber warfare. If an individual launched a cyber attack with the intent of causing psychological distress to another individual, it could be concluded that cyberbullying has taken place. By following this method, we can define almost any cyber situation, including cyber warfare (Sabău-Popa, Bradea, Boloș, & Delcea, 2015).

2.3.5 Cyber Terrorism

The FBI define terrorism as: "Violent acts or acts dangerous to human life that violate federal or state law and appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping. Cyber attacks where the intent is to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination or kidnapping." (Sumner, 2009).

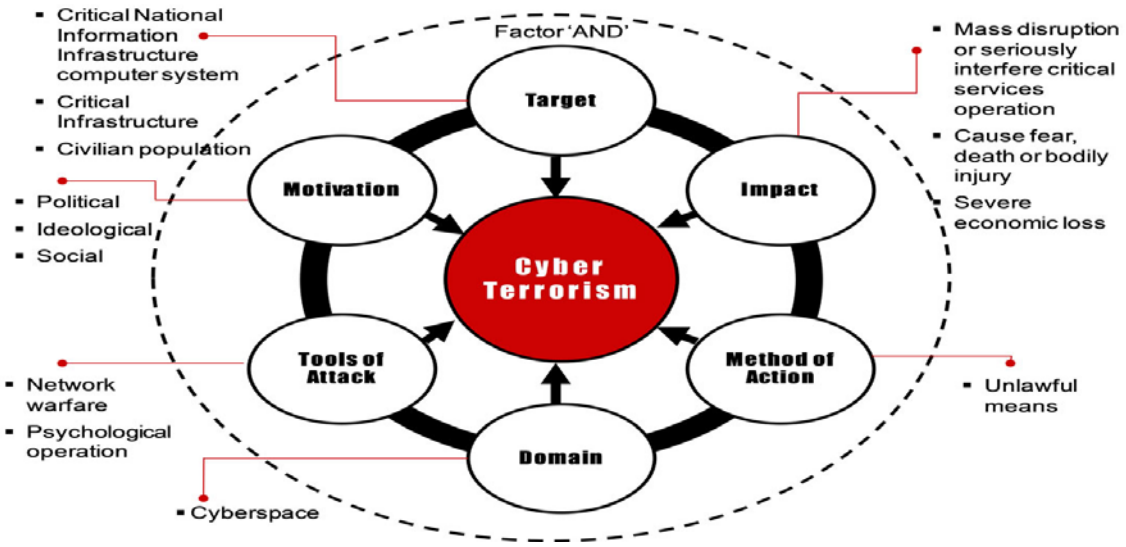


Figure 10: CyberTerrorism Model (Source Journal of Information Security)

Summer, (2009) refers to a cyber attack on a nuclear power plant with the intent of causing mass destruction would be cyber terrorism. While assassination via cyber means may sound extreme, it is possible to envisage an air defense system being compromised by cyber means to target an aircraft it ordinarily would not.

2.3.6 Network Security and Cyber Security Differences

Based on (Cisco, 2010)

It is relevant for this dissertation understand the difference between Network Security and traditional Cyber Security, so the integration of the Deception technology makes sense as complementary and never as a replacement of any of the Network and Cyber Security components.

Figure 11: Network Security (Source Reveille Systems, Inc)

Figure 12: Cyber Security (Source CB Insights)

Network Security primary purpose is to keep the organization's Network safe from the inside. A set of processes, based on a Governance framework like ISO27001, COBIT among others, should be in place to fight all inside threats, as a baseline, we could have:

- Password Policy
  - Password length and structure
    - Contain characters classes:
      - Upper case alphabetic (e.g. A-Z)
      - Lowercase alphabetic (e.g. a-z)
      - Numeric (e.g. 0-9)
      - Special characters (e.g.,! @#$%~)
  - Password blacklists
    - Example: Pa55word, Including name/employee id
  - Password duration
    - Depending on type of account but can be as short as one month
- Internet access
  - Monitoring/Stopping the site's employees visit on the company's computers
    - Sites like Gmail/Cloud Storage sites/Gaming/Sexual Content
- Encryption
  - Email using digital certificates, communications and file transfers outside the company
- Backups
  - The scheduling of regular backups of company information in case of a hardware malfunction or successful outside threat

- Scans
    - Conducting regular virus and malware scans to detect any dormant threat
- Intrusion defense systems (IDS)
    - Deep view inside the network using a protocol analyzer approach
    - Detects policy violations, infections, information leakage, Configuration errors

Cybersecurity focuses on the protection against outside threats by deploying a set of processes, based on a Governance framework like ISO27001, COBIT among others, that relies on specific software and Teams to keep the organizations safe.

The two security layers should work together so the threats, both internals, and externals, are detected in time and recovery is possible in case of data loss. As baseline and adding to the Network Security layer, we could have:

- Firewall
    - Cisco (2012), Network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules uses the "Allow" default setting
- Intrusion prevention systems (IPS)
    - Enforce a policy on what traffic is not allowed through, as the Firewall but with the "Deny" default setting
    - Block known attacks across a network using a set of known rules
- Intelligence
    - External threat intelligence
    - Reputation-based rules discussion forum's

2.3.7 Tactical Deception

To highlight the alignment between the IS Deception concept and the military Deception one, Fowler and Nesbitt (1995) suggest six general principles for effective tactical deception in warfare based on their knowledge of air-land warfare that can be used in information security warfare. They are:

- The deception should reinforce enemy expectations
- The deception should have realistic timing and duration
- The deception should be integrated with operations
- The deception should be coordinated with concealment of true intentions
- Deception realism should be tailored to the needs of the setting

2.4 Information Security Perimeter Defense Suite

2.4.1 Top 10 technologies for IS

Based on Gartner's Top Ten(10) Technologies for Information Security (Panetta, 2017).

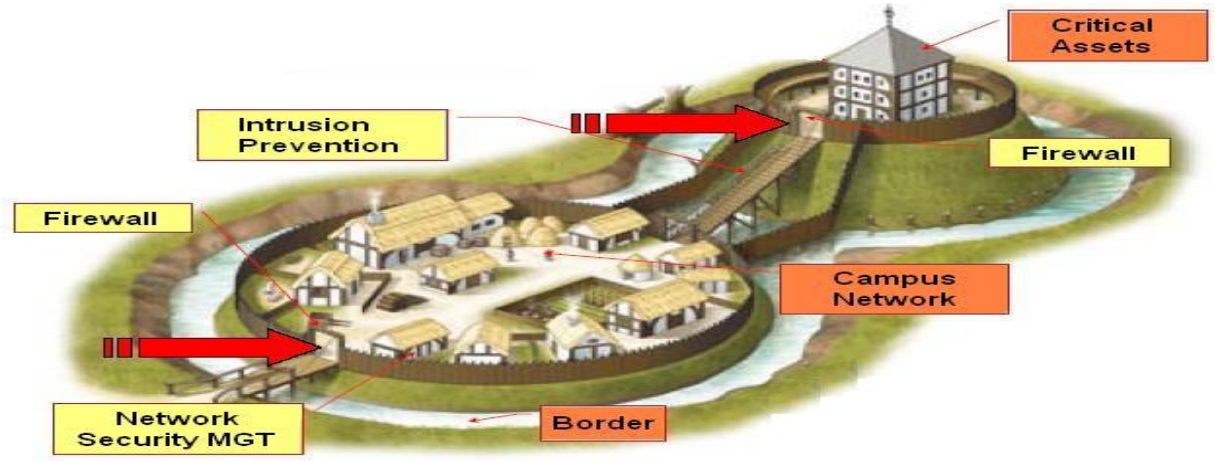


Figure 13. IS Adapted Historical Perimeter Defense Tactics (Source The Security Nige)

The Knowledge Area chapter gave a flavor of the environment, crime trending and the differentiation between Network Security and Cyber Security, important to understand that threats can materialize from the inside or from the outside, cyberspace, of the organizations and that different policies and tools, exist with different objectives. The mentioned Cyber Incident is what all of the ISsecurity technologies are designed to stop from happening.

For this work, the focus should be Cyber Security, but Network Security also plays a significant role to detect attackers lateral movement, meaning they are already inside the perimeter. A mixed top ten(10) Information Security technologies list and comparison table, along with a Deception technology insight, will drive a better understanding regarding Deception technology position among his technological peers when a Cyber Threat materializes into a Cyber Incident.

A special remark concerning a non-inclusion on the top(10) Top 10 technologies for IS of typical IS like Firewall, IDS or IPS. By just looking at the current Cyber Crime, Cyber Terrorism and Cyber Attacks trend and figures we realize that they just don't work, a new paradigm is needed and that's what this work pretend to demonstrate. Just for the record, Firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) definitions:

Firewall

Is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network). The firewall acts as the demarcation point or "traffic cop" in the network, as all communication should flow through it and it is where traffic is granted or rejected access. Firewalls enforce access controls through a positive control model, which states that only traffic defined in the firewall policy is allowed onto the network; all other traffic is denied (known as "default deny").

Intrusion Detection System (IDS)

Is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

Intrusion Prevention System (IPS)

Is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

2.4.1.1 Access Security Brokers

Software as a Service (SaaS) apps, increasingly pervasive in enterprises, provide new challenges to security teams with their limited visibility and control options. Cloud Access Security Brokers (CASB) allow chief information security officers (CISOs) an opportunity to apply enterprise security policies across multiple cloud services.

2.4.1.2 Endpoint Detection and Response

Endpoint detection and response (EDR) solutions allow CISOs to detect potential security breaches and react quickly. These tools record endpoint and network events, and the data are continuously searched using known indicators of compromise (IOC) and machine-learning techniques for early identification of breaches.

2.4.1.3 No signature Approaches to Endpoint Prevention

Techniques such as memory protection and exploit prevention and machine learning-based systems, which uses mathematical models, augment ineffective signature-based approaches for malware prevention against advanced and targeted attacks.

2.4.1.4 User and Entity Behavioral Analytics

User and entity behavioral analytics provide user-centric analytics alongside information about networks, endpoints, and applications.

2.4.1.5 Microsegmentation and Flow Visibility

Microsegmentation, a more granular segmentation, stops attackers already in the system from moving laterally (“east/west”) to other systems. Visualization tools allow security teams to understand flow patterns, set segmentation policies and monitor for deviations. For data in motion, some vendors provide optional encryption of the network traffic.

2.4.1.6 Security Testing for SOC

As SOC integrates security into the workflow, emerging operating models offer an automated, transparent and compliant configuration of underlying security infrastructure based on policy reflecting the currently deployed state of the workloads.

2.4.1.7 Intelligence-Driven Security Operations Center Orchestration Solutions

Intelligence-driven security operations centers (ISOCs) are designed to deal with the new "detection and response" paradigm. This solution requires the evolution of traditional security operation center (SOCs) to offer an adaptive architecture and context-aware components.

2.4.1.8 Remote Browser

Chief Information Security Officer (CISOs) can address malicious malware delivered via email, URLs or websites by isolating the browsing function from the endpoint and corporate network. The attack is done by remotely presenting the browser session from an on-site or cloud-based "browser server." The server sessions are reset to a known good state, and this technique reducesthe surface area for an attack, shifting the risk to server sessions.

2.4.1.9 Deception

Deception tools, as the name implies, use deceit or tricks to thwart attacks. The security team creates fake vulnerabilities, systems, shares, and cookies to tempt attackers. Any real attack on these resources indicates to security teams an attack is occurring, as legitimate users will not see or need access to the fake systems.

2.4.1.10 Pervasive Trust Services

Security models must evolve alongside the projected pervasiveness of the Internet of Things (IoT) and increasing dependency on operational technology. Trust services can manage the needs of billions of devices with limited processing capability. More importantly, trust services are designed to scale and can offer secure provisioning, data integrity, confidentiality, devices identity and authentication.

2.5 Deception Technology

The Deception-based technology enables the organizations to quickly detect, analyze and defend organizational networks against real-time attacks. Deception technology provides accurate information on malware and malicious activity not detected by other types of cyber defense.

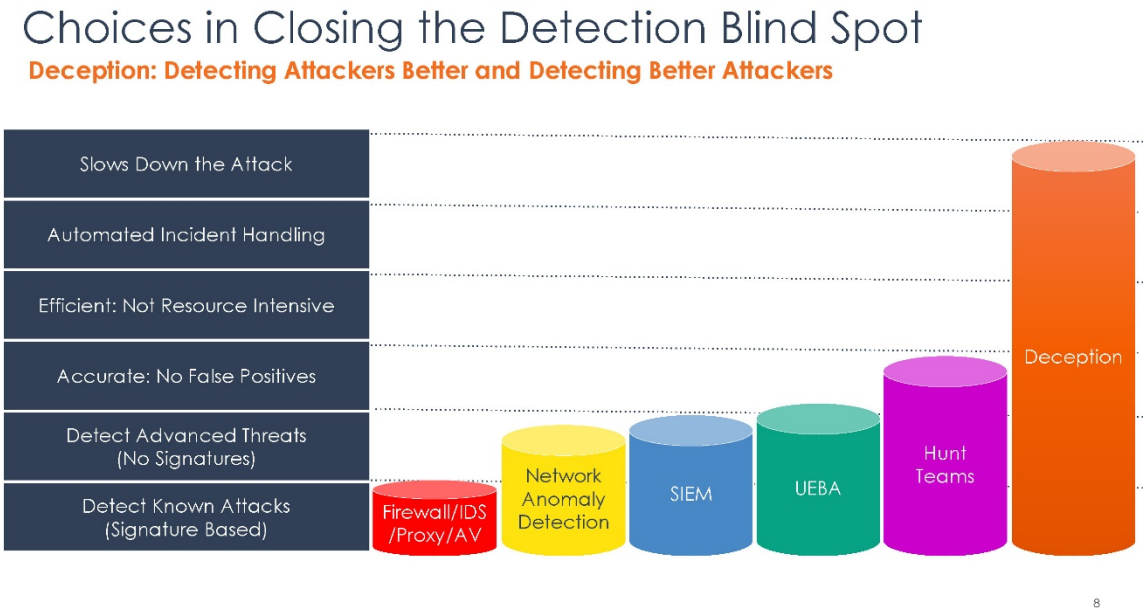


Figure 14. Deception, Closing the Blind Spot (Source Attivo Networks)

Deception technology is a new category of cyber-security designed to meet head-on the threats of malicious software, targeted attacks, zero-day "exploits" and other sophisticated attacks. Deception technology provides for the broad scale deployment of a network of camouflaged malware traps that are interconnected with the enterprise's real information technology resources. The traps appear identical in every way to the organization's real assets.

Once the malware has penetrated the enterprise, the attackers can move laterally to find high-value targets. If the malware touches any one of the traps, they are detected. Deception technology then issues a high accuracy alert. Note that Deception technology alerts do not rely on a probabilistic event or clustering around adjustable thresholds. These are great confidence events. The Deception technology enables the organizations to detect the attacks and data breach.

Some implementation types isolate the malware, tries to decompile it and supply inoculation if a patch is available. The quality of the provided information enhances the quality of the cyber-defense teams that can rapidly begin implementing the best path for remediation and removal. This work intends to explore Deception as a technology that could be strategic, effective detecting cyber-incidents.

The information security model based on Deception technology automates the deployment of a network of camouflaged malware traps that are mixed with the real information technology resources. The traps appear identical in every way to any real IT assets. Once the organization is penetrated the attacker starts moving laterally to find high-value targets. Just one touch on trap by the attacker sets off a high confidence ALERT. Real-time automation isolates the malware used by the attacker and delivers a comprehensive assessment directly to the Red Teams.

