Gestão de Sistemas e Computação

Trabalho Final de Licenciatura

Desenvolvimento de Front-End para Avaliação da Cibersegurança dos Industrial Control Systems

Pedro Duque

20162052

Professor Doutor Alexandre Barão

Barcarena

Novembro de 2019

Universidade Atlântica

Gestão de Sistemas e Computação

Trabalho Final de Licenciatura

Desenvolvimento de Front-End para Avaliação da Cibersegurança dos Industrial Control Systems

Pedro Duque

20162052

Professor Doutor Alexandre Barão

Barcarena

Novembro de 2019

O autor é o único responsável pelas

ideias expressas neste trabalho.

"The real-world implications of Stuxnet are beyond any threat we have seen in the past. Despite the exciting challenge in reverse engineering Stuxnet and understanding its purpose, Stuxnet is the type of threat we hope to never see again."

Symantec - W32.Stuxnet Dossier

RESUMO

Os Industrial Control Systems (ICS) são essenciais para as sociedades atuais e suas infraestruturas. É por isso crucial garantir a sua Cibersegurança, necessitando que sejam implementadas medidas específicas adaptadas à realidade operacional de cada organização. Para facilitar o trabalho dos técnicos de Cibersegurança e dos responsáveis dos diversos ICS, foi criado um protótipo aplicacional, intitulado de “Avaliação da Cibersegurança dos Industrial Control Systems”.

Neste protótipo, os utilizadores têm acesso à lista completa de medidas a tomar para aumentar a segurança destes sistemas, estando estas divididas por secções. Através de um sistema simples de input de dados, estes têm acesso, em tempo real, à visualização gráfica da percentagem das medidas implementadas. O protótipo foi criado tendo por base HTML com PHP e MySQL e estando disponível online em http://questionarioics.epizy.com/.

De modo a proceder à validação do protótipo aplicacional, foi pedido que especialistas da área da Informática e dos ICS que o testassem, tendo sido depois integradas as suas conclusões e considerações neste trabalho.

PALAVRAS CHAVE: Sistemas de Controlo Industrial, Sistemas de Supervisão e Aquisição de Dados, Cibersegurança, Segurança de Redes, Stuxnet, Interface Homem-Máquina e Plataforma Online.

ABSTRACT

Industrial Control Systems (ICS) are essential for today's societies and their infrastructures. Therefore, it's crucial to ensure its cybersecurity, requiring specific measures tailored to each organization operations. To facilitate the work of cybersecurity technicians and the heads of the various ICS, an application prototype was created, entitled "Avaliação da Cibersegurança dos Industrial Control Systems".

In this prototype, users have access to the complete list of tasks, divided into sections, to increase the security of these systems. Through a simple data input system, they have real-time access to the graphical display of the percentage of measures implemented. The prototype was created based on HTML with PHP and MySQL and is available online at http://questionarioics.epizy.com/.

To validate the application prototype, it was tested by specialists in the field of Informatics and ICS and their conclusions and considerations were integrated in this work.

KEYWORDS: Industrial Control Systems, Data Acquisition and Supervision Systems, Cybersecurity, Network Security, Stuxnet, Human Machine Interface and Online Platform.

ABREVIATURAS E SIGLAS

AAA	Authentication, Authorization and Accounting
CCTV	Closed-circuit television
CIA	Central Intelligence Agency
CPWE	Converged Plantwide Ethernet
CSS	Cascading Style Sheets
DCS	Distributed Control System
DS	Distributed Systems
DMZ	Demilitarized Zone
HMI	Human Machine-Interface
HTML	HyperText Markup Language
ICS	Industrial Control Systems
IDS	Intrusion detection System
IoT	Internet Of Things (Internet das Coisas)
IPTV	Internet Protocol television
IT	Information technology
LAN	Local Area Network
MBAP	Modbus Application Protocol (Protocolo Aplicacional de Modbus)
NIST	National Institute of Standards and Technology
OSI	Open System Interconnection (Modelo OSI)
PHP	Hypertext Preprocessor
PLC	Programmable Logic Controller
RDMS	Relational Database Management System
RGPD	Regulamento Geral sobre a Proteção de Dados
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SQL	Structured Query Language

SSH	Secure Shell
USB	Universal Serial Bus
UTP	Twisted Pair Cabling
VLAN	Virtual Local Area Network
WAN	Wide Area Network

ÍNDICE

ÍNDICE DE FIGURAS

CAPÍTULO 1

INTRODUÇÃO

1.1. CONTEXTO

As sociedades atuais, conforme se conhecem, só são possíveis graças a uma presença constante de sistemas automatizados de controlo industrial que através de redes de sensores, atuadores, controladores, computadores e quilómetros de cabos e fibra ótica, controlam as suas infraestruturas essenciais, como por exemplo, as redes de energia, água, gás, telecomunicações, infraestruturas viárias e de transportes.

Embora vitais, a sua presença não é percecionada pela maioria dos seus habitantes no dia-a-dia, sendo que estes apenas utilizam os serviços e recursos disponibilizados por estes sistemas. A falha destes sistemas tem um impacto direto na vida das sociedades modernas, podendo o comprometimento de um “simples” componente destes sistemas, levar a consequências que não afetem apenas o serviço, mas também causem danos para além destes.

Para cada um destes sistemas funcionarem, é necessário que exista uma infraestrutura de supervisão e controlo dos mesmos, permitindo, por um lado, o controlo dos equipamentos e por outro, a sua monitorização. Estes sistemas designam-se: Industrial Control Systems (ICS).

Muitas vezes estes sistemas são também chamados de outros nomes, sendo o caso mais comum o de Supervisory Control And Data Acquisition (SCADA). No entanto, será mais correto considerar-se que estes são uma subdivisão dos ICS. Esta designação está muitas vezes associada ao ICS que se encontram espalhados por extensas áreas geográficas, normalmente associada a distribuição de água, energia ou gás. Todos os SCADA são ICS, contudo, nem todos os ICS são SCADA (Knapp e Langill 2015).

Para que estes sistemas funcionem como esperado, é necessário que funcionem sem falhas, sendo necessária a implementação de medidas que diminuam os erros, quer ocorram ou não por motivos acidentais. Desta forma, é necessário que existam protocolos de comunicação eficazes e seguros, interfaces adequadas, definição de valores threshold e redundâncias, que reduzam a probabilidade de ocorrer uma falha não intencional por parte do operador.

Além das falhas referidas no parágrafo anterior, existem também as falhas intencionais que obrigam a tomada de medidas adicionais, uma vez que os vetores que podem comprometer os sistemas são diferentes, podendo inclusivamente ser efetuados fora do local ou instalação onde estes se encontrem, aumentado assim a dificuldade de os proteger.

Conforme referido anteriormente, os ICS controlam diversos equipamentos, sendo para tal necessário não apenas o seu comando, mas também a análise dos dados recebidos destes e dos equipamentos auxiliares existentes (ex. sensores de temperatura, medidores de fluxo ou detetores de movimento). Desta forma, é necessário a interpretação das inúmeras variáveis geradas e recebidas em simultâneo, sendo praticamente impossível aos operadores dos sistemas fazer o acompanhamento de todas estas. Assim, a aposta tem sido na adoção de interface mais *user friendly*, permitindo, entre outras vantagens, melhorar a focagem e tornar mais ricos e completos os Interfaces Homem-Computador (HMI) (Hollifield, et al. 2008).

Embora que o controlo dos ICS tenha sido melhorado com a evolução dos HMI e dos próprios recursos disponíveis, estes problemas continuam a ser majorados se tratarem de *Distributed Systems* (DS), uma vez que se está a referir a um sistema de equipamentos e computadores independentes que se encontram ligados através de uma rede informática e que o utilizador acede através de uma interface única e coerente (Hayden, Assante e Conway 2014). Logo, ao estarem envolvidos diversos equipamentos dispersos por diferentes locais, é necessário que sejam encontradas soluções que garantam a sua integridade em toda a sua extensão.

Esta questão trás especial importância à forma de como todos estes equipamentos comunicam entre si. Para tal, desde o surgimento destes sistemas que é dada relevância à comunicações e aos protocolos utilizados, sendo que hoje em dia, a maioria dos ICS assenta em MODBUS através de Ethernet TCP/IP, uma vez que este é fiável, fácil de implementar e livre de royalties (Ackerman 2017).

1.2. FORMULAÇÃO DO PROBLEMA

Os ICS são sistemas vitais, devendo por esta razão estar disponíveis sempre que possível. Conforme a história demonstra, este são vulneráveis a falhas, tanto involuntária por quem os controla, como por ataques de partes internas e externas às organizações.

Atualmente existe carência de especialistas em segurança informática, nomeadamente em áreas tão concretas como os ICS, sendo por si só uma dificuldade de implementação das melhores soluções nas Organizações. Assim podemos formular o seguinte problema para este trabalho:

"Necessidade da criação de uma ferramenta online para auxiliar na implementação e avaliação do ICS de uma determinada organização"

1.3. MÉTODOS DE INVESTIGAÇÃO

Para a elaboração do enquadramento teórico, foi feita pesquisa bibliográfica sobre os diversos temas abordados e relevantes para esta tese. Para tal, o método de investigação considerado mais apropriado foi o *Action Research.*

Este baseia-se de forma geral, na investigação consecutiva de um determinado assunto, conseguindo-se a cada ciclo, o aumento do conhecimento do objeto de estudo. De acordo com Susman e Evered (Susman e Evered 1978), podemos considerar que esta metodologia baseia-se em 5 etapas ou fases sendo as definidas na **Figura 1**:

Diagnosing (Diagnóstico) – No início de cada ciclo deverão ser identificados dos problemas que estão na base da investigação, levando em consideração as suas causas e consequências. Deverá ser deduzida uma hipótese que será a base do trabalho da compreensão e desenvolvimento do problema;

Action Planning (Planeamento) – Através da criação de objetivos, devem ser criadas ações que permitiram desenvolver a resolução do problema e a concretização da questão. Assim, poderão ser utilizadas estratégias adaptadas à investigação em causa e à sua complexidade, através da definição de planos, metas, etapas ou indicadores;

Action Taking (Atuação) – Nesta fase, deverá decorrer a investigação, devendo para tal ser executado o definido no ponto anterior.

Evaluating (Avaliação) - Através da avaliação do definido na fase de planeamento, deve ser avaliada a investigação já efetuada, bem como a aplicabilidade e resultados das medidas implementadas. Em investigação, esta avaliação poderá ser quantitativa ou qualitativa, devendo ser adaptada a mais conveniente para cada objetivo.

Specifying Learning (Aprendizagem Específica) – Nesta fase deverá ser analisado o conhecimento adquirido durante a investigação, nomeadamente, através do cumprimento dos planos traçados e dos seus objetivos. Esta análise desencadeia as alterações necessárias para garantir a sua continuação. Deverão ser tomadas, medidas que corrijam eventuais desvios, bem como a identificação das causas destes, servindo de base para que no novo ciclo sejam, se necessário, adotadas novas abordagens à questão.

De acordo com enumerado anteriormente, este trabalho foi estruturado de forma a aplicar este método, sendo claramente incluídas as cinco fases descritas.

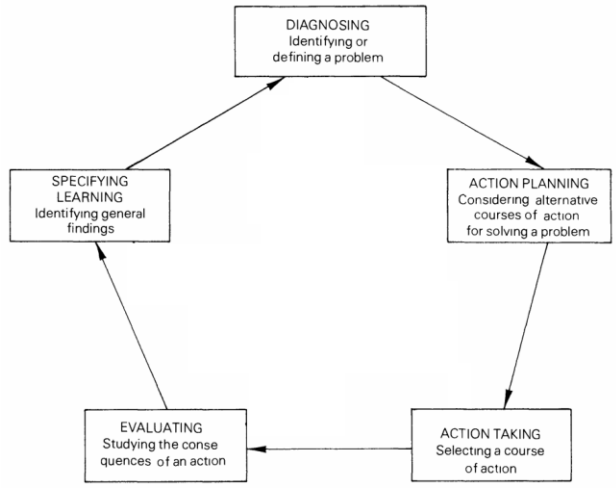


Figura 1 - Diagrama da Action Research
Processo cíclico da Action Research. Adaptado de Susan e Everd (Susman e Evered 1978).

1.4. OBJETIVOS

Com base na identificação do problema, define-se que será criada uma plataforma online onde os gestores dos ICS (especialistas ou não em segurança informática) poderão aceder a uma *check-list* e aplicá-la as suas organizações.

Através do preenchimento dos dados solicitados, deverá ser apresentado um resumo das diversas medidas, sendo não apenas guardados os dados para futura análise estatística, como também serem devolvidas sugestões de medidas a implementar para aumentar a performance de Cibersegurança da organização.

A finalidade deste trabalho não tem como base a análise dos resultados obtidos pelos acessos à plataforma, mas sim a criação da plataforma com base na investigação efetuada para a elaboração dos seus conteúdos e respetiva *check-list.*

Assim, definem-se os seguintes objetivos:

O1 - Identificar os principais fatores que contribuem para a ciber(in)segurança dos sistemas ICS;

O2 - Identificar boas práticas ao nível da Cibersegurança (física/lógica);

O3 - Definir a arquitetura do sistema visando a instanciação de um protótipo;

O4 - Criar uma ferramenta *web* para avaliação das questões de segurança de um ICS existente na organização;

1.5. ESTRUTURA DO DOCUMENTOS

Este documento está dividido em 6 capítulos, sendo cada um composto por diversos subcapítulos. O 1º capítulo é o da **Introdução**, onde é explicado quais as principais questões deste trabalho. Aqui são explicados os motivos que levaram à escolha do tema, bem como as questões relacionadas com a formulação dos objetivos e a metodologia de investigação utilizada.

