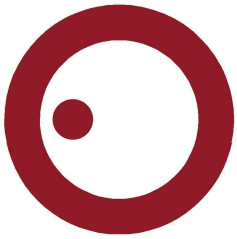


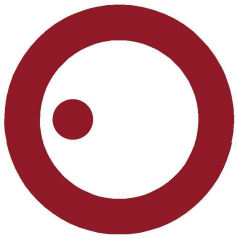
escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Eng.ª Informática – Cibersegurança e Informática Forense

FRAMEWORK DE CIBERSEGURANÇA DA INFORMAÇÃO NO SETOR AUTOMÓVEL

FILIPE JOSÉ DELGADO HENRIQUES

Leiria, Dezembro de 2020



escola superior de tecnologia e gestão
instituto politécnico de leiria

Instituto Politécnico de Leiria
Escola Superior de Tecnologia e Gestão
Departamento de Engenharia Informática
Mestrado em Eng.ª Informática – Cibersegurança e Informática Forense

FRAMEWORK DE CIBERSEGURANÇA DA INFORMAÇÃO NO SETOR AUTOMÓVEL

FILIPE JOSÉ DELGADO HENRIQUES
Número: 2180066

Dissertação realizada sob orientação do Professor Doutor Nuno Alexandre Ribeiro Costa (nuno.costa@ipleiria.pt).

Leiria, Dezembro de 2020

AGRADECIMENTOS

Gostaria de agradecer e dedicar esta dissertação a todas as pessoas que contribuíram para a concretização deste trabalho, nomeadamente à minha família por ter suportado não só durante o desenvolvimento desta dissertação mas também ao longo do mestrado.

Agradeço o apoio oferecido pelo meu orientador, Professor Nuno Costa, e também Professor Leonel Santos por todo o *feedback* dado no melhoramento deste trabalho.

Agradeço o apoio oferecido pelo meu orientador na Altran, Albano Formiga, pela ajuda na escolha no tema para a minha dissertação e pelo fornecimento de documentos necessários para a realização desta dissertação.

Por fim, queria agradecer a todos os meus colegas e professores de mestrado por tornarem este curso numa mais valia para o meu conhecimento na cibersegurança informática, e também, pela oportunidade na minha percepção de que a cibersegurança é algo que está e deve estar cada vez mais presente no nosso quotidiano.

RESUMO

A industria automóvel sofre de uma falta de atenção na cibersegurança dos seus produtos, isto tem sido visível pelo aumento do números de ataques em cada ano. Outro problema é a falta de um entendimento comum na forma de aplicar a cibersegurança, e pelo facto das organizações e empresas praticarem diferentes processos para a cibersegurança dos seus produtos. Para tal, o presente trabalho pretende propor uma *framework* para a cibersegurança do setor automóvel de forma a criar um entendimento geral na aplicação da cibersegurança, e também, para criar uma harmonização deste processo entre as diferentes organizações.

O presente trabalho segue uma metodologia de investigação e análise, onde o processo passa pela investigação de trabalhos relacionados e na análise de *standards* da industria automóvel, como a *ISO 26262* e *SAE J3061*, e *standards* da cibersegurança, como os *standards* da família *ISO 27000* e a *ISO 15408/Common Criteria*. Estas atividades têm como objetivo a proposição de ideias, processos ou métodos para a cibersegurança dos produtos automóveis em cada fase dos seus ciclos de vida.

A partir deste trabalho, foi possível concluir-se que a criação de uma *framework* para a cibersegurança automóvel é um processo bastante complexo de realizar, isto deve-se principalmente pela variedade extensa dos tipos de produtos que aqui existem, e também, pelos diferentes processos envolvidos no desenvolvimento destes produtos automóveis. No entanto, chegou-se também à conclusão que é possível utilizar as ideias e métodos existentes na cibersegurança informática nos produtos automóveis, mas apenas elas não são suficientes para assegurar a cibersegurança completa de todos os processos e atividades do setor automóvel. Para tal, seria necessário uma compreensão detalhada destes processos, algo impossível de concretizar devido à falta de acesso a documentação especifica ao setor automóvel.

ABSTRACT

The automotive industry suffers from a lack of attention to the cybersecurity of its products, this has been visible through the increasing number of attacks each year. Another problem is the lack of a common understanding on how to apply cybersecurity, and the fact that organizations and companies practice different cybersecurity processes for their products. To this end, the present work intends to propose a framework for the cybersecurity of the automotive sector in order to create a general understanding in the application of cybersecurity, and also to create a harmonization of this process between the different organizations.

The present work follows an investigation and analysis methodology, where the process involves the investigation of related works and the analysis of automotive industry standards, such as ISO 26262 and SAE J3061, and cybersecurity standards, such as standards of the ISO 27000 family and ISO 15408/Common Criteria. These activities aim to propose ideas, processes or methods for the cybersecurity of automotive products at each stage of their life cycles.

From this work, it was possible to conclude that the creation of a framework for automotive cybersecurity is a very complex process to perform, this is mainly due to the extensive variety of types of products that exist here, and also due to the different processes involved in the development of these automotive products. Although, it was also concluded that it is possible to use the ideas and methods existing in computer cybersecurity in automotive products, but they alone are not sufficient to ensure complete cybersecurity for all processes and activities in the automotive sector. For that, it would be necessary a detailed understanding of these processes, something impossible to achieve due to the lack of access to documentation specific to the automotive sector.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÓNIMOS

AES	Advanced Encryption Standard.
AUTOSAR	AUTomotive Open Systems ARchitecture.
BSW	Basic Software.
CA	Certificate Authority.
CAN	Controller Area Network.
CAV	Connected and Autonomous Vehicle.
COM	Comunication Manager.
ECU	Electronic Control Unit.
HARA	Hazard Analysis and Risk Assessment.
HMI	Human-Machine Interface.
IACS	Industrial Automation and Control Systems.
IDS	Intrusion Detection System.
IEC	International Electrotechnical Commission.
IOT	Internet of Things.
ISO	International Organization for Standardization.
MANET	Mobile Ad Hoc Network.
NIST	National Institute of Standards and Technology.
OBU	Onboard Unit.
OEM	Original Equipment Manufactures.
PDCA	Plan-Do-Check-Act.

RSA	Rivest–Shamir–Adleman.
RSU	Road Side Units.
RTE	Run-time environment.
SAE	Society of Automotive Engineers.
SARS	Security Assurance Requirements.
SFR	Security Funcional Requirements.
SL	Security Levels.
SOC	Security Operations Center.
TARA	Threat Analysis and Risk Assessment.
V2I	Vehicle-to-Infrastructure.
V2V	Vehicle-to-Vehicle.
VANET	Vehicular ad hoc network.
WLAN	Wireless Local Area Network.

1

INTRODUÇÃO

No presente capítulo são apresentadas as razões para a criação de uma *framework* de cibersegurança da informação nos automóveis. Deste modo, é ilustrado numa breve descrição a evolução do automóvel até aos tempos de hoje, fazendo com isto uma transição para as motivações do presente trabalho. Por fim, são apresentados os objetivos do presente trabalho e a metodologia usado para realizar o mesmo.

1.1 ENQUADRAMENTO

O automóvel é um meio de transporte que teve como origem os carros movidos a vapor (ano 1769). Em 1806, apareceu o primeiro automóvel movido por combustão interna de hidrogénio e oxigénio, no entanto, a industria automóvel só ganhou tração com a invenção do automóvel movido a petróleo ou gasolina pelo seu inventor, Karl Benz (Eckermann, 2001). Também, dentro deste século de evolução surgiram os primeiros automóveis movidos a eletricidade que durante bastante tempo foram o veiculo preferido de utilização pessoal, isto era porque este veículos ofereciam um melhor conforto na utilização em relação aos outros movidos a gasolina. Por fim, esta popularidade acabou quando os automóveis elétricos produzidos na época deixaram de apresentar preços tão económicos como os automóveis de combustão interna de gasolina de Henry Ford. Estes veículos de Ford, tinham a capacidade de serem produzidos em massa e vendidos por valores mais baixos do que os restantes. Só mais recentemente, os automóveis elétricos voltaram a ser produzidos por iniciativa da *Tesla* (Matulka, 2014).

A industria com o passar dos anos desenvolveu os veículos para trazerem melhorias dentro de vários aspetos dos automóveis, como por exemplo: a segurança física do ocupante, conforto, eficiência e entre outros benefícios de qualidade de vida. Muitas funcionalidades digitais foram acrescentadas ao mundo automóvel resultantes dos avanços das tecnologias informáticas digitais. Estas possibilitaram que os automóveis possuíssem programas e aplicações capazes de se ligarem ao mundo exterior, e com isto, estas funcionalidades tornam a utilização do próprio automóvel mais conveniente e interativa para os condutores. Isto é bastante visível nos automóveis da marca

Tesla que tem vindo a ganhar popularidade, principal razão esta também por estes serem movidos a eletricidade (Tesla, 2019). Esta utilização de tecnologia informática dentro dos automóveis vem em parte pelo conceito da *Internet of Things*(IoT), e este conceito influenciou os construtores de automóveis que começassem a adicionar funcionalidades para informatizar, digitalizar e ligar ao mundo exterior nos seus veículos (Malagund et al., 2015).

Outro exemplo da influência do IoT no mundo automóvel são as redes *VANETs*, *Vehicular ad-hoc networks*. As redes *VANETs* foram inicialmente introduzidas em 2001 no livro "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*"de Chai K. Toh, mas como nesta altura as *VANETs* eram vistas como uma aplicação direta dos conceitos de um tipo de rede wireless *ad hoc* já existente, MANET, este não ganhou muita popularidade. Só em 2014 as *VANETs* provaram ser uma tecnologia extremamente útil através do trabalho de C. Sommer e Dressler, 2014. Este trabalho demonstrou as várias formas como as comunicações entre veículos podem ser um bem essencial para melhorar o desempenho dos automóveis, o entretenimento, e os sistemas de informação de tráfego automóvel. Mas tal como mencionado no trabalho de Rehman et al., 2013, as *VANETs* também apresentam desafios na sua cibersegurança que devem ser resolvidos.

A integração das novas tecnologias nos automóveis criou necessidade de cibersegurança nestes, algo que os fabricantes deram pouca importância. Devido a isto, a integração das novas tecnologias foram realizadas sem contabilizar a cibersegurança das novas componentes, o que deixou vulnerabilidades e riscos nos automóveis.

1.2 MOTIVAÇÃO

A cibersegurança no setor automóvel foi um assunto que apenas ganhou impacto quando os primeiros ciberataques e investigações de vulnerabilidades surgiram nos sistemas de automóveis.

Em 2010, ocorreu um incidente de *hacking* aos sistemas de controlo do veículo, de mais de 100 automóveis. Este ataque foi concretizado por um antigo empregado da empresa que vendia estes veículos, sendo que este atacante possuía acesso não autorizado na altura do acontecimento (Poulsen, 2010).

Também em 2010, foi demonstrado por investigadores um ataque onde um atacante conseguia acesso a qualquer *Electronic Control Unit* (*ECU*) do automóvel

alvo, e com este acesso, afetar qualquer sistema crítico do automóvel responsável pela segurança do condutor (Koscher et al., 2010).

Em 2011, um grande número de ocorrências foram documentadas sobre casos onde foi efetuado o roubo da informação pessoal dos donos de automóveis. Um destes ataques aconteceu à empresa da marca *Honda*. Este ataque ocorreu no Canada onde os *hackers* conseguiram roubar informação a 283,000 automóveis das marcas *Honda* e *Acura* (News, 2011).

A partir desta altura o número de casos documentados relacionados com a cibersegurança dos automóveis continuaram a crescer até 2015, onde foi alcançado globalmente cerca de 35 casos documentados. Mas foi a partir de 2016 e até ao ano 2019, que se verificou o maior crescimento do número de casos pelo que foi verificado um número perto dos 90 casos globais (Upstream, 2019a). Muito destes incidentes causaram ou poderão causar perdas enormes para as empresas fabricantes dos automóveis envolvidos, pelo que o impacto financeiro poderá chegar perto dos 560 milhões de dólares se o fabricante tiver de mandar voltar os veículos para reparação. E isto é só o valor de reparação, o valor real seria muito superior com a adição dos danos causados à imagem da marca. Se estes ataques continuarem no futuro, o impacto financeiro poderá alcançar valores superiores considerando que os veículos no futuro estarão cada vez mais interligados com as aplicações dos condutores (Upstream, 2019d).

A *Society of Automotive Engineers* (*SAE*) publicou um guia de orientações para a cibersegurança dos automóveis, a *SAE J3061*, este tem o objetivo de oferecer um conjunto de princípios de cibersegurança de alto nível relacionados com sistemas ciber-físicos dos automóveis. Infelizmente este documento foi considerado insuficiente, pela comunidade, para estabelecer a cibersegurança da mesma forma como a *ISO 26262* conseguiu para a segurança física dos automóveis. Isto deve-se principalmente pelo facto de que a industria automóvel é bastante distribuída no desenvolvimento do seu negócio, o que tornava difícil aplicar diretamente os princípios deste guia.

A falta de um *standard* especifico para a cibersegurança dos automóveis, o aumento exponencial de incidentes documentados e a previsão do impacto financeiro na industria automóvel, levanta as principais motivações para este trabalho: a redução de ocorrências de ciberataques, redução dos perdas no lucro causados pelos problemas de cibersegurança, e permitir uma melhor garantia da cibersegurança nos automóveis.

1.3 OBJETIVOS

Para tentar resolver os problemas causados pela falta de cibersegurança no setor automóvel, esta dissertação pretende propor uma *framework* para ajudar a garantir e analisar a cibersegurança do automóveis. Através de uma conjunto de orientações, esta *framework* pretende auxiliar qualquer pessoa que a use a identificar os fatores de risco em qualquer fase de vida do automóvel; analisar o nível de criticidade e prioridade, e avaliar a cibersegurança necessária para o automóvel.

Esta *framework* terá portanto como objetivo, a analise e avaliação das várias componentes tecnológicas que compõem um automóvel, tanto *software* como *hardware*, durante o ciclo de vida dos automóveis. Esta análise passará principalmente pelos aspetos da conformidade com a segurança da informação.

1.4 METODOLOGIA

Esta dissertação irá seguir uma metodologia de investigação de cinco passos. Estes passos são compostos por uma pesquisa, revisão, definição, implementação e documentação da *framework* proposta.

- O primeiro passo consiste na realização de uma pesquisa sobre as arquiteturas usadas nos automóveis modernos;
- O segundo, revisão dos trabalhos realizados na área relacionado com a temática do presente trabalho;
- O terceiro, definição e estruturação da *framework* e dos conjuntos de regras e guias dentro de cada fase da *framework*;
- O quarto passo, a exemplificação da utilização da *framework* utilizando cenários fictícios de casos de uso;
- E, por fim, a documentação dos resultados através de um documento a apresentar o trabalho desenvolvido e respetivas conclusões.

Como a *framework* irá abranger várias fases da vida do automóvel ou dos seus componentes, a definição da *framework* não irá entrar em grande detalhe em cada fase. Espera-se que ao abranger os vários aspetos dos automóveis que seja possível propor novas ideias para melhorar a cibersegurança no setor automóvel.

1.5 ESTRUTURA

Este relatório está estruturado em cinco capítulos, sendo o primeiro o presente capítulo, a introdução. Este capítulo é apresentado o enquadramento do tema, a motivação, os objetivos e a metodologia usada no presente trabalho.

No segundo capítulo serão exploradas as arquiteturas usadas pelos automóveis modernos e apresentados os trabalhos existentes na cibersegurança do setor automóvel. E, por fim, serão também apresentados os trabalhos relacionados com a temática do presente trabalho.

O terceiro capítulo destina-se à definição da proposta da *framework* para a cibersegurança do sector automóvel. Neste capítulo são apresentados os requisitos necessários para definir a *framework* e os trabalhos que o vão ajudar nesse contexto. Por fim, é explorado a composição da estrutura da *framework* proposta.

No quarto capítulo será apresentado um exemplo ilustrativo da utilização da *framework*. Este capítulo tem o objetivo de mostrar a utilização da *framework* e a utilidade que poderá ter para a cibersegurança automóvel.

E por fim, no quinto e ultimo capítulo serão expostas as conclusões do trabalho realizado, e discussão do trabalho futuro a fazer dentro da temática do presente trabalho.

2

TRABALHO RELACIONADO

No presente capítulo são apresentados informações e trabalhos relacionados com o presente trabalho. É explorado o funcionamento dos automóveis modernos através das arquiteturas usadas, e, por fim, são apresentados os trabalhos relacionados com a cibersegurança no setor automóvel.

2.1 ARQUITETURA DO AUTOMÓVEL MODERNO

Os automóveis modernos têm evoluído de forma a responder às novas necessidades da sociedade, e, do novo mundo interligado das novas tecnologias. Por este motivo, a arquitetura do automóvel moderno evoluiu para um conjunto de sistemas ciber-físicos distribuídos. Isto significa que os automóveis modernos estão não só dependentes do seu *hardware* e componentes mecânicas, mas também, do funcionamento correto do seu *software* para estes operarem corretamente.

2.1.1 *Arquitetura modelo dos ECUs*

Antes de elaborar sobre a arquitetura que é usada como referência pela grande maioria dos *Original Equipment Manufactures* (*OEMs*), é importante perceber a organização dos sistemas de *software* dos automóveis. Para tal existe um modelo que muitos dos *OEMs* seguem para o *design* do seu *software* (visível na Figura 1).

Neste modelo é possível visualizar que os sistemas eletrónicos estão organizados em domínios, por exemplo o sistema de *infotainment* do carro está num desses domínios. Cada um destes domínios tem um conjunto específico de propriedades que detalham o domínio, e estas propriedades podem determinar se este sistema é ou não um sistema crítico para a segurança. Cada domínio é organizado em subsistemas que servem para organizar os domínios dentro de certas funcionalidades do carro, como por exemplo as funcionalidades dedicadas à segurança do condutor. Por sua vez, estes subsistemas agrupam um número de elementos lógicos que são responsáveis por efetuar a funcionalidade do sistema, e da mesma forma como os

domínios, os subsistemas são agrupados em funções. Estas funções são denominadas de funções de *end-to-end* porque estas executam as funcionalidades de interação com o utilizador, como por exemplo a funcionalidade de: Controlo Adaptativo de Viagem, o Aviso da Linha de Faixa, ou Navegação de A a B (Staron, 2017).

Cada subsistema contém um número de componentes que incluem partes mais pequenas dos elementos do *software* que efetuam partes da funcionalidade, estas partes de elementos podem pertencer por exemplo a um *broker* de mensagens para o sistema de *infotainment*. Estas componentes são organizadas em módulos de *software*, que muitas das vezes podem ser ficheiros de código fonte com um conjunto de classes, métodos e outras funções de diferentes linguagens de programação. Estes conjuntos de classes e funções de programação são referidos como componentes lógicos de *software* (Staron, 2017).

A arquitetura dos sistemas de *software* dos automóveis pode ser representada de várias formas e perspetivas, mas as mais importantes são as perspetivas de arquitetura lógica e arquitetura física. A arquitetura lógica dos sistemas de *software* do automóveis é responsável por definir e estruturar as funcionalidades de alto nível do automóvel. Um exemplo destas funcionalidades de alto nível é o sistema de paragem automática para quando um pedestre é detetado na trajetória do automóvel. A arquitetura física dos sistemas de *software* do automóvel é normalmente distribuída em vários dispositivos mais conhecidos como *ECUs* (*Electronic Control Units*). Os *ECUs* são ligados via cabos electrónicos de diferentes tipos e são responsáveis por

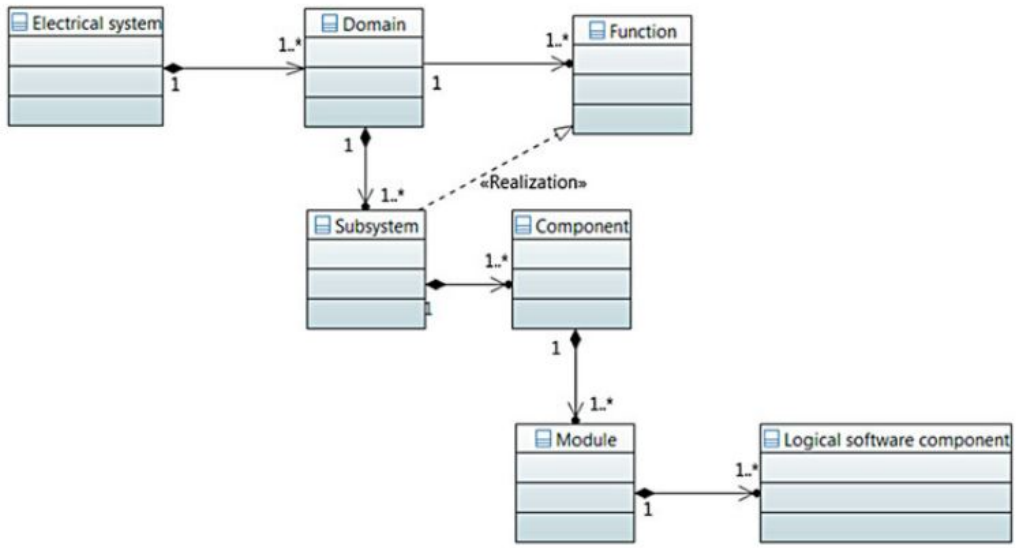


Figura 1: Organização dos sistemas de *software* dos automóveis (Staron, 2017)

executar uma ou mais funcionalidades de alto nível do automóvel definidas na arquitetura lógica (Staron, 2017).