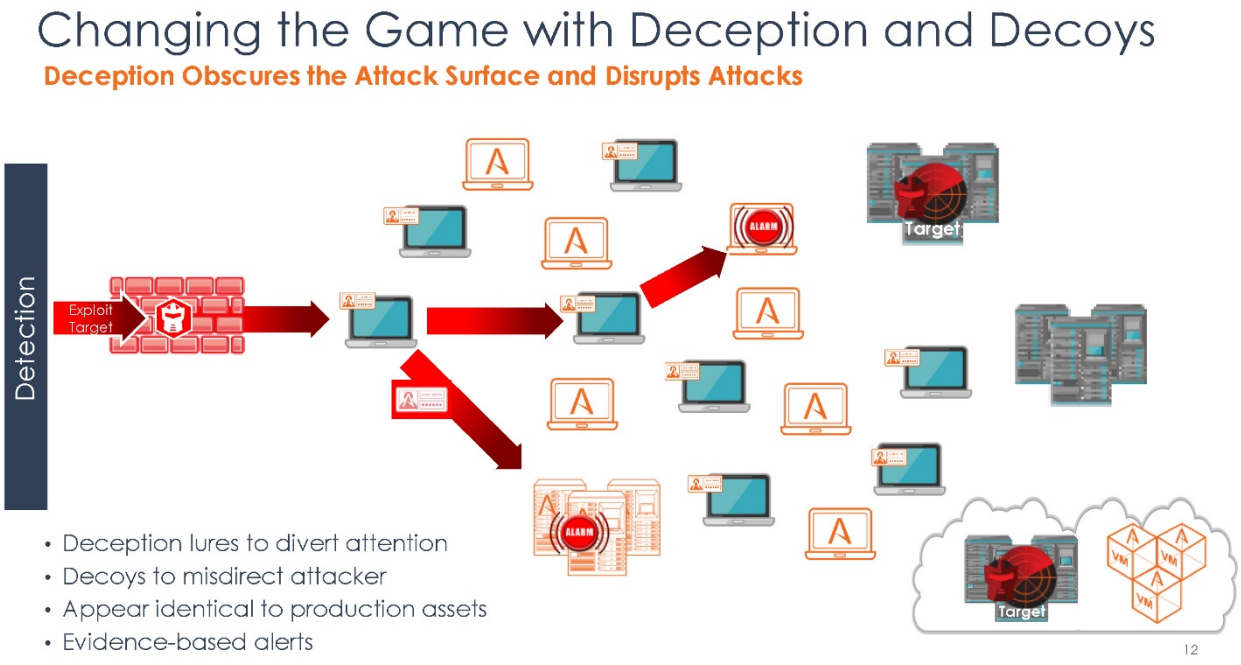


Figure 15. Deception and Decoys (Source Attivo Networks)

Deception technology is categorized into three basic classes of capability.

- Legacy Deception technology has been around for years and utilizes the notion of hand deployed and individually implemented traps.
- Basic Deception technology added some automation and reporting around honeypots. In this case, the operating systems and vendor applications must still install manually; this option is not practical for wide scale or widespread deployment.
- Advanced Deception technology utilizes automation deploy a broad network of emulated computers, servers and in some cases devices (Supervisory Control and Data Acquisition (SCADA) industrial control systems, medical devices, and so forth) and places these throughout your network.

This technology brings effectiveness while at the same time reducing the cost well below the other implementation choices.

Managed Security Service Providers (MSSP) have emerged to fill the gap in operations. They enable the enterprise to integrate new architectures such as Deception technology using the extended resources of the MSSP team.

Based on (Cooke, 2010),

- August 2016. Designs and data regarding India's Scorpene submarines were leaked from the French shipbuilder DCNS. DCNS also builds submarines for Malaysia and Chile and recently won contracts to build submarines in Brazil and Australia.
- February 2016: North Korea was suspected of hacking the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network and stealing $101 million from Bangladesh's Central Bank. The DPRK is also blamed for hacking into banks in Ecuador, the Philippines, and Vietnam earlier this year.
- May 2015. A hack of an online IRS system results in a $50 million loss, which the IRS blames on Russian hackers.
    - October 2011. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Some of the attacks are attributed to computers in Hebei, China.

The above incidents support the recognition by key government officials that large enterprises around the world have been under continued attack, and that most have not yet discovered that their networks are already penetrated. Executive staff and the board of directors have realized that our legacy information security tools are failing to keep attackers out of core information networks and enterprise mission critical infrastructure. Traditional security architectures have not proven to be capable enough to meet these threats.

Cyber-malware attacks continue to grow dramatically with increasing impact across the corporate and government sectors. The damage has become overwhelming as the cost of a single attack continues to rise.

The APTs continue to emergence from well-funded nation states and criminal organizations. Organized crime has funded significant malware and malicious activity operations, becoming their core business. They have found that substantial investments in malware and malicious activity continue to produce significant returns on investment. Organized crime is manufacturing malware for profit and gain. Criminals can be thousands of miles away, yet reach out from any place in the world to steal classified information, divert funds and damage in several aspects.

Organizations information security suite tools are unable to keep ATPs and advanced malware out of critical networks and infrastructure. Traditional security architectures are not dynamic enough to fight these threats. Attackers are very effective at engineering around the perimeter, endpoint, and anti-virus and basic intrusion detection systems in a variety of ways. Defense-in-depth cyber-security software suites continue to grow, but they are proving less and less effective against the new breed of malware and ATPs attacking core systems. Screening out 99% of all threats is not enough. Organizations need to know how to find the last 1% of attackers or the net result of the enterprise will be the same.

The strategy has turned to how to supplement existing cyber-defense suites so the organizations can detect the most of the attackers. Organizations are assuming a breach will happen.

This traditional architecture is reactive and prone to false positives. The Blue Teams are flooded with information that they need to investigate. Repeatedly, Blue Teams waste their time on non-added value tasks, in more detail, going after situations that are not incidents, are not materializations of any threat.

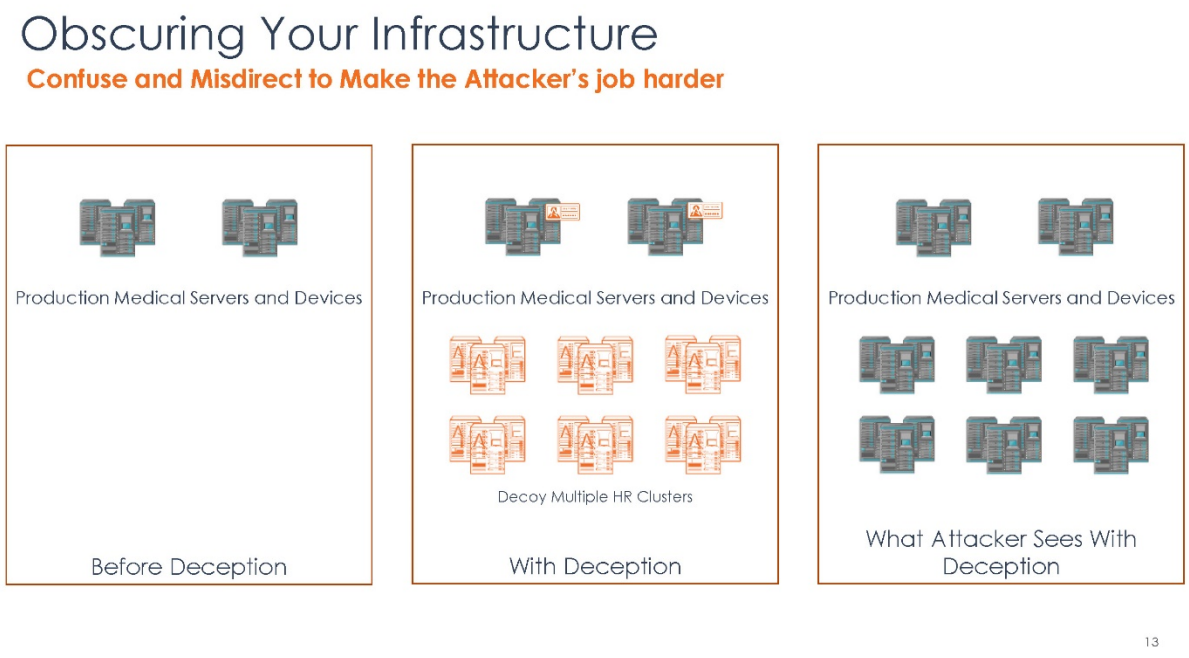


Figure 16. Deception, What You See Is Not What You Get (Source Attivo Networks)

The Deception technology complements both Network and Cyber Security into a more effective security strategy by reducing the false positives, profiling the attack, attacker and the ways of attack. Gathering information using profiling can be useful to feed an Information Security Data Lake that can act as input to the analytics tools generate knowledge. With this knowledge, the Blue and Red Teams can understand better the mechanics behind the threats and anticipate it.

2.5 Information Security Technologies Comparison Table

The IS Technologies under a Cyber Incident view will reveal the strong and weak aspects in terms of effectiveness, more readable version available at Appendix E:

The calculation is ruled by the following criteria:

- Zero (0); The Technology does apply to that particular Threat or effectiveness is Low
- One (1); The Technology applies to that particular Threat and effectiveness is Medium
- Three (3); The Technology applies to that particular Threat and effectiveness is High

Information Security Technologies	Cyber Incident Threats									
	Phishing and Email Spamming	Botnet	Malware and Spyware	Keyloggers	Social Engineering	Denial of Service	Virus	Worm	Advanced Persistent Threat (ATP)	
	Type of threat through the internet, or flooding of the Internet or any unwanted online correspondences	Guard of compromised Systems, sometimes called "zombies," that are under the command and control of a solitary "Botmaster."	Malicious program designed to gather computer information without the awareness of the client.	Programs that can screen and record the client keyboard information while typing in Computer System for later access.	Kind of technique in which it traps or tricks the client to reveal valuable information.	Attack that upsets the normal function of the computer system and thus prevents access to authorized users	Program that spreads itself from one computer to another computer without the users' authorization to do so	Computer Program that moves from one machine environment, then onto the next machine environment often keeping a record of the last environment	Continuous computer hacking that is actively supported by several people that usually targets one specific entity.	
Access Security Brokers	1	0	1	0	0	0	0	0	0	2
Software as a Service (SaaS) apps, increasingly pervasive in enterprises, provide new challenges to security teams with their limited visibility and control options. Cloud Access Security Brokers (CASB) allow chief information security officers (CISOs) an opportunity to apply enterprise security policies across multiple cloud services.										
Endpoint Detection and Response	3	3	3	3	0	0	3	3	0	18
Endpoint detection and response (EDR) solutions allow CISOs to detect potential security breaches and react quickly. These tools record endpoint and network events, and the data are continuously searched using known indicators of compromise (IOC) and machine-learning techniques for early identification of breaches.										
No signature Approaches to Endpoint Prevention	3	0	3	0	0	0	3	0	0	9
Techniques such as memory protection and exploit prevention and machine learning-based systems, which uses mathematical models, augment ineffective signature-based approaches for malware prevention against advanced and targeted attacks.										
User and Entity Behavioral Analytics	0	0	0	0	0	0	0	0	3	3
User and entity behavioral analytics provide user-centric analytics alongside information about networks, endpoints, and applications.										
Microsegmentation and Flow Visibility	0	3	3	0	0	0	3	3	3	15
Microsegmentation, a more granular segmentation, stops attackers already in the system from moving laterally ("east/west") to other systems. Visualization tools allow security teams to understand flow patterns, set segmentation policies and monitor for deviations. For data in motion, some vendors provide optional encryption of the network traffic.										
Security Testing for DevOps	1	1	1	1	0	1	1	1	1	8
As DevOps integrates security into the workflow (DevSecOps) emerging operating models offer an automated, transparent and compliant configuration of underlying security infrastructure based on policy reflecting the currently deployed state of the workloads.										
Intelligence-Driven Security Operations Center Orchestration Solutions	1	1	1	1	0	1	1	1	1	8
Intelligence-driven security operations centers (ISOCs) are designed to deal with the new "detection and response" paradigm. This solution requires the evolution of traditional security operation center (SOCs) to offer an adaptive architecture and context-aware components.										
Remote Browser	3	0	3	0	0	0	3	1	0	10
CISOs can address malicious malware delivered via email, URLs or websites by isolating the browsing function from the endpoint and corporate network. The attack is done by remotely presenting the browser session from an on-site or cloud-based "browser server." The server sessions are reset to a known good state, and this technique reduces the surface area for an attack, shifting the risk to server sessions.										
Deception	1	3	3	3	3	3	3	3	3	25
Deception tools, as the name implies, use deceit or tricks to thwart attacks. The security team creates fake vulnerabilities, systems, shares, and cookies to tempt attackers. Any real attack on these resources indicates to security teams an attack is occurring, as legitimate users will not see or need access to the fake systems.										
Pervasive Trust Services	1	3	1	3	3	1	3	3	0	18
Security models must evolve alongside the projected pervasiveness of the Internet of Things (IoT) and increasing dependency on operational technology. Trust services can manage the needs of billions of devices with limited processing capability. More importantly, trust services are designed to scale and can offer secure provisioning, data integrity, confidentiality, devices identity and authentication.										
	14	14	19	11	6	6	20	15	11	

Table 7. Information Security Technologies Comparison Table

2.6 Information Security Technologies Comparison Table Conclusions

The Cyber Threat that receives less protection is Advanced Persistent Threat (ATP) due to his dynamic type, shifting shape and method very quickly, only Microsegmentation and Flow Visibility, User and Entity Behavioral Analytics and Deception scores on ATP high.

Deception technology scores highest across the Information Security Technologies due to his technology that impersonates assets in the form of decoys. By triggering a real alarm upon being touched, the Deception decoy asset positioning himself systematically strong across the Cyber Threats.

3. Methodology

3.1 Contextualization

The elaboration of this work will obey to the Design Science Research (DSR), research on state of the art for related artifacts.

3.2 Structural Question

The following question is structural to substantiate the work:

- **Is Deception technology an effective and strategy to reduce Cyber Attacks?**

In order to answer the fundamental question the Environment, with the representation of the Organization IT like people, risks, security, and others, will cycle together with the scientific theories to generate Artifacts that can be evaluated and eventually implemented.

As main artifacts, a Related Testimonial, Use-Case from a leading supplier of the technology, proof of concept and workout will support the Relevance sub-cycle

All available information will drive the understanding of the effectiveness and strategic value of the Deception Technology.

3.3 Artifacts Definition

3.3.1 Related Testimonial Artifact

Identify a high ranked member of an organization, Information Security domain, that had implemented Deception technology and retrieved the thoughts and main messages regarding the technology. The identified organization is **Interana**, and the testimonial is given by **Mark la Rosa, Solutions Architecture VP**. Interana is a fast growing Bay Area software company that is defining and leading a new category of behavioral analytics for the digital economy, and his testimonial regarding Deception technology highlights some key aspects that add valuable information to this work.

3.3.2 Use Case Artifact

Identify a Use Case on the Health organizations space that highlights the behavior of the Deception technology under pressure. Regardless of several attempts to identify an academic based Use Case, that was not possible due to no sources were available. Based on the previous situation, the Use Case was selected by the Deception Technology Vendor bearing in mind the Health domain in use.

3.3.3 Proof of Concept Artifact

Actors

Sponsorship

Based on the proximity between this dissertation coordinator and a top organization on the health domain, she will also act as the sponsor for the execution of the work.
The Sponsor is Drª Carla Pereira.

Organization

A top organization on the health domain is to be engaged based on the criticality of the assets and the type of information under his protection, Protected health information (PHI). The relevance of the Deception technology will be under a heavy scrutiny by this type organization.
The organization is **SPMS**.

Deception Technology Vendor

Top Deception Technology Vendor willing to setup a test environment relevant enough to retrieve practical conclusions regarding effectiveness.
The Vendor is **TrapX**. (www.trapx.com)

Organization Infrastructure Team

A team from the organization, available to setup a test environment where the Deception technology is to be deployed. Team member's identification is unknown.

Organization Red Team

A team from the organization, available to detect the test intrusion and reported it promptly. Team member's identification is unknown.

White Hat Hacker(WHH)

WHH is responsible for taking control of the assets and retrieving information.
The WHH is a top professional on the domain, responsible for the management of a Red Team for one of the top 15 organizations (Fortune 500 by Forbes). The identity is classified for privacy reasons.

Organization Management

Persons from the Organization with proper roles in the Information Security space, CIO/CTO/Governance Leader/Compliance Leader/Risk Leader/Internal Audit.
Gracefully available for the Proof-Concept and Workout, the **CIO, Drº Rui Gomes** and **Governance Consultant, Drº Bruno Soares**, **ISACA** Portugal Chapter **President.**

3.3.3.1 Proof of Concept Artifact

The infrastructure should be deployed using a test environment; the setup must include:

- Virtual network that will not expose real organization networks and assets, only accessible to the listed actors
- Minimum two(2) real test workstations with standard organization images
    - A file labeled “M_SIG.txt” will reside on one of the workstations with the text “50033580” inside, content and location unknown for the WHH. The workstation is not infected with malware
- One(1) database server, either SQL Server or Oracle Database Server
    - One(1) table labeled “M_SIG” with one(1) field and one(1) record, content of the record equal to “50033580”, unknown for the WHH
- Deception technology Decoys
    - One(1) workstation based on the organization image
    - One(1) database server that matches the organization database server and naming policy
- Remote access to the test environment to enable the WHH work
- All organization security policies in place as normal deployment for real assets
- Malware enabling remote control on a real test workstation

3.3.3.3 Assumptions

The Organization Red Team does not know that one of the workstation is infected and that a WHH has access to the test environment. Assuming that previous to Deception technology deployment an asset was compromised. The WHH does know that Deception technology is deployed but understands the type of organization involved.