O 2º capítulo do trabalho tem como nome **Enquadramento Teórico** e tem como função a explicação do que são os Industrial Control Systems, sendo descrito quais as suas características, nomeadamente a arquitetura e os seus componentes. Outras duas componentes muito importantes deste capítulo são a análise das questões da Segurança e das Comunicações, servindo de base para muitas das questões abordadas na plataforma. De forma a ser mais facilmente demonstrado quais as questões dos impactos de um ataque a um ICS, foi descrito o caso do Stuxnet.

No 3º Capítulo é abordada a **Arquitetura do Sistema**, servindo de base à conceção do protótipo, sendo definidas todas as componentes necessárias para a elaboração deste. Aqui é possível analisar-se o modelo de domínio, os use cases, os modelos de dados, bem como todos os fluxogramas dos modelos lógicos.

O 4º Capítulo, intitulado de **Protótipo Aplicacional,** apresenta o protótipo desenvolvido neste trabalho, sendo detalhadas todas as questões relativas com a navegacionalidade da plataforma, bem como os detalhes das diversas páginas executadas. São também discutidas as questões relacionadas com as Opções de Implementação.

O 5º Capítulo demonstra a **Validação** do protótipo, sendo aqui definidos os perfis dos especialistas que participaram na avaliação. São também apresentados os resultados dos questionários individuais, bem como as conclusões retiradas destes.

Por fim, o Capítulo 6 **Conclusões**, apresenta as conclusões deste trabalho, nomeadamente, o cumprimento dos objetivos propostos e a sugestão de trabalhos futuros.

CAPÍTULO 2

ENQUADRAMENTO TEÓRICO

2.1. CARACTERÍSTICAS DE UM ICS

Um ICS pode ser compreendido como um sistema de supervisão remota e controlo de processos industriais, que permitem a aquisição de dados e a comunicação entre o operador e os equipamentos (Filali-Yachou 2015).

Conforme é definido pela NIST no seu guia para a implementação de segurança em ICS (Stouffer, et al. 2015), considera-se que este conceito incorpora diversas noções de sistemas de controlo, como sendo os *Supervisory Control And Data Acquisition* (SCADA), *os Distributed Control Systems* (DCS) ou os *Programmable Logic Controllers* (PLC).

Assim, considera-se que os ICS se referem a um conjunto de sistemas compostos por computadores e dispositivos eletromecânicos (como os sensores, atuadores, medidores, entre outros) que interagem com processos automáticos e manuais, supervisionados por humanos e com o objetivo de cariz industrial. Estes sistemas controlam processos, realizando operações de forma automatizada ou parcialmente automatizada, num diverso número de ambientes, como por exemplo em fábricas, indústria transformadora, sistemas de transportes, infraestruturas de transito, produção e distribuição de energia ou a gestão do abastecimento da água (Kott e Colbert 2016).

De acordo com o mesmo autor, podemos considerar que a principal diferença entre os ICS e as IT tradicionais é a forte interação com o ambiente físico. Esta questão faz com que surjam questões únicas do ponto de vista de segurança, apresentando um conjunto de desafios e vulnerabilidades específicas que poderão revelar-se críticos no caso de uma avaria ou mesmo de um ciberataque. Assim, é necessário conhecer e proteger, não apenas as ameaças que genericamente podem atacar os sistemas tradicionais, como também os específicos dos ICS.

Para tal, deverão ser minimizadas as conexões da esfera industrial da empresarial, bem como dos sistemas de gestão das organizações e dos sistemas de controlo e monitorização das operações.

2.2. COMPONENTES

Os ICS são sistemas altamente personalizáveis, uma vez que se adequam à realidade dos processos onde são implementados. Esta questão faz com que existam componentes diversos, havendo, contudo, três componentes comuns e essenciais (Turc 2014): o servidor ICS, a bases de dados ICS e os clientes. De seguida, além destes três, são explicados os componentes mais comuns destes sistemas e a sua importância:

Servidor ICS – O servidor é o principal elemento de um ICS, uma vez que é ele que permite a ligação entre os componentes físicos e as aplicações de monitorização, ou seja, controla a "infraestrutura" e o fluxo de dados, nomeadamente dos diversos componentes e a base de dados, bem como dos operadores e os equipamentos instalados.

A utilização destes sistemas gera um fluxo de informação constante, sendo este em diversos sentidos e em tempo real o que permite por um lado, a concentração de informação nas bases de dados (que poderá ser acedida, tratada e analisada posteriormente) e receber *feedback* dos acontecimentos, através dos sinais enviados por sensores, atuadores e autómatos/PLC (Controlador Lógico Programável).

Base de Dados ICS - O acesso às bases de dados ICS é essencial para o funcionamento do sistema, uma vez que estas dão suporte ao funcionamento do sistema, equivalendo à sua memória, não servindo apenas para a análise de acontecimentos ocorridos, mas também como ferramentas de apoio para a tomada de decisões operacionais dos operadores do sistema.

Segundo Turc (2014), o software utilizado pelos ICS deverá ser implementado como Web Services, sendo as operações de acesso à Base de Dados suportada por comandos SQL. Estas funções vão servir como uma camada intermédia, entre os clientes e o servidor, disponibilizando os dados necessários e garantindo a Abstração e Transparência. Estas características vão permitir que, por um lado, a ligação do cliente (e respetivo operador) não se tenha de preocupar com a forma como a informação é disponibilizada e por outro

lado, permite que os diversos componentes do sistema consigam comunicar entre eles e com o servidor.

Clientes - Estes sistemas apenas são funcionais se permitirem o controlo dos processos industriais remotamente. Esta questão traduz-se normalmente pela existência de clientes ou terminais, onde os operadores têm acesso aos equipamentos do processo. A natureza destes componentes é bastante variável, dependendo da realidade dos processos implementados, devendo traduzir os sistemas físicos existentes.

De forma a que estes componentes de hardware funcionarem, é necessário que exista uma HMI funcional onde o operador "visualmente" tenha acesso ao processo industrial que lhe diz respeito. Para tal é necessário que exista uma boa e eficiente comunicação, de forma a facilitar a deteção de desvios e estado (Filali-Yachou 2015).

Autómatos e PLC – Estes componentes pertencem à família dos computadores e tem como principal função tomarem decisões baseadas em inputs e no seu código, controlando assim os outputs. Este são usados principalmente na indústria e permitem controlar equipamentos de processo (Siemens 2000).

Sensores – Segundo SCME (2011), estes componentes funcionam genericamente através da deteção, alteração ou transferência de alguma forma de energia. Através do transdutor é convertido um sinal de entrada numa saída (analogia ou digital) de energia elétrica, que é compreendida pelo recetor.

Atuadores – Estes componentes têm como função mover e/ou controlar um equipamento ou mecanismo, como por exemplo uma válvula ou uma porta. Estes podem ser comandados por diversas origens, nomeadamente interação direta por parte de um operador, sistemas automáticos mecânicos e hidráulicos ou por sistemas digitais (software e hardware). A fonte de energia para o funcionamento deste equipamento é também diversificada, podendo ser feita através de energia elétrica, hidráulica ou pneumática. Estes componentes podem ser vistos como outputs do sistema (SCME 2011).

2.2.1. ARQUITETURA

Como em todas as tecnologias, também os ICS sofreram alterações e evoluções ao longo do tempo. Segundo o artigo de Ujvarosi (Ujvarosi 2016) sobre esta temática, distingue a sua

evolução em duas abordagens distintas, uma pela Evolução Tecnológica e outra pela Evolução do Mercado. De seguida são apresentadas as principais fases de cada uma:

Evolução Tecnológica

Como o próprio nome indica, considera-se que as melhorias dos ICS segundo esta abordagem, têm por base a tecnologia existente. Segundo o autor do referido artigo, o ponto de viragem é a invenção dos transístores e da sua aplicação à eletrónica. Assim, antes destes, era necessário o controlo manual nos locais por parte de operadores do sistema.

a) Telemetria – Nos finais dos anos 50 foram criados os primeiros ICS, tendo como base as comunicações telefónicas. Através destas, foi possível a criação de Centros de Comando que centralizavam os dados gerados nos diversos locais, possibilitando a libertação da necessidade da comunicação "humana" dos mesmos.
b) Minicomputadores – A continuação da evolução dos ICS foi possível graças ao uso de computadores. Estes embora que limitados em termos de HMI, permitiram alguma análise dos dados recebidos, abrindo a porta à automação dos sistemas, através de funções como monitorização de sistema ou a criação de alarmes condicionados.
c) Microprocessadores – Com a continuação da evolução dos transístores, foi possível às empresas da área, o desenvolvimento dos primeiros PLC. A criação destes permitiu dotar o sistema de "inteligência" ao mesmo tempo que o tornavam mais eficiente e económico. Com a evolução dos microprocessadores e dos computadores associados, foi possível ganhos de velocidade e de capacidade de processamento, permitindo assim o uso de HMI mais complexos, ao mesmo tempo que o sistema se tornava mais fiável e cada vez mais em tempo real.

Evolução do Mercado

Os ICS foram estando disponíveis no mercado de acordo com o desenvolvimento de soluções para áreas de negócio específicas sendo encarado como projetos chave na mão. As vantagens destes sistemas foram rapidamente reconhecidas, levando a sua contínua evolução, tendo por base a necessidade de aumentar a sua inteligência e segurança.

a) Monolíticos – Os primeiros conceitos de ICS tiveram como base os sistemas com mainframe existentes na época, não estando ligados a uma rede. Desta forma, os diversos equipamentos existentes comunicavam apenas localmente, funcionando cada um como um sistema isolado. Neste modelo e com o surgimento do conceito de WAN, passou a

haver alguma conectividade para troca de dados entre estes conjuntos, sendo contudo, limitada aos protocolos utilizados nos PLC de cada fabricante.

b) Distribuídos – O desenvolvimento da computação (através da redução de custos, a sua compactação e aumento de capacidade) e das LAN, foram decisivos para a evolução dos ICS. Desta forma, foi possível a criação de múltiplos locais em que estes podiam comunicar entre si em tempo real, permitindo a troca de dados.

   Uma das características desta evolução foi iniciar-se a utilização dos componentes comuns entre fabricantes, contudo, continuavam a ser utilizados protocolos de proprietários, o que impossibilitava a comunicação para fora da rede e principalmente, entre equipamentos de diferentes fabricantes.

c) Baseados em Rede – A dificuldade de comunicação entre equipamentos de diferentes fabricantes foi precisamente o obstáculo a ser ultrapassado nesta evolução dos ICS. Com a abertura (protocolos abertos) e normalização conseguiu-se não apenas ultrapassar esta dificuldade, como também, abrir o sistema a novo hardware e software.

   Outro grande avanço destes sistemas foi com a utilização de protocolos WAN standard, como por exemplo o Internet Protocol (IP). Assim, passou a ser possível que todos os componentes comunicassem entre si através de conexões Ethernet.

d) Internet of Things – A mais recente evolução dos ICS baseia-se na conceção de IoT, através dos Cloud e de conceitos como "*Platform as a Service"* e "*Software as a Service"*. Desta forma, os equipamentos são cada vez mais ligados às redes IT das organizações e consequentemente a internet, criando nova soluções ao mesmo tempo que levanta novos desafios.

Segundo Turc (Turc 2014) ao nível de Hardware, pode-se considerar a **Figura 2** como sendo uma esquematização dos componentes mais relevantes de uma arquitetura ICS atual. Nos elementos a de cor rosa, encontram-se os elementos que existem em maior quantidade numa instalação industrial, sendo estes componentes principalmente sensores e atuadores.

Estes elementos podem ser mais tradicionais se forem ligados por comunicações com fio, enquanto que nos sistemas mais recentes, estes são por sistemas sem fios. A arquitetura apresentada na figura é para um ICS anterior a implementação do IoT, ou seja, os diversos componentes a rosa não estão ligados à WEB, mas sim a PLC e RTU.

De acordo com alguns autores (CSE-Semaphore 2010) os PLC e os RTU têm basicamente a mesma função, sendo genericamente associada à sua utilização dos primeiros a sistemas mais *hard-wired*, enquanto os segundos a wireless.

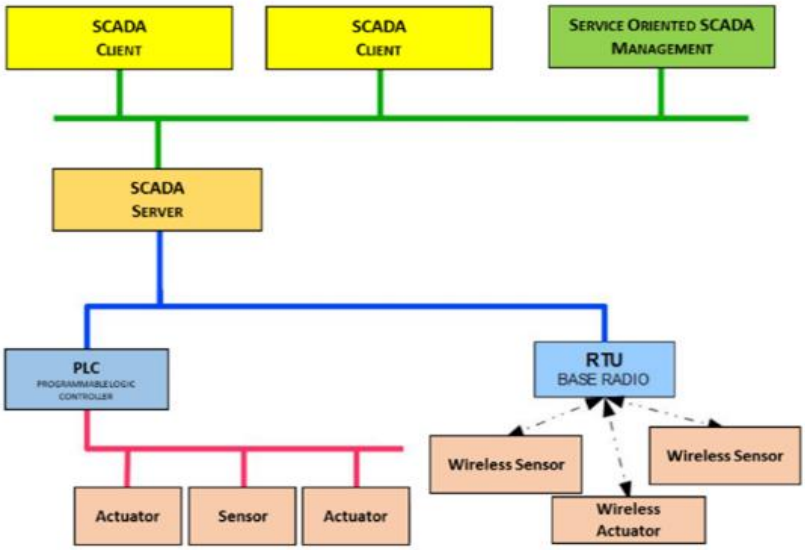


Figura 2 - ***Arquitetura de um ICS Atual***
Esquematização da arquitetura de um ICS/SCADA. Adaptado de Turc (2015).