Para além disto, os *ECUs* tem uma arquitetura física que consiste em três camadas principais (Staron, 2017):

- A camada de Aplicação. Esta consiste num número de componentes de *software* alocados que são responsáveis por executar as funcionalidades efetuadas pelo *ECU*.
- A camada de *Middleware*. Esta é responsável por oferecer serviços ao *software* de aplicação como por exemplo a transmissão ou recepção de dados nos *buses* elétricos.
- E a camada de *Hardware*. Este inclui um número de *drivers* responsáveis por controlar as diferentes unidades de *hardware*, por exemplo os *buses* elétricos e o *CPU* do *ECU*.

O desenvolvimento das perspetivas arquiteturais lógicas e físicas dos sistemas de *software* do automóvel e dos seus *ECUs* é realizado em grande parte seguindo a abordagem *MDA* (*Model-Driven Arquitecture*) (OMG, 2014). O *MDA* é um conjunto de orientações para estruturar especificações de *software* que são expressas como modelos. Desta forma, as arquiteturas dos automóveis e dos *ECU* serão diferentes entre *OEMs*, os *OEMs* são responsáveis pelo *design* das arquiteturas lógicas e físicas dos sistemas, e os fabricantes dos específicos *ECUs* são responsáveis pelo seu *design* físico, implementação do *software* de aplicação e de *middleware*, e são responsáveis pelo *hardware* necessário para os *ECUs* (Staron, 2017).

Devido ao facto do desenvolvimento das arquiteturas dos sistemas de *software* dos automóveis estar largamente distribuída entre várias entidades, *AUTOSAR* (*AUTomotive Open Systems ARchitecture*) em 2003 introduziu um *standard* para facilitar o *design* distribuído, e o desenvolvimento dos sistemas de *software* e das componentes hierárquicas dos automóveis. Agora com cerca de 150 parceiros globais, *AUTOSAR* define uma arquitetura de referência para o *design* do *software* do *ECU* no qual os seus parceiros seguem (Staron, 2017).

O *design* da arquitetura do *software* do *ECU* definido pelo *AUTOSAR*, é feito segundo uma arquitetura de três camadas, como é possível ver na Figura 2. A primeira camada, *software* de aplicação, consiste num número de componentes de *software* que efetuam um conjunto de funcionalidades do automóvel, isto é realizado ao trocar os dados através as *interfaces* definidas nestas componentes de *software* (os portos neste caso). A segunda camada, *Run-time environment* (*RTE*), controla a

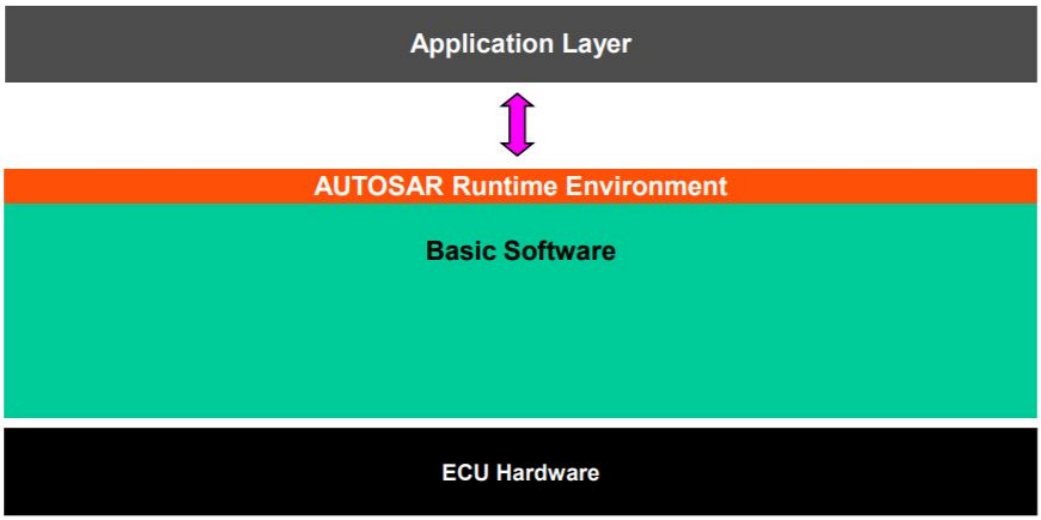


Figura 2: Arquitetura de software do ECU da AUTOSAR (vista simplificada) (AUTOSAR, 2019)

comunicação entre as componentes de *software* independentemente de estes estarem alocados em diferentes *ECUs* ou no mesmo. Esta camada é normalmente gerada automaticamente, baseada nas *interfaces* das componentes de *software*. Quando as componentes de *software* estão alocadas a diferentes *ECUs*, a transmissão dos respetivos sinais nos *buses* elétricos é necessária, e esta é realizada na terceira camada (*Software* básico). A terceira camada, *Software* básico, consiste num número de módulos *Basic Software* (*BSW*) sendo que esta camada é responsável pelas funcionalidades não relacionadas com a aplicação do *ECU*. Uma das funcionalidades mais importantes do *software* básico é a comunicação entre os *ECUs*, isto é, a troca de sinais. Um exemplo de um módulo *BSW* é o *Comunication Manager* (*COM*) que é responsável pela transmissão e a recepção do sinal. A comunicação entre as funcionalidades de alto nível do *software* básico do *ECU* e as *drivers* que controlam o *hardware* do *ECU* são realizadas pelos módulos *BSW Microcontroler Abstraction*, que são executadas pelos módulos *BSW* de abstração do *ECU* (Staron, 2017).

AUTOSAR oferece para esta arquitetura, uma forma alternativa para a comunicação direta das componentes de *software* das aplicações com o *hardware*. A forma de ultrapassar as camadas da arquitetura de *software* do *AUTOSAR* é através de uma implementação personalizada de *Complex Drivers* (visível na Figura 3). Apesar disto ser oferecido pela *AUTOSAR* esta abordagem não é *standard*, sendo que apenas o *RTE* e os módulos da camada de *software* são padronizadas pelo *AUTOSAR*. O objetivo desta padronização vem para os *designers* dos *ECUs* poderem focar na planificação das funcionalidades de alto nível dos automóveis, sem que estes

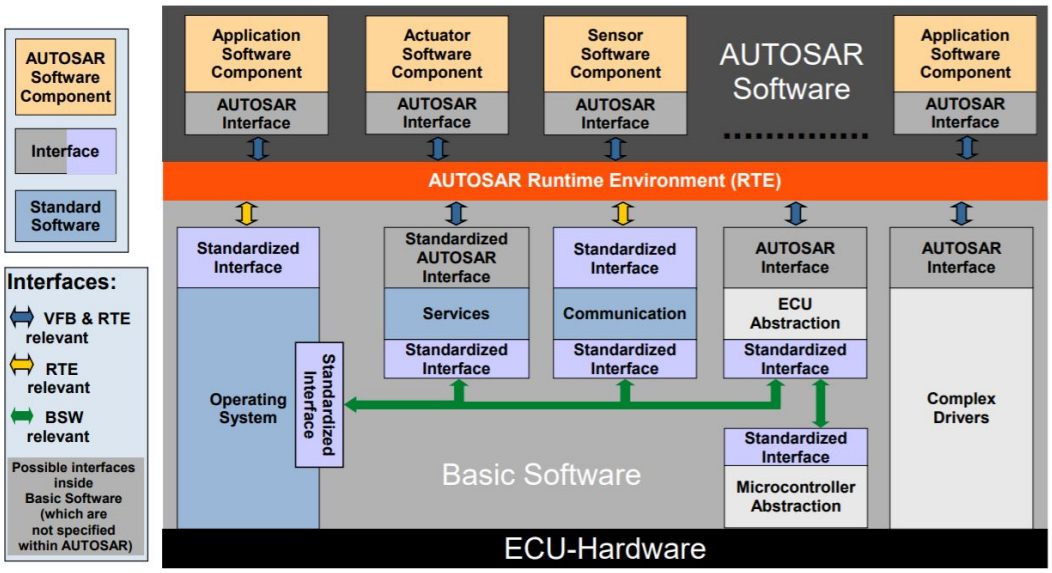


Figura 3: Arquitetura de software do ECU da AUTOSAR (vista detalhada) (AUTOSAR, 2019)

precisem de conhecer o *middleware* e o *hardware* por baixo dessa funcionalidade (Staron, 2017).

2.1.2 *VANET*

Não existe um modelo referência para uma arquitetura usada das comunicações externas dos automóveis, no entanto são usados nos veículos modernos um tipo de rede *ad hoc* para as comunicações entre veículos, as redes *Vehicular Ad hoc Network* (*VANETs*). *VANET* é uma rede de comunicação descentralizada do tipo *wireless*. Esta é usada principalmente para a comunicação entre veículos para a partilha de informações como ocorrências de acidentes e dados de tráfego da estrada. Este tipo de partilha tem o objetivo de melhorar a qualidade e segurança da viagem do condutor. Aqui também é partilhada informação do próprio veiculo, por exemplo quando o automóvel efetua a ação de travagem. Este evento é comunicado a outros veículos ao que permite notificar estes para ajudar a evitar um acidente. Isto é extremamente útil especialmente quando o condutor não está atento, ou, quando este não tem percepção do que está preste a acontecer.

As *VANETs* não têm uma arquitetura ou topologia fixa que todas as redes *VANETs* devem seguir, isto deve-se ao facto de ser uma topologia dinâmica. Este dinamismo está ligado com a alta mobilidade dos veículos o que provoca em grande parte, que as comunicações entre estes sejam muito curtas em duração. Em geral as

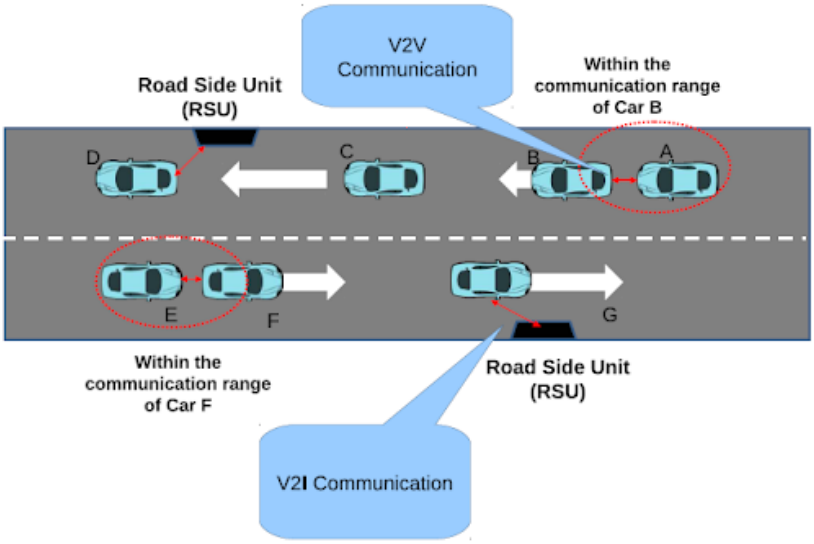


Figura 4: Tipos de comunicações nas redes *VANETs*
(Rehman et al., 2013)

comunicações são entre automóveis e estas são denominadas de comunicações *Vehicle-to-Vehicle* (V2V), mas também existem comunicações de veículos com unidades de infraestrutura de estrada, *Road Side Units* (RSU), e este tipo de comunicação é denominado de *Vehicle-to-Infrastructure* (V2I). Estes tipos de comunicações nas *VANETs* estão ilustradas na Figura 4 (Rehman et al., 2013).

O funcionamento das *VANETs* é similar ao das *Mobile Ad Hoc Networks* (*MANETs*) em termos da comunicação entre os *nodes*, a diferença principal é que os *nodes* da rede *VANET* não se movem de forma aleatória como nos *nodes* das *MANETs*. Isto deve-se ao facto das *nodes* na *VANET* serem principalmente veículos, e estes seguem caminhos lineares e previsíveis. Caminhos estes que são por exemplo as estradas, vias rápidas e auto-estradas. Na arquitetura da *VANET* existe uma unidade de bordo, *Onboard Unit* (*OBU*), dentro do automóvel que serve de transmissor e receptor *wireless* para as comunicações entre os *nodes*. A rede *VANET* apresenta três cenários para as suas comunicações, o primeiro consiste em todos os veículos comunicarem entre si utilizando um *RSU*, neste cenário a arquitetura assemelha-se a uma *WLAN*. O segundo cenário é quando os veículos comunicam diretamente entre si e não existe um *RSU*, a arquitetura aqui é *Ad-hoc*. No último cenário, é realizado uma mistura híbrida do primeiro e segundo cenário, onde alguns veículos comunicam entre si e outros comunicam através de um *RSU* (Rehman et al., 2013).

2.2 CIBERSEGURANÇA NO SETOR AUTOMÓVEL

Já existem vários trabalhos de investigação na área da cibersegurança no setor automóvel, mas em termos de trabalhos mais práticos como aplicações de *software*, ou ferramentas *open source*, poucas são visíveis.

No trabalho de F. Sommer et al., 2019, "*Survey and Classification of Automotive Security Attacks*", é apresentada uma taxonomia dos ataques de cibersegurança nos automóveis. Com este trabalho os autores pretendem conseguir usar a informação obtida nos ataques de cibersegurança para com isso desenvolver e melhorar os conceitos de cibersegurança e depois testar os sistemas automóveis. Esta taxonomia é desenhada tendo em consideração cada fase nos processos de desenvolvimento do automóvel.

No trabalho "*Standard Compliant Hazard and Threat Analysis for the Automotive Domain*"de Beckers et al., 2016, são utilizados os *standards ISO 27001* e *26262* para mostrar como estes podem ser utilizados para a análise de risco e de conformidade no setor automóvel.

No trabalho de Wu et al., 2019, é realizada uma investigação sobre as chaves usadas nos algoritmos de encriptação, mais concretamente, os sistemas de gestão dessas chaves usadas em automóveis que estão para ser utilizadas numa nova arquitetura de rede automóvel. Este trabalho analisa e estuda um esquema baseado no protocolo *Authenticated Key Exchange Protocol 2* (*AKEP2*) e na tecnologia *on-the-air* (*OTA*), sendo que depois é realizada uma simulação deste esquema. Por fim, os autores investigam a possibilidade da utilização do algoritmo *Advanced Encryption Standard with Cipher Block Chaining - Message Authentication Code Mode* (*AES-CCM*) nas comunicações dentro do automóvel como uma melhor alternativa.

Maple et al., 2019 por sua vez, apresentaram uma arquitetura de referência para *Connected and Autonomous Vehicles* (*CAVs*) a partir de um ponto de vista híbrido funcional e de comunicação. Segundo os autores, este ponto de vista possibilita uma análise mais fácil da superfície de ataques pois as componentes e a sua interação podem ser analisadas a partir de um diagrama. São também ilustrado dois exemplos de como instanciar esta arquitetura referência e como esta pode ser utilizada para a análise dos ataques.

Num *white paper* da Symantec, 2016, é apresentado um possível passo em frente para a cibersegurança automóvel. Neste trabalho são abordadas as componentes e *interfaces* que podem ser bloqueadas individualmente, como também os grandes desafios das tecnologias usadas em veículos como o *CAN bus* (*Controller Area*

Network) e o *FlexRay*. Estes são os principais protocolos na integração das complexas *supply chains* no setor automóvel.

Passando agora para um trabalho prático *open source*, foi desenvolvido uma *framework* para efetuar as atualizações do *software* do automóvel de forma segura, o *Uptane*. Este trabalho foi inicialmente desenvolvido por um grupo de académicos de várias universidades americanas, sendo que agora com a organização *Uptane Alliance*, *Uptane* é considerado como um *standard* para o *design* e implementação de atualizações de *software* nos automóveis. *Uptane* tem a capacidade de proteger a entrega de *software* pelo ar nas unidades computorizadas nos automóveis (*ECU*). Esta é uma *framework* que ajuda a abrandar os ataques que pretendam comprometer os servidores e redes usadas para assinar e entregar as atualizações. (Uptane, 2019).

Upstream é uma das empresas que oferece serviços para a cibersegurança automóvel. Um desses serviços é a plataforma *C4*. Segundo Upstream, 2019c, esta é a primeira solução de cibersegurança baseada na tecnologia *cloud* desenhada especificamente para proteger automóveis ligados ao exterior, e para serviços de mobilidade inteligente contra ciberataques ou a má utilização. *C4* fornece deteção de ciberataques no automóvel, agregação e normalização de dados do automóvel, e ferramentas de proteção e controlo do veículo.

Upstream oferece outro serviço designado de *AutoThreat intelligence*. Esta plataforma fornece visibilidade sobre as possíveis ameaças, dando assim uma monitorização das tendências atuais sobre ciberataques no setor automóvel. *AutoThreat intelligence* também indica o comportamento dos atacantes do setor automóvel, e indica qual a vulnerabilidade mais provável a explorar (Upstream, 2019b).

2.3 TRABALHO RELACIONADO COM A TEMÁTICA DA PRESENTE DISSERTAÇÃO

Relativamente a trabalhos relacionados com a temática da presente dissertação, ainda pouco foi realizado sendo que apenas um trabalho foi encontrado. Sendo este tipo de trabalho realizado dentro do domínio das entidades responsáveis por *standards* e organizações de setores específicos, já existe um documento guia para a cibersegurança dos sistemas dos automóveis, o *SAE J3061*. No entanto, foi verificado que este guia não era suficiente para garantir a cibersegurança dos sistemas dos automóveis. Por este motivo, foi iniciado um trabalho conjunto pela *SAE* e *ISO* para criar um *standard* específico nesta área do setor automóvel, a *ISO/SAE DIS 21434*. Este *standard* ainda se encontra em processo de desenvolvimento.

No espaço "*Towards an Information Security Framework for the Automotive Domain*"de Glas et al., 2015, são apresentadas ideias e elementos para uma possível *framework* para a segurança da informação do setor automóvel. Neste trabalho os autores apresentam uma visão geral dos *standards* ligados à segurança de sistemas críticos, sistemas automóveis e sistemas informáticos. Estes *standards* são:

- *Standards* da família *ISO 27000*, o *standards* de segurança de sistemas de informação;
- *Standard IT Grundschutz*, que é um *standard* relativo à cibersegurança de organizações informáticas;
- *ISO 15408/Common Criteria*, este *standard* serve de *framework* para a especificação de requisitos funcionais de segurança e de garantia;
- *Standards* da família ISA99/IEC 62443, que oferecem procedimentos para a implementação segura de *Industrial Automation and Control Systems* (*IACS*);
- *ISO 26262*, é um *standard* que define orientações para segurança funcional de equipamento automóvel, sendo este aplicável a todos os ciclos de vida dos sistemas automóveis elétricos e com a segurança do veículo.

Os autores apresentam depois motivações para existir uma harmonização do sector automóvel mas, por outro lado, também para existir *standards* específicos do setor. Desta forma os autores sublinham ideias base e elementos destes *standards* para oferecer uma possível *framework* para uma engenharia automóvel segura, ilustrando com isso exemplos e também pondo em contexto estes *standards* existentes.

Algum tempo depois da *SAE* publicar o *SAE J3061*, Schmittner, Ma et al., 2016, partilharam no seu artigo as suas experiências com a utilização deste *standard* numa das suas fases iniciais. Após a descrição do *SAE J3061*, os autores passam para a apresentação da experiência com o processo de aplicação do *standard* no desenvolvimento do sistema de *software* para um *ECU*. Neste trabalho é apenas ilustrada uma das fases iniciais definidas pelo *SAE J3061*, a fase conceptual (*Concept phase*). À medida que é apresentada a fase conceptual, é também realizada uma comparação com o *standard ISO 26262* (*standard* em que a *SAE J3061* se baseou), e são também, explicados os aspetos que os autores pretendem que sejam melhorados, como é o caso do *Threat Analysis and Risk Assessment* (*TARA*) do *SAE J3061*.