3.3.3.4 Modus Operandi (MO)

The infrastructure setup completion will enable the WHH access the test. By the defined datetime and for the defined time length, both the WHH and the Organization Red Team will start working. The WHH knows the organization keyword that identifies valuable information, that keyword is “M_SIG.” The exercise will stop when the defined time length expires, when the Organization Red Team detects the WHH or when the Deception technology detects the WHH.

3.3.3.5 Objective

The proof-concept will be considered successful if the WHH is detected by the Deception technology before the Organization Red Team. Other possible scenarios will be regarded as a failure for the Deception technology, like Organization Red Team detects first the WHH, the WHH download the “M_SIG.txt” file or access the Database and retrieve the content of the record.

3.3.4 Workout Artifact

3.3.4.1 Actors

Organization Management

Persons from the Organization with proper roles in the Information Security space, CIO/CTO/Governance Leader/Compliance Leader/Risk Leader/Internal Audit.

Gracefully available for the Proof-Concept and Workout, the **CIO, Drº Rui Gomes** and **Governance and Compliance Consultant, Drº Bruno Soares, ISACA** Portugal Chapter **President**

Assumptions

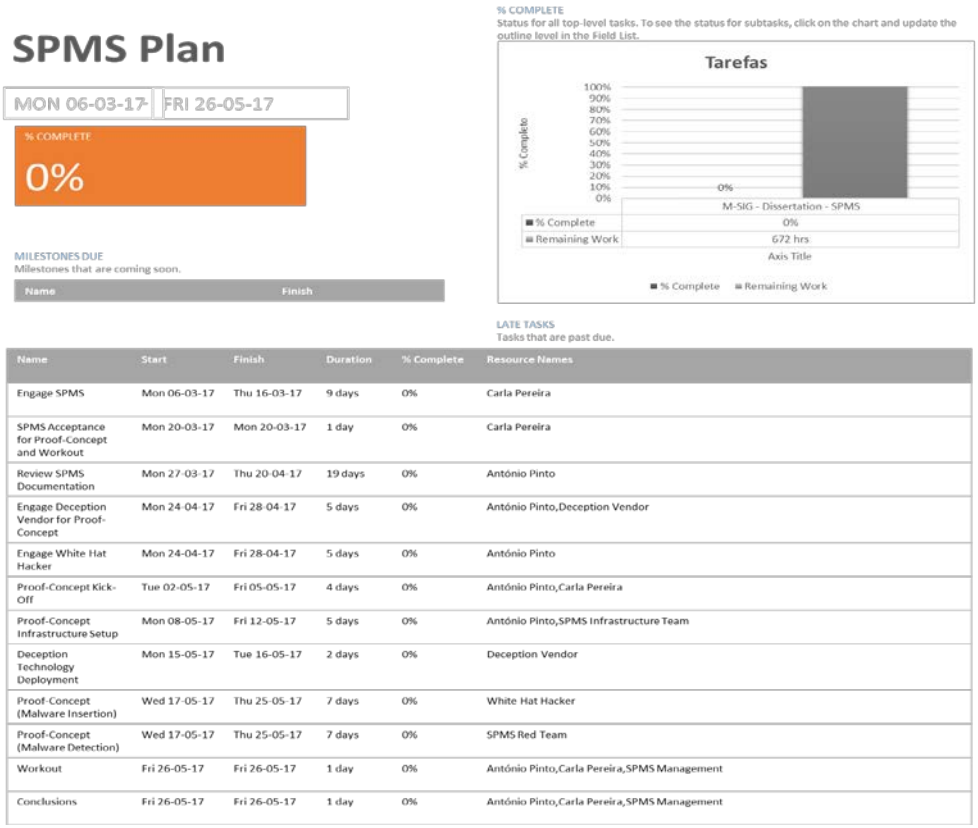
Available information regarding the Governance Model, the Information Security Architecture and other that may reveal himself relevant.

Organization Management availability to be an active part of the workout.

Objective

Based on all the available information on this work, understand if Deception technology is strategic for the organization by matching his key features with the Governance Model and Information Security Architecture.

3.4 The Plan (Initial)



Name	Start	Finish	Duration	% Complete	Resource Names
Engage SPMS	Mon 06-03-17	Thu 16-03-17	9 days	0%	Carla Pereira
SPMS Acceptance for Proof-Concept and Workout	Mon 20-03-17	Mon 20-03-17	1 day	0%	Carla Pereira
Review SPMS Documentation	Mon 27-03-17	Thu 20-04-17	19 days	0%	António Pinto
Engage Deception Vendor for Proof-Concept	Mon 24-04-17	Fri 28-04-17	5 days	0%	António Pinto,Deception Vendor
Engage White Hat Hacker	Mon 24-04-17	Fri 28-04-17	5 days	0%	António Pinto
Proof-Concept Kick-Off	Tue 02-05-17	Fri 05-05-17	4 days	0%	António Pinto,Carla Pereira
Proof-Concept Infrastructure Setup	Mon 08-05-17	Fri 12-05-17	5 days	0%	António Pinto,SPMS Infrastructure Team
Deception Technology Deployment	Mon 15-05-17	Tue 16-05-17	2 days	0%	Deception Vendor
Proof-Concept (Malware Insertion)	Wed 17-05-17	Thu 25-05-17	7 days	0%	White Hat Hacker
Proof-Concept (Malware Detection)	Wed 17-05-17	Thu 25-05-17	7 days	0%	SPMS Red Team
Workout	Fri 26-05-17	Fri 26-05-17	1 day	0%	António Pinto,Carla Pereira,SPMS Management
Conclusions	Fri 26-05-17	Fri 26-05-17	1 day	0%	António Pinto,Carla Pereira,SPMS Management

Figure 17. SPMS Initial Plan

4. Results

As results, the Deception Technology related testimonial, Healthcare Hospital Use Case, SPMS Proof of Concept and SPMS Workout will highlight Deception Technology strengths and weaknesses.

4.1 Deception Technology related testimonial

Mark la Rosa is a Solutions Architecture VP at Interana, Interana is a fast growing Bay Area software company that is defining and leading a new category of behavioral analytics for the digital economy, and his testimonial regarding Deception technology highlights some key aspects that add valuable information to the answer.

“I run a solutions architecture team, and we are dealing with not only our data and our IPs and the code of our software, but we have **customers that trust us with data** for proof of concepts. What struck me about Deception was this idea of a honeypot and the idea of Deception technology, so using the **same tactics as the hackers and use against them**. I think that one of the big mistakes I see in **corporate security** is the fact that it's being done by **corporate guys and they're not hackers**, they don't think the same way in the same wavelength that a hacker would think and Deception really, to me, is almost like it was developed by the same sort of mindset of folks that would be perpetrating attacks, and that's the right way to do security, you got to have the **correct mindset to understand how it works**, what types of things did they'll try and how to really fake them out because they're going to know if it's not an obvious fake and what Deception is done so well is it it's nearly impossible to tell what's real and what's Deception decoys. It's **a lot less expensive to deploy something like this than it is to have an entire team of people monitoring this 24/7** to make sure that these things aren't going down, so in my mind it's actually quite a **good return on investment** from buying the software vs. having people doing it and I also think that the way the implementation is done, the **technology can do a better job than a person** can because it's able to **react a lot faster** to what base does sifting through things that are very hard for people to see it in logs. **Even if you have the best firewall in the world**, there's going to be **human errors**, people are going to set things up improperly, someone will deploy a policy that is not correct, someone is gone to lose their password, and he or she left to take over a machine, these things will be going to happen!

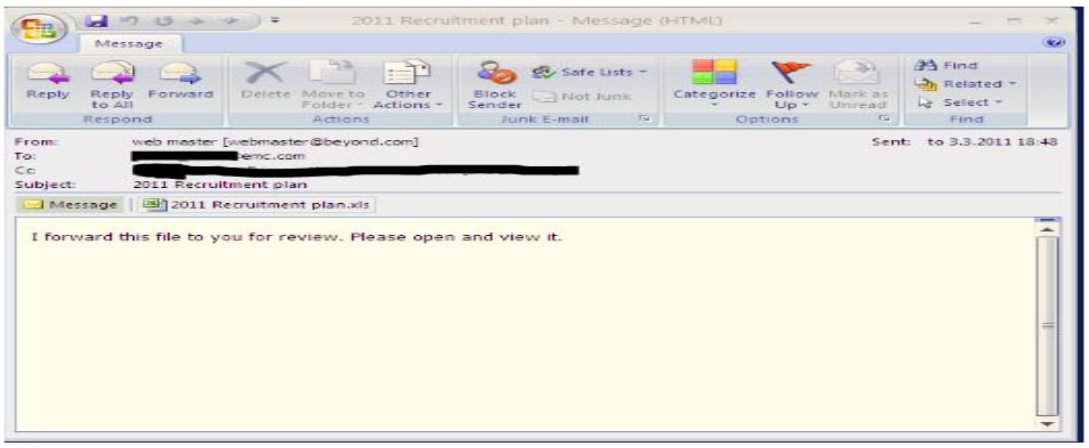


Figure 18: Human Error, eMail allowing the installation of Malware (RSA: 2011)

When I first started using Deception, I was really impressed with a couple of things, the first thing is, it was **straightforward** for me to set it up to **simulate actual traffic** I could literally just go in there and point click and say I want to put a SQL server here, and I want to put a fake web server here, and I want a fake file-share here, and I can literally just go in and **set up a network that looks just like mine network that was all fake** and it would even send traffic back and forth. Is one of those things that is almost that insurance policy that you know is out there and the least you have to do with it, the better really and that's the great thing about it, you really do know that this thing will email me and I'm going to get a phone call if in case of an incident. It is one of those things where I can put it out of my mind and **focus on other things that matter to our business."**

Mark's testimonial contribution touches on several important aspects, the reality of some organizations that not only they need to protect his information but also customer's information, increasing the Risk exposure.

That Deception technology is changing the attack paradigm by allowing the Red teams to incorporate much more information on the defense and counter-attack.

The human error is always present in any activity and is exactly, along with other possibilities, that mistake that attackers will leverage.

Deception technology is a concept easy to understand and implement, importantly, Mark deploy his decoys and set up the Deception grid, meaning no special technical teams from the supplier is needed, with the associated savings to the organizations.

Information Security models are, sometimes, defined by teams that do not have the all the necessary knowledge on how attackers work.

The tradeoff between large Blue teams analyzing the thousands of security logs and the risk of failure are not adding any value to the organization.

Mark considers a good return on investment because huge Blue teams no longer are necessary

As final thoughts is vital that people in his type of position, VPs, will need to focus on adding value to the organizations instead of dealing with false positives. Deception Technology, if deployed, will enable that.

4.2 Healthcare, Hospital Use Case

HEALTHCARE HOSPITAL LABORATORY MEDJACK, TrapX (Chosen to be aligned with SPMS type of business)

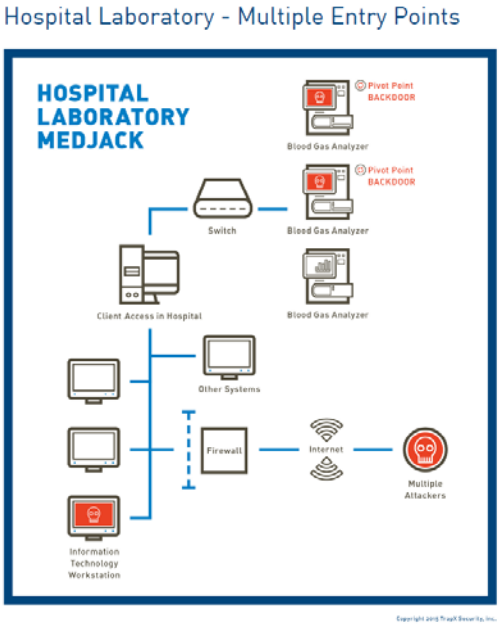
Background

This hospital case study focuses on a healthcare institution (anonymous due to privacy reasons) with Deception technology implemented. Before Deception technology, there were **no indicators of malware infection or persistent threats visible to the hospital**. The customer had an **unyielding industry suite of cyber defense products**. The suite included a strong firewall, intrusion detection (heuristics based), endpoint security, anti-virus and more. The healthcare information technology team included a **team with several highly competent and experienced cyber technologists**. It is important to understand the environment in which a device such as a blood gas analyzer is used. Blood gas analysis is often used with patients within critical care. They are often in the intensive care unit and under duress, perhaps even in a struggle for their lives.

After the implementation of the Deception technology, within a **short window of time**, several **alerts** to malicious activity within the networks **was detected**. Upon inspection, it became apparent that this was a form of **persistent attack** and forensic evidence showed that the attacker continued to move through the hospital's networks looking for appropriate targets. The Deception technology enabled the Red Team to **identify the source** of this lateral movement. The intrusion comes from three (3) of the hospital blood gas analyzers present in the hospital laboratory. These were all infected separately and had now enabled three separate backdoors into the hospital networks.

The lateral movement before Deception technology implementation may have allowed the infection of one of the hospital IT department's workstations. It was identified this infection point separately, and forensics points to a connection with the blood gas analyzers infection. It was determined that **confidential hospital data be being exfiltrated** to a location within the European Community. Although the data breach was identified, there is still uncertainty around how the attacker successfully exfiltrated many data records in total.

Once an attacker established a backdoor within a target, blood gas analyzer, or any other medical device, almost any form of manipulation of the unencrypted data stored and flowing through the device is possible.



Backdoors across the network allowing the attacker lateral move, targeting valuable assets.

From a starting point, blood gas analyzer, infections were spreading, even an Information Technology was infected

Confidential hospital data was being exfiltrated

Figure 19: Hospital Use Case (TrapX: 2015)

This Use Case exposes several organization concerns, in this case, the situation was critical because the infected devices were life support type ones, used with patients within critical care.

4.2.1 Main Considerations:

Based on a FireEye, FireEye is the intelligence-led security company with over 5,800 customers across 67 countries and including more than 40 percent of the Forbes Global 2000. The intrusion detection time is 146 days for the US and an impressive 469 for EMEA, 81% of the intrusions are not detected, organizations are sometimes aware of that fact when becomes public or when the authorities/regulators act in the form of fines or prison time for the Management.

The hospital Information Security was built upon a strong industry suite of cyber defense products and a team of several highly competent and experienced cyber technologists, despite all, the suite of cyber defenses didn't detect the previous attack that installed the trapdoor. The Deception technology was able to detect, within a short window of time, several intrusion alerts, invisible to the hospital Blue and Red Teams.

That confidential hospital data was being exfiltrated, by not knowing that the hospital could not activate the response teams, mainly Red Teams to stop the attack. Other teams will definitely be thankful for any in-time warning of that fact, among others:

- Board of Directors, to manage market/regulatory expectations
- Internal Audit Team, to incorporate the cyber-incident on the Audit model
- Communication Team, to prepare a public statement
- Legal Team, to prepare for legal processes
- Privacy Team, to prepare identification of the lost confidential data
- Risk Team, to increase risk level and calculate new risk appetite
- Compliance Team, to prepare regulatory response
- Finance Team, to prepare for possible fines

Regardless of the strong investment on Information Security, a suite of software and Teams, this hospital was not able to detect an attack with three (3) infection points enabling backdoors for attackers.

Deception technology was effective in intrusion detection and forensics information retrieval, for a brief period, the Blue/Red Teams started receiving intrusion alerts that reveal himself true incidents that required real actions.

The information retrieved by Deception technology pointed to a fact, confidential hospital data was being exfiltrated to a location within the European Community, the fine tuning provided by the technology delimited the physical space where the information, first, was stored.

This Use Case was a successful history where Network/Cyber Security components complemented by Deception technology was able to identify and stop an attack in progress.

4.3 SPMS Proof of Concept

A proof of concept involving the deployment of Deception technology within a test environment was discussed with SPMS management. The goal was to test in a controlled environment the effectiveness of the technology and evaluate the concepts against reality.

A Deception technology vendor along with a White Hat Hacker was engaged and ready, a plan and description of the steps were defined.

Due to the latest cyber threats, the entire SPMS infrastructure activated his high-risk situation plan and is under a lockdown protocol.

The access to all network devices for proof of concepts or experimentations involving SPMS assets is blocked.

SPMS Management didn’t approve the proof of concept based on the criticality of the information security environment.

Based on this situation, the conclusions are only based on the related testimonial, Use Case, and SPMS Workout.