Embora que tradicionalmente ambos permitam o tratamento dos inputs, os RTU conseguem um número maior destes e também uma maior quantidade de algoritmos e operações. Ao nível da transmissão de dados, (na maioria das situações, dependo das configurações adotadas) não está constantemente a transmitir, fazendo-o apenas quando existe alteração de algum estado, definição de tempos de retransmissão ou por pedido do servidor do ICS. Esta questão faz com que o tamanho dos pacotes seja superior, fazendo com que a transmissão seja mais lenta, ao mesmo tempo que é mais suscetível a perda de pacotes.

Por outro lado, os PLC fazem a transmissão dos dados em *loop*, ou seja, estão constantemente a ser transmitidos, sendo enviados com uma determinada ordem. Caso existam grandes quantidades de outputs a serem enviados, então o tempo de integração no Servidor ICS será maior. Em termos de dimensão, estes equipamentos são menores que os RTU, tendo unitariamente um consumo de energia menor. Caso seja necessária a associação de diversos PLC para igualar o número de inputs, o custo de energia será superior.

Ambos os componentes têm vantagens e desvantagens, sendo a transmissão de dados a sua diferença mais significativa, optando por RTU, quando temos equipamentos afastados e ligados por sistemas menos fiáveis, que não permitem o “congestionamento” da rede, ou por PLC, quando os componentes se encontram fisicamente próximos nas instalações fabris.

Sempre que os componentes estejam em diversas instalações, é necessário que sejam assegurados meios dedicados à comunicação dos equipamentos, sendo esta de diversas

naturezas diferentes, como por exemplo a fibra, o wireless direcional, GPRS ou linhas dedicadas. Estes canais, por um lado, devem garantir a largura de banda necessária para a quantidade de dados constantemente (ou quase com RTU) transmitidos, e por outro, a disponibilidade/fiabilidade que permite que o sistema esteja online.

Estes equipamentos enviam os dados recolhidos para o servidor (representado a laranja), que conforme foi referido anteriormente, controla todo o sistema, tendo como um dos componentes principais, a base de dados. A gestão desta é uma das principais funções deste equipamento, sendo este que dá resposta a todos os pedidos de acesso SQL.

Nos elementos de cor verde na **Figura 2** podemos observar um componente que não é comum nos ICS mais antigos, mas que atualmente, é normal ser parte integrante, o "*Service Oriented SCADA Management*". Segundo Turc (2015), esta família de componentes, é responsável pela "abertura" do sistema ao exterior, permitindo que os equipamentos instalados sejam acedidos não apenas do centro de comando, mas por qualquer ponto do mundo.

Os ICS baseados em serviços Web permitem a utilização das interfaces HMI com HTML, possibilitando uma grande capacidade de acesso por diversas plataformas e sistemas. Desta forma, é possível a utilização de qualquer browser (ou software próprio) para o acesso à base de dados e à interface em si.

A abertura dos Sistemas ICS à WEB tem ainda alguns obstáculos, fazendo com que a sua disseminação esteja limitada por três principais motivos (Ozdemi e Karacor 2006):

- Os equipamentos instalados não integrarem nas suas características de fábrica, capacidade para este tipo de acesso;
- Quando tem capacidade para efetuar alguma ligação, existem diversos protocolos e a necessidade de estarem "fisicamente" ligados, necessitando normalmente de sistemas intermédios (por exemplo um computador ligado por cabo ao equipamento).
- Necessidade de garantia de segurança no acesso aos dados e ao acesso e controlo dos equipamentos. Este sentimento é tanto maior quanto a criticidade dos sistemas que são controlados.

Segundo o mesmo autor (Ozdemi e Karacor 2006), a resolução destes problemas é possível, tendo como consequência o aumento dos custos, nomeadamente na substituição de equipamentos e na adquisição de serviços.

Por fim, os elementos representados a amarelo são os clientes. Estes são peças chave para a funcionalidade do sistema. Conforme foi referido anteriormente, embora seja possível o acesso remoto aos equipamentos instalados, na maioria dos casos, estes encontram-se em Centros de Comando, sendo aí que se concentram os operadores das instalações.

Estes são computadores ou terminais com características simples, podendo também ser equipamentos compactos e de baixo custo como sendo Raspberry Pi. A grande diferença na escolha destes está relacionada com o formato da interface, como por exemplo, na utilização de software desenvolvido para o efeito ou na utilização de HTML, e com o número de saídas gráficas, sendo necessária uma maior capacidade (tanto em número como em recursos) quanto maior forem os "ecrãs" a utilizar por cada um.

2.2.2. INTERFACE HOMEM-MÁQUINA (HMI)

Nos antigos Centros de Comando, os operadores esperavam a ocorrência de alarmes para a deteção de ocorrências e avarias, sendo então obrigados a seguir procedimentos de verificação nos locais e entrar em contacto com diversas equipas (ex. manutenção) que iram identificar as causas.

A falta de dados (ou a falta da sua análise) fazia com que houvesse pouca diferenciação dos alarmes, sendo o grau de importância imputado ao equipamento e não à causa. Com a disseminação e massificação dos ICS, nos atuais Centros de Comando, os operadores, através dos seus clientes e interfaces, recebem muitas mais informações específicas, permitindo não só perceber qual a causa do alarme, como também perceber quais os recursos a alocar para determinado problema.

Conforme foi referido anteriormente, a interface a ser utilizada é grandemente responsável pelo sucesso de qualquer ICS. Estes têm de garantir o controlo dos equipamentos instalados e os dados guardados aos utilizadores aos equipamentos, bem como a parametrização dos mesmos. Esta questão faz com que seja essencial que este esteja protegido, não só para utilizações indevidas, mas também, para garantir o pretendido para cada utilizador

Segundo Dieu (2001), para garantir o correto acesso a cada utilizador, o sistema deve permitir a elaboração de diversos perfis diferentes, como sendo de Visualização, Operação, Supervisão ou Manutenção, tendo associado a cada um destes responsabilidades e funcionalidades distintas.

Cabe a cada gestor do sistema a atribuição e definição dos perfis aos diversos *players*, devendo este ter em consideração que quanto mais acesso for atribuído aos utilizadores, mais falhas de segurança e de operação podem ocorrer. Estas estão não só relacionadas com ações propositadas, mas também com a má utilização por parte dos utilizadores, que podem, sem que haja necessidade para tal, alterar parâmetros operacionais, ou por exemplo, aceder a um periférico contaminado (ex. armazenamento usb).

Com o aumento da capacidade dos computadores e dos restantes componentes existentes nos sistemas industriais, é possível criar interface com uma quantidade de dados, cores, animações e imagens muito superior ao de antigamente. Contudo, conforme é citado por Gruhn (2011) "*More data does not equal more information*", ou seja, mais dados não equivale a mais informação.

No desenvolvimento destas interfaces, é necessário ter em consideração três pontos essenciais, de forma a garantir que o utilizador consiga dispor das informações que lhe são úteis e não dos dados fornecidos pelos sensores. Desta forma, (Gruhn 2011) defende que a "construção" destas interfaces deve ter em consideração os seguintes focos:

Focar no Utilizador – É necessário que a tecnologia seja centrada nos objetivos, tarefas e funções do utilizador, transmitindo-lhe as informações necessárias.

Focar na forma de processar a informação e na tomada de decisão – Para a tomada de decisão, é necessário que os operadores e os utilizadores tenham o máximo de informação possível. Assim, a tecnologia deve fornecer não só o que está a ocorrer, mas também o histórico e outras variáveis relacionadas.

Focar no estado do sistema – Com os grandes níveis de automatização, os utilizadores tendem a afastar-se dos processos, diminuindo assim a sua *Awareness* (consciência) para o funcionamento e estado destes. Contudo, é desejável que estes mantenham o controlo e a atenção no sistema, diminuindo assim o risco de falhas e de capacidade para a tomada de decisões.

No mesmo alinhamento de conceito, Hollifield (Hollifield, et al. 2008) escreve que grande parte das interfaces existentes mostram um grande número de dados, mas pouca informação, sendo que, em alguns casos mais de 100 valores são apresentados em apenas um ecrã. Esta questão está atualmente a ser alterada, estando a avançar-se para um HMI baseado na Alto Desempenho, diminuindo assim, a possibilidade de falha humana do sistema.

Um exemplo desta situação pode ser visto na **Figura 3**, onde, na imagem do lado esquerdo, observa-se uma interface com diversos elementos "estéticos" que têm como objetivo o enquadramento do processo ao operador, existindo o cuidado de o tornar reconhecível no sinótico. Esta questão faz com que os dados do sistema estejam misturados de forma pouco evidente, aumentando assim o risco de não deteção do desvio de uma ou mais variáveis, sendo por isso caracterizada como tendo poucas características de Alto Desempenho.

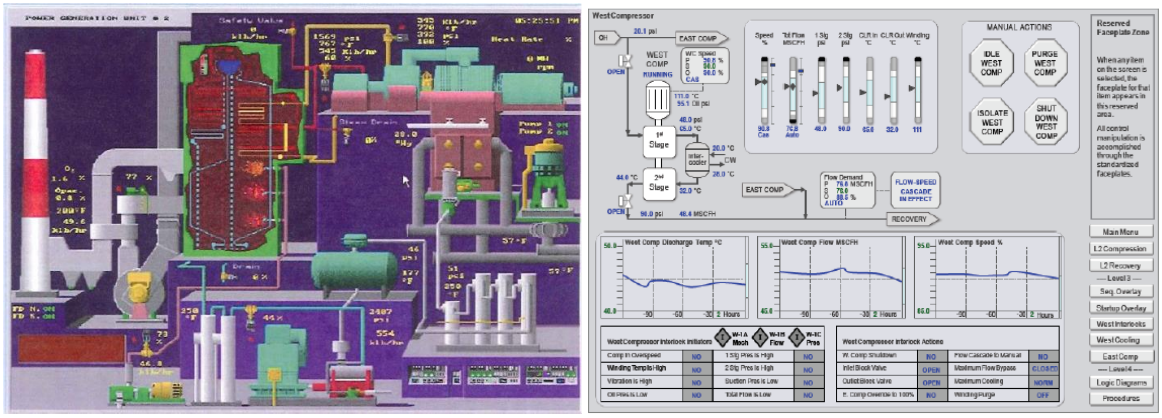


Figura 3 - HMI Tradicional e de Alta Performance
À esquerda um sinótico de um centro de comando de central energética com poucas características de Alto Desempenho. (Gruhn 2011). À direita Exemplo de Sinótico de Alto Desempenho (Evans 2017).

Por outro lado, a imagem do lado direito mostra um sistema baseado no Alto Desempenho. Neste, todas as opções da interface foram escolhidas tem por base a diminuição do risco de falha do operador. Por exemplo, esta questão aplica-se desde a cor escolhida para o fundo e para os textos apresentados, para a existência de gráficos com histórico e tendência, a aplicação de mostradores digitais para as variáveis com a visualização de *threshold* ou a quantidade de dados apresentados neste nível do sinótico.

2.3. SEGURANÇA

Como foi referido anteriormente, a segurança dos sistemas ICS tem alguns desafios próprios, o que obriga a que sejam tomadas algumas preocupações específicas. Conforme defendido por Ackerman (2017), ICS são sistemas menos flexíveis que os típicos sistemas IT, uma vez que têm componentes físicos. Muitos destes foram construídos e desenvolvidos com equipamentos e protocolos *legacy*, anteriores a proliferação da internet e dos serviços baseados nesta (Knapp e Langill 2015). Esta questão faz com que estes equipamentos ou

sejam demasiados antigos para receberem atualizações de segurança mais recentes, ou são demasiados limitados ao nível dos recursos para serem protegidos (Ackerman 2017). Desta forma, autores como Ackerman defendem que deverá ser aplicado o modelo da Bolha de Sabão neste tipo de sistemas.

2.3.1. TEORIA DA BOLHA DE SABÃO

Segundo Ackerman (Ackerman 2017) este conceito é serve para se visualizar a segurança destes sistemas como uma frágil bolha de sabão, que ao ser penetrada por qualquer objeto, rebenta. Fazendo a analógica para os ICS, deverá ser considerado que os equipamentos dentro da bolha podem comunicar livremente entre si. Estes, atuam e ajustam o sistema físico com base nestas informações, estando a operação dependente nesta relação de confiança.

Desta forma, apenas os equipamentos realmente necessários para o funcionamento e monitorização do ICS devem estar dentro da bolha e principalmente, todos estes devem estar verificados ee reação à presença de malware e atualizados ao nível de segurança.

De acordo com a mesma analogia, a comunicação com o interior deverá apenas ocorrer por canais claramente identificáveis, controláveis e monitorizáveis. Desta forma, todas as tentativas de comunicação anómalas com o interior por parte dos equipamentos autorizados ou qualquer tentativa por canais não espectáveis, resultariam num rebentar da bolha, ou seja, num alarme claro ou mesmo na paragem de parte do sistema. Esta deteção de anomalias é possível através da existência de IDS, tanto físicos como lógicos.

Desta forma, o perímetro de deteção representado pela bolha, corresponde ao universo físico e lógico, sendo a fronteira correspondente a um *Air Gap* que separa a área de negócio da industrial (Knapp e Langill 2015). Este vai garantir que não existe ligação física ou lógica entre ambas as componentes da organização.

Conforme é referido por Ackerman (2017), ao ser assegurado que tudo o que é colocado dentro da bolha está “limpo” de *malware* e que não existe entrada de nenhuma informação exterior, o sistema está seguro, mesmo que os seus componentes não disponham de poderosos e modernos sistemas de segurança.

Contudo, a operacionalização desta teoria, torna-se difícil de implementar e manter, principalmente à medida que os sistemas mesmos evoluem e crescem.