Sendo que a *SAE J3061* não foi suficiente para responder às necessidades da comunidade de segurança do setor automóvel, o desenvolvimento de um novo *standard* foi iniciado. Como explicado por Schmittner, Griessnig et al., 2018, no seu relatório do estado do desenvolvimento do *ISO/SAE 21434*, a razão pela qual o *SAE*

J3061 não conseguiu desempenhar a sua função, como a *ISO 26262* conseguiu, deve-se às características específicas dos processos de engenharia dos sistemas automóveis, que é o caso do desenvolvimento distribuído que provoca a aplicação direta de *standards* existentes da cibersegurança difícil. Também, o mesmo se verifica com as diferenças nas avaliações de risco para a área automóvel, e nas particularidades da engenharia segura que complicam a aplicação direta de *standards* de cibersegurança da área da informática.

O presente trabalho pretende propor uma *framework* para ajudar a melhorar a cibersegurança do setor automóvel, isto não só através da referência dos *standards* mais indicados para as diferentes fases ou processos durante o ciclo de vida do produto, mas também através da proposta de novas ideias para analisar e identificar a cibersegurança necessária. Este trabalho vem desta forma assemelhar-se ao trabalho de Glas et al., 2015, pelo que ambas as *frameworks* apresentam estruturas semelhantes onde seguem um fluxo de fases representativas das diferentes fases do ciclo de vida de um produto. Também, em ambas as *frameworks* são utilizados perfis de segurança como um auxílio para analisar e identificar qual a cibersegurança adequada para o produto, e a utilização de ideias de *standards* de segurança para estas serem reaproveitadas nas diferentes fases da *framework*. Mas, é a partir deste ponto que as duas *frameworks* divergem. No presente trabalho são utilizadas ideias de diferentes fontes utilizadas no trabalho de Glas et al., 2015, e são exploradas em maior pormenor as fases posteriores à fase inicial do planeamento do produto. Nessas fases, são exploradas e apresentadas as possíveis medidas e controlos que podem ou devem ser utilizadas nas diversas fases do ciclo de vida do produto.

3

FRAMEWORK PARA A CIBERSEGURANÇA DA INFORMAÇÃO

No presente capítulo é apresentada a proposta para uma *framework* de cibersegurança da informação para o setor automóvel. Aqui são referidos os requisitos necessários para elaborar o trabalho e apresentadas as ideias e propostas para esta *framework*. A apresentação da *framework* passa pela descrição da sua estrutura e depois pela apresentação do que é proposto em cada fase da *framework* proposta.

3.1 REQUISITOS DE TRABALHO

De forma a alcançar os objetivos para criar uma *framework* de cibersegurança focada no setor automóvel, é necessário analisar os procedimentos e orientações já existentes em *standards* e *guidelines* de ambos os lados dos setores críticos, como o setor automóvel e do setor informático. Ao estabelecer uma relação nos *standards* existentes no setor automóvel com os do setor informático, poderá ser possível reutilizar alguns dos seus procedimentos para serem utilizados ou adaptados na cibersegurança da informação automóvel. Desta forma, o material necessário para esta *framework* consiste num conjunto de *standards* e guias, nomeadamente:

- *ISO 26262*
- *IEC 62443*
- *ISO 27K family*
- *ISO 15408/Common Criteria*
- *NIST - Framework for Improving Critical Infrastructure Cybersecurity*
- *ENISA - Good practices for security of Smart Cars*
- *ENISA - Good practices for security of IoT*

Em termos de funcionalidades, esta *framework* deverá ser capaz de oferecer orientações relativas aos processos e medidas que devem ser exercidos para assegurar a melhor cibersegurança possível para a informação dos automóveis. Isto implica também fornecer para cada etapa no ciclo de vida do automóvel um conjunto de

aspetos que devem ser postos em consideração, aspetos esses que estão dependentes da etapa dentro do ciclo de vida em que o automóvel se encontra.

3.2 FRAMEWORK PROPOSTA

Segundo o contexto do presente trabalho, uma *framework* pode ser uma estrutura real ou conceptual com o objetivo em oferecer orientações ou ajuda na construção de algo que irá transformar essa estrutura em algo utilizável. No presente trabalho a *framework* que se pretende propor será um conjunto de regras, orientações e princípios os quais deverão ajudar na cibersegurança dos automóveis, mais especificamente na segurança da informação.

Com isto, a presente *framework* pretende apresentar ideias de alto nível, tiradas de *standards* e documentos fonte de boas práticas, para serem utilizadas numa *framework* para a cibersegurança da informação dos automóveis. Esta *framework* tem, também, o objetivo de averiguar se a utilização de *standards* e boas práticas do setor informático para a cibersegurança da informação, são viáveis para o setor automóvel. De modo a garantir uma boa percepção da cibersegurança aplicada no automóvel, uma metodologia de garantia deverá existir. No presente trabalho será também feita uma abordagem deste tema através de uma exemplificação de uma metodologia de garantia de alto nível para esta *framework*.

Relativamente às atividades não relacionadas com o desenvolvimento de um produto especifico do setor em que a empresa se enquadra, os processos de cibersegurança que devem ser aplicados podem ser semelhantes aos de uma empresa de outro setor, como o da informática. Mas no que diz respeito à execução desses processos durante o desenvolvimento de um produto automóvel, a cibersegurança nesses processos já deve ser personalizada para o tipo de produto em desenvolvimento. Também, a execução de processos de segurança deve ser diferente de produto para produto, isto é, os requisitos de segurança devem ser derivados a partir do produto em questão porque um produto pode não apresentar as mesmas características ou funcionalidades que outros. Desta forma, devem ser decididas para cada produto um conjunto de medidas/processos de cibersegurança para serem implementados e testados durante o seu desenvolvimento, e também para as fases posteriores ao seu desenvolvimento.

Mas para garantir que exista uma harmonização da segurança que é aplicada no setor automóvel, uma *framework* que aplique aos processos do setor automóvel os elementos existentes nas boas práticas da cibersegurança informática deve ser

proposta. Tal como na *framework* proposta por Glas et al., 2015, esta *framework* também funcionará com base em perfis de segurança como meio de harmonização.

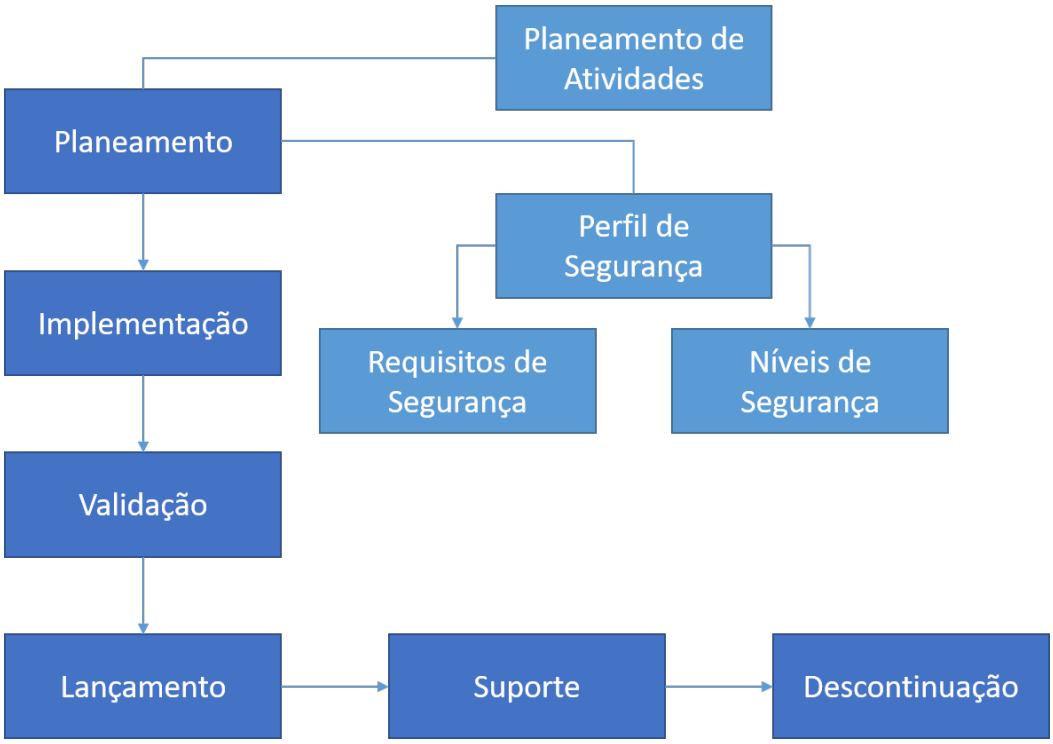


Figura 5: Diagrama representativo da *framework* proposta

Como se pode visualizar de forma resumida na Figura 5, a estrutura da *framework* segue as seguintes fases no ciclo de vida de um produto:

- Planeamento. Nesta fase são definidos conceitos, identificados requisitos de cibersegurança e planeado o design seguro para a arquitetura do produto;
- Implementação. Nesta fase são postas em prática o planeamento da fase anterior de forma a desenvolver o *software* do produto com os aspetos de cibersegurança em mente;
- Validação. Na fase de validação são realizados todos os passos necessários para verificar que o *software* desenvolvido vai de encontro com os requisitos identificados na primeira fase, e para verificar se a implementação do produto está livre de *bugs*.
- Lançamento. A fase do lançamento do produto consiste nos testes de aceitação do produto consoante os requisitos identificados na fase de planeamento. Aqui é realizada a avaliação e certificação da cibersegurança aplicada no produto;

- Suporte. Na fase de suporte são aplicadas as medidas necessárias para garantir uma manutenção segura, e monitorização, se necessária, segundo o que está definido nos requisitos;
- Descontinuação. Por fim, na fase de descontinuação são exercidos os procedimentos necessários para garantir a disposição segura do produto.

O grande foco nesta *framework* deve ser na fase do planeamento, aqui é definido o perfil de segurança específico para o produto. E será a partir do perfil definido que os processos e medidas nas fases seguintes irão ser determinadas e implementadas.

A *NIST - Framework for Improving Critical Infrastructure Cybersecurity*, carateriza os perfis no seu documento como o alinhamento dos *standards*, guias e boas práticas para uma *framework* dado um cenário de implementação em particular. Para desenvolver um perfil de segurança, ou um perfil da *framework* como é definida pela *National Institute of Standards and Technology* (*NIST*), a empresa tem de rever as categorias e subcategorias de segurança, e escolher quais destas são as mais importantes com base nas motivações do negócio e na análise de risco.

3.3 PLANEAMENTO

A fase do planeamento consiste em várias atividades de preparação para definir o perfil de segurança para o produto. O perfil será composto por categorias da cibersegurança que irão ajudar a definir:

- Requisitos de segurança
- Nível de segurança
- Metodologia de garantia

As Categorias serão escolhidas com base nos objetivos de segurança do negócio, e na análise de risco. Desta forma o planeamento é composto por várias atividades, nomeadamente:

- **Definição de critérios**: Aqui são identificados os objetivos de negócio e os critérios de alto nível da empresa. Com esta informação são tomadas decisões sobre quais as implementações de cibersegurança que devem ser tomadas, e identificados os sistemas e ativos que irão suportar o produto de forma a obter o âmbito de cada um deles.
- **Análise de Risco**: Com os ativos já identificados, é realizada a análise de risco que irá ajudar a criar o perfil de segurança. Esta análise serve principalmente

para distinguir as diferentes probabilidades de um risco acontecer e o impacto que este irá provocar.

- **Criação do Perfil de segurança**: A criação do perfil envolve a identificação das categorias que descrevem os objetivos de cibersegurança pretendidos para o produto, e a atribuição de uma classificação da sua cibersegurança.
- **Determinação dos Requisitos de segurança**: Com o perfil criado é possível especificar com mais facilidade os requisitos de cibersegurança. Este requisitos serão depois utilizados como a definição do design de segurança para ser aplicado na implementação do produto.
- **Identificação do Nível de segurança**: A identificação do nível de segurança consiste na análise dos requisitos de cibersegurança para poder determinar qual a quantidade de controlos, alcance dos testes e a profundidade que devem existir para ir de encontro aos requisitos de segurança determinados.
- **Determinação da Metodologia de garantia**: A metodologia de garantia serve como avaliação e certificação para validar e assegurar a aplicação de medidas de cibersegurança no produto. Deste modo, nesta atividade são identificadas as avaliações que devem ser consideradas para ir de encontro ao perfil de segurança.
- **Planeamento de atividades**: As atividades que devem ser planeadas consistem principalmente em formações que sejam importantes para a percepção e conhecimento das boas praticas de cibersegurança no local de trabalho. Algumas destas formações serão especificas perante os critério definidos pela empresa ou produto.

3.3.1 *Definição dos critérios*

A definição dos critérios tem como base os próprios objetivos funcionais que uma empresa tem perante o produto, isto significa que cada produto que a empresa pretende desenvolver poderá apresentar diferentes critérios. Com isto, a entidade poderá definir os objetivos de cibersegurança e critérios para garantir que essa segurança seja aplicada ao produto. Os objetivos neste caso, podem ser a garantia de confidencialidade na transmissão de dados para um *node* no exterior do produto (no caso das redes *VANET* por exemplo), e o critério de aplicar a segurança para esse objetivo poderá ser definida com base na criticidade dos dados que vão ser transmitidos. Este processo deverá ser feito para todos os ativos existentes em

qualquer ciclo de vida do produto, o que significa que deverão ser identificados todos os ativos do produto durante a fase de **planeamento**, **implementação**, **validação**, **pós-lançamento** e **descontinuação**.

No contexto do sector automóvel o produto poderá ser um automóvel, e neste caso os ativos são todas as componentes e funcionalidades do automóvel que afetam a cibersegurança deste, isto é, os *ECUs* do veículo. Em muitos casos o produto não é o automóvel em si mas sim os seus *ECUs* individuais, ou as funcionalidades que podem ser compostas por vários *ECUs* como, por exemplo, o sistema de controlo de navegação dinâmica. Este é o caso das entidades contratadas para o desenvolvimento destas componentes ou das funcionalidades do produto final, o veículo.

A entidade responsável pelo desenvolvimento do produto deve também definir critérios de segurança para serem aplicados no desenvolvimento do produto. Os critérios deverão ser definidos de forma a que todos os membros da organização, associados ao produto, apliquem a cibersegurança de forma consistente durante os vários ciclos de vida do produto.

Desta forma a definição de critérios serve para identificar as várias atividades que vão ocorrer nas fases de cada ciclo de vida do produto, e para que a análise de risco e a definição dos objetivos de cibersegurança sejam realizados indo de encontro aos critérios para a cibersegurança do produto.

Para a definição de critérios, é proposta a utilização da *ISO 27001* para ajudar neste processo. Este *standard* oferece um guia para a implementação de um sistema de gestão da segurança da informação, e apresenta também conceitos que podem ser utilizados por qualquer organização no que toca a definição de critérios, definições de contextos e outros tipos de atividades de planeamento. Isto pode ser utilizado numa empresa que esteja a desenvolver um produto automóvel. Uma vez que este *standard* não oferece métodos ou processos específicos para um setor de atividade, este pode ser utilizado como referência no contexto do setor automóvel e para a cibersegurança da sua informação.

No trabalho de Glas et al., 2015, os autores mencionam o uso destes *standards* da família *ISO 27000* para ser utilizado o catálogo de requisitos presente nesta família, o que na presente *framework* também deverá ser utilizada para a definição de requisitos. O caso da definição de critérios é um assunto que os autores não elaboraram no seu trabalho. Este tipo de tópicos não é abordado em *standards* como a *ISO 26262* e *SAE J3061*, pelo que estes tem o foco principal nos processos de desenvolvimento do produto e não da organização em si. Desta forma, a utilização da *27001* e *27002* será uma mais valia para a proteção dos dados informáticos

relativos aos produtos automóveis, porque, a cibersegurança para um produto deve ser aplicada não só nos seus processos de desenvolvimento mas também nas próprias organizações e entidades responsáveis pela sua criação.

3.3.2 *Análise de risco*

Com os ativos identificados na atividade anterior, a empresa poderá focar na análise de risco dos ativos. Para a análise de risco propõe-se a utilização do *standard* de gestão de risco da segurança da informação, a *ISO 27005*. Esta *ISO* introduz de forma muito abrangente como abordar a análise de risco da informação de uma organização, e muitas destas técnicas de análise poderão ser facilmente adaptadas para um ambiente automóvel. A gestão do risco definida pela *27005* está dividida por várias fases:

- Estabelecimento do contexto;
- Avaliação do risco, que por sua vez é composto por:
  - Identificação de risco;
  - Análise de risco;
  - Avaliação do risco.
- Tratamento do risco;
- Aceitação do risco.

Para além disto, este processo também apresenta duas atividades paralelas ao longo do processo: a Comunicação e partilha de informação do risco; e a Monitorização e revisão do risco. Estas atividades provam ser bastantes importantes para o contexto automóvel onde a recolha de informação sobre novos riscos mostra ser um fator crítico para a segurança do produto e do próprio condutor.

Como se pode ver na Figura 6, a gestão de risco pode ser um processo iterativo onde este processo pode ser realizado várias vezes consoante um evento especificado pela entidade responsável. Uma das causas pelo início de uma nova iteração pode ser pelo resultado da avaliação do risco não ser satisfatório, ou, pelo tratamento escolhido para o risco não ser suficiente. Mas tirando estas causas ligadas com o processo em si, também deve ser necessário voltar a fazer uma nova iteração sempre que algo seja alterado no contexto do produto. Por exemplo a adição de uma nova funcionalidade ou a alteração de uma funcionalidade já existente.

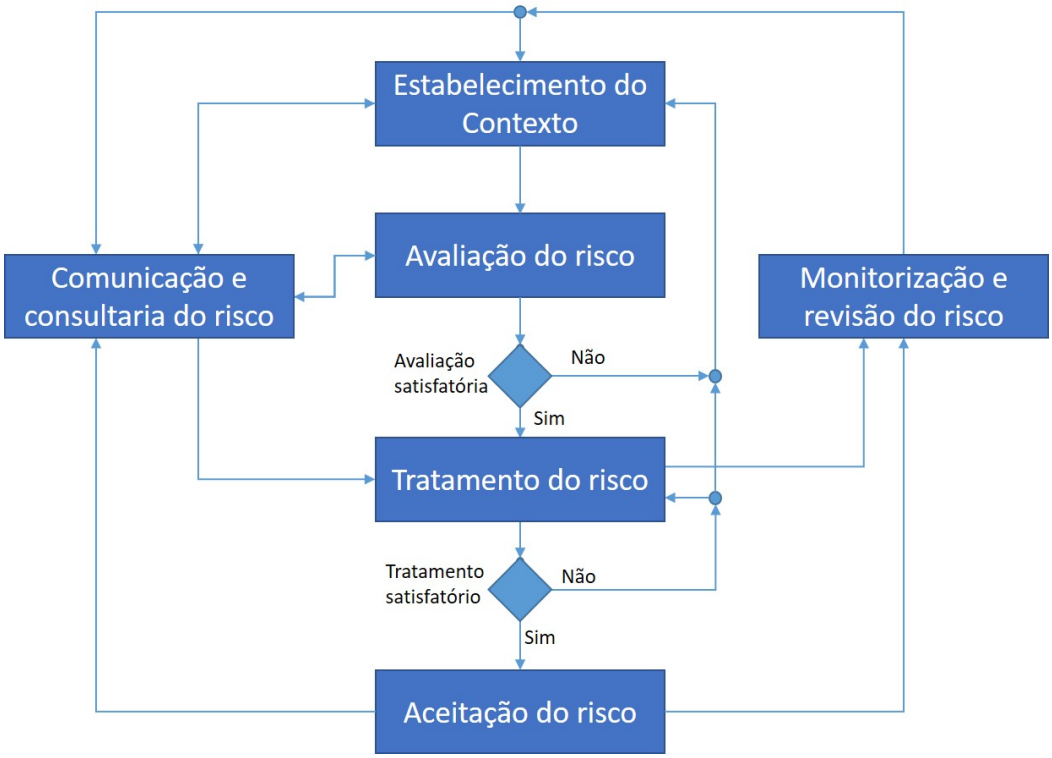


Figura 6: Diagrama representativo da Gestão de risco de segurança da *ISO 27005*

Todas estas atividades e processos podem ser adaptados para os produtos do setor automóvel. Por exemplo, uma adaptação que deve ser realizada neste processo é a aceitação do risco, sendo que os produtos automóveis apresentam a maioria das vezes, altos requisitos de segurança que devem ser garantidos. Assim, a aceitação do risco terá de ser reajustada para aceitar o menor risco inerente possível. Caso contrário esse produto deverá ser reformulado para evitar apresentar riscos inerentes demasiados altos.