4.4 SPMS Workout

During the dissertation planning, the inclusion of an organization in the healthcare space was the first choice for the Deception technology thematic proof of concept. The main factor for this choice was the type of information managed by this kind of organization, mainly:

- Personal Identifiable Information (PII) (Infosec Institute, n.d.)
  This information can identify an individual. According to a definition by the National Institute of Standards and Technology (NIST), PII is information about an individual maintained by an agency which:
  - Can be used to distinguish or trace an individual's identity based on identifiers, such as name, date of birth, biometric records, social security number; and
  - Additional information that may identify a person – that is medical, financial, employment and educational information
- Protected Health Information (PHI)
  PHI is any information on a health condition that can be linked to a specific person

Handling this type of information requires extra security measures. Additionally, life support and diagnostics devices are also under SPMS management.

SPMS Main Areas of Intervention are:

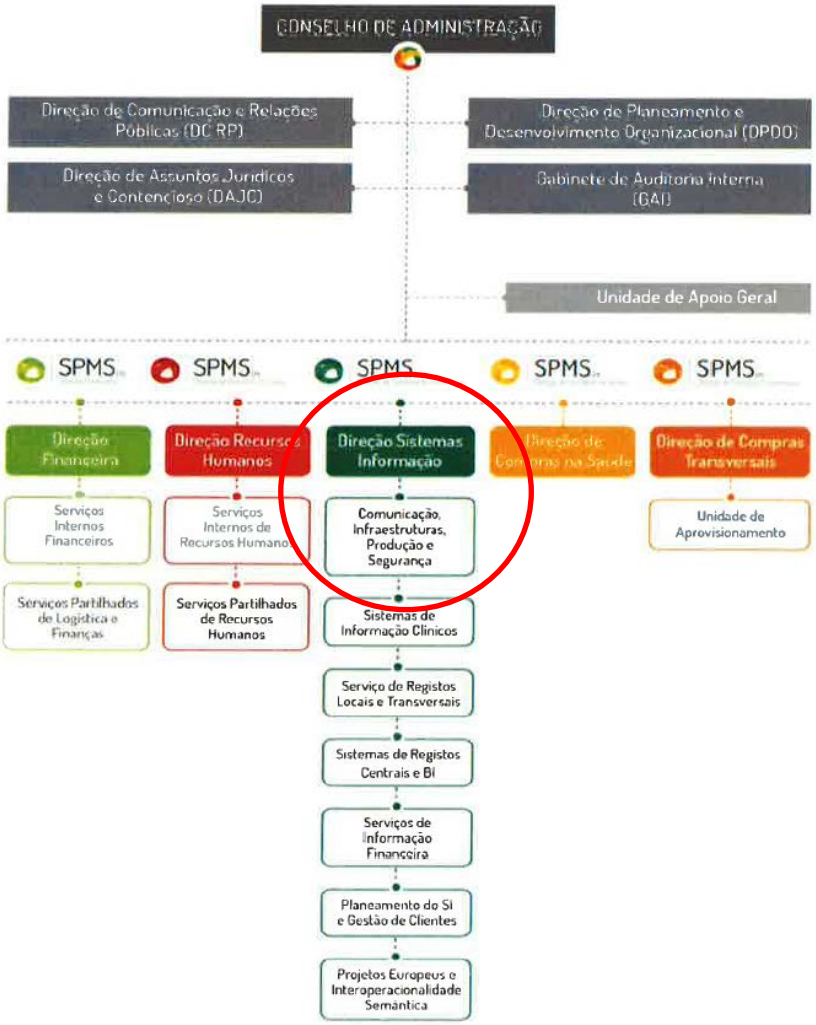


Figure 20: SPMS 2014-2016(last version) Strategic Plan

The identified target for the proof of concept was the Information Systems Unit, Communications, Infrastructure, Production, and Security Department, Managed by Drº Rui Gomes, teaming with Drº Bruno Soares, ISACA Portugal Chapter President and principal SPMS consultant for Information Technology Governance and Information Security.

The following strategic topics were identified:

- Reinforce authority on IT and Sourcing
- Move closer service delivery and Heath Minister/National Health Service
- Reinforce reputation and branding
- Strengthen finance sustainability by different sources usage

To understand if Deception technology is strategic, the SPMS Risk and Information Security Framework was subject to the principal components analysis:

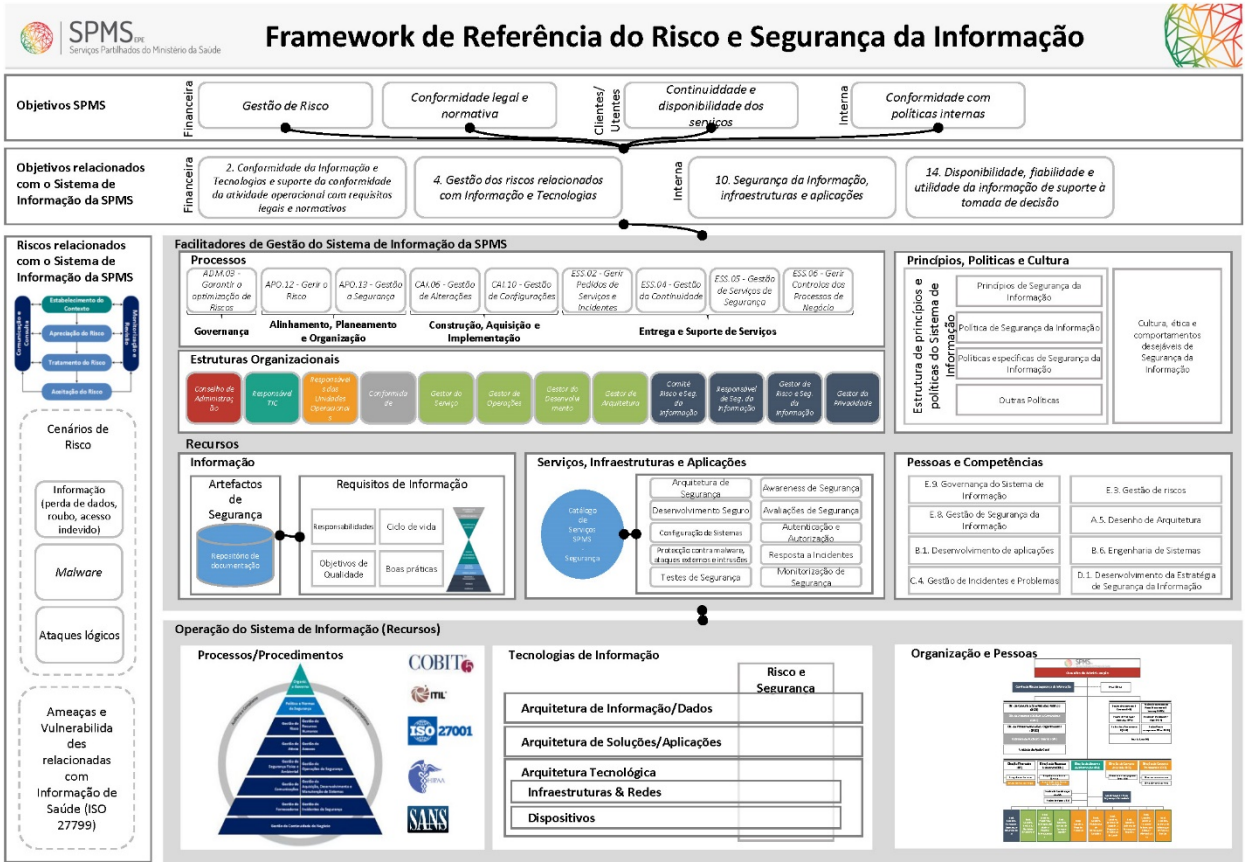


Figure 21: SPMS Risk and Information Security Framework

The SPMS overall objectives refer to risk management and compliance with legal, external and internal standards. The information systems objectives inherit the overall objectives and bound it to his domain.

Figure 22. SPMS Risk Scenarios

ISO 27799:2016 Address the special information security management needs of the health sector and its unique operating environments.

While the protection and security of personal information are important to all individuals, corporations, institutions, and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability, and availability of personal health information.

The risks scenarios were build based on the threats, like malware and logic attacks, data access and lost/stolen, governed by ISO 27799:2016.

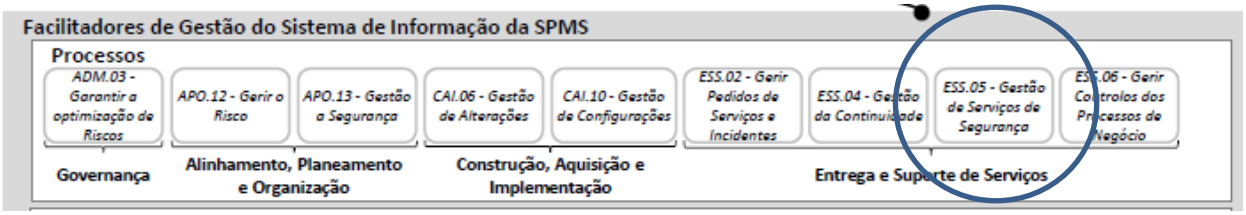


Figure 23: SPMS Information System Management Controls

The governance model covers all the main domains, relevant for information security, and integrates the controllership component of ISO/IEC 27001:2013, in more detail, the ESS.05 Control (Security Services Management).

SPMS integrate several reference frameworks and the decision to shape his Governance model was based on those frameworks.

Figure 24: Risk Management Lifecycle

By using the most relevant, applicable, mandatory components of each framework, SPMS guarantees a strong strategy definition, alignment with the objectives, the reinforcement of his authority on IT, and establishes the basis for an effective Risk Management.

Figure 25. SPMS Governance, Controllership and Service Delivery Frameworks

The procedures and processes are based on reference frameworks like:

- COBIT 5 (http://www.isaca.org/Cobit/pages/default.aspx)
    - COBIT 5 framework for the governance and management of enterprise IT is a leading-edge business optimization and growth roadmap that leverages proven practices, global thought leadership and ground-breaking tools to inspire IT innovation and fuel business success.
- ITIL (https://www.itil.org.uk/)
    - ITIL is a globally recognized best practice methodology for IT service management which is used all over the world by organizations to ensure that their IT services are aligned to the needs of their business. ITIL provides trusted guidance on how businesses can use their IT services to support their goals and facilitate business growth.
- ISO 27001 (https://www.iso.org/standard/54534.html)
    - ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to apply to all organizations, regardless of type, size or nature.
- HIPAA (https://www.hipaa.com/)
    - HIPAA establishes national standards for electronic health care transactions. HIPAA reflects a move away from cumbersome paper records and an increased emphasis on the security and privacy of Health data.
- SANS (https://www.sans.org/)
    - SANS is the most trusted and by far the largest source for information security training in the world

4.5 SPMS Plan (Updated)

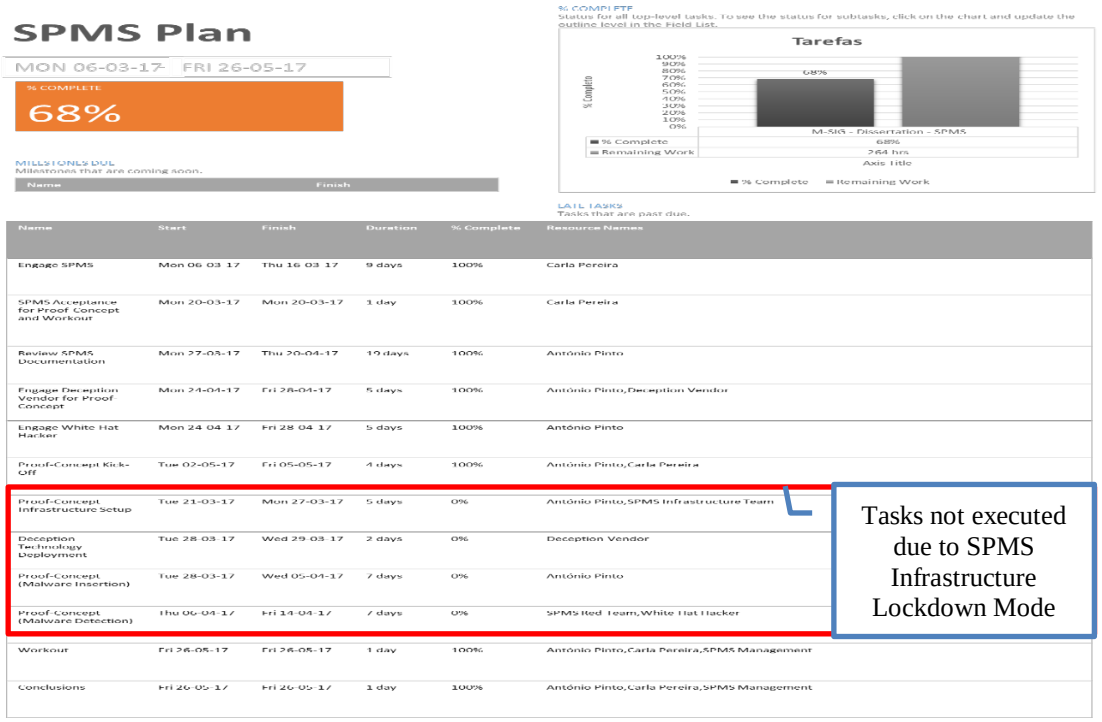


Figure 26. SPMS Plan Updated

5. Conclusions and Future Work

5.1 Conclusions

Revisiting this work question:

- Is Deception technology **effective** and **strategic** to reduce Cyber Attacks?

So one of the goals is to understand Deception Technology components and behavior, where he is positioned on the information security landscape and evaluate the effectiveness when targeted by a cyber treat that materializes into a cyber-incident.

Based especially on the SPMS Workout, was a shared understanding that Deception Technology could play a major role by feeding the Governance model with the necessary evidence that a process is in place and is effective, fulfilling internal/external audit and risk, either operational or enterprise. In more detail, this technology will address the Risk Scenarios requirements and align with the Governance control requirements helping to enable the organization goals.

One of the SPMS Workout conclusions was made by **Drº Rui Gomes**, that considered Deception Technology a strategic artifact to integrate the SPMS Information Technology Governance Model.

The second goal touches the strategic value of the Deception Technology when facing an organization governance model.

Deception Technology does not position himself inside the “stop an attack” type of information security suite of tools like for example, firewall or anti-virus, on the contrary, Deception Technology value are shown when the perimeter is penetrated, the attacker is already inside the organization network, and assets are already compromised.

The paradigm changes with Deception Technology, no longer the organizations plan and act based on the illusion that the attacks can be stopped but with the certainty that, almost for sure, the attackers will get through either by exploiting a zero-day vulnerability or a simple human error.

Looking at the available results, Deception Technology exposed several theoretical strengths that can be used to reduce Cyber Attacks.

One is the ability to fast detect an intrusion allowing the Blue and Red Teams to react in time and stop the attack from spreading. This is a major breakthrough when compared with the endless hours looking to event logs produced by the traditional defense tools.

Other is acting as the first line of defense, by detecting malware attacks and intrusions, among others, ensuring forensics evidence of any lost/stolen information and overall threats to an organization information/infrastructure.

The amount of high-quality information generated by the Deception Technology can be used to feed the Information Security repository that could be utilized in the Risk scenarios build/discussion, Analytics, to predict next attacks and improve defense robustness.

Drº Bruno Soares also concluded, SPMS Workout, that cognitive security, self-learning systems that use data mining, machine learning, natural language processing and human–computer interaction to mimic the way the human brain works, is the next logical/mandatory step when facing ATPs. Here, Deception Technology can play a major role, based on the high-quality data generated.