2.3.2. SEGMENTAÇÃO

Para ser possível implementar o conceito por trás do ponto anterior, é necessário que se perceba como deve ser organizada a rede e os seus componentes. Para tal, foi criado uma arquitetura chamada de *Converged Plantwide Ethernet* (CPwE). Conforme é definido por Ackerman (2017), podemos defini-la como "(…)*an architecture that provides network and security services to the devices, equipment, and applications found in an Industrial Automation and Control System (ICS), and integrates them into the enterprise-wide network."*

Conforme se pode perceber pela **Figura 4** (Ackerman 2017), a arquitetura CPwE baseia-se na divisão por níveis dos processos, permitindo conectar ou convergir redes ICS com redes corporativas de maneira eficiente, conveniente e segura. Os níveis baseiam-se na segmentação por zonas funcionais, onde os perímetros de segurança são estabelecidos com a capacidade de controlar, restringir e inspecionar o tráfego entre as regiões.

Por padrão, dentro de uma rede ICS, a comunicação é geralmente aberta. Esta "abertura" da rede facilita a coexistência de tecnologia e a interoperabilidade de dispositivos ICS de diversas marcas e gerações. Ao conciliarmos esta abertura com o facto de que, em muitos casos, os

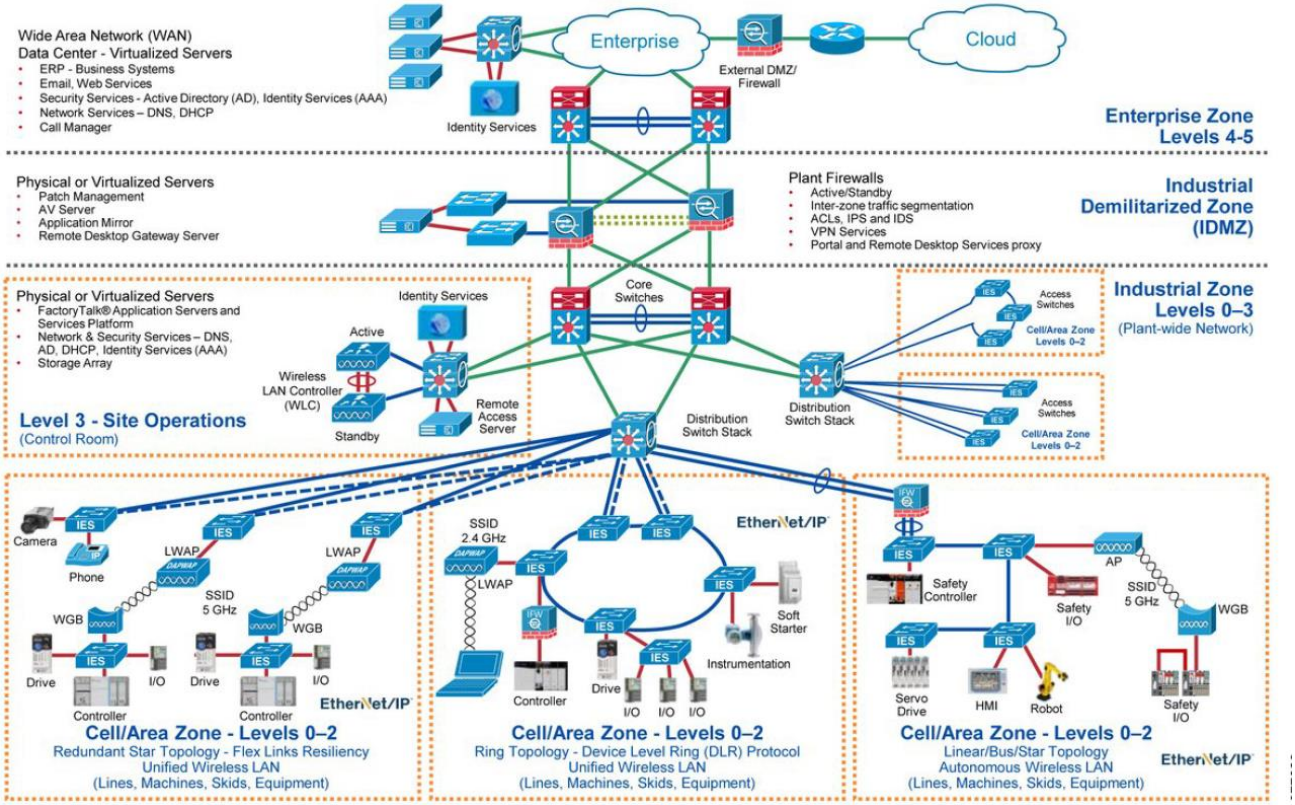


Figura 4 - Exemplo de aplicação da arquitetura CPwE

dispositivos ICS não podem ser protegidos devido a restrições de idade ou dispositivo, faz com que sejam necessárias uma configuração e uma arquitetura que proteja e fortaleça as redes ICS. Esta varia em extensão e profundidade de acordo com a avaliação de risco efetuada ao sistema e aos requisitos de segurança definidos e grau criticidade identificado. (Ackerman 2017).

O fortalecimento da configuração e da arquitetura devem fazer parte de uma estratégia de defesa mais ampla. Assim, esta deve levar em consideração a noção de que nenhum equipamento, tecnologia ou metodologia pode proteger totalmente os ICS, necessitando que existam defesas diferentes para os diversos níveis e as suas comunicações (Knapp e Langill 2015). Desta forma, a estratégia deverá assentar numa mistura de soluções que eliminem as lacunas nos controles de segurança, por exemplo através da instalação de uma firewall baseado no *host* nos diversos perímetros, bem como a implementação de um sistema de backups (Ackerman 2017).

Além das questões referidas anteriormente, a segmentação é importante por vários motivos, como sendo o desempenho da rede ou a comunicação entre os diversos espaços físicos. Segundo (Knapp e Langill 2015) o conceito de segmentação de rede foi originalmente desenvolvido devido à limitação das comunicações Ethernet, tendo sido projetada em torno das comunicações e equipamentos de rede (hubs e switchs). As limitações das primeiras ICS modernas, foram sendo superadas com o aumento da capacidade dos equipamentos, permitindo atualmente a existência de redes muito maiores e distantes (por exemplo através do uso de fibra ótica), estando agora muito relacionadas com o uso de VLAN. Estas permitem uma gestão superior, ao tornar a sua configuração mais flexível, uma vez que permite uma “libertação” da necessidade de os componentes estarem fisicamente próximos e interligados aos mesmo equipamentos de rede.

De acordo com Ackerman (Ackerman 2017), a estratégia de segurança e a respetiva segmentação deverá assentar nas seguintes camadas:

a) **Procedimentos e Políticas:** Esta camada é crítica para determinar o comportamento e papel dos trabalhadores da organização. Estes deverão seguir as políticas implementadas, garantindo assim as práticas mais seguras e a correta utilização das tecnologias à sua disposição. Como exemplo temos a definição das interações e procedimentos dos trabalhadores com os componentes industriais, com os postos de trabalho ou o HMI.

b) **Físico**: Limitação do acesso físico dos trabalhadores às áreas, quadros elétricos, bastidores, painéis de controle, dispositivos, cablagem e centros de comando, através de sistemas de bloqueios, gradeamentos, chaves, cartões de autenticação ou sistemas biométricos. Além destas limitações de acesso, deverão também ser implementadas políticas, procedimentos e tecnologia para acompanhar *guests* e utilizadores com menos privilégios.
c) **Rede:** Aplicação de *frameworks* de segurança, por exemplo através de políticas de firewall, políticas de lista de controle de acesso para os *switchs* e routers, métodos de AAA (*Authentication, Authorization and Accounting*) ou IDS (*Intrusion Detection System*).
d) **Computador**: Gestão de atualizações de segurança, software anti-malware, desinstalação e desativação de aplicações, protocolos e serviços não utilizados, fecho das portas lógicas desnecessárias e proteção das portas físicas utilizadas.
e) **Aplicação**: Métodos de AAA (*Authentication, Authorization and Accounting*), bem como de gestão das vulnerabilidades, de atualização dos *patches* e acompanhamento do ciclo de vida de desenvolvimento do software.
f) **Dispositivo**: Proteção dos dispositivos e equipamentos, encriptação das comunicações e dos dados armazenados, restrições de acesso e acompanhamento do ciclo de vida de desenvolvimento dos dispositivos.

Ao nível de implementação da segmentação, esta deverá ser adaptada à realidade da organização e à sua avaliação de risco, não havendo uma estrutura rigidamente definida para cada situação. Uma das divisões possíveis é apresentada por Knapp & Langill (Knapp e Langill 2015) e divide esta 8 partes, sendo a confiança crescente à medida que se desce na lista:

- Redes públicas (como a internet);
- Rede empresarial;
- Rede de operações;
- Rede nível da planta;
- Rede de supervisão e controlo (servidor ICS, postos de trabalho, HMI);
- Equipamentos de controlo local (PLC, controladores, RTU, sensores, atuadores…);
- Processos de rede (equipamentos de rede, analisadores de rede, equipamentos de monitorização…);
- Equipamentos de segurança de rede (deteção de intrusões (IDS) e monitorização).

2.3.3. VULNERABILIDADES UTILIZADAS POR ATAQUES COMUNS

Conforme será demostrado de seguida pelo exemplo do Stuxnet, tem aumentado o número de ataques aos ICS, bem como a complexidade e os recursos investidos nos mesmos. A continuação do uso destes, com as tecnologias atualmente existentes, é essencial para a sociedade atual, não sendo possível de forma razoável eliminar todos os vetores de risco para estes sistemas. Para a determinação do risco destes e atuação sobre o mesmo, é essencial que se conheçam estes vetores que potencializam estas vulnerabilidades.

Tendo por base as publicações de (Bartman e Carson 2018) e (Butterworth 2013), são apresentados de seguida alguns dos vetores de ataques mais relevantes:

A. ESPIONAGEM

Os ataques aos sistemas SCADA não se limitam a "ataques digitais", sendo utilizado todo o tipo de técnicas. A espionagem e vigilância tradicional que permitem o roubo de informações relacionadas com o próprio ICS (por exemplo a segurança, equipamentos utilizados ou a sua infraestrutura) e com a organização e seus trabalhadores.

Atualmente, com o avanço da eletrónica, da miniaturização e das comunicações sem fios existe uma grande variedade de equipamentos de vigilância e de captura de informação (por exemplo *keyllogers* físicos e microcâmaras) que permitem a um atacante obter estes dados. Desta forma, este tipo de ataques muitas vezes está na base dos ataques mais direcionados e evoluídos, uma vez que, permitem a personalização os seus métodos.

B. PHISING

Existem diversas formas de Phising, tendo por base o mesmo conceito, a "pesca" de informações (normalmente credenciais de acesso) de um alvo através da falsificação da identidade do remetente. O caso mais banal deste tipo de ataques é o uso de email, onde, por exemplo, o utilizador recebe um email "disfarçado" de fonte fidedigna, onde é direcionado para uma página externa onde é solicitado a inserção das suas credenciais de acesso ou são executados, sem que este se aperceba, scripts ou programas maliciosos.

À semelhança do ataque anterior, estes ataques são muitas vezes preparativos para um ataque aos ICS existente, focando-se normalmente nas camadas de IT da organização. Após a penetração desta, torna-se mais fácil aos atacantes a instalação de software malicioso e o emprego de outros vetores de ataque já dentro da rede da organização, aumentado assim, a probabilidade de avançarem para as áreas de operacionais onde se encontram os ICS.

C. DICTIONARY ATACK

Este ataque é considerado também como sendo de Brute Force, tendo como grande diferença face ao anterior, usam palavras, conjuntos de palavras e derivações destas que se encontram em listas. Nos casos em que estes ataques são mais "inteligentes", estas são geradas de acordo com a língua utilizada e dados personalizados (conseguidos por exemplo através de Engenharia Social) referentes a gostos, hábitos ou características sociais dos alvos.

Uma vez que os utilizadores têm por hábito utilizar chaves/passwords curtas e com palavras das suas línguas nativas, este ataque tem uma maior probabilidade de sucesso que apenas o brute force. Contudo, este continua a necessitar de uma grande quantidade de recursos a listas, podendo ter milhões de possibilidades.

D. BRUTE FORCE

Estes ataques têm como alvo, por exemplo, os dados criptografados ou as senhas de acesso. Este normalmente só é usado quando os restantes não são viáveis ou não tiveram os resultados desejados, uma vez que este ataque necessita de um grande poder de computação e tempo. Esta questão prende-se por este se basear no uso de todas as combinações possíveis de forma sistemática para descodificar a chave pretendida.

A resistência a este ataque baseia-se principalmente na extensão da chave de encriptação (por aumentar o número de potenciais soluções) e da "clareza" dos dados encriptados (por facilitarem a perceção do sucesso do ataque).

E. WAR DIALING

Embora este tipo de ataque seja muito mais empregue no advento da fibra ótica, este método ainda hoje é utilizado. Conforme foi referido anteriormente, os ICS nem sempre são mantidos atualizados como os equipamentos da camada IT das organizações.

Este baseia-se na conexão do sistema do atacante a um número pseudoaleatório de alvos que são *dial-up* de forma a verificar a obtenção de resposta por parte do destino. Caso exista, então é identificada a existência de um modem. Após esta conexão, o atacante tenta obter mais respostas por parte do destinatário, nomeadamente, pelos dados presentes no banner do login (por exemplo nome da organização, informações sobre o dispositivo, seu fabricante ou a sua localização) ou testar credenciais de acesso (obtidas anteriormente ou através de ataques informáticos.

F. PASSWORDS INSEGURAS

Embora os sistemas operativos mais atuais já não permitam o uso de passwords de autenticação *default*, o mesmo continua a não acontecer com equipamento de infraestrutura ou mesmo com os ICS. Normalmente, estes equipamentos são fabricados com um conjunto de passwords, que são, na maior dos casos, uma informação disponível ao público, sendo esta vulnerabilidade explorada por diversos *malwares*, como por exemplo o Stuxnet referido anteriormente.