Para calcular o risco inerente, primeiro, a entidade tem de efetuar a avaliação do risco, e como já foi indicado anteriormente, este tem como primeira atividade a identificação de riscos. No contexto automóvel devem ser considerados, para além dos riscos associados aos ativos do produto, os riscos associados no caso de existirem outras entidades que são contratadas para o desenvolvimento de peças ou funcionalidades do produto. De seguida, é realizada a análise do risco e a sua avaliação. O processo destas duas atividades envolve a determinação do tipo de vulnerabilidade, aviso prévio, duração para calcular o impacto resultante, e a determinação da probabilidade de ocorrência do risco. Por fim, com o impacto resultante e a probabilidade de ocorrência, é determinado o risco inerente. Todo este processo é aplicável num produto automóvel porque o processo oferecido por este

standard não é limitado a uma industria, o que desta forma permite ser facilmente adaptado para o setor automóvel.

Por último, as duas atividades seguintes envolvem a escolha do tratamento do risco e a aceitação do risco. Estas atividades permitem determinar principalmente o risco residual que um risco obtém depois de serem aplicadas as medidas de tratamento para o mesmo. Isto permite avaliar se o produto está pronto para aceitar o risco residual, ou, se ainda é necessário escolher ou melhorar as medidas para responder ao risco identificado no produto.

Neste tópico, no trabalho de Glas et al., 2015 é também referido a possibilidade de utilizar este *standard*, mas também, outros *standards* de análise de risco existentes. Porém, para a presente *framework*, considera-se que seja possível utilizar o formato da análise de risco apresentado na *SAE J3061* e utilizar os métodos de análise de risco da *ISO 27005*.

A análise de risco na *SAE J3061*, a *Threat Analysis and Risk Assessment* (*TARA*), é baseada na análise de risco realizado na *ISO 26262*, *Hazard Analysis and Risk Assessment* (*HARA*). A diferença entre estas está no foco que cada uma tem, o *TARA* tem o foco nas ameaças de cada funcionalidade e o *HARA* tem o foco na identificação e categorização do mau funcionamento das componentes do produto, mau funcionamento este que pode causar a ocorrência de um perigo para o veículo. Em geral, o *TARA* abrange mais detalhes para analisar do que o *HARA*. Mas, ao contrário do *HARA* que tem apenas de se focar no desvio das funcionalidades pretendidas no qual podem levar a falhas, o *TARA* tem de se focar não só nessas funcionalidades mas também nos dados usados para avaliar os diferentes impactos para o produto e para a organização (Schmittner, Ma et al., 2016). Como o *J3061* não especifica métodos ou técnicas para a realização do *TARA*, aqui é uma boa oportunidade para aplicar os métodos de análise de risco já existentes na *ISO 27005* para complementar o processo do *TARA*.

3.3.3 *Perfil de segurança*

O perfil de segurança junta os critérios definidos e a análise de risco realizada para determinar os objetivos de cibersegurança mais importantes que o produto deve possuir. Depois, são classificados e atribuídos categorias de segurança para cada objetivo de segurança. E, com base nos critérios definidos, são também atribuídos um nível de segurança necessário a cada objetivo. A ideia de utilizar as categorias de cibersegurança nesta fase é baseada na forma como a *IEC 62443*

efetua o seu processo de classificação da segurança necessária para um produto. Para as categorias, as principais deverão ser as definidas segundo o conceito do trio Confidencialidade, Integridade e Disponibilidade (*CIA*), e também no conceito chave de Responsabilidade. No entanto, a organização deve estar livre de criar as suas subcategorias de forma a desenvolver um catálogo de categorias conforme os seus critérios da organização.

As categorias de segurança ajudam a determinar o estado corrente, e esperado, dos objetivos de segurança para o produto. Estas categorias são organizadas pelo género de cibersegurança, o que possibilita que cada categoria ajude na representação do resultado esperado para assegurar a cibersegurança de uma determinada funcionalidade no produto. As categorias ajudam assim a ilustrar o possível risco do produto tanto dentro da empresa como entre diferentes organizações, sendo que esta é uma ajuda para a harmonização no estabelecimento da cibersegurança entre entidades.

Com este formato pretende-se criar uma forma *standard* simples de determinar e definir Perfis de Segurança. Através destes processos, qualquer organização ou entidade poderá determinar de forma compreensiva a cibersegurança que o produto tem e deve apresentar.

Os Perfis de Segurança permitem depois determinar os requisitos de segurança para o produto, que por sua vez definem a cibersegurança no *design* do produto. Da mesma forma os Perfis de Segurança ajudam, também, a definir o nível de segurança necessário para determinar quais as medidas de segurança para o produto.

No trabalho de Glas et al., 2015, estes utilizam ideias dos *standards IEC 62443*, *IT Grundschutz* e *ISO 26262* para determinar o Perfil de Segurança. Este processo está dividido em 3 passos:

- Determinação de níveis de segurança para classificar risco;
- Determinação de níveis de segurança a objetivos de segurança;
- Calcular o risco acumulado dos casos de risco de cada objetivo de segurança.

Para a definição do Perfil de Segurança na presente *framework*, propõe-se apenas a utilização dos dois primeiros passos para a determinação do Perfil de Segurança. O terceiro passo é necessário para o processo desta *framework*, mas para esta atividade de definição do Perfil de Segurança, neste considera-se não ser necessário. Assim, para o Perfil desta *framework*, propõe-se utilizar ideias não só do *IEC 62443* mas também da *NIST - Framework for Improving Critical Infrastructure Cybersecurity*. A partir desta *NIST* utiliza-se a ideia de que um perfil de segurança deve representar

o objetivo corrente e futuro para a cibersegurança do produto. Para este processo, propõe-se apenas a utilização da avaliação de risco dos ativos do produto de forma a determinar a prioridade desse ativo, determinar os objetivos de segurança para cada um destes ativos, e determinar as categorias de segurança para cada objectivo.

Tabela 1: Exemplo de um Perfil de Segurança

Categoria de Segurança	**Objetivo de Segurança**	**Descrição**	**Nível de Segurança**
Confidencialidade	Confidencialidade dos dados	Quaisquer dados transferidos para o exterior do veículo devem estar protegidos contra a exposição a entidades maliciosas	3
	...	...	
Integridade	Confiança na integridade dos dados	Dados recebidos e enviados devem ser protegidos contra possíveis alterações ao seu conteúdo original	4
	...	...	
Disponibilidade	Recuperação do serviço de *infotainment*	Quando por qualquer motivo o serviço de *infotainment* passa a um estado de indisponibilidade, este deve estar disponível após um curto intervalo de tempo	2
	...	...	
Responsabilidade	Comunicação de dados Autenticados entre *nodes*	Por forma a evitar a fuga à responsabilidade nas ocorrências de erros no envio de dados, qualquer dado enviado deve estar autenticado pelo emissor	3
	...	...	

Como alternativa ao passo final para definir o Perfil de segurança, propõe-se o cálculo do nível de segurança médio, obtido por cada grupo de categorias no Perfil. Isto requer primeiro, identificar um nível inicial de cibersegurança para cada objetivo de segurança, isto através de uma classificação dos objectivos com o níveis de segurança pretendido, como é realizado nos *Security Levels* (*SL*) do *IEC 62443*. Depois de cada objetivo estar classificado com um nível de segurança, será efetuada a média dos níveis de segurança pretendido por cada grupo de categorias ou subcategorias do Perfil de Segurança. Desta forma será possível entender melhor quais são os objetivos principais para a cibersegurança no produto automóvel. No *IEC 62443* são definidos quatro *Security Levels*:

- *SL1*: casual, não intencional;
- *SL2*: meios simples, isto é, poucos recursos, habilidades de *hacking* genéricas e pouca motivação;
- *SL3*: meios moderados, isto é, recursos moderados, boas habilidades e motivações moderadas;
- *SL4*: meios mais sofisticados, isto já requer muitos recursos, habilidades altas e grande motivação.

Estes níveis são designados a cada requisito funcional dependendo das capacidades e motivações de um atacante. Neste caso os requisitos funcionais serão os objetivos de segurança, e de maneira a que seja possível calcular uma média por grupo de categorias dos níveis de segurança de cada objetivo, cada nível deverá estar atribuído com um valor numérico representante desse nível. Por exemplo os valores poderão ser atribuídos numa escala de um a dez:

- *SL1*: valor numérico de 1,
- *SL2*: valor numérico de 4,
- *SL3*: valor numérico de 6,
- *SL4*: valor numérico de 10.

Desta forma, o Perfil de Segurança está representado por todos os objetivos de segurança de cada ativo do produto. Os objetivos de segurança serão determinados através do resultado da análise de risco dos ativos do produto, dando depois uma breve descrição de cada objetivo. Depois da definição dos objetivos, será feito a associação das categorias de segurança e a classificação de um nível de segurança a cada objetivo de segurança. Por fim, é calculado o nível de segurança médio por

cada categoria. Na Tabela 1 é apresentado um exemplo de um Perfil de Segurança da presente *framework*.

3.3.4 *Requisitos de segurança*

O objetivo dos requisitos de segurança é a definição de um conjunto de regras específicas para o produto por forma a alcançar a melhor cibersegurança possível. Estes requisitos vão detalhar as características funcionais e de sistema, que servem de apoio para descrevem as medidas de segurança associadas aos objetivos de segurança.

Os requisitos ajudam a determinar que medidas são necessárias para cumprir os objectivos de segurança do produto. A definição dos requisitos de segurança é um passo que será aproveitado para a determinação dos níveis de segurança, onde juntamente com as medidas identificadas nesta secção e o nível de segurança, será determinado o tipo de implementação da medida de segurança. Os requisitos de segurança e a determinação das medidas são o proposto para ser utilizado na fase de *design* do produto, sendo que depois na fase de implementação ou desenvolvimento, são aplicadas as medidas de segurança.

Para esta atividade propõe-se utilizar vários documentos que apresentam este tipo de informação, este é o caso da *ISO 27001* e *27002*, *SAE J3061*, *NIST - Framework for Improving Critical Infrastructure Cybersecurity*, *ENISA - Good practices for security of Smart Cars* e *ENISA - Good practices for security of IoT*. De cada um destes documentos propõe-se a reutilização de ideias para a definição de requisitos de segurança associados às várias fases da vida do produto, especialmente para a fase final, a descontinuação, que é algo pouco mencionado em trabalhos na área da cibersegurança do automóvel.

Para iniciar este processo, devem ser determinados os requisitos de alto nível. Os requisitos de alto nível serão essencialmente baseados nos ativos do produto e nos objetivos, por exemplo o objectivo de segurança **confidencialidade dos dados** ou **transferência de dados autenticados**. Por cada um destes requisitos de alto nível serão determinados os requisitos de segurança, os requisitos de sistema e os requisitos funcionais. Ao fazer a identificação dos requisitos de segurança desta forma, os requisitos estarão organizados por objetivo de segurança em vez de estarem associados diretamente ao produto em si. No trabalho de Glas et al., 2015, é precisamente proposto o oposto, a associação dos requisitos diretamente ao produto.

Ao separar os requisitos por objetivo de segurança, disto irá resultar em requisitos replicados pelos diferentes objetivos. Mas ao manter os requisitos associados a cada objetivo, é possível oferecer uma visualização mais perceptível das medidas de segurança que devem ser aplicadas para cada ativo/funcionalidade do produto.

Uma fase que considera-se relevante e que em muitos trabalhos não é mencionado é a fase de descontinuação do ciclo da vida de um produto. Quando um produto chega ao fim da sua vida é necessário que as devidas medidas sejam tomas para garantir que os dados e informações ainda dentro do produto, não sejam acedidas por entidades maliciosas. A partir da *ISO 27002* poderão ser tiradas medidas, ou controlos como são referidas no *standard*, para evitar a fuga de dados para o exterior. Este tipo de medidas são essenciais não só para proteger a confidencialidade e privacidade dos dados dos clientes, mas também para proteger o negócio da empresa que desenvolveu o produto. Um caso de um requisito que poderemos utilizar para um produto automóvel poderá ser a destruição dos dados sensíveis nas componentes do automóvel, como está ilustrado na Tabela 2.

Em termos de diferença com o trabalho de Glas et al., 2015, o presente trabalho procura obter mais ideias de outras fontes como a *ENISA* e a *NIST*. Outra diferença está na separação dos requisitos por nível de segurança, no caso da presente *framework* esta não efetua uma separação de requisitos por níveis de segurança porque um requisito só deve ter associado um nível de segurança. Por exemplo, se uma aplicação do produto tem uma funcionalidade de *login* e o objetivo de segurança é garantir a confidencialidade dos dados nessa aplicação, então o acesso deve ser sempre realizado fisicamente, e não permitir a existência de meios alternativos para o acesso remoto. Outra particularidade que é abordada no presente trabalho é a necessidade de requisitos para a realização da descontinuação do produto.

3.3.5 *Níveis de segurança*

Os níveis de segurança são determinados com base na probabilidade de um ataque ocorrer no produto. Apesar de este tipo de análise já ser realizada na análise de risco, é importante rever este fator que vai influenciar na determinação do tipo de implementação das medidas de segurança. Da mesma forma que o *IEC 62443* atribui um nível de segurança a cada um dos seus 7 requisitos fundamentais, no presente trabalho também será atribuído a cada medida um nível de segurança.

A probabilidade de existir uma ameaça ou de ocorrer um ciberataque ao produto varia consoante as suas caraterísticas e funcionalidades. Por esta razão, estas carate-

Tabela 2: Exemplo de Requisitos de segurança para a Fase da Descontinuação

Fase de Descontinuação		
Objetivo de Segurança	**Medida**	**Descrição**
Confidencialidade dos dados	Remoção de dados confidenciais dentro dos *ECUs*	Quaisquer dados sensíveis ainda existentes no produto devem ser transferidos e removidos das componentes.
	...	...
Confiança na integridade dos dados	Remoção de dados não confidenciais dentro dos *ECUs*	De forma a garantir que a integridade dos dados não seja comprometida após descontinuação do produto, todos os dados devem ser apagados por completo das componentes do produto.
	...	...
Recuperação do serviço de *infotainment*	Remoção de dados de *backup* dentro dos *ECUs*	Caso os dados de *backup* contenham alguma informação sensível ou confidencial, estes devem ser removidos por completo do sistema.
	...	...
Transferência de dados Autenticados	Transferência de registo do movimentos de pacotes	Os registos de quem enviou dados devem ser transferidos ou removidos por completo do sistema do produto.
	...	...

rísticas devem ser registadas de forma a que seja possível assegurar a implementação mais adequada para a medida de segurança. A probabilidade pode ser determinada com base nos motivos do atacante, e no que o atacante poderá ganhar ao conseguir entrar no produto ou comprometer a cibersegurança do produto.

Para este trabalho propõe-se a utilização de níveis de segurança baseados nos *Framework Implementation Tiers* da *NIST - Framework for Improving Critical Infrastructure Cybersecurity*, e dos *Security Levels* do *IEC 62443*.

Os níveis de segurança que propõe-se serão baseados nos motivos e capacidades para um atacante tem ao efetuar uma ação contra a cibersegurança que afeta um ou mais requisitos (como são definidos pelo *IEC 62443*), e baseado no âmbito e contexto do produto no qual a empresa está responsável, como por exemplo as obrigações legais que a empresa tem perante aquele produto (que é definido pela *NIST - Framework for Improving Critical Infrastructure Cybersecurity*).

O tipo de implementações e o número de medidas a implementar serão diferentes consoante o nível de segurança estabelecido, isto será aplicado para qualquer medida dentro de cada fase no ciclo de vida do produto. Por exemplo no ciclo de vida final do produto, a descontinuação, esta deverá apresentar controlos e implementações específicos para o tipo de informação existente no produto, ou nas componentes do produto. Ou, no caso da implementação do produto, se existir uma medida que requer encriptar os dados de forma a garantir a confidencialidade dos dados, o tipo de algoritmo de encriptação a ser aplicado vai depender no nível de segurança definido. Os níveis de segurança neste contexto também vão ajudar na determinação do número de medidas que são necessárias para alcançar um determinado requisito, por exemplo se um requisito apresenta um alto nível de segurança, isto irá implicar que a implementação de apenas uma medida poderá não ser suficiente para concretizar o requisito.

As medidas e implementações que poderão ser utilizadas no contexto automóvel serão exploradas nas próximas secções referentes a cada fase do produto, posterior ao planeamento.

3.3.6 *Metodologia de garantia*

A metodologia de garantia define a forma como o produto desenvolvido será avaliado para validar que as medidas de cibersegurança estão bem implementadas e que são as medidas mais adequadas para o produto. Um produto só deverá estar válido para poder ser colocado em circulação no mercado, se a avaliação for positiva. E tal como o nome indica, a metodologia de garantia serve também para obter um certificado sobre os níveis de segurança aplicados no produto, garantindo assim aos possíveis clientes do produto que os objetivos de cibersegurança foram alcançados.

Tal como proposto por Glas et al., 2015, é necessário criar uma metodologia especifica para o setor automóvel, e para este fim os autores propõem a utilização de *standards* como a *ISO 15408/Common Criteria*. No caso do presente trabalho, propõe-se que seja também criada uma metodologia baseada na estrutura já existente

do *standard ISO 15408/Common Criteria*. Isto deve-se pelo facto da *ISO 15408* apresentar um estrutura de avaliação bastante genérica, o que pode ser utilizada em diferentes contextos.

A metodologia de garantia deverá ser utilizada para garantir que as componentes do produto foram integradas de forma segura, seguindo os objetivos definidos no perfil de segurança alvo. Esta deverá servir para garantir que as capacidades de cibersegurança do produto são aquelas pedidas e incorporadas, segundo os requisitos de segurança definidos para o produto. E, deve servir acima de tudo, como um meio para certificar o perfil de segurança criado para a cibersegurança de todos os aspetos do produto.

Como é explicado na *ISO 15408/Common Criteria*, para garantir que as medidas de segurança foram aplicadas num produto, existem dois elementos importantes para provar essa garantia de segurança:

- As medidas são as corretas: as medidas fazem o que estas afirmam fazer
- As medidas são suficientes: se as medidas fazem o que estas afirmam fazer, isto é, as ameaças dos ativos do produto são travadas

Como muitos dos responsáveis dos ativos de um produto não possuem os recursos ou conhecimentos para avaliar a suficiência e a correção das medidas, é necessário existir uma metodologia de garantia para a cibersegurança por forma a que estas entidades estejam preparadas para apresentarem que as medidas de cibersegurança foram aplicadas no produto, de forma correta e segura à entidade avaliadora.

Esta metodologia será explorada na secção da fase de Lançamento desta *framework*, secção 3.6.

3.3.7 *Planeamento de atividades*

No que toca ao planeamento de atividades, nesta primeira fase da *framework* é importante estabelecer os conhecimentos necessários para garantir as boas práticas na cibersegurança. Sejam estas as boas práticas de escritório, as boas práticas de desenvolvimento de código seguro e sem *bugs*, ou, o que deve ser efetuado no caso da ocorrência de uma falha na segurança do produto. Este tipo de atividades devem ser sempre efetuados e disponíveis em qualquer fase do produto.

A disponibilização de formações é importante para garantir a cibersegurança da informação em qualquer setor industrial, mas saber quando e quem precisa, poderá ser uma resposta difícil de encontrar. Com certeza que no início de qualquer projeto é

fácil perceber e encontrar as formações que todos os elementos da equipa necessitam, especialmente aquelas para saber como efetuar o seu trabalho de forma segurança. Mas após esta fase inicial, qualquer falta de conhecimento de boas práticas nos elementos da equipa que não tenha sido detetado inicialmente, irá ser algo difícil de detetar se os elementos não mostrarem iniciativa própria para melhorarem os seus conhecimentos de cibersegurança.

Este problema poderia ser facilmente resolvido ao efetuar auditorias e formações obrigatórias regulares, e desta forma já não existiria lugar para descuidos na falta de boas práticas para a cibersegurança. No entanto, esta resposta provoca uma redução na produtividade do desenvolvimento do produto, o que muitas empresas querem evitar. Como ambas a produtividade e segurança são aspetos essenciais para o negócio de uma empresa, aqui é importante estabelecer um equilíbrio entre os dois, para tal, propõe-se que apenas sejam realizadas auditorias e formações ao início de cada fase mas mantendo depois a possibilidade de novas formações a qualquer pessoa que mostre interesse. Este método irá depender na iniciativa das pessoas, o que não é muito prático, mas, este é o método menos intrusivo para garantir a produtividade e segurança no negócio das empresas.