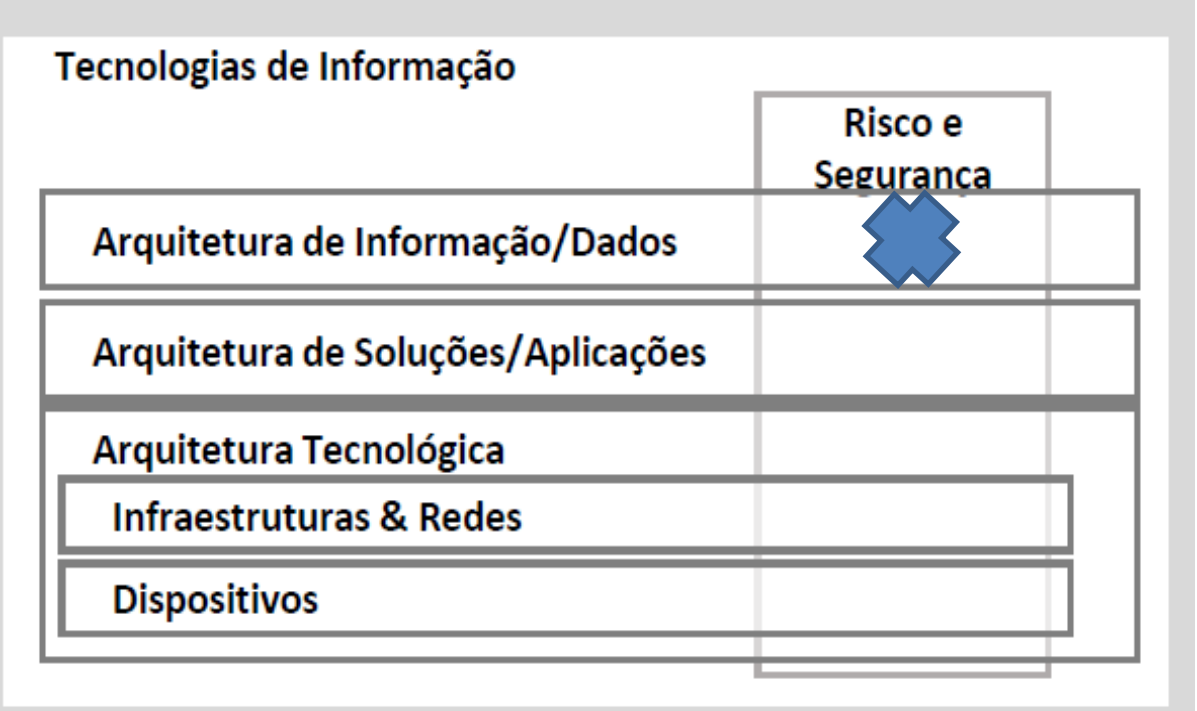


Figure 27. SPMS Information Technology Artifacts

SPMS Security Architecture could integrate Deception Technology to improve defense robustness and comply with internal Goals and Regulatory Requirements.

The high-quality data generated can feed security repositories to increase response levels and enable cognitive security approach.

Workwise, the final conclusions in terms of the effectiveness and strategic, theoretical values, are summarized as follows.

5.1.1 Effective?

Deception technology, integrated into the Network and Cyber Security technologies, delivers what's expected by successfully detecting cyber-attacks coming from the cyberspace or within the internal network.

Today's violent acts, like cyber terrorism, are not an isolated occurrence but part of an information warfare reality that touches not only governments but all organizations.

5.1.2 Strategic?

The SPMS Workout revealed that Deception technology as a positive strategic impact, by his integration on the Governance Model and contributor to SPMS objectives.

The SPMS Governance model is structured on reference frameworks that majority relies on a set of controls, here, the Deception technology is one more artifact that can provide the necessary evidence of monitoring and compliance as required by "Appendix B – SPMS Programa de Melhoria Contínua do Risco e Segurança da Informação."

Deception technology can also integrate globally with "Appendix A, Framework de Referência do Risco e Segurança da Informação," and specifically with "Appendix D – SPMS Arquitetura de Referência da Informação on the dimension 09. Gestão de Comunicações".

5.2 Future Work

As logical next step for this topic, the proof of concept that "Augmenting the Information Security tool suite with Deception technology, empower the organizations to fight better Cyber-Crime," is mandatory to fully understand and prove the value of Deception technology as the last Information Security defense line.

In future work we aim to progress, starting from the results achieved by this work, to a more realistic situation by executing a:

5.2.1 Proof of concept

The lack of real world results under a controlled attack situation, not present on this dissertation, is key to understand the true value of the technology. A hackathon is one of the approaches here a group of white hat hackers will infiltrate a test network being the Blue/Red Teams in charge of defense and counterattack roles.

The lead time between the concretization of the intrusion and the detection is one of the indicators, other, will be the quality of the information provided by the technology like the method of intrusion, type of threat used, attack origin, and so forth.

6. Bibliography

Arce, I., Daswani, N., Delgrosso, J., Dhillon, D., Kern, C., Kohno, T., … West, J. (2014). Avoiding the Top 10 Software Security Design Flaws. IEEE Computer Societys Center for Secure Design.

Barrett, E. T. (2013). Warfare in a New Domain: the Ethics of Military Cyber-Operations. Journal of Military Ethics, 12(1), 4–17. https://doi.org/10.1080/15027570.2013.782633.

Benbasat, I., Goldstein, D.K., & Mead, M. (1987). The Case Strategy in Studies of Information Systems. MIS Quarterly, 11, 3, 369-386.

Bratus, S. (2007). Hacker curriculum: How hackers learn networking. IEEE Distributed Systems Online, 8(10), 1–7. https://doi.org/10.1109/MDSO.2007.4384582

Cisco. (2016). Protecting Your Digital Business : The Case for Next-Generation Intrusion Prevention, 1–6.

Cooke, J. (2010). Center for Strategic and International Studies (Csis) Welcome :, (March).

Dinicu, A. (2014). Cyber Threats To National Security. Specific Features, 2(2), 109–114.

ECPI University. (n.d.). What's the Difference Between Network Security & Cyber Security? Retrieved June 13, 2017, from https://www.ecpi.edu/blog/whats-difference-between-network-security-cyber-security.

Fowler, C. A., & Nesbit, R. F. (1995). Tactical deception in air-land warfare. Journal of Electronic Defense, 18(6). (June), pp. 37-44 & 76-79.

Gervais, M. (2012). Cyber Attacks and the Laws of War Cyber Attacks and the Laws of War *. Berkley Journal of International Law, 30(2). https://doi.org/10.15779/Z38R66C.

Haeni, R. E. (1997). Information Warfare: An Introduction. An Introduction, (January), 1–16. Retrieved from papers3://publication/uuid/3286C29C-2FD1-45E6-9EB1-42B86721EA3A.

Health, T., & Portability, I. (n.d.). About HIPAA.com.

Hevner, Alan R, Salvatore T March, Jinsoo Park, and Sudha Ram. 2004. "Design Science in Information Systems Research." MIS Quarterly 28(1): 75–105. http://dblp.uni-trier.de/rec/bibtex/journals/misq/HevnerMPR04.

Ho, C. Y., Lai, Y. C., Chen, I. W., Wang, F. Y., & Tai, W. H. (2012). Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems. IEEE Communications Magazine, 50(3), 146–154. https://doi.org/10.1109/MCOM.2012.6163595

Hutchinson, W. (2006). Information warfare and deception. Informing Science, 9, 213–223.

Infosec Institute. (n.d.). Information and Asset Classification. Retrieved June 14, 2017, from http://resources.infosecinstitute.com/information-and-asset-classification/.

Institute, S. (2004). Interested in learning SANS Institute InfoSec Reading Room In tu , All r igh. Worm Propagation and Countermeasures, 36.

IEEE, the institute. (2015). Special Report: Cybersecurity - IEEE - The Institute. Retrieved June 16, 2017, from http://theinstitute.ieee.org/static/special-report-cybersecurity

IEEE Cyber Security. (n.d.-a). Avoiding the Top 10 Software Security Design Flaws – IEEE Cybersecurity. Retrieved June 16, 2017, from https://cybersecurity.ieee.org/blog/2015/11/13/avoiding-the-top-10-security-flaws/

IEEE Cyber Security. (n.d.-b). Try-CybSI. Retrieved June 16, 2017, from http://try.cybersecurity.ieee.org/trycybsi/

ISACA. (n.d.). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Retrieved June 12, 2017, from http://www.isaca.org/cobit/pages/default.aspx.

ISO. (n.d.). ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements. Retrieved June 13, 2017, from https://www.iso.org/standard/54534.html.

ITIL.org. (n.d.). ITIL - IT SERVICE MANAGEMENT BOOKSHOP - What is ITIL? Retrieved June 13, 2017, from https://www.itil.org.uk/.

Kopp, C. (2001). Classical Deception Techniques and Perception Management vs. the Four Strategies of Information Warfare. World.

Kostadinov, D. (n.d.). Information and Asset Classification. Retrieved June 13, 2017, from http://resources.infosecinstitute.com/information-and-asset-classification/.

Koumoutsos, G., & Thramboulidis, K. (2009). A knowledge-based framework for complex, proactive and service-oriented e-negotiation systems. Electronic Commerce Research, 9(4), 317–349. https://doi.org/10.1007/s10660-009-9040-6.

Kuechler, Bill, and Vijay Vaishnavi. 2011. "Promoting Relevance in IS Research: An Informing System for Design Science Research." Informing Science - the International Journal of an Emerging Transdiscipline 14: 125–38. http://www.inform.nu/Articles/Vol14/ISJv14p125-138Kuechler570.pdf.

Kuehl, D. T. (n.d.). Information Operations, Information Warfare, and Computer Network Attack, 76.

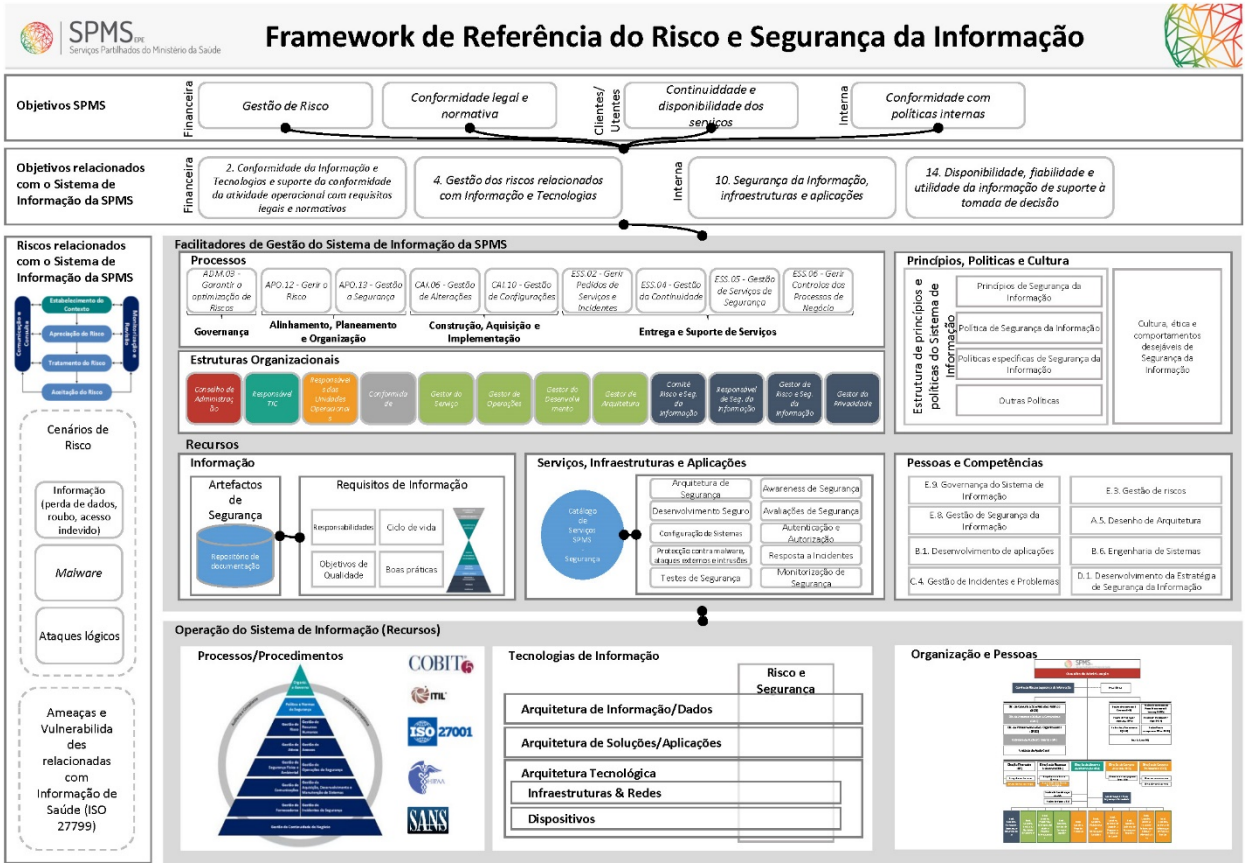
McFarland, K.P., & Stansell, J.C. (1993). Historical perspectives. In L. Patterson, C.M. Santa, C.G. Short, & K. Smith (Eds.), Teachers are researchers: Reflection and action. Newark, DE: International Reading Association.

Mirkovic, J., Reiher, P., Papadopoulos, C., Hussain, A., Shepard, M., Berg, M., & Jung, R. (2008). Testing a collaborative DDoS defense in a red team/blue team exercise. IEEE Transactions on Computers, 57(8), 1098–

1112. https://doi.org/10.1109/TC.2008.42.
Missouri State University. (2017). Password Complexity Requirements - Missouri State University. Retrieved June 13, 2017, from https://cams.missouristate.edu/selfservice/complexity.aspx.
Nabukenya, J. (2012). Combining Case Study, Design Science and Action Research Methods for Effective .Collaboration Engineering Research Efforts. 2012 45th Hawaii International Conference on System Sciences, 343–352. https://doi.org/10.1109/HICSS.2012.162.
Noffke, S.E., & Stevenson, R.B. (Eds.). (1995). Educational action research: Becoming practically critical. New York: Teachers College Press.
Okenyi, P. O., & Owens, T. J. (2007). On the Anatomy of Human Hacking. Information Systems Security, 16(6), 302–314. https://doi.org/10.1080/10658980701747237..
Pettey, C., & van der Meulen, R. (n.d.). Gartner Identifies the Top 10 Technologies for Information Security in 2016. Retrieved June 13, 2017, from http://www.gartner.com/newsroom/id/3347717.
Reswick, J. B. (1994). What constitutes valid research? Qualitative vs. quantitative research: EBSCOhost. Journal of Rehabilitation Research & Development, Vol. 31(Issue 2), Vii. https://doi.org/0748-7711.
Rowe, N. C. (2007). Deception in Defense of Computer Systems from Cyber Attack. Cyber Warfare and Cyber Terrorism, 97–104. https://doi.org/10.4018/978-1-59140-991-5.
Rowe, N. C., & Postgraduate, U. S. N. (2008). THE ETHICS OF DECEPTION IN CYBERSPACE Neil C. Rowe U.S. Naval Postgraduate School.
Rowe, N. C. (2003). Counterplanning deceptions to foil cyber-attack plans. IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, (June), 221–228. https://doi.org/10.1109/SMCSIA.2003.1232425
Sabău-Popa, D., Bradea, I., Boloș, M., & Delcea, C. (2015). The Information Confidentiality and Cyber Security in Medical Institutions. Annals of the University of Oradea, Economic Science Series, 24, 95–96. Retrieved from http://libproxy.albany.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=103190369&site=eds-live&scope=site.
Shim, J., & Arkin, R. C. (2013). A taxonomy of robot deception and its benefits in HRI. Proceedings - 2013 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2013, 2328–2335. https://doi.org/10.1109/SMC.2013.398
Vidgen, Richard, Brian Donnellan, Sabine Matook, and Kieran Conboy. 2012. “Practical Aspects of Design Science.” Communications in Computer and Information Science 286(March): 171–77. http://www.scopus.com/inward/record.url?eid=2-s2.0-84867457873&partnerID=tZOtx3y1.
Watts, H. (1985). When teachers are researchers, teaching improves. Journal of Staff Development, 6 (2), 118-127.