Muitas das boas práticas aplicáveis as regras de passwords das organizações (por exemplo: passwords longas, não repetição de caracteres, caducidade ou diferentes tipos de caracteres), devem ser também aplicáveis aos ICS. Assim, de forma a aumentar a segurança, quando o login é feito por parte de um utilizador, estes não devem usar as mesmas de combinações *user/password* no OT que utilizam no resto dos sistemas da organização. Por outro lado, quando este acesso é feito de forma automática entre equipamento, devem ser escolhidas passwords muito longas e aleatórias.

G. REPLAY ATTACK

Este tipo de ataques tem como metodologia a captura de determinada mensagem entre equipamentos, sendo depois a mesma reproduzida de forma intencional por parte do atacante. Este tipo de ataque permite utilizar cópias das mensagens originais, mesmo estas estando encriptadas, ou seja, o emissor não necessita de entender totalmente o conteúdo do comando enviado (ao nível de autenticação por exemplo). Contudo, o recetor que não esteja preparado para este tipo de ataque, irá receber o pacote “fraudulento” e atuara de forma convencionada para uma mensagem legítima, por exemplo abrindo uma válvula. Este tipo de ataque poderá acontecer nas redes com e sem fios.

H. MAN-IN-THE-MIDDLE

Este tipo de ataques é efetuado através do posicionamento do atacante entre dois dispositivos, por exemplo, um atuador e o servidor. Para tal, este tem de se conectar à rede e interromper a comunicação entre os dois alvos. Após isso, assume o papel do dispositivo sobre ataque, encaminhando todas as comunicações recebidas para o destino original. Este ataque permite não só o envio de mensagens adulteradas (como os dados errados de sensores) ou comandos não autorizados por parte de uma origem não autorizada, como o armazenamento dos dados produzidos pelos equipamentos “monitorizados” ou dados de autenticação dos utilizadores e software. Estas últimas potencialidades são chave para os ataques mais complexos, por permitirem as informações necessárias para a elaboração de

software específico, permitindo dotar este de "inteligência". Geralmente este tipo de ataque explora a falta de medidas de autenticação eficazes das redes e equipamentos.

I. DENIAL-OF-SERVICES

Uma das características dos ICS é a necessidade de troca de informações entre os dispositivos e os servidores. Embora que os PLC e autómatos tenham alguma capacidade de atuarem autonomamente com base nas suas programações, caso a falta de comunicação se mantenha, o funcionamento do sistema poderá ficar severamente comprometido. Esta questão é explorada por este tipo de ataque. A negação de serviço (DoS) pode basear-se principalmente em 2 tipos de estratégia.

A primeira estratégia é através da "inundação" da rede com dados e *requests* para a infraestrutura de rede. Este ataque faz que com o tráfego legítimo tenha de concorrer com a gigantesca quantidade injetada, provocam perda de qualidade de serviço, nomeadamente pelo aumento da latência, a perda de dados relevantes ou mesmo a rotura do sistema.

A segunda estratégia dos DoS é bastante direcionada para os ataques às ICS, aproveitando-se das características dos componentes, para explorar limitações de recursos e vulnerabilidades dos mesmo. Em contraste com a anterior, não se baseia em enviar grandes quantidades de *requests* e informações, mas sim, enviar *requests* específicos para estes fazendo com que os mesmos fiquem impossibilitados de procederem em normalidade.

2.3.4. ESTRATÉGIAS DE SEGURANÇA

2.3.4.1. SEGURANÇA FÍSICA

Para ser contrariado o descrito no ponto anterior, deverão ser tomadas medidas que impeçam ou dificultem o acesso aos equipamentos e sistemas instalados. Desta forma, serão descritas de seguida algumas das medidas que poderão ser tomadas (Ackerman 2017). Na figura seguinte (**Figura 5**), podemos ver o exemplo de uma instalação com algumas das medidas implementadas.

A. LOCALIZAÇÃO

A localização dos ICS deverá ser escolhida levando tendo em consideração as questões relativas à segurança. No caso dos ICS mais extensos, esta questão poderá ser limitada pela própria natureza dos processos, sendo, contudo, aplicado à escolha do centro de comando principal e o mais relevante, ao nível da avaliação do risco.

Esta questão, deve levar em conta a segurança da própria instalação em relação a fenómenos naturais (inundações incêndios, terramotos), mas também às perturbações que poderão ocorrer nas imediações, causadas por atividade como os aeroportos, os grandes complexos industriais ou as prisões.

B. ARQUITETURA COM FOCO NA SEGURANÇA

Ao serem colocados centro de comandos e outros componentes críticos de um ICS numa determinada instalação, esta deverá ser projetadas, ou adaptada, levando em consideração as características paisagísticas e arquitetónicas que permitiam por exemplo, uma boa visualização por parte dos sistemas de vídeo vigilância e de patrulhamento. Para tal, deverão

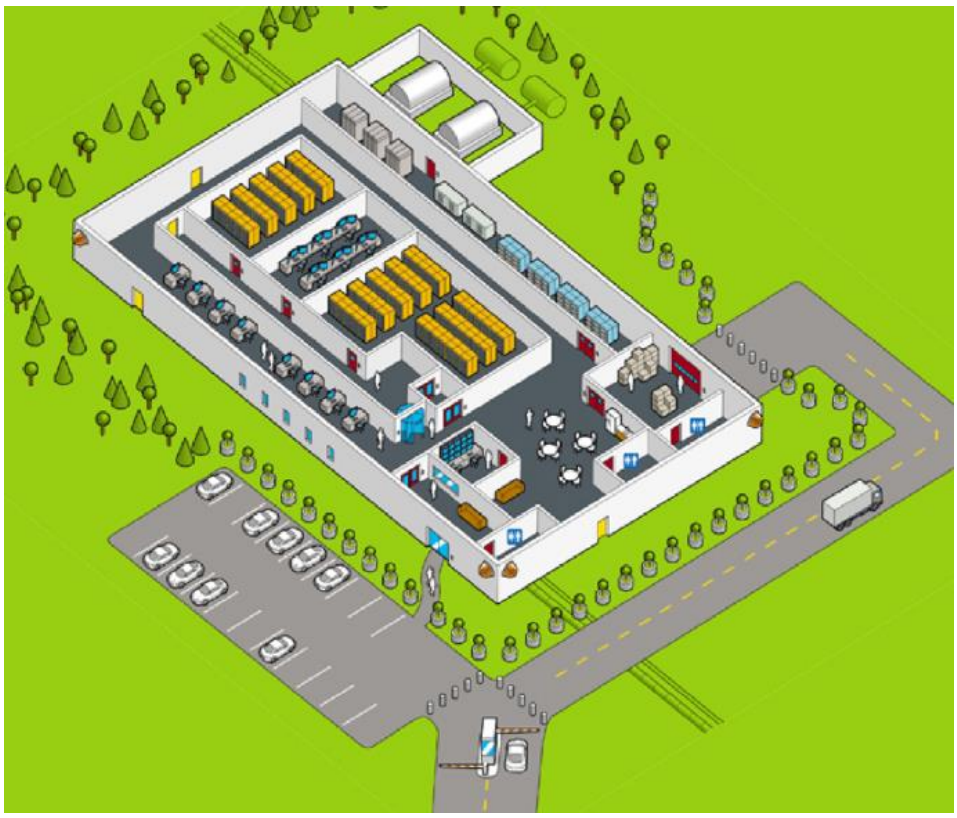


Figura 5 - Exemplo de uma instalação segura
Instalação com algumas das medidas implementadas, como sendo, o controlo de acessos, proteções físicas, videovigilância e a separação física (Ackerman 2017).

ser retirados do perímetro exterior obstáculos que dificultem os ângulos de visão, bem como que proporcionem esconderijo. Esta situação é principalmente relevante quando estes obstáculos facilitam o acesso ao interior das instalações. Desta forma, deverá ser criado um buffer entre o exterior e o interior.

Deverão ser colocadas medidas que dificultem o acesso de viaturas não autorizadas, bem como limitar a circulação para dentro do perímetro, através de barreiras anti viaturas.

A mesma lógica deverá ser utilizada para as pessoas, devendo ser colocada vedação no perímetro. Dependendo da relevância da atividade a proteger, as barreiras e vedações deverão ser mais altas, mais resistentes e mais afastadas, dissuadindo e dificultando o acesso não autorizado.

No caso das saídas de emergência, estas deverão apenas permitir a passagem do interior para o exterior. Além disso, deverão desencadear os alarmes necessários para assegurar que caso sejam usadas indevidamente, o sistema consiga detetar.

C. ACESSOS DE VEÍCULOS E PESSOAS

O acesso ao interior do perímetro deverá ser verificado (se necessário em mais do que um ponto), através de métodos ativos. Estes podem ser através do controlo de segurança ou de outro meio eletrónico, devendo a abertura de portas e de acessos rodoviários serem limitados a pessoal credenciado.

Os visitantes deverão aceder de forma controlada, devendo existir políticas internas para estas situações. Estas deverão ter enfoque nas regras e acompanhamento e de limitação dos acessos destes as áreas mais críticas, bem como minimizar o contacto com equipamentos e informações críticos.

Os pontos de acesso deverão ser limitados, aumentando assim a deteção indevida ou não controlada. Deverão ser equacionadas as questões logísticas (entrada e saída de material) onde poderá ser necessário criar limitações extra como sendo sub-perímetros e pontos de controlo adicionais.

D. VÍDEO VIGILÂNCIA

Atualmente, as instalações dos ICS deverão ser servidas de um sistema de vídeo vigilância (IPTV ou CCTV). Esta necessidade é muito importante, tando ao nível da segurança e funcionamento dos processos, como na salvaguarda dos acessos e atividades não

autorizadas. Os sistemas atuais permitem além da visualização e gravação, a deteção de movimentos e perturbações, bem como o uso de imagem noturnas e com baixa luminosidade.

Deverá ser dada especial atenção às questões relacionadas com o RGPD, uma vez que será necessário definir os limites destas bem como o seu "alvo". É também necessário que existam procedimentos para dar resposta a manutenção das imagens e às requisições que poderão ser efetuadas pelas entidades competentes.

Ao nível do armazenamento das gravações, estas deverão ser guardadas de forma segura e, de preferência, fora do próprio recinto.

E. PAREDES E TETOS FALSOS

As paredes exteriores das instalações críticas deverão ser resistentes e de preferência de betão armado. Outros métodos poderão ser implementados, como por exemplo da aplicação kevlar ou de sistemas anti-explosão, devendo, contudo, ter-se em mente que estas são chave na proteção da instalação principalmente por servirem de fixação às janelas, portas e grelhas de climatização.

Todos os equipamentos referidos anteriormente, são pontos sensíveis numa instalação deste tipo, devendo ser minimizados e protegidos, por exemplo, através da instalação de grades ou de vidros blindados.

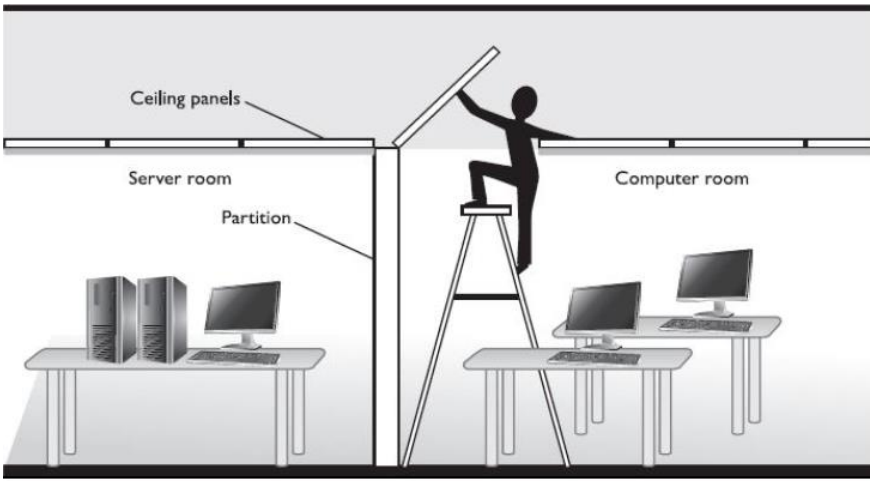


***Figura* 6 - Barreiras Físicas**

Exemplo da necessidade de garantir a existência de barreiras físicas entre salas de equipamentos (Ackerman 2017).

Conforme se pode ver na **Figura 6**, no interior, as paredes que circundam os equipamentos sensíveis devem ser igualmente resistentes e devem ser completos, ou seja, devem impedir o acesso entre divisões pelo teto falso.

F. ACESSOS ÀS ZONAS CRÍTICAS

As zonas ou equipamentos críticos devem estar isolados da restante instalação. Desta forma, é necessário que existam meios físicos de verificação e autenticação dos trabalhadores que tenham de aceder a estas áreas. Para tal, deverão utilizar mecanismos de autenticação (como por exemplo cartões, códigos ou biométricos) sendo de preferência feitos logs de acessos.

Ao nível de pessoal externo à organização, não deverá ser dado acesso a áreas e/ou equipamentos sem que exista supervisão. Além disso, deverá existir uma política rígida sobro o uso de computadores e similares destas dentro das instalações críticas.

G. ACESSO A INFRAESTRUTURA IT E DE PROCESSO

Os equipamentos de IT existentes deverão ter o seu acesso limitado, tanto ao próprio equipamento, como ás suas configurações (passwords de acesso, por exemplo). A localização dos bastidores das comunicações e de controlo de processos deverá ser escolhida tendo como base a segurança dos mesmos, sendo instalados mecanismos que impeçam o seu acesso indevido (chaves de quadro codificadas ou outro método analógico ou digital de fecho). Deverá ser dada especial atenção à segurança dos equipamentos mais sensíveis, como sendo os PLC, uma vez que, conforme foi referido anteriormente, tendo acesso a estes, obtem-se acesso a um fluxo constante de informação.