Nesta fase propõe-se a utilização de ideias dos documentos de boas práticas como a *ENISA - Good practices for security of Smart Cars* e *ENISA - Good practices for security of IoT* para utilizar em atividades de boas práticas. E, para a forma como devem ser efetuadas as auditorias e o planeamento de atividades, os *standards* da *ISO 27001* e *27002* são boas fontes de orientações generalizadas para organizações que pretendam implementar um sistema de segurança da informação.

3.4 IMPLEMENTAÇÃO

Na fase da implementação são aplicadas as medidas definidas na fase do planeamento. Muitas destas envolvem os processos relacionadas com o desenvolvimento do produto, como também, a forma da criação de código para as funcionalidades do produto. Com isto, considera-se que sejam utilizadas muitas das medidas já existes no mundo da informática, visto que em muitos casos estas medidas são universais e adaptáveis para qualquer contexto atual. Um destes exemplos são documentos de boas práticas que a *ENISA* disponibiliza. Daqui propõe-se explorar dois documentos que consideram-se úteis para o sector automóvel, juntando também com outros *standards*, nomeadamente:

- *ENISA - Good practices for security of Smart Cars*

- *ENISA - Good practices for security of IoT*
- *ISO 27001*
- *ISO 27002*

A primeira escolha dos documentos da *ENISA* é as boas práticas para carros inteligentes. Este documento é claramente uma fonte obrigatória que deve ser utilizada como referência para criar uma *framework* de cibersegurança. Relativamente ao segundo documento da *ENISA*, sendo os produtos automóveis largamente influenciados pelo mundo da *IoT*, isto mostra que muitas das ideias e boas práticas do *IoT* poderão ser utilizadas para a cibersegurança de produtos automóveis. Por fim, temos os *standards* da ISO que introduzem uma ampla gama de controlos para a gestão do sistema de segurança da informação.

ENISA - Good practices for security of IoT

No documento *ENISA - Good practices for security of IoT*, as boas práticas estão dividas em três grupos: Pessoas, Processos e Tecnologias. Muitas das boas práticas no grupo das Pessoas constituem nas práticas relativas a formações e à propagação de conhecimento das boas práticas. Estas práticas são bastante universais e considera-se que podem ser utilizadas em empresas automóveis. Ainda no conjunto de boas práticas para as Pessoas, são também definidas medidas para estabelecer cargos e privilégios dentro da fase de desenvolvimento do projeto. Por fim, neste grupo são ainda indicadas formas de manter uma cultura de segurança na organização, isto tudo é aplicável no contexto automóvel. Estas são medidas que devem ser preparadas já na fase de planeamento para que ao inicio da implementação estas práticas sejam utilizadas o mais cedo possível.

No segundo grupo de boas práticas, os Processos, são apresentadas várias medidas de segurança para os vários processos como por exemplo a gestão de terceiras entidades. Isto é algo importante e que as empresas automóveis precisam bastante, razão esta devida ao facto de nesta industria serem contratados recursos externos para desenvolver as componentes e funcionalidades do produto. Além deste tipo de medidas, também são apresentadas boas práticas essenciais para a gestão das operações. Isto é o caso da definição de planos de gestão de incidentes e de alterações, e também, os planos para a gestão de vulnerabilidades e correção dessas vulnerabilidades que poderão surgir. Neste grupo de boas práticas também são abordados os processos para o *design* seguro, destas, destacam-se medidas como a aplicação do princípio do menos privilegiado e a realização de revisões periódicas ao *design* do produto. Por fim, no último subconjunto deste grupo de boas práticas apresentam algumas práticas para as regras internas da organização. Deste conjunto,

a medida mais importante para a cibersegurança será o controlo do processo do desenvolvimento contra a divulgação de informação sobre a segurança. Isto é algo importante para prevenir o comprometimento da segurança do produto.

Por fim, no último grupo são apresentadas boas práticas ligadas às tecnologias. Apesar destas práticas estarem mais direcionadas a produtos da *IoT*, estas não deixam de ser úteis para um contexto automóvel, que é o caso das práticas referentes ao controlo de acesso. É importante que seja implementado um controlo de acesso para garantir que o sistema valide se o utilizador tem as permissões corretas para usar no sistema. É também essencial no sector automóvel o controlo de acesso físico às zonas criticas, o que é essencial aplicar na fase de desenvolvimento do produto. Este grupo apresenta boas práticas para o desenvolvimento de código seguro, o que é feito, principalmente, pelo estabelecimento de quais são as melhores práticas para exercer durante o desenvolvimento do código. São também estabelecidas as técnicas que devem ser utilizadas durante o desenvolvimento do código, e da mesma forma que é feito no desenvolvimento de código para produtos informáticos, devem também ser implementadas medidas para deteção de mau código. O último subconjunto é composto por boas práticas para a implementação segura, por exemplo, medidas para reforçar que no primeiro acesso do utilizador este altere a sua *password* inicial. Outra medida que é própria do *IoT*, mas também é importante para um produto automóvel, é a implementação de *standards* abertos para a interoperabilidade nos sistemas. Isto é algo difícil de aplicar na industria automóvel visto que cada fabricante automóvel desenvolve os seus produtos de forma diferente, mas com a interoperabilidade dos sistemas, esta seria uma mais valia para aplicar soluções de cibersegurança já existentes.

ENISA - Good practices for security of Smart Cars

Tal como no documento anterior, neste a *ENISA* separa as boas práticas para a segurança de carros inteligentes em três grupos: Políticas, práticas organizacionais e práticas técnicas. Comparando com as práticas apresentadas no documento anterior da *ENISA*, muitas destas estão presentes aqui mas agrupadas de forma diferente. Neste documento de boas práticas para os carros inteligentes, os grupos principais apresentam subconjuntos de medidas focadas para certas atividades do setor automóvel. Isto é visível nos subconjuntos do primeiro grupo:

- Segurança por *design*
- Privacidade por *design*
- Gestão de ativos, e

- Gestão de risco e ameaças

Nestes subconjuntos são apresentadas as políticas que devem ser implementadas para criar, desde o início, uma cultura de cibersegurança no desenvolvimento do produto, tendo sempre em perspetiva a infraestrutura do setor automóvel que é aquilo que mais causa distinção perante o setor da informática.

O segundo grupo tem um foco nas práticas organizacionais, o que é algo comum em qualquer industria que tire partido de tecnologias informáticas para o seu negócio. As práticas aqui estão divididas por subconjuntos para a relação com os fornecedores, a gestão da segurança, e a gestão de incidentes. É importante que sejam aplicadas medidas para reforçar as comunicações com os fornecedores e controlar com quem é partilhada a informação. E para a gestão da segurança, é essencial que seja estabelecido um *Security Operations Center* (*SOC*) para poder antecipar e prevenir riscos desnecessários. A gestão de incidentes é algo que deve existir em todas as fases ativas do produto, e desta forma devem ser consideradas medidas para a eventualidade de um incidente durante o desenvolvimento do produto. Uma fonte que propõe-se para este aspeto será o documento da *NIST - Special Publication 800-34*, que é uma fonte de informação no qual se apresentam ideias para a forma de lidar com incidentes, e, como criar os planos para preparar a organização contra desastres naturais e não naturais.

Por fim, no último grupo de práticas são apresentadas as práticas e técnicas que devem ser seguidas para proteger os próprios automóveis, como também os sistemas de *back-end* associados aos produtos. Estas práticas cobrem várias áreas de cibersegurança e estão agrupadas por:

- Deteção de intrusões
- Proteção de redes e protocolos
- Segurança de *software*
- Segurança da *cloud*
- Criptografia
- Controlo de acesso
- Auto-proteção e ciber resiliência
- Auto-proteção e ciber resiliência para sistemas autónomos, e
- Continuidade de operações

Como se pode ver, este documento apresenta uma vasta quantidade de práticas para a cibersegurança dos automóveis. Muitas destas são práticas já existentes no

mundo da informática, o que ajuda a provar que é possível reutilizar as práticas já existentes para a cibersegurança do setor automóvel. No entanto, é de destacar o subconjunto acima mencionado, Auto-proteção e ciber resiliência para sistemas autónomos. O tópico dos veículos autónomos é algo bastante delicado sendo que qualquer ataque que comprometa o funcionamento dos sensores, a segurança do condutor e de quem está no exterior poderá estar em risco. Para tal, as práticas que são apresentadas pela *ENISA* para combater este problema são medidas como a redundância de *hardware*, ou redundância de dados. O produto deve estar reforçado contra ataques adversos que possam enganar os sensores, por exemplo, através da falsificação ou manipulação dos dados usados no *Machine Learning* e pela inteligência artificial do veiculo autónomo.

ISO 27001 e 27002

Os *standards 27001* e *27002* da *ISO* apresentam vários controlos que consideram-se ser adequados para os processos de desenvolvimento de um produto automóvel. Muito do que é apresentado na *27001* é um resumo das boas práticas que uma organização pode seguir para melhorar a segurança nas atividades do seu negócio. Como estas práticas não são específicas para uma industria, estas podem ser aplicadas em qualquer fase de vida do produto. O *standard* que mais oferece em termos de medidas é o *27002*. Este apresenta essencialmente o que é ilustrado no *standard 27001*, mas com maior desenvolvimento no detalhe de cada medida e controlo que podem ser utilizados para os diferentes ambientes de trabalho. Neste existem vários grupos de controlos que devem ser utilizados nesta fase de implementação, como por exemplo:

- **Gestão da direção da segurança da informação**. Este grupo tem o objetivo de oferecer orientações na gestão e suporte da segurança da informação de acordo com os requisitos de negócio e legislações. Aqui temos um controlo que deve estar presente durante a fase de implementação, ou seja, as políticas para a segurança da informação. Nestas políticas deve ser definido o que deve ser feito para garantir a segurança por qualquer membro da organização e entidades terceiras, como é o caso dos fornecedores de produtos automóveis.
- **Dispositivos móveis e tele-trabalho**. Neste grupo são apresentados controlos para a segurança da informação ao utilizar dispositivos móveis e para o uso do tele-trabalho. No caso dos dispositivos móveis, atualmente o uso de um telemóvel da empresa é algo presente em qualquer empresa de médio e grande tamanho, para tal deve ser necessário criar políticas e medidas de apoio para assegurar a segurança perante os riscos associados destes disposi-

tivos. Desta forma o controlo apresentado pelo *standard* é de facto essencial para o contexto deste trabalho. O tele-trabalho é algo que muitas vezes é evitado, e deve ser evitado, ao desenvolver este tipo produtos, no entanto em momentos excepcionais como é o caso de uma pandemia, o tele-trabalho prova ser a melhor alternativa para muitas empresas, e deste modo devem ser sempre previstas medidas e políticas para continuar a assegurar a segurança da informação nestes cenários. Isto é algo que a *27001* e *27002* apresenta como controlo ao prever este tipo de situações.

- **Responsabilidades de ativos**. Durante o desenvolvimento de qualquer produto é importante identificar os ativos da empresa e definir quem será responsável pela sua proteção. Para tal, são apresentados vários controlos nestes *standards*. Um destes é relativo ao inventário dos ativos, ou seja, qualquer ativo associado com informação ou que faça algum tipo de processamento deve ser identificado e mantido numa lista de inventário. Isto é algo importante porque ajuda na proteção contra a fuga de dados durante esta fase de implementação do produto. Outro controlo importante é a forma como devem ser utilizados os ativos, isto implica que sejam estabelecidas regras para a forma aceitável de utilização da informação, e dos ativos que interagem com essa informação. Isto é algo que é relevante para os produtos automóveis sendo que é essencial garantir o máximo de segurança possível ao manusear um ativo. Por exemplo, um fornecedor que está encarregue em desenvolver uma certa funcionalidade do automóvel. Para esta funcionalidade a entidade construtora do automóvel, muito certamente, disponibiliza o *hardware* onde é esperado a funcionalidade. Perante estas situações é essencial serem estabelecidas regras para como e quando utilizar o *hardware* disponibilizado.
- **Manuseamento de equipamento multimédia**. Durante o desenvolvimento de um produto é necessário armazenar os dados e informações associadas. Isto é algo que deve ser controlado de forma a prevenir a divulgação não autorizada, modificação, transferência e destruição de informação guardada nos equipamentos de armazenamento. Em muitos casos as empresas ao desenvolverem os produtos possuem os seus próprios equipamentos de armazenamento locais de dados, por forma a evitar o uso de serviços armazenamento na *cloud*. Nestes casos a empresa está responsável pela segurança desse equipamento. Este é um assunto que o *standard ISO 27001* apresenta controlos não só para estes equipamentos, mas também, para os equipamento de armazenamento móveis como as *pens USB*. Um controlo importante que é apresentado neste grupo é a gestão de equipamentos removíveis (por exemplo,

discos externos), para as quais devem ser implementados procedimentos para gerir este tipo de equipamentos ao serem utilizados no local de desenvolvimento do produto. Como já foi referido, isto é importante para prevenir que a informação dentro destes equipamentos não seja comprometida.

- **Gestão do acesso de utilizadores**. O controlo do acesso dos utilizadores de um sistema, ou de serviços, é essencial para garantir a cibersegurança em qualquer organização. Tal como nos documentos de boas práticas, esta *ISO* aborda este tema trazendo com isto outros aspetos relevantes, como é o caso do registo e remoção de utilizadores. Este controlo implica que seja definido um formato para o registo e a remoção de utilizadores para possibilitar o controlo de direitos de acesso. Outro controlo importante, é a preparação de um processo de provisionamento para o acesso, ou revogação dos direitos de acesso dos utilizadores, aos sistemas/serviços quando necessário. Isto tudo deve ser gerido e controlado, o que é também apresentado como um controlo neste grupo.
- **Áreas seguras**. Durante o desenvolvimento de um produto automóvel é essencial prevenir o acesso físico de pessoas não autorizadas por forma a evitar danos e interferências à cibersegurança do produto. Estes *standards* tem precisamente um grupo de controlos para este efeito, e aqui são definidos os controlos para estabelecer perímetros de segurança, para proteger as áreas que contenham ativos ou informações críticos para a cibersegurança. Outro exemplo de um controlo neste grupo é a garantia que os escritórios, salas e estabelecimentos estão devidamente seguros contra o acesso físico de indivíduos não autorizados. É também aqui que é apresentado o controlo para garantir a segurança física contra ataques maliciosos. Este controlo não é muito elaborado mas é algo que uma organização deve ter em consideração ao desenvolver qualquer tipo de produto sensível.

Estes são apenas alguns dos grupos que podem ser utilizados nesta fase da implementação do produto. Existem mais *standards* que poderão ser utilizados como referência para uma *framework* de segurança automóvel, como é o caso da *IEC 62443*, *IT Grundschutz* e da *ISO 26262*, mas estes já são abordados no trabalho de Glas et al., 2015. Porém, por falta de acesso a este tipo de *standards* não será explorado em muito detalhe os conteúdos destes documentos no presente trabalho.

3.5 VALIDAÇÃO

Durante o desenvolvimento da maior parte de produtos no ramo automóvel é utilizada uma metodologia de desenvolvimento de *software* em cascata. Este tipo de metodologia é um processo linear o que torna o desenvolvimento do produto mais moroso. É também bastante utilizado o *V-Model*, pelo que este modelo segue a metodologia em cascata. Isto é algo que até os *standards 26262* da *ISO* e *J3061* da *SAE* incorporam na sua *framework* de cibersegurança. Visto que o *V-Model* é bastante utilizado no desenvolvimento deste tipo de produtos, é essencial que uma *framework* para este sector siga o mesmo processo de desenvolvimento para a aplicação da cibersegurança.

Depois da implementação do *software*, segue-se a fase de validação das funcionalidades desenvolvidas do produto. Nesta fase são realizadas uma variedade de testes como os testes de integração, de sistema e de aceitação. É importante para além de nesta fase ser realizado a validação de *bugs* no produto, de forma a evitar a exploração de vulnerabilidades por *hackers*, seja também importante a verificação das medidas que foram tomadas para a cibersegurança do produto. Aqui devem ser realizados essencialmente testes de penetração, o que é algo moroso mas é extremamente necessário para certificar que cibersegurança do produto está bem implementada, e está implementado segundo o definido nos requisitos de segurança. É neste cenário que propõe-se à industria automóvel em tomar a iniciativa de contratar fornecedores precisamente para este efeito de teste de penetração, isto apenas se as entidades fornecedoras das funcionalidades e de *hardware* dos seus produtos, não apresentarem as pessoas indicadas para realizar testes de penetração.

Os testes de penetração são algo também utilizado no *IoT*, tal como em qualquer produto informático. Isto é visível no documento de boas práticas da *ENISA* para o *IoT*, referido no capítulo anterior. Este mostra a importância de definir um plano de estratégia para estes testes, e construir um ambiente adequado para os executar, como por exemplo:

- Simulações ou emulação de ambiente
- *Digital twins*
- *Datasets* de teste
- Captura de *outputs* para pós-processamento
- *Fuzzing*
- *Sandboxing*

Estes testes, nesta fase, ajudam a não só a verificar que as medidas estão bem implementadas mas também a encontrar *bugs* ou vulnerabilidades, como é o caso do exemplo dado, *Fuzzing*. Estes são apenas alguns dos exemplos que podem ser utilizados em produtos automóveis, a partir de medidas e técnicas já existentes no *IoT* e no mundo da informática. Neste documento da *ENISA* são listados os vários testes que podem ser utilizados para esta fase de validação.

Este tipo de validações também é referido no documento de boas práticas para automóveis inteligentes da *ENISA*, mas este tema não é tão elaborado como no documento do *IoT*. Aqui, este tipo de testes são mencionados dentro das práticas para a gestão de risco, e apesar de estes não estarem claramente destacados como uma atividade que deve ser realizada depois da implementação, este continua ser apresentado como uma atividade necessária para o setor automóvel.

No que toca a outros *standards* do mundo automóvel, não poderá ser destacado nenhum para esta fase sendo que o acesso a estes não foi possível. Mas certamente este tema deve ser abordado em *standards* e documentos como a *SAE J3061* , *IEC 62443*, ou *ISO 26262* onde poderá ser reutilizado alguma ideia, destes, para a fase de validação do produto.

3.6 LANÇAMENTO

A fase de Lançamento será focada principalmente na avaliação e certificação da cibersegurança aplicada no produto. Como já foi mencionado inicialmente na secção 3.3.6, existe a necessidade de uma metodologia de garantia *standard* para que seja possível provar a cibersegurança do produto. Isto é feito através da evidenciação das medidas que foram usadas para aplicar a segurança no produto foram suficientes, e, que foram as medidas corretas para o produto.

Desta forma é importante que na metodologia de garantia seja essencial identificar os ativos do produto e as medidas para proteger esses ativos. Esta identificação dos ativos e de medidas já é realizado na primeira fase da *framework* com a definição do Perfil de Segurança. Com isto, o que falta para a metodologia de garantia é saber como provar que estas medidas são as corretas e suficientes para a cibersegurança.

A *ISO 15408/Common Criteria* vem desta forma ajudar nesta atividade. Neste *standard* é referido a utilização de um *Security Target*, o que na presente *framework* é essencialmente o Perfil de Segurança. Através deste *Security Target*, é possível descrever as medidas de segurança e demonstrar que estas medidas são suficientes

ao mostrar que elas aplicam a segurança garantida. Isto leva à necessidade da existência de uma entidade certificada para efetuar a avaliação em si. A entidade que desenvolve o produto apenas precisa de se focar na identificação das medidas para poder provar a cibersegurança aplicada, durante a avaliação. A definição de métodos de avaliação não cabe a esta *framework* pois a determinação do que está correto e errado cabe a entidades certificadas para a definição dos critérios de avaliação. Para a presente *framework*, apenas sugiro a utilização de um formato de alto nível utilizado neste *standard* com o objetivo de preparar a entidade responsável pelo produto, a perceber como obter a garantia de segurança no seu produto.

Para avaliar se as medidas são suficientes, a entidade deve apresentar:

- Os ativos que a medida protege;
- Descrição da medida;
- Detalhe dos objetivos de segurança para os *Security Functional Requirements* (*SFR*);
- E por fim, demonstrar a medida.

Exceptuando a demonstração, com esta *framework* o resto do esforço já deve estar preparado depois da fase de Planeamento, com as atividades da definição do Perfil de Segurança.