7. Appendix

7.1 Appendix A – SPMS Framework de Referência do Risco e Segurança da Informação



7.2 Appendix B – SPMS Programa de Melhoria Contínua do Risco e Segurança da Informação

Programa de Melhoria Contínua do Risco e Segurança da Informação

Implementação de Boas Práticas de Gestão, Controlo e Operação do Risco e Segurança da Informação na SPMS

SPMS EPE
Serviços Partilhados do Ministério da Saúde

SPMS EPE Serviços Partilhados do Ministério da Saúde

ENQUADRAMENTO

Os vetores primordiais de lançamento do projeto na SPMS visaram a **informação** e a **infraestrutura** como **ativos fundamentais** de suporte à atividade operacional

Promover a **adoção dessas práticas** internamente através da sensibilização de todos os colaboradores para a temática da segurança da informação

Orientar os **fundamentos base** de melhoria das práticas de governança, gestão e operação do Risco e Segurança da Informação na SPMS

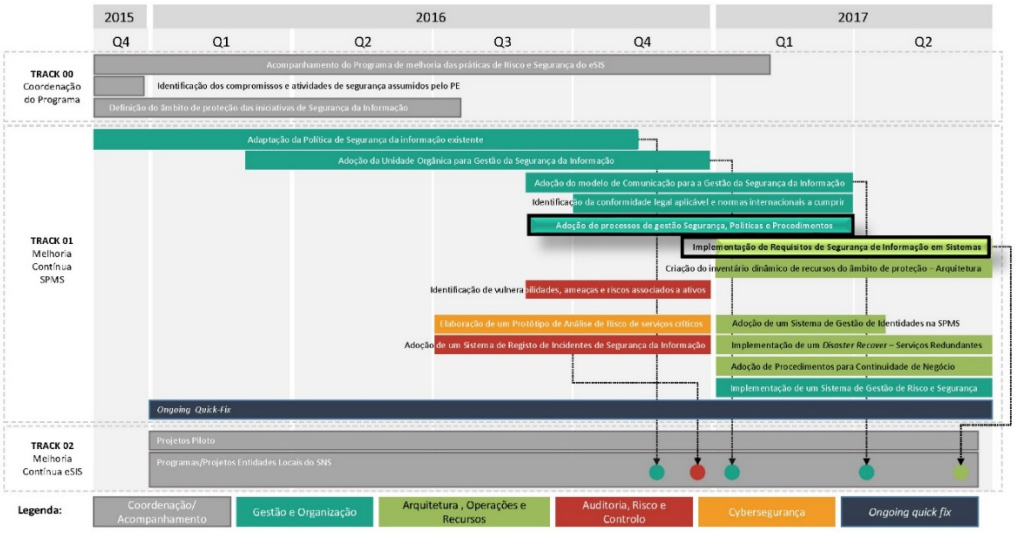
Suportar e monitorizar a implementação das práticas, no sentido de sustentar os objetivos e proteger os ativos de suporte à atividade operacional e os serviços disponibilizados

Contribuir para o **desenvolvimento de boas práticas** de referência (e.g. COBIT® 5, ISO/IEC 27001:2013) na SPMS

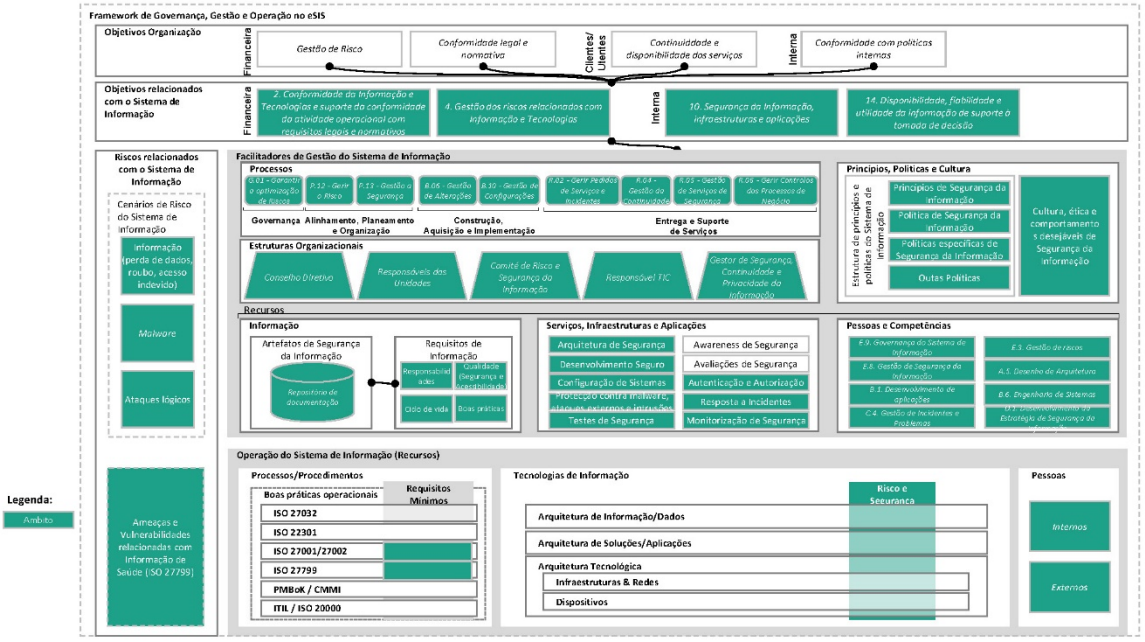
Fonte: *Declaração do Conselho de Administração [SPMS_SGSI_ORGOV_DOR_Declaração CA]*

03/06/2017 SPMS - Serviços Partilhados do Ministério da Saúde, E.P.E. www.spms.pt 2

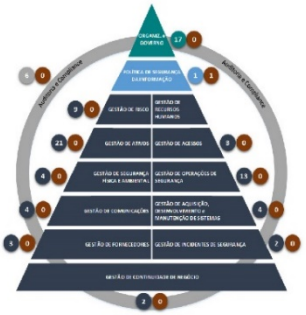
Cronograma inicial das iniciativas de Risco e Segurança da Informação



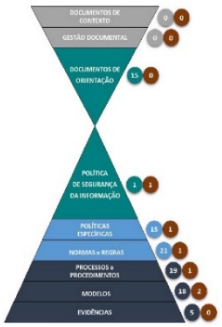
Framework de Referência do Risco e Segurança da Informação (2016)



Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
Documentos de Contexto	0	0	0	0	0	0,0%
Gestão Documental	0	0	0	0	0	0,0%
Documentos de Orientação	15	0	0	15	0	66,7%
Política de Segurança da Informação	1	0	0	0	1	100,0%
Políticas Específicas	15	0	0	14	1	68,9%
Normas e Regras	21	0	0	20	1	68,3%
Processos e Procedimentos	19	0	0	18	1	68,4%
Modelos	18	0	0	16	2	70,4%
Evidências	5	0	0	5	0	66,7%
Total	94	0	0	88	6	68,8%



Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
Organização e Governo	17	0	0	17	0	66,7%
Política de Segurança da Informação	1	0	0	0	1	100,0%
Gestão de Risco	9	0	0	9	0	66,7%
Gestão de Recursos Humanos	5	0	0	0	5	100,0%
Gestão de Ativos	21	0	0	21	0	66,7%
Gestão de Acessos	3	0	0	3	0	66,7%
Gestão de Segurança Física e Ambiental	4	0	0	4	0	66,7%
Gestão de Operações de Segurança	13	0	0	13	0	66,7%
Gestão de Comunicações	4	0	0	4	0	66,7%
Gestão de Aq., Des. e Man. de Sistemas	4	0	0	4	0	66,7%
Gestão de Fornecedores	3	0	0	3	0	66,7%
Gestão de Incidentes de Segurança	2	0	0	2	0	66,7%
Gestão de Continuidade de Negócio	2	0	0	2	0	66,7%
Auditoria e Compliance	6	0	0	6	0	66,7%
Total	94	0	0	88	6	68,8%



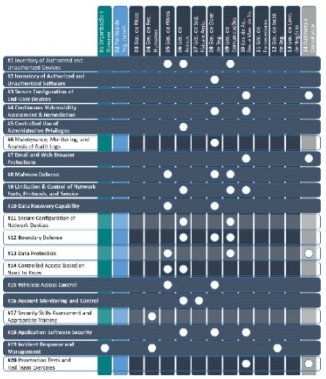
CONCLUSÕES

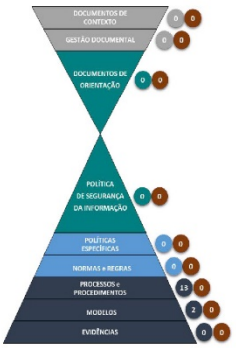
- 14 dimensões cobertas;
- Entregáveis em caderno de encargos respondidos (exceção workshop CA);
- Toda a documentação submetida à revisão das principais áreas envolvidas;
- 88 documentos estão em processo de aprovação formal;
- 6 documentos estão em produção e publicados na Intranet;
- 6 webinars efetuados;
- Totalidade das 12 gravações já concluídas.

(SharePoint\Sandra Santos\SPMS Inic. Sec. 06\02 Proj\03 Docs Rev\01 SGSI)

Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
Documentos de Contexto	0	0	0	0	0	0,0%
Gestão Documental	0	0	0	0	0	0,0%
Documentos de Orientação	0	0	0	0	0	0,0%
Política de Segurança da Informação	0	0	0	0	0	0,0%
Políticas Específicas	0	0	0	0	0	0,0%
Normas e Regras	0	0	0	0	0	0,0%
Processos e Procedimentos	13	0	0	13	0	66,7%
Modelos	2	0	0	2	0	66,7%
Evidências	0	0	0	0	0	0,0%
Total	15	0	0	15	0	66,7%

Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
#1 Inventory of Authorized & Unauthorized Devices	1	0	0	1	0	66,7%
#2 Inventory of Authorized & Unauthorized Software	1	0	0	1	0	66,7%
#3 Secure Configurations for Hardware & Software	1	0	0	1	0	66,7%
#4 Continuous Vulnerability Assessment & Remediation	1	0	0	1	0	66,7%
#5 Controlled Use of Administrative Priviledges	1	0	0	1	0	66,7%
#6 Maintenance, Monitoring & Analysis of Audit Logs	0	0	0	0	0	0,0%
#7 Email & Web Browser Protections	1	0	0	1	0	66,7%
#8 Malware Defense	1	0	0	1	0	66,7%
#9 Limitation & Control of Network Ports	1	0	0	1	0	66,7%
#10 Data Recovery Capability	1	0	0	1	0	66,7%
#11 Secure Configurantions for Network Devices	0	0	0	0	0	0,0%
#12 Boundary Defense	0	0	0	0	0	0,0%
#13 Data Protection	0	0	0	0	0	0,0%
#14 Controlled Access Based on the Need to Know	0	0	0	0	0	0,0%
#15 Wireless Access Control	1	0	0	1	0	66,7%
#16 Account Monitoring & Control	1	0	0	1	0	66,7%
#17 Security Skills Assessment and Appropriate Training to Fill Gaps	0	0	0	0	0	0,0%
#18 Application Software Security	1	0	0	1	0	66,7%
#19 Incident Response & Management	1	0	0	1	0	66,7%
#20 Penetration Tests & Red Team Exercises	0	0	0	0	0	0,0%
Total	13	0	0	13	0	66,7%





CONCLUSÕES

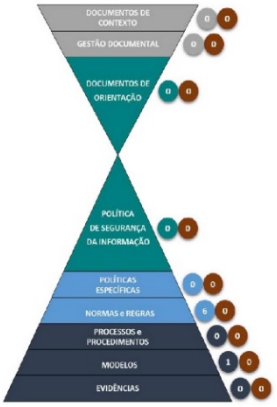
- 13 controlos cobertos de um total de 20;
- Todos os controlos de cibersegurança definidos e devidamente alinhados com as dimensões do modelo de referência;
- Todos os controlos submetidos à revisão e validação da SPMS (OSI).

(SharePoint\Sandra Santos\SPMS Inic. Sec. 06\02 Proj\03 Docs Rev\02 CyberCtrls)

ESTRUTURAS ORGANIZACIONAIS

Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
Documentos de Contexto	0	0	0	0	0	0,0%
Gestão Documental	0	0	0	0	0	0,0%
Documentos de Orientação	0	0	0	0	0	0,0%
Política de Segurança da Informação	0	0	0	0	0	0,0%
Políticas Específicas	0	0	0	0	0	0,0%
Normas e Regras	6	0	0	6	0	66,7%
Processos e Procedimentos	0	0	0	0	0	0,0%
Modelos	1	0	0	1	0	66,7%
Evidências	0	0	0	0	0	0,0%
Total	7	0	0	7	0	66,7%

Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
EO.01 Conselho de Administração	1	0	0	1	0	66,7%
EO.02 Responsáveis das Unidades Operacionais	1	0	0	1	0	66,7%
EO.03 Responsáveis de Processos	0	0	0	0	0	0,0%
EO.04 Comité Estratégico e de Arquitetura	0	0	0	0	0	0,0%
EO.05 Comité de Programas e Projetos	0	0	0	0	0	0,0%
EO.06 Comité de Risco e Segurança da Informação	1	0	0	1	0	66,7%
EO.07 Responsável de Segurança da Informação	1	0	0	1	0	66,7%
EO.08 Responsável de Recursos Humanos	0	0	0	0	0	0,0%
EO.09 Auditoria e Conformidade	0	0	0	0	0	0,0%
EO.10 Responsável TIC	1	0	0	1	0	66,7%
EO.11 Gestor de Arquitetura	0	0	0	0	0	0,0%
EO.12 Gestor de Desenvolvimento	0	0	0	0	0	0,0%
EO.13 Gestor de Operações	0	0	0	0	0	0,0%
EO.14 Gestor de Serviço	0	0	0	0	0	0,0%
EO.15 Gestor de Risco e Segurança da Informação	1	0	0	1	0	66,7%
EO.16 Gestor de Privacidade	0	0	0	0	0	0,0%
Total	6	0	0	6	0	66,7%



CONCLUSÕES

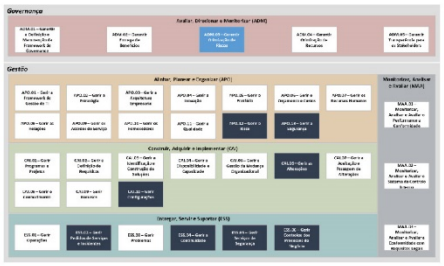
- 6 estruturas organizacionais detalhadas de um total de 16;
- Definição das responsabilidades e funções das estruturas com impacto na segurança da informação;
- Todas as estruturas devidamente mapeadas e assignadas na documentação desenvolvida;
- Todas as estruturas estão prontas para aprovação por parte da SPMS.

(SharePoint\Sandra Santos\SPMS Inic. Sec. 06\02 Proj\03 Docs Rev\04 EstOrg)

PROCESSOS DE GOVERNANÇA

Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
Documentos de Contexto	0	0	0	0	0	0,0%
Gestão Documental	0	0	0	0	0	0,0%
Documentos de Orientação	0	0	0	0	0	0,0%
Política de Segurança da Informação	0	0	0	0	0	0,0%
Políticas Específicas	0	0	0	0	0	0,0%
Normas e Regras	8	0	0	8	0	66,7%
Processos e Procedimentos	0	0	0	0	0	0,0%
Modelos	1	0	0	1	0	66,7%
Evidências	0	0	0	0	0	0,0%
Total	9	0	0	9	0	66,7%

Documentos	Total	Por Iniciar	Em Progresso	Em Aprovação	Em Produção	Percentagem de Conclusão
Avaliar, Direcionar e Monitorizar (ADM)	0	0	0	0	0	0,0%
Alinhar, Planear e Organizar (APO)	2	0	0	2	0	66,7%
Construir, Adquirir e Implementar (CAI)	2	0	0	2	0	66,7%
Entregar, Servir e Suportar (ESS)	4	0	0	4	0	66,7%
Monitorizar, Analisar e Avaliar (MAA)	0	0	0	0	0	0,0%
Total	8	0	0	8	0	66,7%

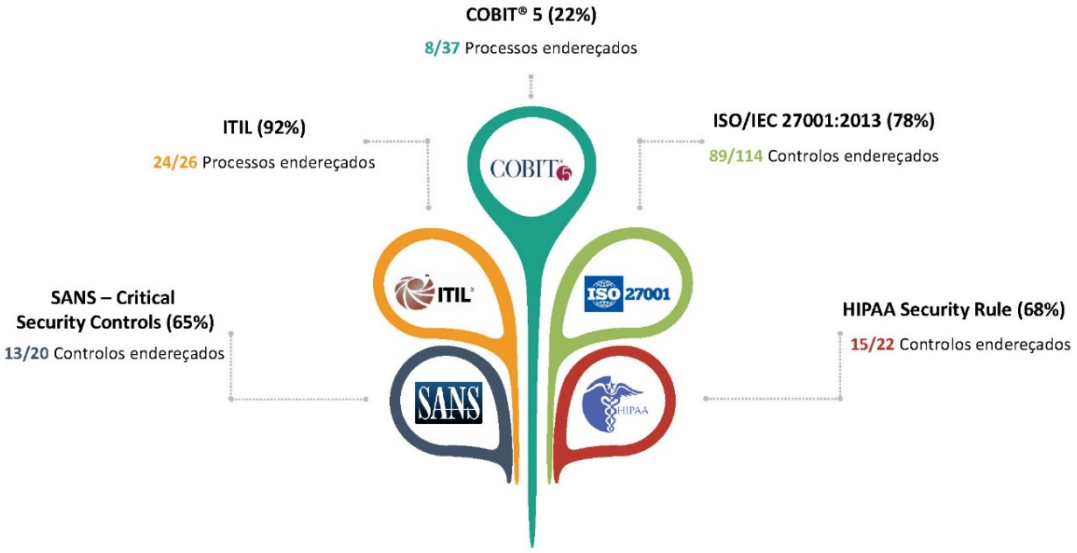


CONCLUSÕES

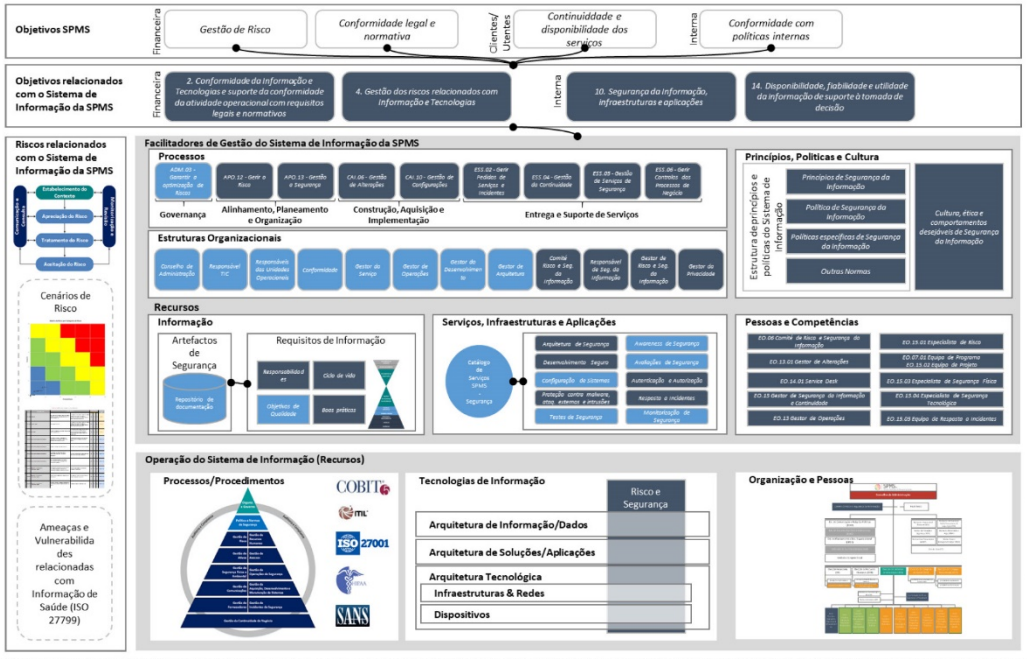
- 8 processos de governança detalhados de um total de 37;
- Alinhamento e mapeamento com as restantes normas internacionais (ISO/IEC 27001:2013, HIPAA Security Rule e ITIL);
- Todos os processos estão prontos para aprovação por parte da SPMS.