H. PROTEÇÃO DE INTERFACES

As portas de rede que não estão a ser utilizadas, por exemplo em routers, switchs ou hubs são pontos extremamente vulneráveis da rede. Estes deverão ser desligados ao nível das configurações dos equipamentos, bem como deve-se limitar a sua má utilização. Devem assim ser bloqueadas as portas que se encontrem ativas, mas que não estejam a ser usadas, ao mesmo tempo que deverão ser implementados mecanismos que garantam que as utilizadas não são desligadas.

As portas USB são atualmente uma das maiores vulnerabilidades dos sistemas, uma vez que cada vez mais pessoas têm este tipo de interface num sem número de dispositivos. À

Figura 7 - Sistemas de proteção contra uso indevido de interfaces

Exemplos de sistemas de proteção (Ackerman 2017): Solução para bloquear o acesso a uma interface de rede RJ45 (esquerda); Solução de fixação de interface de rede, obrigando o uso de chave para debilitação do cabo (centro); Sistema com chave para bloqueio de porta USB (direita).

semelhança do referido para as interfaces de rede, deverão ser desabilitadas as portas não necessárias e bloqueadas as que estão abertas. Existem atualmente uma grande variedade de mecanismos deste género no mercado, sendo na **Figura 7** apenas demostrada uma solução possível.

I. AUTENTICAÇÃO DE ACESSOS

Principalmente nas áreas e equipamentos mais sensíveis, deverá ser necessária uma autenticação forte para o seu acesso. Este é por exemplo o caso de salas de servidores, data centres e salas de processo. Embora existam diversas formas de fazer esta autenticação, as mais usuais são a combinação entre 2 ou mais fatores como a impressão digital, a palma da mão, a retina, pins ou cartões de acesso.

J. REDUNDÂNCIAS

As redundâncias são essenciais na natureza dos ICS. Ao falarmos de equipamentos críticos, estamos a partir do pressuposto que estes não podem estar offline ou a trabalhar de forma deficiente. Assim, os processos têm sistemas redundantes e suplentes que permitem que em caso de falha ou manutenção de parte do sistema, continuam a funcionar de forma normal. O mesmo conceito deve-se aplicar aos componentes de segurança dos ICS.

2.3.4.2. SEGURANÇA LÓGICA

No ponto anterior, a segurança era baseada no princípio de impedir que os invasores acedessem à rede e aos equipamentos do ICS, sendo uma defesa de ativos tangíveis. De acordo com Ackerman (Ackerman 2017) e Weiss (Weiss 2016), em termos de lógica, o âmbito

deve-se focar na proteção dos dados e da rede em si, focando-se em temas como a sua resiliência, a sua estrutura ou da deteção de intrusões.

De forma a garantir a proteção dos ICS, a arquitetura para a segurança deve começar logo nos alicerces do próprio sistema, por exemplo, na definição de pontos de estrangulamento de tráfego nas redes e na implementação nos pontos críticos de redundâncias e alternativas. Opções como as referidas anteriormente, irão permitir que uma falha em determinada localização ou equipamento da rede não coloque em risco o sistema como um todo, limitando as suas consequências a uma área local.

De seguida são apresentadas algumas das opções de segurança mais relevantes segundo Ackerman.

A. RESILIÊNCIA E REDUNDÂNCIA

A Disponibilidade é um dos 3 fatores da tríade de CIA (sendo os outros dois são a Confidencialidade e Integridade), sendo este o mais importante quando se aplica este conceito a um ICS. Uma vez que é essencial que os processos críticos sejam assegurados, deverão existir equipamentos que garantam a continuidade deste, sendo os equipamentos redundantes. Um exemplo típico de redundância ao nível das infraestruturas são as duplas fontes de alimentação ou a existência de mais de uma interface de rede (**Figura 8**).

Figura 8 - Equipamentos com opções redundantes
À esquerda observa-se uma fonte de alimentação dupla para um bastidor, garantindo que em caso de falha de um destes equipamentos, a alimentação elétrica é garantida. À direita, observa-se um PLC com redundância de portas SERIAL e de ETHERNET.

Além disso, os próprios sistemas devem ser resistentes a ataques, não apenas para não impedirem a penetração de um ataque, mas por conseguirem aguentar as suas consequências, tanto a nível de deteção como a limitar a extensão do mesmo. Desta forma, deve considerar-se que ambos estes conceitos estão ligados e é essencial que sejam implementados em conjunto.

B. FIREWALLS

É essencial, para a segmentação da rede, a existência de equipamentos que limitem o tráfego das redes, tanto seja entre pontos de rede, com base da sua origem/destino, quer seja por proteger *ports* dos equipamentos quer seja limitando a direção. Neste caso, esta função é assegurada pela Firewall.

Estas controlam o tráfego da rede dentro dos diversos níveis do ICS e também a gerir a entrada e saída da DMZ. Estas também devem procurar comportamento anómalos, buscando padrões e verificando assinaturas de *malware* conhecido.

C. MONITORIZAÇÃO E LOG

Para uma rede ICS ser adequadamente segmentada, os controlos de segurança devem ser distribuídos pelas diversas zonas como forma a reduzir o risco de comprometimento por parte de uma atacante, adicionando recursos de monitorização para aumentar a visibilidade da rede e das atividades dos *hosts* (Ackerman 2017). Segundo o mesmo autor, as duas maiores fontes destas informações são os *network packet* captures e a criação de *event logs*.

Os *network packet captures* têm como função fazer *sniffing* à rede. Para tal, estes softwares necessitam de verificar os pacotes que passam por determinado equipamento de rede, fazendo SPAN ou MIRROR a uma porta de um *switch* instalado num ponto nevrálgico da rede.

Sempre que as *firewalls*, os network *packet* captures ou qualquer outro software de monitorização dos sistemas e políticas detetam alguma atividade anómala, é gerado um Log. Este registo pode ser guardado no próprio *host* ou em alguma localização de rede, e a sua criação pode despoletar um *trigger* que avisa da sua ocorrência

D. INTRUSION DETECTION SYSTEM

Um *Intrusion Detection System* (IDS) é um dispositivo de hardware ou software que monitoriza as redes de um ICS, detetando atividades não padronizadas ou anómalas. Qualquer deteção

deve ser é registada (*Log*) e comunicada a um administrador do sistema (ou a um sistema centralizado de gestão de eventos).

E. PROTEÇÃO DE ENDPOINT

Os *host* são dos pontos com mais riscos associados para um ICS. Por este motivo, deve ser reduzida a "superfície" de ataque destes equipamentos como forma de reduzir as hipóteses de acesso aos níveis mais importantes do sistema. Para tal, devem ser desativados todos os serviços, aplicações e protocolos que não sejam necessários para a função destinada para o *host*. Por exemplo, caso não sejam utilizados protocolos como sendo telnet, SSH ou SNMP, estes devem ser desativados. Além desta medida, deverá também ser limitado os privilégios dos utilizadores, para o caso do acesso destes serem comprometidos.

Nos *hosts* deverá ser instalado software que os protejam, tanto de *malware* como de ações dos utilizadores. Os exemplos mais comuns destes são as aplicações anti-malware e as *Host-based firewalls*.

No primeiro caso, este software tem como função monitorizar passivamente os ficheiros utilizados pelo utilizador. Esta monitorização deve funcionar não apenas com os ficheiros acedidos no computador, como também com os que se encontram na memória e com os *rootkits*.

O software referido no segundo caso, tem um comportamento similar ao das *firewalls* referidas anteriormente, com a diferença de, em vez de monitorizarem troço de rede, vão monitorizar o *host*. Esta diferença concede um novo nível de proteção, ao permitir descentralizar a defesa da rede e acedendo às outras camadas da transferência de dados.

F. PERFIS DE UTILIZADORES

De forma a gerir melhor os privilégios dos utilizadores, devem ser criados perfis e grupos. A partir desta função, é possível definir qual o software e serviços que podem ser utilizados, devendo por defeito, serem todos os que não estão incluídos na *whitelist* bloqueados.

Uma vez que os ICS são em geral sistemas estáticos e com arquiteturas estáveis, a definição clara das permissões não é de difícil aplicação.

G. ATUALIZAÇÕES DE SEGURANÇA

Como em todos os softwares de IT, também os ICS podem sofrer de bugs em *firmware* e software, sendo necessário que sejam atualizados regularmente. Contudo, e conforme foi

referido anteriormente, os hardwares dos ICS nem sempre podem ser facilmente atualizados. Além desta dificuldade, principalmente ao nível da zona industrial, é necessário um especial cuidado com os dados externos introduzidos para as atualizações, podendo esta ação servir de porta de entrada para *malware*.

Outra dificuldade inerente das atualizações é o risco de incompatibilidade com os restantes equipamentos instalados, podendo esta ação afetar a disponibilidade, não apenas do equipamento que foi atualizado, como do restante processo.

H. VALIDAÇÃO E ACESSOS

A grande parte dos ataques informáticos tem como alvo as vulnerabilidades das aplicações. Assim, é essencial que existam critérios na seleção do software a instalar nos diversos equipamentos. Um dos meios mais gerais para a execução de ataques é o uso dos INPUTS dos softwares, correndo scripts e comandos maliciosos que poderão por em causa o sistema. Para tal, as aplicações e os *host* devem ter mecanismos para verificação dos inputs, devendo para tal existir uma cadeia de alarmes e bloqueios caso alguma anomalia seja detetada.

Como foi referido anteriormente, para o acesso e uso de aplicações, deverão ser utilizados mecanismos de autenticação. Muitas vezes nos equipamentos dos ICS, os *firmware* tem fracos mecânicos de autenticação, ou as vulnerabilidades tornam-se conhecidas e bastante divulgadas. Por este motivo, deverão ser, sempre que possível, níveis adicionais de autenticação. As falhas de autenticação podem permitir não apenas acessos a utilizadores não autorizados, como também, o aumento das autorizações detidas por um utilizador.

I. VULNERABILIDADES DE SESSÃO

Os dados transmitidos pelas redes de computadores estão sempre vulneráveis a serem intercetados. Ataques como os *Session Hijacking, Sesson Replay* ou os *Man-in-the-middle*, permitem que um utilizador aceda aos dados transmitidos, podendo não só impedir que estes façam o seu trajeto normal, mas principalmente, aceder aos mesmo e proceder à alteração dos dados.

Esta vulnerabilidade é tão válida para os sistemas tradicionais como para os ICS, podendo neste caso, além de aceder aos dados, manipulá-los de forma a dar informações erradas aos controladores, PLC e autómatos, o que trás consequências potencialmente desastrosas.

De forma a serem prevenidos estes ataques, deverão ser implementadas técnicas de gestão de sessões eficientes como sendo a adição de chaves aleatórias, *tracking* de sessão e finalização de sessão eficientes.

J. SEPARAÇÃO DA REDE ICS E IT

Conforme já foi referido anteriormente neste trabalho, ao nível de arquitetura dos sistemas da organização, um dos pontos mais importantes é a separação da rede do ICS e IT. Esta questão é muito importante devido a exposição que normalmente a rede IT está sujeita, sendo possível assim, salvaguardar os componentes críticos do ICS, uma vez que, mesmo que as áreas de negócios sejam atacada e fiquem offline, a operação fica salvaguardada.

Contudo, esta decisão nem sempre é facilmente aceite pelos decisores de topo das organizações, uma vez que esta opção acarreta normalmente custos adicionais, visto que para funcionar com o máximo nível de segurança, todo o sistema deve ser paralelo ao de IT, nomeadamente, infraestrutura de rede, servidores e hosts.

2.4. COMUNICAÇÕES

2.4.1. MEIOS DE TRANSMISSÃO

Conforme foi referido anteriormente, os primeiros ICS eram apenas controlados por *relays*, contactores, temporizadores e contactos mecânicos/eletromagnéticos que tinham como base de funcionamento sistemas elétricos, estando muito limitados espacialmente e não permitindo uma grande distancia entre os seus componentes. Na maioria dos casos, eram utilizados os sistemas telefónicos, não apenas para o contacto direto com os operadores nas diversas estações, mas também para a transmissão de dados analógicos.

De acordo com o descrito pela SANS em (Hayden, Assante e Conway 2014) sobre os primeiros ICS utilizados, a grande maioria destas instalações, utilizaram as redes existentes das operadoras, sendo apenas conseguido alcançar velocidades de cerca de 300 bits/segundo. Esta solução, além de acarretar custos operacionais, criava dependências de terceiros, ao mesmo tempo que tinha problemas de fiabilidade. Desta forma, algumas organizações optaram por utilizar infraestruturas próprias, através da passagem de cabos

elétricos e de telecomunicação entre as suas instalações. Contudo, a melhoria dos serviços não foi necessariamente alcançada.

A opção para a resolução dos problemas referidos, passou em muitas situações, pela implementação de sistemas de comunicação sem fio, nomeadamente por rádio e micro-ondas. Esta solução foi gradualmente mais utilizada, à medida que estas tecnologias se tornaram mais modernas, traduzindo-se na redução dos preços dos equipamentos e no aumento da fiabilidade e da largura de banda como diz (Hayden, Assante e Conway 2014).

A utilização de sistemas de telecomunicação moveis abriu um novo capítulo na comunicação sem fios. Atualmente, é possível através das redes 2G, 3G e 4G aceder a uma rede desde que a instalação área tenha cobertura de rede móvel. Esta questão faz com que os custos sejam drasticamente reduzidos aquando da conexão de instalações espacialmente distanciadas. Além do uso de redes móveis, a criação de links e bridges ligados por antenas direcionais, permitiu a criação de comunicações muito potente que, conforme se pode ver por exemplo no catálogo da Ubiquiti (Ubiquiti s.d.), permitem um alcance superior a 300 km com taxas de transmissão superiores a 1,2 Gbps.