A avaliação da fidelidade da cibersegurança do produto, impõe que o produto seja bem desenhado e implementado de modo a evitar erros que poderão causar comportamentos inesperados, isto é, o surgimento de vulnerabilidades e riscos para o produto. Para validar isto, a entidade deve garantir que o produto seja testado ao longo do seu desenvolvimento, ou, logo depois do seu desenvolvimento. Esta fase é discutida na secção 3.5 - Validação do produto. Os vários *designs* do produto devem ser examinados de forma a procurar possíveis erros do desenho da arquitetura do produto, funcionalidades e requisitos. Esta examinação deve ser realizada antes de iniciar a implementação do produto ou quando são introduzidas novas funcionalidades ao produto.

A *ISO 15408* também menciona a examinação da segurança física do local de desenvolvimento do produto, e visto que os produtos do sector automóvel são de grande criticidade para a segurança do consumidor, este tipo de examinação é também igualmente importante para esta avaliação da fidelidade da segurança aplicada. Tal como na examinação anterior, antes da implementação do produto deve ser revisto se o local de desenvolvimento oferece o tipo de segurança física necessária, para garantir o desenvolvimento seguro do produto. Aqui entram os

Security Assurance Requirements (*SARS*) que tal como os *SFRs* estão presentes nos requisitos de segurança definidos a partir Perfil de Segurança. Estes requisitos oferecem uma descrição do que o produto deve fazer, e ajudam a determinar a fidelidade da segurança do produto.

Com isto temos os dois passos necessários para efetuar uma avaliação de garantia da segurança do produto: a avaliação da fidelidade sobre a suficiência das medidas e a verificação se as medidas são as corretas para a cibersegurança. Resumindo, o resultado da avaliação da segurança do produto só poderá ser um dos dois: os requisitos de segurança foram alcançados, ou, não foram alcançados para garantir a cibersegurança definida pelo Perfil de Segurança. A *ISO 15408/Common Criteria* apresenta métodos que podem ser utilizados no setor automóvel, e o que foi aqui apresentado pretende provar que este *standard* pode ser utilizado para uma metodologia de garantia, num aspeto de alto nível, para ser aplicada numa *framework* de cibersegurança automóvel. Esta *ISO* oferece também linguagens *standard* para definir o requisitos de segurança, o que ajuda na harmonização na garantia da segurança neste setor, tal como é estabelecido na industria informática.

Sendo o setor automóvel uma industria composta por várias entidades que se relacionam entre si, para o desenvolvimento de um produto, estes aspetos devem ser considerados numa metodologia de garantia, o que a *ISO 15408/Common Criteria* não o faz por este ser um *standard* generalizado, com o objetivo de ser utilizado por qualquer industria. Assim a metodologia de garantia terá de usar as ideias base deste *standard* e adicionar as especificidades do contexto automóvel, por exemplo, para cada entidade que desenvolve funcionalidades diferentes durante o desenvolvimento de um automóvel, cada entidade terá requisitos e critérios diferentes para serem avaliados, visto que cada uma desempenha atividades distintas.

A utilização da *ISO 15408/Common Criteria* é também proposta no trabalho de Glas et al., 2015, onde sugerem também a utilização de ideias tiradas de *standards* já existentes para a sua *framework* de segurança de informação, por exemplo o *standard IEC 62443*. Mas o autores notam que esta metodologia de garantia não é uma prioridade da *framework* de segurança da informação, o foco deste deve ser apenas na aplicação e não na certificação da cibersegurança, e neste ponto de vista o presente trabalho não concorda com os autores. Sendo que para melhorar a cibersegurança no setor automóvel, a certificação e a garantia da cibersegurança aplicada nos seus produtos, a certificação é um meio de motivador para ajudar a alcançar este fim. Ao existir uma obrigatoriedade de garantir a cibersegurança nos produtos, isto promove o desenvolvimento de novas medidas para proteger a informação armazenada nos produtos automóveis. Sendo que no futuro as tecnologias

informáticas serão cada vez mais presentes nos automóveis, também deverá ser a cibersegurança aplicada nestes, e isto será um fator influenciador no consumidor do produto. Desta forma, a certificação é um aspeto importante e necessário para uma *framework* de segurança da informação.

3.7 SUPORTE

A fase de suporte representa a fase onde o produto automóvel está nas mãos do consumidor final, e cabe à entidade vendedora do produto, ou outra terceira entidade, a prestação de um serviço de suporte. Aqui devem existir planos, requisitos e processos para ajudar o cliente a manter a cibersegurança do produto. Isto pode ser feito através de atualizações do sistema quando este está desatualizado, ou quando existe a necessidade de aplicar uma atualização no sistema do automóvel para corrigir uma vulnerabilidade detectada depois do lançamento do produto. Este tipo de atividades devem ser serviços obrigatórios nos automóveis modernos tal como a segurança física do automóvel, condutores e passageiros são também obrigatórias.

Num aspeto de gestão de risco, as mesma medidas usadas na implementação devem continuar a ser aplicadas aqui devido ao risco residual, ou devido à possibilidade da descoberta de vulnerabilidades. Exemplo de uma destas medidas é a utilização de uma plataforma de partilha de informação sobre riscos, ameaças e vulnerabilidades entre organizações da mesma industria. Este tipo de medida seria algo que ajudaria a aumentar a cibersegurança no sector automóvel e ao mesmo tempo, prevenia perdas económicas causadas por ciberataques.

Este é apenas um aspeto da fase de suporte que a empresa deve disponibilizar. Outro aspeto que deve continuar no suporte vindo da implementação são as medidas de análise e de auditoria. Estas análises referem-se ao comportamento do produto perante possíveis anomalias no seu funcionamento ou do tráfego da rede. Em muitos casos estas análises são realizadas por sistemas de deteção de intrusões (IDS). Esta é uma área bastante explorada no mundo da informática e do IoT, que deve ser utilizada também em produtos automóveis com a capacidade de comunicações externas. A análise dos resultados do *IDS* é algo que a empresa deverá oferecer de forma a conseguir prestar auxílio ao cliente caso for necessário. As auditorias também são atividades que devem continuar nesta fase. Durante o suporte do produto é importante manter as práticas de cibersegurança atualizadas de forma a

acompanhar as mudanças das tecnologias usadas pela organização para desenvolver o seu negócio.

O *standard ISO 27001* aborda o tema de suporte precisamente da mesma forma. A organização responsável deve disponibilizar recursos para continuar a garantir a cibersegurança do produto. A organização deve definir requisitos e planos para como fazer o suporte, como por exemplo quais as competências necessárias que as pessoas responsáveis pelo suporte devem possuir. Outro aspeto importante que se pode retirar deste *standard* é a comunicação durante o suporte. Devem ser definidos planos para como proceder em certos eventos da cibersegurança, saber como os eventos devem ser comunicados, quando e a quem deve ser comunicado o evento, quem irá fazer a comunicação e que processos serão afetados pela comunicação. Por fim, a *ISO 27001* dá ênfase à importância da documentação destes processos. Como em qualquer processo, devem ser documentados os planos e medidas realizados numa fase, e para isto é necessário também estabelecer regras de como fazer este processo de documentação. Estas regras são por exemplo como e quem faz a criação e atualização da documentação. Outro exemplo são as regras para efetuar o controlo da documentação, isto é, como devem ser realizadas as atividades de distribuição, acesso e uso da documentação. Estas são apenas algumas das atividades que o *standard* apresenta onde o setor automóvel pode seguir na fase de suporte, e também em qualquer outra fase.

Portanto, na *27002* conseguimos encontrar vários controlos também úteis para o suporte. Um grupo de controlos importante para esta fase é a de *Logging* e monitorização, e aqui os controlos que são apresentados tem o objetivo de registar eventos e criar evidências. A recolha de evidências é uma atividade que possibilita perceber melhor as ameaças a que o produto está vulnerável, e a partir delas, determinar a melhor solução para as combater.

Todas estas medidas de gestão e de análise contribuem para a necessidade de aplicar atualizações de *software* no produto. Quando isto acontece, o consumidor deve ser notificado, o que é algo que a organização responsável pelo suporte do produto deve fazer. Ao existir um sistema de notificações para atualizações, o produto tem a oportunidade de continuar menos tempo exposto a um risco conhecido. Mas as atualizações de *software* podem ser alturas de grande risco para um produto, são nestas ocasiões que um atacante tem a oportunidade de comprometer o sistema do produto através da modificação ou falsificação da actualização. Para tal deve ser utilizado um sistema de atualizações de *software* seguro, este é o caso do *Uptane* que é uma *framework open source*. Esta *framework* é uma ferramenta que irá ajudar na harmonização do sector automóvel, se esta vier a ser utilizado pelas empresas

automóveis. Devido à falta de um documento norma para a utilização de um sistema de atualizações de *software* seguras, *Uptane* é a melhor solução que propõe-se para as atualizações de *software* no mundo automóvel.

O Suporte é algo que deve ser garantido durante o ciclo ativo do produto até este chegar à sua fase de descontinuação.

3.8 DESCONTINUAÇÃO

A fase de descontinuação tem início quando o produto já não apresenta as capacidades adequadas para funcionar dentro dos requisitos para o bom funcionamento nas estradas, ou quando a entidade responsável pelo suporte decide terminar o suporte no modelo de um automóvel (como também ocorre em muitos cenários no mundo informático). Quando isto acontece é importante que sejam tomadas medidas para garantir que nada sensível no produto permaneça, para ser explorado para fins maliciosos.

Esta fase é algo pouco discutido nos trabalhos de cibersegurança no setor automóvel. No trabalho de Glas et al., 2015 não são referidas sugestões para ideias nesta fase final na vida de um produto, muito porque este tópico não é abordado pelos autores. Em termos de *standards*, os *standards* do setor automóvel mostram abordar a fase de descontinuação para os automóveis, como é o caso da *ISO 26262*. O que indica ser possível, extrair ideias de como proceder a esta fase segundo a perspetiva automóvel. Mas como o presente trabalho não obteve acesso a *standards* automóveis, para esta fase serão apenas explorados *standards* e documentos relacionados com a cibersegurança do setor informático.

No documento da *ENISA* para as boas práticas da cibersegurança no *IoT*, quando um produto se torna obsoleto neste documento é expresso a importância de existirem mecanismos para garantir a disposição do produto em segurança. O *IoT* tem o problema de lidar com uma grande variedade de tipo de dados que são usados ou guardados em *cache* para processamento, o que é algo que os automóveis modernos poderão apresentar também. Dados que poderão passar pelos automóveis podem ser por exemplo os dados pessoais do condutor, dados usados pelos sensores do veículo, dados referentes aos certificados das autenticações, ou dados das chaves usadas por mecanismos de cifragem. Desta forma, o que deve ser principalmente realizado é a definição de uma estratégia para a disposição do produto. Como cada produto poderá variar em termos de dados usados, estes devem ser documentados previamente e classificados em termos de criticidade dos dados perante as diferentes categorias.

Por exemplo a privacidade do cliente, ou o impacto do negocio da organização se os dados forem comprometidos. Isto deve ser estabelecido para quando a fase de descontinuação for iniciada, seja realizado a disposição de forma correta e segura. Esta é a prática que se pode retirar deste documento da *ENISA*.

A partir do *standard ISO 27002* é possível utilizar alguns controlos para esta fase. Um destes controlos é referente à disposição de equipamento *media*, isto é um assunto que o setor automóvel pode retirar ideias na disposição das componentes de *infotainment*. Este controlo apresenta vários aspetos que devem ser considerados para o estabelecimento de um plano da disposição da *media*. Alguns aspetos para serem considerados no contexto automóvel são:

- A *media* contendo informações confidenciais, deve ser guardada e disposta de forma segura. Isto implica destruir completamente a componente, ou apagar os dados da componente caso este tenha o objetivo de ser reutilizado.
- Procedimentos devem ser estabelecidos para identificar as componentes que necessitam de disposição segura.
- As componentes ou itens dispostas devem ser registadas de forma a manter um linha de rastreamento.

Este controlo também apresenta uma consideração quanto à quantidade agregada destes equipamentos de *media*, com informação não sensível. Esta agregação tem um efeito que pode provocar que a informação não sensível aqui guardada, pode passar a informação sensível. Desta forma é importante evitar manter *media* junta durante muito tempo, sendo que o melhor poderá ser a sua reutilização para outros fins, ou a sua destruição ou remoção dos dados existentes nestes.

Em termos de controlos para a disposição segura ou reutilização de equipamento, a *ISO* apresenta um. Este controlo é aplicado aos equipamentos específicos para o armazenamento de dados, e aqui são definidas procedimentos como a identificação destes equipamentos que contenham dados sensíveis, ou que contenham *software* licenciado que devam ser removidos ou *overwritten* de forma segura antes de realizar a disposição ou reutilização. Mas este controlo também aborda um cenário onde este tipo de equipamento está apenas danificado. Neste contexto é necessário voltar a realizar uma análise de risco de forma a verificar se o equipamento deve ser completamente destruído, em vez de ser reparado ou disposto. Outro ponto levantado neste controlo é o uso alternativo da encriptação dos dados em vez da erradicação dos dados, mas isto é uma alternativa que só é viável se:

- o processo de encriptação é forte o suficiente e cobre todas as partições do equipamento;
- as chaves de encriptação são fortes e grandes o suficientes para serem mais resistentes contra ataques de força bruta;
- as chaves de encriptação são guardadas de forma segura e confidencial.

Da mesma forma, as técnicas usadas para efetuar o *overwrite* de forma segura devem ser analisadas e revistas. Isto deve-se ao facto dos equipamentos serem constituídos por tecnologias diferentes, o que pode implicar a utilização de técnicas diferentes de *overwrite*.

Um controlo que não está diretamente associado à fase de descontinuação mas pode ser utilizado nesta fase, dentro do contexto automóvel, é o controlo para equipamentos ativos sem um utilizador a interagir. Este tipo de situações pode acontecer quando o produto é entregue ou é considerado para entrar na fase de descontinuação. Nestas situações, poderá existir um período onde o produto está em espera para os procedimentos de disposição serem aplicados a este. Caso isto aconteça, é importante que sejam tomadas medidas para proteger o produto que não tem um utilizador ativo encarregue deste.

Este controlo serve precisamente para este fim, onde os utilizadores responsáveis devem estar cientes dos requisitos e procedimentos de segurança para manter o produto fora de uso, protegido, e da responsabilidade de implementar esses requisitos e procedimentos. Para tal este controlo oferece recomendações como:

- terminar sessões ativas;
- efetuar o *logout* de aplicações, ou desativação de serviços de redes;
- para os equipamentos que não prestam forma de efetuar *logout*, deve ser garantido um controlo de acesso aos equipamentos.

4

CASO DE USO

No presente capítulo é apresentado um exemplo da aplicação da *framework* proposta, para a cibersegurança num produto automóvel. Aqui serão abordadas as fases principais do ciclo de vida do produto, entre elas a fase do planeamento da *framework* com a exemplificação do processo de definição do Perfil de Segurança, e a conjugação dos requisitos e medidas de cibersegurança para cada uma das fases posteriores ao planeamento.

4.1 ETAPAS DA FRAMEWORK

Para recapitular, a presente *framework* está estruturada por cinco fases, sendo que cada uma representa uma fase do ciclo de vida de um produto. Como se pode visualizar na Figura 7, a primeira fase é a mais importante da *framework* pois é aqui onde são concentradas grande parte das atividades planeadas. Deste modo, a primeira fase é aquela que envolve mais esforço e trabalho para que a presente *framework* apresente bons resultados nas suas fases seguintes.

A primeira fase, a fase do planeamento, envolve as actividades de definição de critérios do produto, análise de risco e definição do perfil de segurança do produto. Com o perfil de segurança criado, será possível identificar os requisitos e definição dos níveis de cibersegurança para o produto. Estas duas últimas atividades ajudam a obter as medidas de cibersegurança necessárias para cada fase do produto.

A partir desta fase seguem-se as fases de implementação, validação, lançamento, suporte e descontinuação. Nestas fases são implementadas as medidas de cibersegurança que foram definidas durante a fase de planeamento para as diferentes fases no ciclo de vida do produto. Neste caso, a implementação refere-se à fase de desenvolvimento do *software* e *hardware* do produto, e a sua montagem. A validação representa a fase de testes que verifica o funcionamento e a cibersegurança do produto. O lançamento representa a fase de certificação da cibersegurança aplicada no produto. O suporte representa a fase pós lançamento do produto, isto é, todo o espaço de tempo entre a saída da fábrica até ao momento de descontinuação do

produto. Por fim, a descontinuação representa a fase onde é decidido como deve ser tratado o produto quando este não é mais utilizado.

Figura 7: Resumo de atividades em cada fase da *framework*

4.2 PRODUTO AUTOMÓVEL ALVO DO CASO DE USO

O produto automóvel exemplo para este caso de uso é retirado do trabalho de Schmittner, Ma et al., 2016.

O produto para desenvolvimento é um *ECU* que inclui o *hardware* e as instalações de *software* que oferecem conectividade remota para a rede interior. Este *ECU* serve de entrada para vários serviços remotos incluindo a aquisição de dados, controlo remoto, manutenção e atualizações de *software over-the-air*. Porém, este também possibilita a interação com um operador humano através de uma *interface* (*HMI*, *human-machine interface*) para certas ações de controlo no *cockpit* do veículo.

O *hardware* é baseado num controlador de topo, com *interfaces* de rede que suportam as funcionalidades planeadas. Como se pode ver na Figura 8, este está equipado com *interfaces* de comunicação celular e *WLAN* para a conectividade sem fios. Este também inclui uma *interface Ethernet* para o *debug* e ligação de dispositivos locais, como por exemplo cameras *Ethernet*. Um porto *USB* é usado para a atualização de *software* local ou para o fornecimento do *software* operativo do *ECU*. A *interface CAN* é usada para conectar este *ECU* com os outros *ECUs* do veículo.

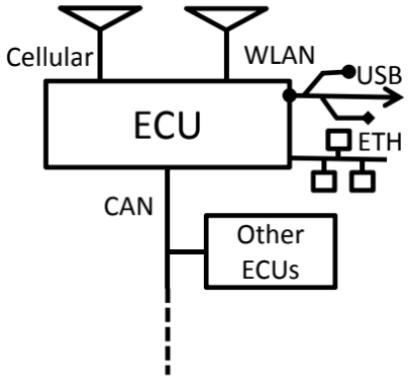


Figura 8: Diagrama representativo do ECU exemplo
(Schmittner, Ma et al., 2016)

O objetivo principal deste *ECU* é oferecer uma ligação remota a várias operações de acesso e controlo, sendo que previamente este tipo de operação era apenas possível localmente através da *interface HMI*. O sistema operativo no qual o *software* opera é baseado numa distribuição *Linux*. É de notar que esta representação é uma versão simplificada do sistema do produto suficiente para poder demonstrar a aplicação da *framework*.

4.3 APLICAÇÃO DA FRAMEWORK

A presente secção apresenta o resultado da aplicação em cada fase da *framework* no produto. Como já foi ilustrado antes, as fases da framework passam pelo planeamento, implementação, validação, lançamento, suporte e descontinuação do produto.

4.3.1 *Planeamento*

Nesta sub-secção é apresentada a aplicação da framework, Planeamento. Este planeamento envolve a definição de critérios, análise de risco, definição do Perfil de segurança, definição dos requisitos de segurança, definição dos níveis de segurança e o planeamento de atividades.

4.3.1.1 *Definição de Critérios*

Seguindo a estrutura da *framework*, em primeiro lugar será realizada a definição de critérios de funcionamento do produto. Os critérios são definidos baseando-se na descrição das funcionalidades do Produto, como é o caso da permanência das funcionalidades antigas para interação local com o veículo. Desta forma poderão ser definidos os seguintes critérios:

- O *ECU* tem de oferecer interligação de um utilizador remoto com os processos internos do veículo (os vários *ECUs* internos);
- O *ECU* deve permitir acesso de vários serviços remotos como a aquisição de dados, acesso remoto, manutenção e atualizações de *software*;
- E, o *ECU* tem de manter as funcionalidades locais no veículo, e outras funcionalidades antigas também, tais como:
  - Uma ligação *Ethernet* para dispositivos locais;
  - Uma ligação *USB* para atualizações de *software* local e fornecimento de aplicações *software*;
  - Uma interface *HMI* para interação local com os *ECUs*.

4.3.1.2 *Análise de Risco*

A análise de risco é iniciada com a identificação dos ativos do produto. Com isto é realizado o processo normal da *ISO 27005* e ao mesmo tempo seguindo os princípios do *TARA* da *SAE J3061* onde são identificadas as vulnerabilidades e riscos, e é iniciada a análise de risco do produto automóvel.

O próximo passo nesta análise é a identificação dos ativos. É importante referir que durante esta fase, apenas uma informação parcial está disponível para a análise, sendo que o que existe são conceitos e vagas descrições do sistema e funcionalidades. Usando os objetivos de alto nível do *TARA* para iniciar a análise, irão ser identificados os ativos que estão relacionados com o seu funcionamento e com a conformidade dos dados.