(SharePoint\Sandra Santos\SPMS Inic. Sec. 06\02 Proj\03 Docs Rev\03 Proc)

A informação produzida encontra-se alinhada com as **boas práticas de referência**



Framework de Referência do Risco e Segurança da Informação (2017)



A solução está na partilha!

Obrigado

7.3 Appendix C – SPMS Framework da Documentação no Âmbito de Segurança da Informação

Framework da Documentação no Âmbito de Segurança da Informação

SPMS_SGSI_ ORGOV_DOR_Framework Documentação

VERSÃO:	1.0
DATA DE APROVAÇÃO:	<dd – mm – aaaa>
DATA DA ÚLTIMA REVISÃO:	<dd – mm – aaaa>
VALIDO ATÉ:	<dd – mm – aaaa>
RESPONSÁVEL:	Responsável de Segurança da Informação
APROVADOR:	Conselho de Administração
CLASSIFICAÇÃO DO DOCUMENTO:	INTERNO
LOCALIZAÇÃO	<LINK>

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

Índice

1. Introdução

1.1 Enquadramento do Documento

A "Framework da Documentação no Âmbito de Segurança da Informação" é um documento que surge com base no documento "Framework da Documentação da SPMS" para organizar a documentação da Segurança da Informação da SPMS.

1.2 Âmbito do Documento

A "Framework da Documentação no Âmbito de Segurança da Informação" aplica-se a todos os documentos (artefactos) de Segurança da Informação produzidos internamente ou recebidos do exterior.

1.3 Finalidade do Documento

a) Instituir o modelo de gestão documental e adaptar para a Segurança da Informação a linguagem comum utilizada transversalmente para toda a documentação da SPMS.

2 Framework da Documentação no Âmbito de Segurança da Informação

2.1 Estrutura Documental de Segurança da Informação

A documentação da SPMS no âmbito de Risco e Segurança da Informação deve ser organizada de acordo com a "Framework da Documentação no Âmbito da Segurança da Informação" para estruturar e suportar a Segurança da Informação num conjunto de documentos que é dividido em quatro níveis hierárquicos descritos na Figura 1.

Esta estrutura documental assenta numa base estabelecida e definida de estruturas organizacionais devidamente explanadas no documento "Estruturas Organizacionais de Suporte ao Risco e Segurança da Informação".

Todas as alterações relativas à documentação constante desta estrutura deverão obedecer o procedimento instituído e definido "Procedimento de Gestão de Documentação (Segurança da Informação)".

Figura 1 - Estrutura Documental no âmbito de Segurança da Informação

NÍVEL		TIPOS DE DOCUMENTOS	EXEMPLOS DE DOCUMENTOS	RESPONSÁVEL	APROVADOR	INFORMADO
1	CONTEXTO	DOCUMENTOS DE CONTEXTO	Descrição do Contexto interno e externo Requisitos legais e contratuais Requisitos das partes interessadas	Responsável de Segurança da Informação	Conselho de Administração	Comité de Risco e Segurança da Informação e Responsável TIC
		GESTÃO DOCUMENTAL	*Frameworks* da Documentação Modelo de Capacidade da Documentação Procedimentos de Gestão Documental	Responsável de Segurança da Informação	Conselho de Administração	Comité de Risco e Segurança da Informação e Responsável TIC
2	ESTRATÉGICO	DOCUMENTOS DE ORIENTAÇÃO	Âmbito do SGSI, Princípios SI, Estratégia SI, Objetivos SI, Estruturas Organizacionais SI	Responsável de Segurança da Informação	Conselho de Administração	Comité de Risco e Segurança da Informação e Responsável TIC
		POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Política de Segurança da Informação Declaração de Compromisso	Responsável de Segurança da Informação	Conselho de Administração	Comité de Risco e Segurança da Informação e Responsável TIC
3	TÁTICO	POLÍTICAS ESPECÍFICAS	Políticas específicas de alto nível dentro das respetivas áreas de SI mapeadas às cláusulas da norma ISO/IEC 27001:2013;	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação	Comité de Risco e Segurança da Informação, Responsáveis dos Processos e Responsáveis das Unidades Operacionais
		NORMAS E REGRAS	Normas e Regras técnicas dentro das respetivas áreas de SI mapeadas às cláusulas da norma ISO/IEC 27001:2013;	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação	Comité de Risco e Segurança da Informação, Responsáveis dos Processos e Responsáveis das Unidades Operacionais
4	OPERACIONAL	PROCESSOS E PROCEDIMENTOS	Processos e procedimentos detalhados	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação	Responsáveis dos Processos e Responsáveis das Unidades Operacionais
		MODELOS	Modelos de registos, relatórios, planos e programas, Exemplos de cláusulas contratuais	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação	Responsáveis dos Processos e Responsáveis das Unidades Operacionais
		EVIDÊNCIAS	Registos, Relatórios, Planos etc.	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação	Responsáveis dos Processos e Responsáveis das Unidades Operacionais

Tabela 1 - Responsabilidade pela Gestão Documental no âmbito de Risco e Segurança da Informação

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

Tendo em conta que a estrutura documental da SPMS no âmbito de Risco e Segurança da Informação inclui um grande número de políticas e normas e respetivos processos e procedimentos que orientam as atividades operacionais e asseguram a proteção da informação da SPMS dia-a-dia, foi detalhada a estrutura dos Normativos de Segurança da Informação da SPMS que se encontra no **Anexo A - Estrutura dos Normativos de Segurança da Informação da SPMS**. Adicionalmente, o **Anexo A** apresenta o mapeamento dos Normativos de Segurança da Informação com as cláusulas da norma NP ISO/IEC 27001:2013.

Os normativos afetos especificamente à Segurança da Informação da SPMS são expressos nos quadrantes a seguir especificados.

2.1.1 Nível Estratégico (Documentos de Orientação e Política de Segurança da Informação)

Este nível é constituído por documentação de base orientada aos fundamentos do estabelecimento das responsabilidades de segurança da informação. Como alinhamento macro deste vetor estratégico existem dois documentos, entre outros, que toldam a atuação e definem os pilares de suporte, são eles, o "Documento de Âmbito de Segurança da Informação" e a "Política de Segurança da Informação" (PSI).

A documentação constante do Nível Estratégico deve ser revista no mínimo anualmente ou sempre que ocorram alterações significativas que impactem a mesma.

2.1.1.1 Documento de Âmbito de Segurança da Informação

O "Documento de Âmbito de Segurança da Informação" pressupõe o alinhamento e estratégias internas à equipa de Segurança da Informação, nomeadamente no que concerne aos Princípios, Objetivos e Políticas de Segurança da Informação necessários a um nível de segurança coerente e robusto com as necessidades expectáveis.

O documento é assente no Modelo de Referência que pretende ser uma representação gráfica e diretamente mapeada às cláusulas da norma ISO/IEC 27001:2013, com ajustes onde necessário às necessidades da SPMS, devendo a mesma ser encarada como a contextualização interna de funcionamento da Equipa.

O Modelo de Referência engloba 14 dimensões e representa, por isso, a visão holística da Segurança da Informação da SPMS, cobrindo todos os domínios pertinentes da arquitetura da Segurança da Informação.

2.1.1.2 Política de Segurança da Informação

A PSI é o documento do nível Estratégico que tem caráter permanente e define a Segurança da Informação da SPMS para orientar o desenvolvimento de todos os documentos dos níveis Tático e Operacional da *framework*, bem como todas as atividades operacionais relacionadas com a Segurança da Informação. Todos os normativos de Segurança da Informação dos níveis Tático e Operacional (e.g. políticas específicas, normas internas, procedimentos) devem ser baseados ou refletir as preocupações e considerações estabelecidas por este documento.

2.1.2 Nível Tático (Políticas Específicas, Normas e Regras)

Este nível é constituído por documentação de formada por Políticas Específicas, Normas e Regras. Estas visam determinar e guiar as atividades materializadas no Nível Operacional estabelecendo a base mínima de conformidade que tem de ser garantida.

A documentação constante do Nível Tático deve ser revista no mínimo anualmente ou sempre que ocorram alterações significativas que impactem a mesma.

2.1.2.1 Políticas Específicas

A Políticas Específicas de Segurança da Informação são os documentos que estabelecem regras, orientações e responsabilidades de alto nível dentro das respetivas áreas de Segurança da Informação mapeadas às cláusulas da norma ISO/IEC 27001:2013. As Políticas Específicas devem ser baseadas ou refletir as preocupações e considerações estabelecidas pela PSI e respeitar os "Princípios de Segurança da Informação".

2.1.2.2 Normas e Regras

As Normas e Regras de Segurança da Informação são os documentos mais detalhados que fazem menção especial às tecnologias, métodos, procedimentos de implementação e outros detalhes, sendo o tempo da sua aplicabilidade inferior ao das políticas, tendo em conta a sua natureza mais técnica. As Normas e Regras devem ser baseadas ou refletir as preocupações e considerações estabelecidas pela(s) Política(s) Específica(s) dentro do respetivo domínio de Segurança da Informação.

2.1.3 Nível Operacional (Processos e Procedimentos, Modelos e Evidências)

Os Processos e Procedimentos, Modelos e Evidências de Segurança da Informação são documentos que materializam nas atividades da SPMS as tarefas relacionadas com a Segurança da Informação, bem como definem do ponto de vista operacional o que deve ser assegurado pelas áreas responsáveis. Os Processos e Procedimentos, Modelos e Evidências devem ser baseados ou refletir as preocupações e considerações estabelecidas pelas Normas e Regras dentro do respetivo domínio de Segurança da Informação.

A documentação constante do Nível Tático deve ser revista sempre que ocorram alterações significativas que impactem a mesma, nomeadamente, alterações em qualquer da documentação dos Níveis Estratégico ou Tático.

2.2 Nomenclatura de Codificação da Estrutura Documental

Os critérios e regras que devem ser seguidos no processo de codificação de todos os documentos relacionados com a Segurança da Informação e que visão otimizar o processo de gestão documental são:

- Evitar a ambiguidade de identificação dos documentos, através da referência e identificação unívoca; e
- Evitar inconsistências decorrentes da caducidade ou alteração da documentação;

De seguida, é apresentado um exemplo de codificação que agrega os sete campos separados por "_" (*underscore*), que definem a nomenclatura a aplicar nos documentos relacionados com Segurança da Informação:

SPMS_SGSI_Dimensão_Tipo_Nome do documento_v1.0_AAAAMMDD

Onde cada um dos sete campos representa:

1. **SPMS:** Serviços Partilhados do Ministério da Saúde;
2. **SGSI:** Sistema de Gestão de Segurança da Informação;
3. **Dimensão:** Dimensão alinhada com o Modelo de Referência (código de cinco caracteres);
4. **Tipo:** Tipo de documento de acordo com a "Estrutura Documental no Âmbito de Segurança da Informação" (código de três caracteres);
5. **Nome do documento:** Nome abreviado do documento no âmbito de Segurança de Informação;
6. **v1.0:** Número a identificar a versão do documento; e
7. **AAAAMMDD:** Data da modificação do documento em causa, composta pela concatenação do ano, mês e dia.

2.2.1 Códigos de Dimensões e Tipos de documentação

O conjunto de códigos definidos para as 14 dimensões e os nove tipos de documentação são apresentados nas duas tabelas abaixo.

#	DIMENSÃO	CÓDIGO
01	Organização e Governo	ORGOV
02	Política de Segurança da Informação	PLTSI
03	Gestão de Risco	GRISC
04	Gestão de Recursos Humanos	GESRH
05	Gestão de Ativos	GATIV
06	Gestão de Acessos	GACES
07	Gestão de Segurança Física e Ambiental	GSFIS
08	Gestão de Operações de Segurança	GOSEG
09	Gestão de Comunicações	GCOMU
10	Gestão da Aquisição, Desenvolvimento e Manutenção de Sistemas	GADMS
11	Gestão de Fornecedores	GFORN

12	Gestão de Incidentes de Segurança	GISEG
13	Gestão da Continuidade de Negócio	GCNEG
14	Auditoria e Compliance	AUCOM

Tabela 2 - Códigos de dimensões do Modelo de Referência

NÍVEL	#	TIPO DE DOCUMENTO	CÓDIGO
Contexto	01	Documentos de Contexto	DOC
	02	Gestão Documental	GDO
Estratégico	03	Documentos de Orientação	DOR
	04	Política de Segurança da Informação	PSI
Tático	05	Políticas Específicas	PES
	06	Normas e Regras	NRM
Operacional	07	Processos e Procedimentos	PRC
	08	Modelos	MOD
	09	Evidências	EVI

Tabela 3 - Códigos de tipos de documentação (3 caracteres)

2.3 Classificação da Documentação de Segurança da Informação

A classificação da documentação de Risco e Segurança da Informação deve ser feita de acordo com a "Política Específica de Classificação da Informação (Segurança da Informação)".

2.4 Aprovação Final da Documentação

Após todas as revisões e validações terem sido efetuadas à documentação criada ou alterada, quer pela área de Segurança da Informação ou outra, deve ser as mesmas aprovadas mediante ferramenta interna (*Smart Governance*) e de acordo com o seguinte fluxo:

NÍVEL		TIPOS DE DOCUMENTOS	SUBMETIDOS POR	APROVADOR
1	CONTEXTO	DOCUMENTOS DE CONTEXTO	Responsável de Segurança da Informação	Conselho de Administração
		GESTÃO DOCUMENTAL	Responsável de Segurança da Informação	Conselho de Administração

2	ESTRATÉGICO	DOCUMENTOS DE ORIENTAÇÃO	Responsável de Segurança da Informação	Conselho de Administração
		POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Responsável de Segurança da Informação	Conselho de Administração
3	TÁTICO	POLÍTICAS ESPECÍFICAS	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação
		NORMAS E REGRAS	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação
4	OPERACIONAL	PROCESSOS E PROCEDIMENTOS	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação
		MODELOS	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação
		EVIDÊNCIAS	Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação

Tabela 4 – Workflow de aprovação final de documentação no âmbito da Segurança da Informação

Anexo A - Estrutura dos Normativos de Segurança da Informação da SPMS

A estrutura completa de normativos de segurança da informação encontra-se especificada no documento "Arquitetura de Referência da Informação (Segurança da Informação)".