Ao nível interno das instalações, também houve evoluções na comunicação entre os diversos equipamentos. Os dois melhores exemplo de tecnologias que foram amplamente disseminadas foram o Wifi e o Bluetooth. Ambas são similares na fácil ligação de componentes, tem alcance no interior de instalações com até cerca de 30 metros, baixo consumo de energia e com possibilidade da ligação a diversos equipamentos. Contudo, existem algumas diferenças ao nível da segurança e nas taxas de transmissão de dados, sendo em ambos os casos favoráveis para o Wifi (Goldsmith 2005).

Ao mesmo tempo que as redes sem fio evoluíam, também as redes com fios evoluíam, nomeadamente com a passagem de analógico para digital. Estes sistemas deixaram de ser transmitidos por cabos elétricos para cabos dedicados à passagem de dados, como sendo os UTP ou *Twisted-pair* (cabo trançado, tradicionalmente chamado de cabos de rede) e por cabos coaxiais (Grami 2016). Ambos os cabos, permitiram melhorar as comunicações, tendo, contudo, um problema comum, a perda de sinal sobre grandes distâncias, obrigando a instalação de repetidores ao longo do trajeto. A solução mais eficiente atualmente implementada para drasticamente reduzir o problema da distância, foi a escolha pela fibra ótica.

Tendo por base autores como Grami (Grami 2016), Temprana (Temprana, et al. 2015) e Curran e Shirk (Curran e Shirk 2015) são apresentadas de seguida algumas características de cada uma destas três tecnologias.

a) Cabo UTP

Este tipo de cabo foi inicialmente concebido para voz, sendo posteriormente melhorado e aperfeiçoado para a transmissão de dados. Atualmente, este cabo é geralmente composto por 4 pares de condutores de cobre, isolados entre si, e por mecanismo de isolamento e proteção mecânica opcionais que vão variar a categoria (e qualidade) do cabo. Os pares são estreitamente torcidos como forma de reduzir a suscetibilidade à diafonia (passagem de sinais elétricos entre fios adjacentes) e ao ruído, permitindo uma ampla game de frequências.

O aumento do diâmetro dos condutores permite atenuar estes problemas, havendo, contudo, uma diminuição da largura de banda com o aumento da distância, obrigando a implementação de repetidores a cada 2km. Para distâncias curtas, os cabos UTP permitem o uso de uma grande largura de banda, ao mesmo tempo que permitem uma boa performance ao nível da diafonia e do ruído.

Atualmente, estes cabos são a base da comunicação das LAN Ethernet, tando em IT como nos ambientes industriais com ICS, tendo diferentes larguras de banda, apresentando-se em diversas Categorias (entre Cat1 a 0,4 MHz e Cat8.2 a 2000 MHz), variando com diversas características construtivas (diâmetros dos condutores, isolamentos, blindagem ou o *foil*).

b) Cabo Coaxial

Este cabo não é uma invenção recente, tendo sido criado em 1880 para a transmissão de sinais de rádio. Este é composto por um condutor interno de fio de cobre rígido e um condutor externo, normalmente uma malha metálica. Estes são separados por material isolante dielétrico nas diversas camadas, por uma camada de folha metálica isolante e por material polímero para proteção mecânica.

Ao contrário dos anteriores, este tem uma melhor resistência às interferências, oferecendo larguras de banda muito maiores, mas tem uma atenuação do sinal maior, traduzindo-se numa perda de sinal maior para distâncias superiores, obrigando a um uso maior de repetidores.

Em situações específicas nas instalações industriais, a construção dos cabos coaxiais tornam-no vantajoso face aos restantes, uma vez que, a sua blindagem permite reduzir as interferências e o ruído. Como exemplo desta situação temos a existência de campos

eletromagnéticos fortes ou a passagem junto a cabos elétricos e das fontes de geração de energia.

c) Fibra Ótica

A fibra ótica é atualmente a melhor solução para a transmissão digital de dados com fio. Esta, ao contrário das anteriores, não foi criada para a transmissão de sinais elétricos digitais, mas sim de luz. Esta funciona através da passagem desta através do Core, ou seja, um orifício num minúsculo tubo de vidro com um baixo nível de refração. Este é revestido por diversas camadas de materiais, que conferem resistência mecânica ao cabo de fibra. Dependendo das características, este é composto por um determinado número de pares, sendo estes agrupados e separados em material protetor. Este pode ser mais ou menos flexível dependendo do número de pares e do revestimento.

Em termos de funcionamento, este funciona através da emissão de um sinal luminoso no orifício de entrada do cabo, designado por *core*, sendo que esta luz "encaminha" através do choque das paredes do tubo de vidro. Os dados são transmitidos através da variação da intensidade da fonte de luz, sendo o final do cabo detetado por um fotodíodo que a converte em binário interpretável pela máquina.

O uso desta energia em vez da elétrica faz com que a comunicação, através de fibra ótica, seja virtualmente imune a interferências eletromagnéticas e que tenha baixas perdas de transmissão, por outro lado, esta tem potencialmente uma enorme largura de banda e uma capacidade de transmissão a centenas de quilómetros de distância, apenas com a necessidade de algumas repetições e regenerações. Exemplo desta capacidade, foi a possibilidade do envio de dados entre dois pontos distanciados de 1020 km com apenas a necessidade de proceder à regeneração do sinal (Temprana, et al. 2015).

Atualmente existem dois tipos de fibra ótica, o monomodo e o multimodo. As do primeiro tipo, tem um *core* mais estreito e utilizam apenas um feixe de luz, obtendo desta forma um maior alcance sem a necessidade de tanta repetição, conseguindo uma menor taxa de perda e de dispersão. Estas são mais aconselhadas para distâncias maiores, tendo como contra o preço mais elevado (Curran e Shirk 2015).

Por seu lado, as de multimodo, têm um *core* com um diâmetro maior, o que permite a emissão de diversos feixes de luz, ou seja, diversos modos, sendo cada um "caminho" conhecido pelo recetor. Esta é a melhor opção para curtas e médias distâncias, uma vez que largura de banda aumenta ao serem emitidos mais dados ao mesmo tempo. Contudo, com o aumento da

distância a percorrer, a taxa de erros também aumenta, tanto devido à chegada de demasiados feixes praticamente ao mesmo tempo, com tempos de chegada iguais em mais que um modo. Outra grande vantagem deste são os custos inferiores desta também é inferior às anteriores (Curran e Shirk 2015).

A diminuição dos custos com esta tecnologia fez com que as aplicações de fibra ótica aumentassem, passando de estar associado apenas *backbone* para grandes redes de telecomunicações para método de ligação entre infraestruturas de rede dentro de uma instalação ou a conexão de componentes em aeronáutica.

2.4.2. PROTOCOLOS DE COMUNICAÇÃO

A evolução e digitalização dos ICS fez com que desde cedo tivessem de ser utilizados protocolos de comunicação entre componentes, existindo mais de uma centena, sendo que a maioria destes são de proprietário. Esta grande quantidade de "linguagens" utilizadas pelos equipamentos de diferentes marcas e gerações, faz com que a comunicação entre estes seja um desafio (Hayden, Assante e Conway 2014).

De seguida são apresentados dois protocolos, o Modbus TCP/IP e o PROFINET. O primeiro foi escolhido por ser um dos que alcançou maior sucesso, sendo ainda hoje um dos mais utilizados. O segundo foi escolhido não só por se estar a tornar um dos mais populares do mundo, mas por também ter diversas características de segurança que o tornam bastante mais seguro e resiliente.

a) MODBUS

Enquanto o Modbus por Serial Line foi concebido para utilização ponto-a-ponto (master/slave), normalmente entre um PLC e uma HMI, o Modbus TCP/IP foi desenvolvido para permitir diversos equipamentos (clientes) conectados a um ou mais servidores. Ao contrário da sua antecessora, esta não necessitaria de N conexões para cada um dos equipamentos conectados, utilizando-se um link partilhado (normalmente por UTP) traduzindo-se na simplificação da infraestrutura, diminuindo preços e facilitando a sua instalação e manutenção (Thomas 2008).

Para a utilização da lógica de multiligações, a Modicon, detentora à data do protocolo, decidiu adotar as redes Ethernet através de IP. Conforme se pode ver na tabela seguinte e segundo o mesmo autor (Thomas 2008), a estrutura deste modelo foi adaptada, utilizando-se principalmente 5 camadas em vez das 7 convencionais do Modelo OSI.

Camada	Função OSI	Função Modbus
5, 6, 7	Aplicacional	Protocolo de aplicações Modbus
4	Transporte	Protocolo de Transmissão Modbus
3	Rede	Protocolo de Internet
2	Data Link	IEEE 802.3
1	Física	IEEE 802.3

Na **Figura 9** podemos observar o diagrama do funcionamento do Modbus TCP/IP, sendo percetível um BUS central baseado em IP por onde são transmitidas as comunicações dos diversos componentes. A este são conectados os diversos Clientes, como sendo PLC ou HMI e um ou mais servidores, sendo por sua vez utilizadas ligações MODBUS SERIAL para conectar outros equipamentos (Clientes e/ou Servidores), segundo (Thomas 2008).

A tipologia de comunicação utilizada permite vantagens, tais como a possibilidade de existirem diversos servidores a conectarem-se a mais equipamentos, não havendo a necessidade de modificação física da rede para alteração das conexões entre estes. Além disso, esta possibilidade permite uma capacidade de adaptação e resiliência superior, como diz (Thomas 2008).

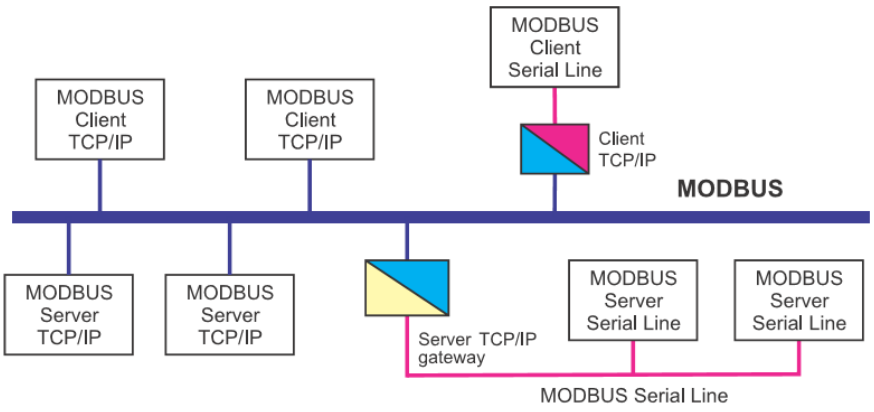


Figura 9 - Diagrama do funcionamento do Modbus
Na figura é representado o modelo de funcionamento do Modbus TCP/IP, utilizando a arquitetura Cliente/Servidor (Thomas 2008).

Na **Figura 10** (Thomas 2008) observa-se como é formado o Modbus TCP/IP ADU, ou seja, o formato da mensagem enviada através deste protocolo. Isto é possível através do uso de gateways com IP para ligação dos equipamentos ligados por serial, ou seja, as mensagens são enviadas entre os gateways, sendo depois desencapsuladas e transmitidas por Serial. De forma a ser possível, a esta comunicação é adicionado um Modbus Application Protocol (MBAP), composto por 4 partes:

a) Transaction Identifier – É utilizado pelo cliente para identificar qual o número do *request* ao qual a mensagem pertence, permitindo assim acompanhar e agrupar os pacotes. Desta forma, o servidor utiliza o mesmo número na sua resposta. A existência deste campo permite também ao cliente enviar diversas mensagens sem esperar por resposta anteriores;
b) Protocol Identifier – Este header permite a utilização de diversos protocolos, sendo neste caso utilizado 00, equivalendo ao Modbus;
c) Lenght – Identifica o tamanho total da mensagem;
d) Unit Identifier – Identifica o endereço original Serial do Slave.

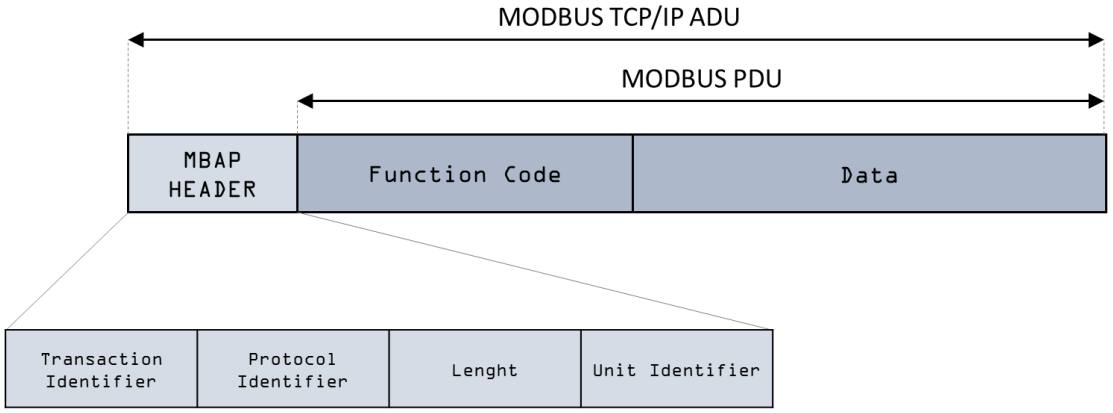


Figura 10 - Formato do pacote do Modbus TCP/IP
Na figura é representado o pacote de dados do Modbus TCP/IP e em pormenor do MBAP HEADER (Thomas 2008).

b) PROFINET

Este protocolo tem como base o PROFIBUS, um dos descendentes do MODBUS. A grande diferença deste é o uso de Ethernet em vez de serial fieldbus como os seus antecessores. Em termos gerais, os conceitos do funcionamento deste é semelhante aos explicados

	PROFIBUS	PROFINET
Organization	PROFIBUS & PROFINET International	
Hardware definition	GSD files	
Application profiles	Same	
Physical layer	RS-485	Ethernet
Speed	12 Mbit/s	1 Gbit/s or 100 Mbit/s
Telegram	244 bytes	1440 bytes (cyclic)[1]
Address space	126	unlimited
Technology	master/slave	provider/consumer
Wireless	Possible[2]	IEEE 802.11, 15.1
Machine-to-machine	No	Yes

[1] with multiple telegrams: up to 232-65 (acyclic)
[2] not in specification, but solutions available

Figura 11 - Comparação entre PROFIBUS e PROFINET
Na figura são apresentadas as diferenças das características do PROFIBUS e do PROFINET (adaptado de Ayllon 2016).

anteriormente. De seguida é apresentada a **Figura 11** com algumas características deste e do seu antecessor PROFIBUS.