- Sistema operativo de distribuição *Linux*;
- *Software* que suporta a funcionalidade do *ECU*;
- Dados transferidos nos serviços remotos;
- Dados dos certificados e licenças do *software*;
- *Hardware* que suporta o *ECU*;
- *Interface HMI*.

O passo seguinte é a identificação das possíveis vulnerabilidades, ameaças e cenários de impacto. As possíveis vulnerabilidades serão:

- *hardware*:
  - Manutenção insuficiente e falha na instalação de dispositivos;
  - Suscetibilidade a variações de energia;
  - Armazenamento desprotegido;
  - Falta de cuidado no despacho de equipamento de armazenamento;
  - Cópia de informação/dados descontrolada.

- *software*:
  - Testes insuficientes ao software;
  - Falhas bem conhecidas no Sistema operativo do *ECU*;
  - Utilizadores do sistema não efetuam *logout*;
  - Falta de cuidado na reutilização de equipamento (por exemplo o equipamento de armazenamento);
  - Má alocação dos direitos de acesso;
  - Fraca gestão de passwords e certificados;
  - Software à medida novo e imaturo.
- Rede:
  - Linhas de comunicação desprotegidas;
  - Tráfego de dados desprotegido;
  - Ponto único de falha;
  - Transferência de passwords em texto livre;
  - Conexões a redes públicas desprotegidas.

Para além destas vulnerabilidades, como é usado um *software* à medida, este produto é susceptível a ataques de *Denial of Service*, ataques *zero-day*, *eavesdropping*, entre outros.

Para a identificação dos riscos recorre-se a escalas da *ISO 27005* que ajudam a obter as ameaças ao produto e classificá-las quanto o seu tipo de risco inerente. Estas escalas podem ser visualizadas no Anexo A - Escalas e Métodos Classificação de risco. No final desta análise obtém-se uma lista de nove riscos, avaliados utilizando as escalas já mencionadas. Este resultado poderá ser visualizado no Anexo B - Avaliação do risco - Caso de uso.

4.3.1.3 *Definição do Perfil de segurança*

Com a avaliação de risco terminada são iniciadas as atividades de definição dos objetivos de cibersegurança. Através dos riscos identificados poderão ser identificados os seguintes objetivos de cibersegurança:

- Proteção do produto contra intrusões maliciosas
- Promoção de conhecimentos de cibersegurança na equipa de desenvolvimento e de manutenção/suporte
- *Software* do produto sem falhas técnicas
- *Hardware* do produto sem falhas técnicas
- Controlo de acesso ao sistema
- Proteção dos dados armazenados e transmitidos pelo produto
- Proteção contra ações não autorizadas ou por engano
- Cumprimento das legislações e regulamentos no tratamento dos dados
- Atualizações de *software* certificadas
- Instalação de novas aplicações de *software* certificadas

O perfil de segurança pode depois ser definido através da atribuição de um nível de segurança (*SL*), e de categorias de segurança. As categorias de segurança têm o objetivo de ajudar a organizar os objetivos de segurança de modo a que o utilizador consiga ter uma melhor percepção do nível de abrangência dos objetivos de cibersegurança do produto. Aos *SLs* são atribuídos uma classificação numérica, como uma escala de um a dez: para os *SL1* um valor de **1**, os *SL2* um valor de **4**, os *SL3* um valor de **6**, e os *SL4* um valor de **10**. O importante aqui é estabelecer um valor numérico que represente a criticidade do objetivo de segurança. O resultado deste processo é visível na Figura 9. Através deste método de criação do Perfil, podemos obter outras métricas como o tipo de cibersegurança mais importante para no produto. Isto é visível pela média dos *SLs* na Tabela 3.

4.3.1.4 *Definição dos Requisitos de segurança*

A definição dos requisitos será realizada utilizando os objetivos de segurança presentes no Perfil de segurança, e para cada fase na *framework* definir quais o requisitos de segurança essenciais para que se cumpram os objetivos subjacentes. A identificação dos requisitos estão ao critério do utilizador da *framework*, pelo que a *framework*

Categoria de Segurança	Objetivo de Segurança	Descrição	Nível de Segurança
Confidencialidade, Integridade, Disponibilidade	Proteção do produto contra intrusões maliciosas	O produto deve estar preparado contra ameaças de *malware*, e outro tipo de ataques intrusivos no sistema.	10
	Promoção de conhecimentos de cibersegurança na equipa de desenvolvimento e de manutenção/suporte	A equipa de desenvolvimento e de suporte devem estar cientes das boas práticas da cibersegurança no trabalho.	1
Integridade, Disponibilidade, Responsabilidade	Software do produto sem falhas técnicas	O *software* deve estar bem implementado, e o seu funcionamento operacional deve ser mantido dentro das condições *standard*.	4
	Hardware do produto sem falhas técnicas	O *hardware* deve estar bem implementado, e o seu funcionamento operacional deve ser mantido dentro das condições *standard*.	6
Integridade, Responsabilidade	Controlo de acesso ao sistema	O acesso ao sistema deve estar protegido contra acessos indevidos remotos e locais.	6
	Proteção contra ações não autorizadas ou por engano	O produto deve estar com o sistema preparado para evitar ações dentro dele não autorizadas.	6
Confidencialidade, Integridade, Responsabilidade	Proteção dos dados armazenados e transmitidos pelo produto	Os dados existentes no produto e que são transmitidos por ele devem estar protegidos.	6
	Atualizações de software certificadas	Devem ser garantidas que as atualizações de *software* provem de entidades confiáveis.	10
	Instalação de novas aplicações de software certificadas	Devem ser garantidos que os dispositivos permitidos ao acesso no produto devem estar certificados para estes poderem efetuar ações nele, como a instalação de software.	10
Responsabilidade	Comprimento das legislações e regulamentos no tratamento dos dados	Devem ser garantidas que as legislações relativas ao produto estão a ser compridas e responsabilizadas.	1

Figura 9: Perfil de Segurança do caso de uso

apenas deve orientar da melhor forma possível o utilizador na sua identificação. O resultado desta secção está presente em cada secção de cada fase da *framework*.

4.3.1.5 *Definição dos Níveis de segurança*

Para a definição dos níveis de segurança, a *framework* oferece um método para determinar o nível de implementação que o requisito de segurança deve apresentar.

Tabela 3: Perfil de Segurança - Média dos níveis de segurança por categoria

Categoria de Segurança	Nível de segurança	Média
Confidencialidade, Integridade, Disponibilidade	10	6
	1	
Integridade, Disponibilidade, Responsabilidade	4	5
	6	
Integridade, Responsabilidade	6	8
	6	
Confidencialidade, Integridade, Responsabilidade	6	9
	10	
	10	
Responsabilidade	1	1

Isto é realizado através do uso dos níveis definidos no Perfil de segurança, o que mostra a utilidade do Perfil nesta fase de planeamento. Ao juntar o tipo de implementação esperado para o requisito com o nível definido nos objetivos de segurança, o utilizador consegue através desta *framework* encontrar a medida ou os métodos necessários para cumprir cada requisito. Aqui a *framework* consegue oferecer ao utilizador uma lista de medidas, controlos e métodos de cibersegurança, incluída nesta o local onde o utilizador pode encontrar o documento fonte para cada medida, oferecendo assim orientação ao utilizador de como ele pode utilizar estas no seu produto. Tal como na secção anterior, o resultado desta secção está presente em cada secção de cada fase da *framework*.

4.3.1.6 *Planeamento de Atividades*

Será a partir deste ponto que as atividades de planeamento estarão concluídas, restando apenas o planeamento de atividades para cada fase. Estas atividades serão essencialmente formações ou treinos para melhorar os conceitos e regras de cibersegurança durante cada fase da *framework*. As medidas oferecidas pela *framework* não deverão ser um substituto para documentos *standard*, sendo que o objetivo desta *framework* é oferecer orientação suficiente ao utilizador para este saber o que fazer e onde pode encontrar o que precisa. Desta forma, a presente *framework* deve conseguir indicar uma listagem de medidas úteis e onde pode ser encontrada a sua documentação detalhada.

4.3.2 *Implementação*

Para cada fase posterior ao planeamento, a *framework* apresentará uma lista de medidas referente a essa fase. Na fase de implementação, alguns dos requisitos definidos são:

- **Proteção do produto contra intrusões maliciosas**:
  - Utilização de um *Intrusion Detection System* (*IDS*): Este sistema serve de detetor de intrusões e anomalias no *ECU*.
- **Proteção contra ações não autorizadas ou por engano**:
  - Definição de *Roles* de sistema: A aplicação de *roles* com diferentes direitos e permissões de acesso ao sistema serve para que cada elemento da equipa tenha apenas as permissões necessárias para desempenhar as suas funções.
  - Princípio do *Least Privilege*: este princípio serve para que o privilégio padrão seja sempre o mais baixo possível para evitar ações descontroladas no sistema.

A partir da *framework* o utilizador escolhe a medida mais adequada ao seu nível de segurança identificado. Neste cenário, as medidas utilizadas nesta fase poderão ser:

- **Utilização de um *Intrusion Detection System* (*IDS*)**: Sistema *IDS* baseado em dispositivos de *IoT* (*ENISA - Good practices for security of IoT*). Este *IDS* deverá ser uma implementação ajustada às capacidades do *hardware* do produto, e seguindo os princípios de cibersegurança e do funcionamento de um *IDS* usado no *IoT*.
- **Definição de *Roles* de sistema**: *Roles* para a segurança da informação e responsabilidades (*ISO 27002*). Devem ser planeadas e definidas as diferentes *roles* de cada membro no projeto, para depois serem devidamente criados e atribuídos os *roles* apropriados para cada membro, no sistema do produto durante o seu desenvolvimento.

- **Principio de *Least Privilege***: Implementação de *Least Privilege* no sistema (*ISO 27002*). Deve ser planeado a implementação dos utilizadores de sistema para que estes apresentem sempre os privilégios mais baixos o possível, sendo que para executar uma ação de maior privilégio no sistema, aqui deverá ser inserido a *password* do utilizador no caso de este apresentar as permissões para essa ação, caso contrário não será possível de forma nenhuma a execução da ação.

4.3.3 *Validação*

Já na fase de validação, existem apenas requisitos para alguns dos objetivos de cibersegurança. Razão esta porque nesta fase os requisitos usados na fase anterior continuam a ser aplicáveis nesta fase. No entanto, o que é realizado de diferente são as validações das medidas de cibersegurança implementadas durante o desenvolvimento do produto. Aqui, os requisitos serão apenas para o teste da implementação de cada requisito dos objectivos de cibersegurança.

Em geral, a grande maioria das medidas de validação serão testes de penetração, o que equivale a um conjunto de diferentes testes e técnicas para validar a implementação, mas noutros casos, será apenas necessário a utilização de apenas uma técnica (definido consoante o nível de segurança estabelecido):

- **Utilização de um *Intrusion Detection System* (*IDS*)**: Testes de *Sandboxing* (*ENISA - Good practices for security of IoT*)
- **Implementação de código seguro**: Testes unitários, *Fuzzing testing* (*ENISA - Good practices for security of IoT*)
- **Utilização de *Roles* no sistema**: Testes de penetração
- **Principio de *Least Privilege***: Testes de penetração
- **Autenticação dos dados transmitidos**: Testes de penetração
- **Encriptação dos dados transmitidos e armazenados**: Testes de penetração

- **Gestão de certificados e assinaturas digitais**: *Fuzzing testing* (*ENISA - Good practices for security of IoT*)

4.3.4 *Lançamento*

Com a fase de Lançamento, a *framework* apenas orienta um utilizador a preparar-se para a defesa da cibersegurança aplicada ao produto perante uma entidade certificadora. Neste aspeto a presente *framework* orienta o utilizador a seguir documentos *standard* como a *ISO 15408/Common Criteria*. Com isto, o resultado da presente fase é o trabalho, em termos de documentação, já realizado nas fases anteriores a esta.

4.3.5 *Suporte*

Tal como na fase de implementação, a fase de suporte apresenta requisitos de segurança como:

- ***Software* do produto sem falhas técnicas**:
  - Manutenção de *software* do produto: Devem ser realizadas manutenções ao *software* para analisar o funcionamento do produto e avaliar se este está dentro das condições esperadas.
- ***Hardware* do produto sem falhas técnicas**:
  - Manutenção de *hardware* do produto: Devem ser realizadas manutenções ao *hardware* para analisar o funcionamento do produto, e avaliar se este está dentro das condições esperadas.

Sendo que as medidas oferecidas para estes requisitos são:

- **Manutenção de *software* do produto**: Revisão técnica das aplicações *software*, depois de alterações na plataforma (*ISO 27002*). A partir da aplicação deste controlo, devem ser definidos todos os processos que devem ser cobertos para proceder à manutenção do *software*. Aqui deve ser revisto o funcionamento e a integridade dos processos do sistema, para desta forma garantir que nada foi comprometido desde a última manutenção, ou devido a uma atualização de *software* do produto ou de outra componente do automóvel. Para a manutenção do *software*, deve ser previamente preparado o produto para garantir que neste não existem dados sensíveis. Isto serve como medida de prevenção na conformidade dos dados durante as manutenções.
- **Manutenção de *hardware* do produto**: Manutenção de equipamento (*ISO 27002*). Com este controlo pretende-se executar uma manutenção para garantir a integridade e disponibilidade do produto. Desta forma, é necessário definir os intervalos de tempo necessários para efetuar as manutenções do produto, definir quem está apto para executar essas manutenções, e devem ser estabelecidos os procedimentos de como fazer a manutenção. Para a manutenção do *hardware*, deve ser previamente preparado o produto para garantir que neste não existem dados sensíveis. Isto serve como medida de prevenção na conformidade dos dados durante as manutenções.

4.3.6 *Descontinuação*

Na fase de descontinuação apenas são definidos requisitos para alguns dos objectivos. Sendo que nem todos os objetivos e requisitos de segurança se aplicam a todas as fases, os requisitos presentes nesta fase são:

- **Controlo de acesso ao sistema**:
  - Ligações e sessões terminadas no sistema: Deve ser verificado que qualquer sessão ou ligação a serviços externos no sistema está devidamente terminada e fechada.
- **Instalação de novas aplicações de *software* certificadas**:

  - Certificados e licenças removidas do sistema descontinuado: Todos os certificados digitais existentes no sistema devem ser transferidos ou apagados de forma segura para evitar o comprometimento de outros produtos ainda em circulação.

Neste cenário, as medidas listadas que poderão ser usadas para estes requisitos serão:

- **Ligações e sessões terminadas no sistema**: Equipamento de utilizador não atendido (*ISO 27002*). Aqui devem ser estabelecidos procedimentos para os equipamentos com sessões abertas e sem o utilizador por perto. Estes procedimentos devem definir as ações a tomar quando o equipamento não tem o utilizador responsável para as proteger, isto envolve terminar qualquer sessão de utilizador ou ligação a serviços ainda ativos. Esta medida serve principalmente para o estado transitório entre as fases de suporte e de descontinuação do produto.
- **Certificados e licenças removidas do sistema descontinuado**: Disposição segura ou reutilização de equipamento (*ISO 27002*). Devem ser definidos procedimentos para identificar os tipos de dados existentes no produto, avaliar quais dados devem ser transferidos e quais devem ser apagados, e como devem ser realizados os procedimentos de transferência e remoção desses dados de forma segura. Deve também ser identificado o tipo de sistema no qual os dados residem para permitir identificar o método apropriado para remover ou transferir os dados desse sistema.

4.4 ANÁLISE DE RESULTADOS

O resultado da primeira fase é uma preparação para o estabelecimento da cibersegurança no produto. Esta é uma preparação focada na identificação das medidas de segurança e atividades necessárias para cada fase no ciclo de vida do produto.

Desta forma, o resultado final desta fase será uma listagem completa de todos os requisitos e níveis de segurança para serem aplicados nas fases seguintes.

Comparando com a *framework* apresentada no trabalho de Glas et al., 2015, a presente apresenta resultados diferentes visto que estas também têm objetivos diferentes, a presente pretende ajudar o utilizador a analisar e encontrar as medidas que mais precisa para o seu produto, e a *framework* de Glas et al., 2015 pretende criar novas formas de analisar e implementar a cibersegurança no setor automóvel. A presente *framework* segue algumas das ideias introduzidas no trabalho de Glas et al., como é o caso do Perfil de Segurança, mas escolhendo uma forma mais simples de obter esse perfil. Isto é visível pelo resultado final do perfil de segurança onde os objetivos de segurança estão identificados e organizados consoante o tipo e nível de cibersegurança avaliado. Isto não significa que uma *framework* seja melhor que a outra, simplesmente que existem formas diferentes para chegar ao mesmo objetivo.

No que toca à análise de risco, o resultado do proposto aqui não deverá ser muito diferente da utilização normal da *ISO 27005*. Este processo não é possível comparar com o da *framework* de Glas et al., 2015 pois este não explora este processo no seu trabalho. O resultado principal desta análise é a identificação dos objetivos de segurança através dos riscos analisados. Assim, a presente *framework* não tem o foco na apresentação de um novo processo detalhado para a análise de risco, mas a apresentação de metodologias já existentes para que sejam utilizados no processo da análise de riscos de um produto automóvel. A utilização do *TARA* juntamente com o *ISO 27005* vem por este fim como uma opção que poderá ser apresentada nos processos de análise de risco identificados elegíveis para a presente *framework*.

Como já foi dito, o método de criação do Perfil de Segurança é bastante simplificado, mas o resultado final é útil ao ser utilizado como uma referência importante na definição da cibersegurança exigida para o produto. Isto permite oferecer como resultado uma lista organizada por categorias e prioridades dos objetivos de segurança do produto. Este tipo de perfil serve tanto para indicar a cibersegurança alvo durante a implementação como também para mostrar qual a cibersegurança existente no produto depois do seu lançamento no mercado. O Perfil de Segurança serve portanto como conjunto de informação organizada, a qual pode ser utilizada como auxílio para o planeamento do produto, e para representar qual a cibersegurança aplicada no mesmo. Neste aspeto, o resultado do Perfil de Segurança apresentado no trabalho de Glas et al., 2015 é igual ao da presente *framework* sendo que a presente pretende seguir os mesmos princípios razões demonstradas no trabalho destes autores. Razão esta que é a harmonização da *framework* de cibersegurança na industria automóvel.

A definição dos requisitos e níveis de segurança permite a identificação das possíveis medidas que o utilizador pode usar no produto. O resultado aqui será portanto uma listagem de medidas indicadas para os requisitos e níveis de segurança para cada fase do produto, mais concretamente para as fases de desenvolvimento (implementação), suporte (pós-lançamento) e descontinuação. Aqui a diferença principal com a proposta por Glas et al., 2015 é na apresentação de opções para as medidas que podem ser escolhidas por cada requisito e nível de segurança, que no caso do trabalho dos autores é pretendido que sejam propostas novas abordagens para a cibersegurança nos automóveis. No entanto, a presente *framework* pretende oferecer ajuda no estabelecimento de cibersegurança através da apresentação completa de todas as possibilidades existentes no mercado. Esta é a principal diferença entre as duas *frameworks*. Através deste formato é possível manter esta ferramenta atualizada ao adicionar novas medidas que possam surgir ao longo do tempo sem causar grande impacto na própria *framework*.

A fase de validação irá apresentar um resultado parecido às outras fases mas com destaque para as metodologias de validação da cibersegurança. Este é um ponto que a *framework* estende ao também apresentar uma lista para os tipos de validações que podem ser realizadas à cibersegurança num produto alvo. Um exemplo de uma validação são os testes de penetração.

Para a fase de lançamento o resultado será uma preparação para a certificação da cibersegurança do produto. Neste caso de uso, a preparação inicia-se logo na fase de planeamento quando os requisitos são definidos e documentados posteriormente para esta fase. Isto possibilita um trabalho de preparação distribuído, evitando assim concentrar todo o esforço para a fase de certificação em si. Comparando com o trabalho de Glas et al., 2015, os objetivos para esta fase são diferentes. Na presente *framework* o objetivo é na preparação para a certificação do produto, tendo como referencias as certificações já existentes. E na *framework* de Glas et al., o objetivo é a proposta de uma nova metodologia de certificação da cibersegurança para o setor automóvel. O resultado da utilização da presente *framework* será a preparação e documentação do trabalho implementado para a cibersegurança para ser apresentado, avaliado e certificado por uma metodologia já existente.