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

3 Controlo do Documento

Histórico de Revisões/Alterações

VERSÃO	DATA	AUTOR	APROVADOR	REVISÃO/ALTERAÇÃO
1.0		Responsável de Segurança da Informação	Conselho de Administração	Primeira versão do documento

Lista de Distribuição

DESTINATÁRIOS
SPMS

Termos e Acrónimos

TERMO OU ACRÓNIMO	DESCRIÇÃO
PSI	Política de Segurança da Informação
SPMS	Serviços Partilhados do Ministério da Saúde, E.P.E.
SI	Segurança da Informação
SGSI	Sistema da Gestão de Segurança da Informação
TIC	Tecnologias de Informação e Comunicação

Documentos Relacionados

REFERÊNCIA	TÍTULO
SPMS_SGSI_ORGOV_DOR_Âmbito SegInfo	Documento de Âmbito de Segurança da Informação

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

SPMS_SGSI_ORGOV_DOR_Princípios SegInfo	Princípios de Segurança da Informação
SPMS_SGSI_ORGOV_DOR_Estruturas Org	Estruturas Organizacionais de Suporte ao Risco e Segurança da Informação
SPMS_SGSI_PLTSI_PSI_Política SegInfo	Política de Segurança de Informação
SPMS_SGSI_GATIV_PES_Classicação Info	Política Específica de Classificação da Informação (Segurança da Informação)
SPMS_SGSI_GATIV_MOD_Arq Info	Arquitetura de Referência da Informação (Segurança da Informação)

Boas Práticas de Referência

REFERÊNCIA	TÍTULO
COBIT® 5	*A Business Framework for the Governance and Management of Enterprise IT*
ISO/IEC 27000:2016	*Information technology - Security techniques - Information security management systems - Overview and vocabulary*
ISO/IEC 27001:2013	*Information technology - Security techniques - Information security management systems - Requirements*
ISO/IEC 27002:2013	*Information technology - Security techniques - Code of practice for information security controls*
NP 4438-1 2005	Informação e documentação - Gestão de documentos de arquivo: parte 1: princípios diretores

Fim de Documento

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

7.4 Appendix D – SPMS Arquitetura de Referência da Informação

Arquitetura de Referência da Informação (Segurança da Informação)

SPMS_SGSI_GATIV_MOD_Arq Info

VERSÃO:	1.0
DATA DE APROVAÇÃO:	<dd – mm – aaaa>
DATA DA ÚLTIMA REVISÃO:	<dd – mm – aaaa>
VALIDO ATÉ:	<dd – mm – aaaa>
RESPONSÁVEL:	Gestor de Segurança da Informação e Continuidade
APROVADOR:	Responsável de Segurança da Informação
CLASSIFICAÇÃO DO DOCUMENTO:	INTERNO
LOCALIZAÇÃO	<LINK>

Índice

1. Introdução

1.1. Enquadramento do Documento

A "Arquitetura de Referência da Informação (Segurança da Informação)" é um documento que se enquadra ao nível Operacional e na dimensão de Gestão de Ativos da "Framework da Documentação no Âmbito da Segurança da Informação".

1.2. Âmbito do Documento

A Segurança da Informação é relevante para todos os tipos de informação e para todos os sistemas que a guardam, processam ou transferem, seja no contexto de simples sistemas de indexação e arquivo em papel ou em sistemas especializados e tecnologicamente avançados.

1.3. Finalidade do Documento

a) Formalizar a Arquitetura de Referência da Informação relacionada com a Segurança da Informação na SPMS; e
b) Contribuir para o enquadramento de cada documento na arquitetura global de informação de Segurança da Informação, assim como os outros documentos relacionados.

2. Arquitetura de Referência da Informação

2.1. Modelo de Referência de Segurança da Informação da SPMS

O Modelo de Referência representa a visão holística da Segurança da Informação da SPMS e cobre todos os domínios pertinentes da arquitetura da Segurança da Informação. Este Modelo de Referência engloba 14 dimensões, as quais encontram-se alinhadas com a Norma de referência ISO/IEC 27001:2013.

As 14 dimensões são apresentadas em detalhe no "Documento de Âmbito de Segurança da Informação". Estas dimensões foram modeladas em Archimate como *business objects*, tal como apresentado no modelo na Figura 1.

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

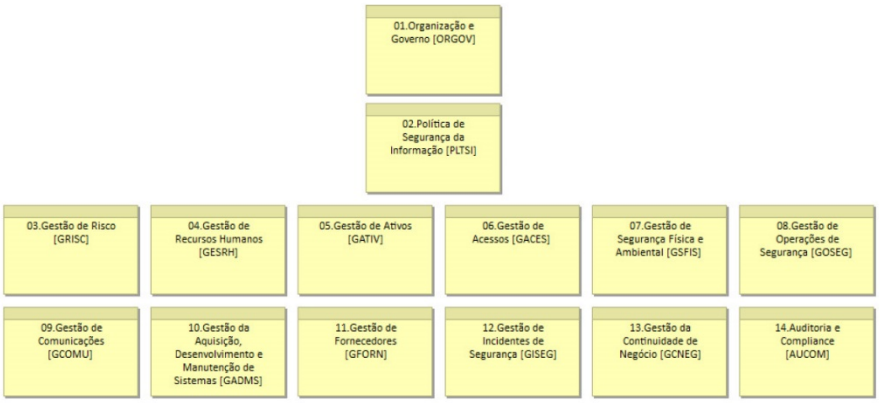


Figura 1 - Modelo de Referência da SPMS e respetivas dimensões em Archimate

2.2. Estrutura Documental da Segurança da Informação

A documentação da SPMS no âmbito de Risco e Segurança da Informação está descrita no documento "Framework da Documentação no Âmbito de Segurança da Informação".

Esta estrutura documental foi modelada em Archimate através de *business objects*, tal como apresentado na Figura 2.

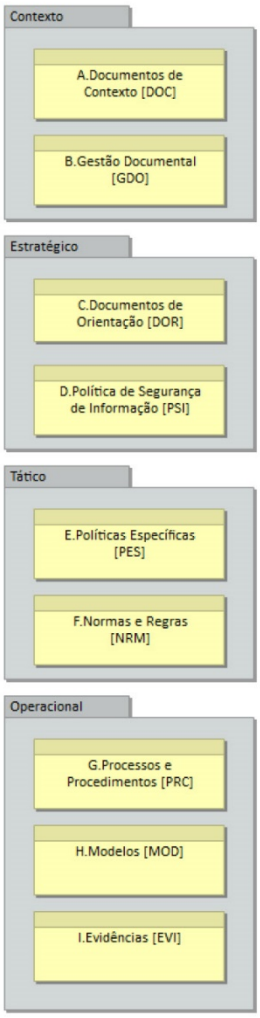


Figura 2 - Estrutura Documental no âmbito de Segurança da Informação em Archimate

2.3. Modelação da Arquitetura de Informação

A modelação em Archimate da Arquitetura de Referência da Informação permite uma visão holística da documentação no âmbito de Segurança de Informação na SPMS. Deste modo, é possível compreender onde cada documento se encaixa na arquitetura de informação global, nomeadamente a respetiva dimensão do modelo de referência, assim como o tipo de documento. Adicionalmente, as relações entre documentos também se encontram modeladas, o que facilita a compreensão das inter-relações.

A visão global da arquitetura de referência da informação pode ser consultada no ficheiro abaixo.

Arquitectura de Referência da Inforr

De seguida, são apresentadas as 14 dimensões, bem como uma breve descrição do conteúdo do ponto de vista documental de cada uma.

01. Organização e Governo

Os documentos relacionados com a dimensão Organização e Governo incluem artefactos como missão, valores, enquadramento, representação no Conselho de Administração, objetivos, âmbito, organização interna, funções, responsabilidades, segregação de funções e contactos com entidades externas.

02. Política de Segurança da Informação

Os documentos relacionados com a dimensão Política de Segurança da Informação inclui o documento da "Política de Segurança da Informação" (PSI).

03. Gestão de Risco

Os documentos relacionados com a dimensão Gestão de Risco incluem artefactos como modelos e metodologia de Gestão de Risco, bem como toda a documentação de suporte à gestão e tratamento do risco.

04. Gestão de Recursos Humanos

Os documentos relacionados com a dimensão Gestão de Recursos Humanos incluem artefactos como cláusulas de segurança na gestão pré contratual, durante contrato e pós contrato e cultura e promoção da segurança da informação.

05. Gestão de Ativos

Os documentos relacionados com a dimensão Gestão de Ativos incluem artefactos como regras relativas às responsabilidades dos ativos, classificação da informação, gestão da informação e controlos de criptografia.

06. Gestão de Acessos

Os documentos relacionados com a dimensão Gestão de Acessos incluem artefactos como requisitos para o controlo de acessos, gestão de acessos, responsabilidades dos utilizadores, gestão de entidades e utilizadores nas aplicações.

07. Gestão de Segurança Física e Ambiental

Os documentos relacionados com a dimensão Gestão de Segurança Física e Ambiental incluem artefactos como controlo físico de equipamentos, controlo físico de pessoas e definições de perímetro.

08. Gestão de Operações de Segurança

Os documentos relacionados com a dimensão Gestão de Operações de Segurança incluem artefactos como procedimentos operacionais e responsabilidades nas operações, proteção contra código malicioso, *backups*, monitorização e *logging*, controlo do software operacional e gestão de vulnerabilidades técnicas

09. Gestão de Comunicações

Os documentos relacionados com a dimensão Gestão de Comunicações incluem artefactos como gestão da segurança de rede, controlo das comunicações, proteção de serviços e transferência de informação.

10. Gestão da Aquisição, Desenvolvimento e Manutenção de Sistemas

Os documentos relacionados com a dimensão Gestão da Aquisição, Desenvolvimento e Manutenção de Sistemas incluem artefactos como requisitos de segurança para sistemas de informação, segurança no desenvolvimento e processos de suporte, dados para testes e testes de segurança.

11. Gestão de Fornecedores

Os documentos relacionados com a dimensão Gestão de Fornecedores incluem artefactos como cláusulas de segurança para garantir a segurança da informação com entidades terceiras e a gestão do serviço de entidades terceiras.

12. Gestão de Incidentes de Segurança

Os documentos relacionados com a dimensão Gestão de Incidentes de Segurança incluem artefactos como gestão de incidentes de segurança, planos de resposta e melhoria contínua.

13. Gestão da Continuidade de Negócio

Os documentos relacionados com a dimensão Gestão da Continuidade de Negócio incluem artefactos de continuidade da segurança da informação, bem como de planos de continuidade de negócio.

14. Auditoria e Compliance

Os documentos relacionados com a dimensão Auditoria e Compliance incluem artefactos de conformidade com questões legais e auditorias de segurança.

3. Controlo do Documento

Histórico de Revisões/Alterações

VERSÃO	DATA	AUTOR	APROVADOR	REVISÃO/ALTERAÇÃO
1.0		Gestor de Segurança da Informação e Continuidade	Responsável de Segurança da Informação	Primeira versão do documento

Lista de Distribuição

DESTINATÁRIOS
SPMS

Termos e Acrónimos

TERMO OU ACRÓNIMO	DESCRIÇÃO
Archimate	Linguagem de modelação para Arquitetura Empresarial, aberta e alinhada com as boas práticas do mercado
PSI	Política de Segurança da Informação
SPMS	Serviços Partilhados do Ministério da Saúde, E.P.E.

Documentos Relacionados

REFERÊNCIA	TÍTULO
SPMS_SGSI_ORGOV_DOR_Framework Documentação	*Framework* da Documentação no Âmbito de Segurança da Informação
SPMS_SGSI_PLTSI_PSI_Política SegInfo	Política de Segurança da Informação

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

SPMS_SGSI_ORGOV_DOR_Âmbito SegInfo	Documento de âmbito de segurança da informação

Boas Práticas de Referência

REFERÊNCIA	TÍTULO
ISO/IEC 27000:2016	*Information technology - Security techniques - Information security management systems - Overview and vocabulary*
ISO/IEC 27001:2013	*Information technology - Security techniques - Information security management systems - Requirements*
ISO/IEC 27002:2013	*Information technology - Security techniques - Code of practice for information security controls*
ArchiMate® 3.0	*ArchiMate® 3.0 Specification, an Open Group Standard*

Fim de Documento

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. República, nº 61 - 8º piso, 1050-189 Lisboa Tel.: 211 545 600 | Fax: 211 545 649
Capital Estatutário: 25.637.140,00 €, N.º único de matrícula na C.R.C. Lisboa e de pessoa coletiva 509 540716

7.5 Appendix E – Information Security Technologies Comparison Table

Information Security Technologies	Cyber Incident Threats									
	Phishing and Email Spamming	**Botnet**	**Malware and Spyware**	**Keyloggers**	**Social Engineering**	**Denial of Service**	**Virus**	**Worm**	**Advanced Persistent Threat (ATP)**	
	Type of threat through the internet, or flooding of the Internet or any unwanted online correspondences	Guard of compromised Systems, sometimes called "zombies," that are under the command and control of a solitary "Botmaster."	Malicious program designed to gather computer information without the awareness of the client.	Programs that can screen and record the client keyboard information while typing in Computer System for later access.	Kind of technique in which it traps or tricks the client to reveal valuable information.	Attack that upsets the normal function of the computer system and thus prevents access to authorized users	Program that spreads itself from one computer to another computer without the users' authorization to do so	Computer Program that moves from one machine environment, then onto the next machine environment often keeping a record of the last environment	Continuous computer hacking that is actively supported by several people that usually targets one specific entity.	
Access Security Brokers	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**2**
Software as a Service (SaaS) apps, increasingly pervasive in enterprises, provide new challenges to security teams with their limited visibility and control options. Cloud Access Security Brokers (CASB) allow chief information security officers (CISOs) an opportunity to apply enterprise security policies across multiple cloud services.										
Endpoint Detection and Response	**3**	**3**	**3**	**3**	**0**	**0**	**3**	**3**	**0**	**18**
Endpoint detection and response (EDR) solutions allow CISOs to detect potential security breaches and react quickly. These tools record endpoint and network events, and the data are continuously searched using known indicators of compromise (IOC) and machine-learning techniques for early identification of breaches.										
No signature Approaches to Endpoint Prevention	**3**	**0**	**3**	**0**	**0**	**0**	**3**	**0**	**0**	**9**
Techniques such as memory protection and exploit prevention and machine learning-based systems, which uses mathematical models, augment ineffective signature-based approaches for malware prevention against advanced and targeted attacks.										
User and Entity Behavioral Analytics	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**3**	**3**
User and entity behavioral analytics provide user-centric analytics alongside information about networks, endpoints, and applications.										
Microsegmentation and Flow Visibility	**0**	**3**	**3**	**0**	**0**	**0**	**3**	**3**	**3**	**15**
Microsegmentation, a more granular segmentation, stops attackers already in the system from moving laterally ("east/west") to other systems. Visualization tools allow security teams to understand flow patterns, set segmentation policies and monitor for deviations. For data in motion, some vendors provide optional encryption of the network traffic.										
Security Testing for DevOps	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**8**
As DevOps integrates security into the workflow (DevSecOps) emerging operating models offer an automated, transparent and compliant configuration of underlying security infrastructure based on policy reflecting the currently deployed state of the workloads.										
Intelligence-Driven Security Operations Center Orchestration Solutions	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**8**
Intelligence-driven security operations centers (ISOCs) are designed to deal with the new "detection and response" paradigm. This solution requires the evolution of traditional security operation center (SOCs) to offer an adaptive architecture and context-aware components.										
Remote Browser	**3**	**0**	**3**	**0**	**0**	**0**	**3**	**1**	**0**	**10**
CISOs can address malicious malware delivered via email, URLs or websites by isolating the browsing function from the endpoint and corporate network. The attack is done by remotely presenting the browser session from an on-site or cloud-based "browser server." The server sessions are reset to a known good state, and this technique reduces the surface area for an attack, shifting the risk to server sessions.										
Deception	**1**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**25**
Deception tools, as the name implies, use deceit or tricks to thwart attacks. The security team creates fake vulnerabilities, systems, shares, and cookies to tempt attackers. Any real attack on these resources indicates to security teams an attack is occurring, as legitimate users will not see or need access to the fake systems.										
Pervasive Trust Services	**1**	**3**	**1**	**3**	**3**	**1**	**3**	**3**	**0**	**18**
Security models must evolve alongside the projected pervasiveness of the Internet of Things (IoT) and increasing dependency on operational technology. Trust services can manage the needs of billions of devices with limited processing capability. More importantly, trust services are designed to scale and can offer secure provisioning, data integrity, confidentiality, devices identity and authentication.										
	14	**14**	**19**	**11**	**6**	**6**	**20**	**15**	**11**	