Em síntese, a *framework* proporciona uma ajuda na obtenção da cibersegurança necessária para o produto, através das atividades iniciais de definição de critérios, análise de risco e criação do Perfil de Segurança. E com os requisitos e níveis de segurança a *framework* consegue ajudar o utilizador a escolher as medidas mais adequadas às suas necessidades para o produto apresentando uma listagem detalhada das opções existentes no mercado. E no final da utilização da *framework*, o utilizador

consegue obter uma identificação completa de todas as medidas necessárias para cada fase no ciclo de vida do seu produto. Tal é visível na listagem dos requisitos e medidas de cibersegurança obtidas pela aplicação da *framework* em cada fase, permitindo facilmente ao utilizador determinar quais os passos seguintes que deve tomar para aplicar a cibersegurança no seu produto. Como tal, o resultado final da *framework* é a apresentação de um conjunto de medidas para a cibersegurança do produto nas suas várias fases, testes para a validação da cibersegurança e uma preparação para a certificação da cibersegurança. Ao contrário da *framework* proposta por Glas et al., 2015, o foco da presente não é a descrição de um novo processo ou medida para a cibersegurança mas a apresentação daquilo que já existe e pode ser utilizado na cibersegurança de um produto automóvel.

5

CONCLUSÃO E TRABALHO FUTURO

O setor automóvel é uma área cuja utilização e desenvolvimento da cibersegurança ainda é recente. Com a modernização gradual dos automóveis através da utilização de novas tecnologias digitais, a cibersegurança é um assunto que deve ser tratado com a extrema importância. O presente trabalho vem desta forma tentar dar um contributo para a cibersegurança dos automóveis, tentando aqui propor meios e formas já existentes em outras industrias para serem reutilizadas neste setor.

O presente trabalho tinha como um dos objetivos a análise de *standards* do setor automóvel, por forma a desenvolver ideias conjuntas com outros *standards* da cibersegurança já existentes noutros setores. Infelizmente este objetivo não foi concretizado por falta de acesso a *standards* ligados ao setor automóvel. Posto isto de parte, o trabalho focou-se na apresentação de ideias para a cibersegurança, utilizado para isto apenas os *standards* de cibersegurança e outros documentos contendo informações de boas práticas na cibersegurança, tanto em veículos inteligentes como em dispositivos IoT.

Com o presente trabalho foi possível chegar à conclusão que ainda existe a necessidade de uma harmonização dos conceitos de cibersegurança no setor automóvel. Isto deve-se principalmente à falta de fontes concretas para estabelecer a cibersegurança nos produtos automóveis o que leva muitas das empresas automóveis, e empresas fornecedoras das componentes, a estabelecerem diferentes processos para aplicar a cibersegurança. Esta dispersão causa dificuldades na aplicação de medidas de cibersegurança já utilizadas noutros mercados. A criação de uma *framework* poderá ser uma boa iniciativa no encontro da harmonização, mas existe uma falta de conhecimento sobre os processos mais elaborados da industria automóvel neste trabalho. Processos esses que são importantes para perceber os diferentes aspetos que devem ser contabilizados na aplicação eficiente da cibersegurança. É possível aplicar muitos dos controlos e medidas de *standards* já existentes para melhorar a cibersegurança dos automóveis, mas apenas estes não são suficientes porque tal como é composto cada industria, cada uma tem particularidades diferentes que devem ser contabilizadas. E desta forma, é necessária a definição de medidas muito especificas para cada uma dos setores ou industrias. Felizmente existe um novo

standard, *ISO/SAE 21434*, que está em fase de conclusão, que poderá ser o que esta industria necessita para concretizar uma firme cibersegurança e bem harmonizada.

É de destacar também que, com este trabalho foi possível concluir que muitos dos conceitos de segurança do *IoT* estão bastante interligados com os conceitos dos automóveis inteligentes. Como analisado nos documentos da *Enisa*, existem bastantes conceitos e processos no *IoT* que pretendem resolver os mesmos problemas de cibersegurança que as componentes dos automóveis enfrentam. Existem vários aspetos, como a segurança de diferentes tipos de dados, que os produtos *IoT* enfrentam e os produtos automóveis também estão a começar a sentir. Outro aspeto em comum são os diferentes tipo de produtos que comunicam entre si, como é o caso dos diferentes *ECUs* existentes num automóvel. Isto tudo ajuda a indicar que muitos dos conhecimentos do *IoT* podem ser aplicados na industria automóvel.

Para trabalho futuro, o presente trabalho requer uma análise dos *standards* automóveis para formular melhor a *framework* proposta. Isto é algo que deverá incluir a análise detalhada de *standards* como a *ISO 26262*, *SAE J3061* e *ISA99/IEC 62443*. Também deverão ser explorados mais documentos do mundo do *IoT* como fontes de ideais para serem utilizadas nesta *framework*. Adicionalmente, deverá ser também importante o melhoramento da descrição das medidas, processos e métodos apresentados no presente trabalho. Também seria importante efetuar uma melhor exploração do impacto das redes *VANET* na cibersegurança dos dados dentro do automóvel. Por fim, será importante a avaliação do novo *standard* que está para ser lançando, a *ISO/SAE 21434*. A análise deste *standard* será importante para poder avaliar se o que nele está a ser apresentado é ou não suficiente para a cibersegurança automóvel, e através disto apresentar melhorias no que poderá estar em falta ou incompleto no *standard*.

BIBLIOGRAFIA

AUTOSAR (2019). *AUTOSAR - Layered Software Architecture*. Website. https://www.autosar.org/fileadmin/user_upload/standards/classic/19-11/AUTOSAR_EXP_LayeredSoftwareArchitecture.pdf.

Beckers, Kristian, Jürgen Dürrwang e Dominik Holling (2016). «Standard Compliant Hazard and Threat Analysis for the Automotive Domain». Em: *MDPI*.

Eckermann, Erik (2001). *World History of the Automobile*. Society of Automotive Engineers.

Glas, B., J. Gramm e P. Vembar (jan. de 2015). «Towards an information security framework for the automotive domain». Em: *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, pp. 109–124.

Koscher, Karl et al. (2010). «Experimental Security Analysis of a Modern Automobile». Em: *2010 IEEE Symposium on Security and Privacy*.

Malagund, Keertikumar, Shubham Mahalank e Rajeshwari Banakar (out. de 2015). «Evolution of IoT in smart vehicles: An overview». Em: pp. 804–809. DOI: 10.1109/ICGCIoT.2015.7380573.

Maple, Carsten et al. (2019). «A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis». Em: *MDPI*.

Matulka, Rebecca (2014). *Timeline: History of the Electric Car*. Website. https://www.energy.gov/articles/history-electric-car.

News, The Hacker (2011). *Honda hacked - 283,000 car owners personal data Leaked*. Website. https://thehackernews.com/2011/05/honda-hacked-283000-car-owners-personal.html.

OMG, Object Management Group (2014). *MDA® - The Architecture of Choice for a Changing World*. Website. https://www.omg.org/mda/.

Poulsen, Kevin (2010). *Hacker Disables More Than 100 Cars Remotely*. Website. https://www.wired.com/2010/03/hacker-bricks-cars/.

Rehman, Sabih et al. (jan. de 2013). «Vehicular ad-Hoc networks (VANETs)—An overview and challenges». Em: *Journal of Wireless Networking and Communications* 3, pp. 29–38. DOI: 10.5923/j.jwnc.20130303.02.

Schmittner, Christoph, Gerhard Griessnig e Zhendong Ma (jan. de 2018). «Status of the Development of ISO/SAE 21434: 25th European Conference, EuroSPI

2018, Bilbao, Spain, September 5-7, 2018, Proceedings». Em: pp. 504–513. ISBN: 978-3-319-97924-3. DOI: 10.1007/978-3-319-97925-0_43.

Schmittner, Christoph, Zhendong Ma et al. (set. de 2016). «Using SAE J3061 for Automotive Security Requirement Engineering». Em: vol. 9923, pp. 157–170. ISBN: 978-3-319-45479-5. DOI: 10.1007/978-3-319-45480-1_13.

Sommer, Christoph e Falko Dressler (2014). *Vehicular Networking*. Cambridge University Press. DOI: 10.1017/CBO9781107110649.

Sommer, Florian, Jürgen Dürrwang e Reiner Kriesten (2019). «Survey and Classification of Automotive Security Attacks». Em: *MDPI*.

Staron, Miroslaw (jun. de 2017). *Automotive Software Architectures*. DOI: 10.1007/978-3-319-58610-6.

Symantec (2016). *White Paper - Building Comprehensive Security Into Cars*. Website. https://www.symantec.com/content/dam/symantec/docs/white-papers/building-comprehensive-security-into-cars-en.pdf.

Tesla (2019). *Carros elétricos, painéis solares e armazenamento de energia limpa | Tesla*. Website. https://www.tesla.com/pt_pt/.

Upstream (2019a). *Rapid growth in cyber-attacks on smart mobility 2010-2019*. Website. https://www.upstream.auto/research/automotive-cybersecurity/.

— (2019b). *Upstream AutoThreat - Automotive Cyber Threat Intelligence*. Website. https://www.upstream.auto/autothreat-intelligence/.

— (2019c). *Upstream C4 - Centralized Connected Car Cybersecurity*. Website. https://www.upstream.auto/upstream-c4-platform/.

— (2019d). *Upstream security global automative cybersecurity report 2019*. Website. https://industrytoday.com/wp-content/uploads/2018/12/Upstream-Security-Global-Automotive-Cybersecurity-Report-2019.pdf.

Uptane (2019). *Uptane - Securing Software Updates for Automobiles*. Website. https://uptane.github.io/.

Wu, Zhihong et al. (2019). «Research on In-Vehicle Key Management System under Upcoming Vehicle Network Architecture». Em: *MDPI*.

APÊNDICES

APÊNDICE A

A.1 ESCALAS E MÉTODOS CLASSIFICAÇÃO DE RISCO

CRITÉRIO	CLASSIFICAÇÃO	DESCRIÇÃO	VALOR
Vulnerabilidade (V)	Muito Elevada	Exposição elevada; sem estratégias de resposta	4
	Elevada	Exposição elevada; existe uma estratégia de resposta parcial	3
	Média	Exposição elevada/moderada; existe uma estratégia de resposta	2
	Baixa	Exposição baixo; com ou sem estratégias de resposta	1
Duração (D)	Longa	Mais de uma semana	3
	Intermédia	Até uma semana	2
	Curta	Até um dia	1
Aviso prévio (AP)	Não	Não é possível antecipar a ameaça, logo não será possível ser previamente informado de um eventual ataque	2
	Sim	É possível antecipar a ameaça, logo será possível ser previamente informado de um eventual ataque	1
Valor do Impacto (V+D+AP)	Elevado [8;9]	A ocorrência desta ameaça poderá constituir uma anomalia grave na operação da empresa comprometendo de forma significativa a sua operação global	3
	Médio [6;7]	A ocorrência desta ameaça poderá constituir uma anomalia localizada, sendo o impacto restrito a um grupo de processos/recursos críticos	2
	Baixo [3;5]	A ocorrência desta ameaça representar anomalias pontuais na empresa	1
Probabilidade de ocorrência	Elevada	Existe conhecimento de mais do que uma ocorrência anual	3
	Média	Existe conhecimento de uma ocorrência anual	2
	Baixa	Não existe conhecimento de ocorrências.	1
Controlos de Mitigação	Eficiente	Todas ou quase todas as estratégias de controlo encontram-se implementadas. Poucas oportunidades de melhoria.	3
	Aceitável	Algumas estratégias de mitigação encontram-se implementadas. Algumas oportunidades de melhoria.	2
	A melhorar	Inexistência/ poucas estratégias de mitigação implementadas. Oportunidades de melhoria substanciais.	1

Figura 10: Escala para a avaliação de risco

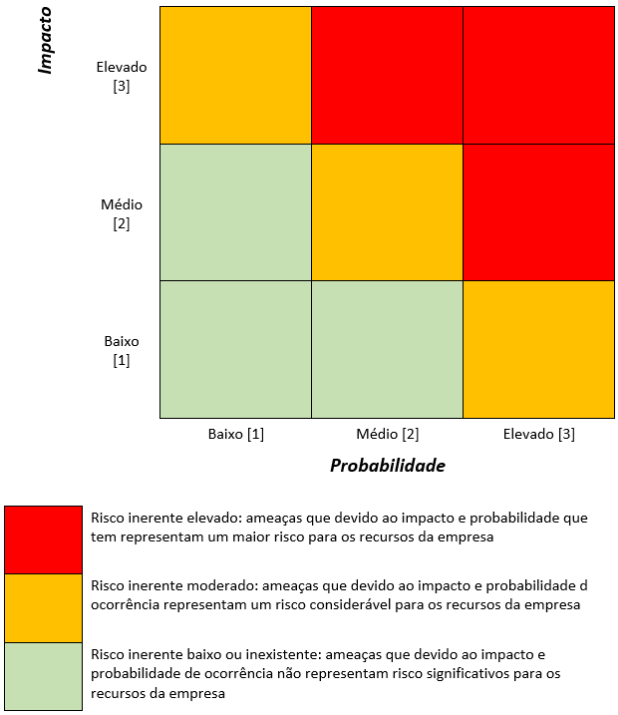


Figura 11: Classificação do risco inerente

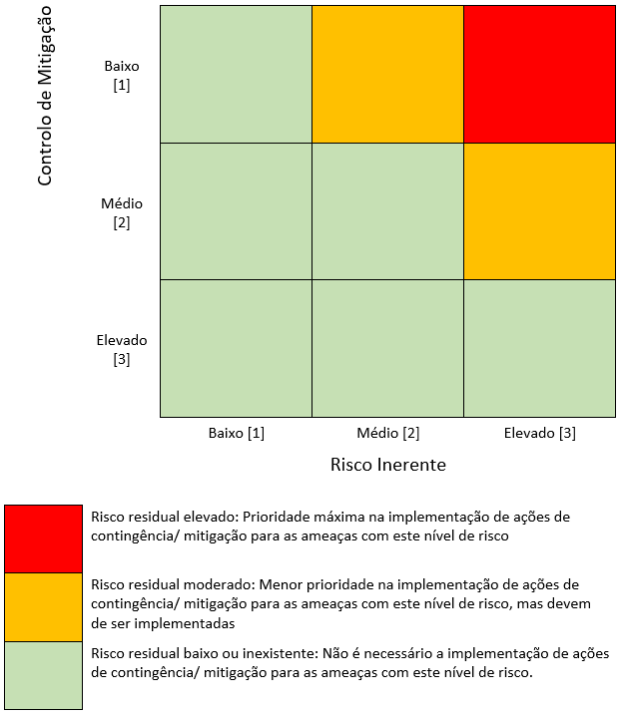


Figura 12: Classificação do risco residual

B

APÊNDICE B

B.1 AVALIAÇÃO DO RISCO - CASO DE USO

Ameaça 1	*Malwares*		
Impacto Resultante	Impacto médio. A ocorrência pode representar uma anomalia localizada na organização. Uma fonte desta ameaça serão os dispositivos pessoais ligados à rede durante o desenvolvimento do produto.	Vulnerabilidade	3
		Aviso prévio	2
		Duration	2
		Valor do Impacto(V+E+D)	7
			Médio
Probabilidade de Ocorrência	Devido ao uso da internet e dispositivos conectados à rede, a probabilidade de ocorrência é elevada.	Probabilidade de Ocorrência	3
			Elevado
Risco Inerente			Elevado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3
			Eficiente
Risco Residual			Baixo

Ameaça 2	Erro no uso		
Impacto Resultante	Impacto elevado. A má utilização dos equipamentos / *software* , poderá implicar o comprometimento do sistema ou perda total /parcial dos ativos.	Vulnerabilidade	3
		Aviso prévio	2
		Duração	3
		Valor do Impacto(V+E+D)	8
			Elevado
Probabilidade de Ocorrência	A probabilidade de um erro acontecer na utilização dos ativos é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Elevado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será moderado.	Valor dos controlos	2
			Aceitável
Risco Residual			Moderado

Ameaça 3	Falhas técnicas de *software*		
Impacto Resultante	Impacto médio. Algum do ***software*** utilizado na empresa é feito à medida, pelo que podem existir ***bugs*** no mesmo, provocando mau funcionamento. Isto poderá afetar a prestação dos serviços ou até a perda de dados parcial ou total	**Vulnerabilidade**	**3**
		Aviso prévio	**2**
		Duração	**2**
		Valor do Impacto(V+E+D)	**7**
			Médio
Probabilidade de Ocorrência	A probabilidade de um ***bug*** ou congestionamento no sistema é elevado. Devido à falta de testes efetuados em ***software*** à medida.	**Probabilidade de Ocorrência**	**3**
			Elevado
Risco Inerente			Elevado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será moderado.	**Valor dos controlos**	**2**
			Aceitável
Risco Residual			Moderado

Ameaça 4	Comprometimento da informação		
Impacto Resultante	Impacto elevado. Poderá ocorrer na empresa ou no grupo. Poderá existir perda de credibilidade da empresa e terceiros. Poderá ter impacto negativo no negócio.	**Vulnerabilidade**	**3**
		Aviso prévio	**2**
		Duração	**3**
		Valor do Impacto(V+E+D)	**8**
			Elevado
Probabilidade de Ocorrência	A probabilidade de comprometimento é baixa.	**Probabilidade de Ocorrência**	**1**
			Baixo
Risco Inerente			Moderado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	**Valor dos controlos**	**3**
			Eficiente
Risco Residual			Baixo

Ameaça 5	Abuso de direitos		
Impacto Resultante	Impacto médio. Os direitos podem estar mal distribuidos pelos vários perfis levando a que se tenham mais previlégios do que os necessários para exercer o cargo. Também poderá ocorrer abuso de direitos devido a más intenções de um ator, o que poderá implicar o comprometimento do sistema ou perda total /parcial dos ativos.	Vulnerabilidade	2
		Aviso prévio	2
		Duração	3
		Valor do Impacto(V+E+D)	7
			Médio
Probabilidade de Ocorrência	A probabilidade de ocorrer o abuso de direitos é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Moderado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3
			Eficiente
Risco Residual			Baixo

Ameaça 6	Ações não autorizadas		
Impacto Resultante	Impacto médio. As ações dependerão da intenção do ator, mas poderá implicar o comprometimento do sistema ou perda total /parcial dos ativos.	Vulnerabilidade	3
		Aviso prévio	2
		Duração	2
		Valor do Impacto(V+E+D)	7
			Médio
Probabilidade de Ocorrência	A probabilidade de uma ação não autorizada acontecer é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Moderado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3
			Eficiente
Risco Residual			Baixo

Ameaça 7	*Hacker* ou *crackers*		
Impacto Resultante	Impacto elevado. Poderá existir destruição ou roubo de informação. Poderá existir negação de serviço, entre outros, o que pode comprometer o normal funcionamento da organização.	Vulnerabilidade	3
		Aviso prévio	2
		Duração	3
		Valor do Impacto(V+E+D)	8
			Elevado
Probabilidade de Ocorrência	A probabilidade de um indivíduo ou organização querer prejudicar a empresa é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Moderado
Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	2
			Aceitável
Risco Residual			Baixo

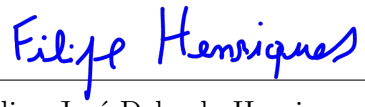
Ameaça 8	Falhas técnicas de *hardware*		
Impacto Resultante	Impacto médio. Algum do *hardware* poderá deixar de funcionar corretamente, provocando mau funcionamento. Isto poderá afetar a prestação dos serviços ou até perda de dados parcial ou total.	Vulnerabilidade	3
		Aviso prévio	2
		Duração	2
		Valor do Impacto(V+E+D)	7
			Médio
Probabilidade de Ocorrência	A probabilidade de um disco rígido ou equipamento falhar é reduzida, pois estes dispositivos são extensivamente testados pelos fabricantes.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo
Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	2
			Aceitável
Risco Residual			Baixo

Ameaça 9	Coimas por incumprimento de legislação e regulamentos		
Impacto Resultante	Impacto baixo. Poderá existir perda de credibilidade da empresa no caso de uma coima ser aplicada e esta ser notificada aos *media* .	Vulnerabilidade	1
		Aviso prévio	1
		Duração	3
		Valor do Impacto(V+E+D)	5
			Baixo
Probabilidade de Ocorrência	A probabilidade de uma autoridade de controlo / fiscalizadora aplicar uma coima é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo
Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3
			Efeciente
Risco Residual			Baixo

DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado nesta dissertação, com o título *"Framework de Cibersegurança da Informação no Setor Automóvel"*, é original e foi realizado por Filipe José Delgado Henriques (2180066) sob orientação de Professor Doutor Nuno Alexandre Ribeiro Costa (nuno.costa@ipleiria.pt).

Leiria, Dezembro de 2020



Filipe José Delgado Henriques