Conforme se pode ver na **Figura 11**, algumas das principais vantagens do uso de PROFINET prendem-se com o aumento da velocidade, do tamanho das mensagens e na capacidade dos diversos equipamentos poderem falar entre si, sem que haja sempre a necessidade de intervenção do servidor. A esta característica é chamada de *provider/consumer* (Ayllon 2016).

Este modelo, ao permitir o uso de comunicações Full-Duplex (uma característica atual de Ethernet) através do uso de switchs, consegue praticamente eliminar a colisão de pacotes, permitindo assim o aumento da estabilidade do sistema, essencial em sistemas críticos.

Conforme já foi referido, os ICS mais antigos tinham algumas falhas de segurança, uma vez que os próprios equipamentos utilizados não tinham sido concebidos com essas preocupações como prioritárias. Atualmente, protocolos como o PROFINET, já foram projetados com estas preocupações, bem como as restantes tecnologias e protocolos também o fizeram. Uma das características de ETHERNET transposta para PROFINET que permite um aumento significativo de segurança é todos os componentes comunicarem por MAC Address.

Quando o sistema em PROFINET é inicializado, todos os equipamentos são “apresentados” ao IO-Controller, sendo só atribuído o seu IP após a verificação do seu MAC. Para tal é utilizada outra característica de ETHERNET, o DHCP. Na imagem seguinte (**Figura 12**) é possível perceber-se o processo de atribuição de endereço (PROFIBUS, Nutzerorganisation; 2014).

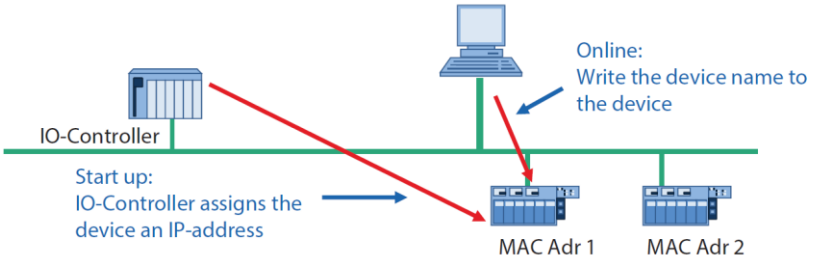


Figura 12 - Processo de atribuição de endereço

Na figura está esquematizado o processo de atribuição de endereço de um equipamento em PROFINET. Neste exemplo, após a inicialização do sistema, o IO-Controller atribui um IP tendo por base o MAC Address, sendo depois a supervisão do sistema, atribui-lhe um nome pelo qual vai ser reconhecido dentro da rede (PROFIBUS, Nutzerorganisation; 2014).

De forma a aumentar a segurança do processo e do sistema em si, o PROFINET tem construído de raiz sistemas que permitem a monitorização da rede, detetando ao nível de hardware, alterações da rede, acionando assim um conjunto de alarmes e processo de resposta em caso de alguma variação (PROFIBUS, Nutzerorganisation; 2014).

Com a chegada da Industria 4.0 e o IoT, o protocolo PROFINET também começou a incorporar algumas características necessárias mas que não se traduzem num aumento da sua segurança, antes pelo contrário. Uma destas é a capacidade de interação com os standards das comunicações Wi-Fi e Bluetooth, abrindo assim a oportunidade ao uso de mais soluções sem fios, permitindo também aos fabricantes de equipamento, a possibilidade de maiores interações com as suas próprias marcas (Knapp e Langill 2015, Ayllon 2016). Outra é a possibilidade de integração com a Internet, sendo possível a ligação ao ICS através do exterior desta. Esta possibilidade depende da contada dos decisores das organizações, sendo possível em teoria, o total controlo pelo exterior.

Esta questão torna imperativo que sejam tomadas diversas medidas para minimização do risco, principalmente, analisar a necessidade de acesso pelo exterior e quais os privilégios a disponibilizar.

2.5. EXEMPLO DE UM ATAQUE: STUXNET

Em 2011, a temática da Cibersegurança nos sistemas industriais ganhou uma nova relevância a nível internacional, a partir da revelação da existência do *malware* Stuxnet. Este vírus informático ganhou a sua notoriedade por possivelmente se ter tornado, aquando a sua revelação, na mais poderosa ciberarma usada até então por uma nação com outra.

Segundo o site Techtarget (Rouse 2017) podemos definir um worm informático como um tipo de software malicioso que tem como função principal a "infeção" de outros computadores enquanto este se mantém ativo nos sistemas já infetados. Ou seja, este vírus é capaz de se auto-replicar, atuando ao nível do sistema operativo e sendo, na maioria dos casos, invisível para o utilizador. No caso o Stuxnet, o seu intuito não era a infeção generalizada de sistemas, mas sim, a infeção seletiva de sistemas ICS, equipados com determinados componentes (Matrosov, et al. 2010). Assim, pode-se definir como o derradeiro objetivo deste *malware*, o ataque das instalações Iranianas de enriquecimento de urânio através da reprogramação dos PLC das centrifugadoras aí existentes (Falliere, Murchu e Chien 2011).

Esta "missão" foi desempenhada como grande sucesso pelo Stuxnet, tendo em setembro de 2010, infetado de forma autónoma mais de 100.000 hosts em todo o mundo, sendo que na maioria das ocorrências deram-se em instalações iranianas relacionadas com o seu desenvolvimento nuclear (Falliere, Murchu e Chien 2011).

No decorrer deste capítulo irá ser explicada a forma o Stuxnet como se disseminou, a sua mecânica e os seus impactos no mundo atual.

2.5.1. TIMELINE

De acordo com Falliere (Falliere, Murchu e Chien 2011) a descoberta e a compreensão do Stuxnet deu-se ao longo de pouco mais de 2 anos. Na tabela (**Figura 13**) seguinte pode ver-se a evolução cronológica por trás da revelação pública deste malware.

Segundo os autores, as primeiras amostras do Stuxnet só foram analisadas em junho de 2009, sendo esta uma versão inicial. Embora este já usasse alguns Zero Days, ainda não utilizava todas as ferramentas que as versões mais avançadas têm a sua disposição. Conforme se pode ler, apenas em janeiro de 2010, descobriu-se o uso de certificados fidedignos para a autenticação ilícita do próprio *malware*, sendo que até Julho do mesmo ano, se identifica o

uso de outros 2 certificados nessa mesma altura que se associa este código aos autómatos da Siemens.
Uma das provas do avanço deste *malware*, foi que durante os 2 anos em que foi acompanhado e estudado, foram detetados diversos *Zero Days* que foram sendo aproveitados pelas diversas versões do Stuxnet. Conforme referido anteriormente neste trabalho, o afastamento dos ICS das redes IT e a não atualização recorrente dos seus componentes, fez com que mesmo após o conhecimento destas vulnerabilidades e dos respetivos lançamentos de atualizações, estes sistemas continuassem vulneráveis.

Em Setembro de 2010, foi apresentado o primeiro relatório exaustivo sobre o Stuxnet à comunidade de especialistas, sendo desde então, amplamente divulgado pelo público em geral, sendo inclusivo, realizados diversos documentários e filmes.

2.5.2. MÉTODO

A complexidade do Stuxnet atingiu um nível extremamente elevado, sendo utilizado neste código um conjunto de estratégias muito específicas e direcionadas. Segundo o próprio relatório da Sysmantec, este *malware* foi "*one of the most complex threats we have analyzed*". Esta complexidade deveu-se a diversos fatores, nomeadamente, devido ao uso de 4 *Zero Days* diferentes (vulnerabilidade anteriormente desconhecidas) e da sua especificidade para atacar ICS (Falliere, Murchu e Chien 2011).

Conforme foi falado anteriormente, estes sistemas por estarem isolados das redes IT das organizações, são teoricamente mais seguros. Esta situação fez com que a intrusão pelo Stuxnet demorasse a ser identificada, conseguindo, entretanto, manipular o funcionamento das centrifugadoras de enriquecimento de urânio.

Segundo os autores do relatório da Sysmantec que estudaram exaustivamente este *malware*, para conseguir atingir os seus objetivos, este usa uma grande variedade de ataque e de métodos de evasão, nomeadamente:

- *Zero-Days;*

- Windows *rootkit*;

- PLC *rootkits* (registado pela primeira na história da computação);

- Técnicas de evasão de antivírus (desligar de serviços, *whitelist*, ocultação de processos…)

W32.Stuxnet Timeline	
Date	**Event**
November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.
April, 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June, 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.
March, 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.
July 17, 2010	Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

Figura 13 - Stuxnet Timeline
Cronologia dos eventos relacionados com a investigação do Stuxnet (Falliere, Murchu e Chien 2011).

- Processos complexos de injeção e *hooking*;

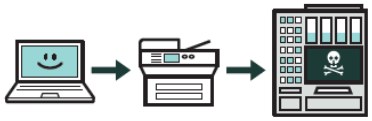
- Rotinas de injeções de rede;

- Atualizações por *peer-to-peer;*

- *Hijack* e controlo de interfaces.

Com base no esquema de Kushner (Kushner 2013) e dos dados do relatório anteriormente referido (Falliere, Murchu e Chien 2011), foi construída a tabela seguinte onde estão sistematizadas as diversas fases do ataque deste *malware*:

Fase	Descrição
Reconhecimento 	A primeira fase da conceção deste *malware* foi a necessidade de conhecimento muito exaustivo do processo e dos equipamentos existentes dentro da instalação. De acordo com alguma especulação, diversos métodos de espionagem foram utilizados nesta fase, nomeadamente a existência de versões anteriores do Stuxnet.
Criação Stuxnet 	Com base nas informações disponíveis, houve necessidade de construção de um "*mirror*" da instalação alvo, como forma de testar e desenvolver o código. De forma a garantir o sucesso, foi necessário "adquirir" certificados legítimos de duas empresas distintas, como forma de assinar digitalmente os drivers de hardware utilizadas no ataque. Para o início da propagação deste, foi utilizado um dispositivo USB que terá sido introduzido manualmente na rede da instalação por alguém com credenciais de acesso.
Infeção Inicial 	Na fase seguinte, através de diversos *Zero Days*, o vírus tenta começar a aceder a todas as máquinas ligadas na rede com o sistema operativo Microsoft Windows. Para esta propagação, o vírus utiliza os certificados válidos adquiridos, permitindo-lhe que seja este instalado nos sistemas de forma fidedigna e fazendo *bypase* aos sistemas de segurança instalados.
Pesquisa 	Uma vez dentro da rede, o Stuxnet vai procurar se o *host* faz parte de um ICS com componentes Siemens. Através dos dados recolhidos anteriormente, vai procurar o software de programação e controlo Step 7, utilizado para programar os PLC alvo.
Calling Home 	Caso o Stuxnet não esteja a infetar uma instalação pretendida, este não faz nada. Contudo, caso tenha "encontrado um alvo", o vírus, através de uma ligação à internet, contacta um servidor remoto de onde, através de P2P, vai atualizar-se para a sua versão mais recente. Através deste método, é expectável que o Stuxnet também enviasse informações de volta ao seu criador, mantendo os seus progressos monitorizados.
Propagação	A propagação é feita através da rede através de uma vulnerabilidade da partilha de impressoras do SO Windows. Uma vez que muitos dos equipamentos e computadores usados pelo ICS



não estão ligados à rede, o Stuxnet usava também os dispositivos USB usados internamente nas operações da instalação para chegara estes.

Sempre que um computador infetado comunicava com um PLC (por exemplo para manutenção ou para alteração de parâmetros) este copiava-se para o equipamento, alterando o seu código e ocultando a sua presença.

Controlo

Embora este vírus tivesse capacidade de comunicar para o exterior, quando estava na área isolado dos ICS, tinha de ser autónomo, capaz de sabotar os equipamentos ao mesmo tempo que ocultava a sua presença.

Para tal, o vírus mantinha-se "adormecido" por 30 dias, estando nesse período a adquirir informações das operações, estudando as mesmas e criando outputs falsos que seriam posteriormente enviados para as interfaces.

Desta forma, a "normal" operação iria ser sempre vista pelos operadores do sistema, havendo apenas alarme quando os equipamentos deixam de trabalhar.

Seek and Destroy

Uma vez passando o tempo de "estudo" do funcionamento do processo, o vírus começava gradualmente a alterar as parametrizações do PLC, fazendo com que as centrifugadoras deixassem o seu normal funcionamento, entrando em regimes prejudiciais para as mesmas.

Além destas terem sofrido um desgaste muito superior ao esperado, também o resultado do seu trabalho foi reduzido, traduzindo-se numa diminuição na capacidade de enriquecimento de urânio.

2.5.3. CONSEQUÊNCIAS

A criação deste *malware* requereu inúmeras horas e recursos para o seu desenvolvimento. Se considerarmos que além desta questão, foi necessário um grande investimento na sua distribuição, na adquisição dos certificados e na compra de *Zero Days*, estamos perante um marco na história dos *malware* e da *cyberwar* (Matrosov, et al. 2010). Esta questão faz com que as consequências deste ataque fossem para além dos resultados diretamente conseguidos, ou seja, a destruição das centrifugadoras (Kushner 2013).

Embora o ataque tenha levado a destruição de quase 1.000 das 9.000 destes equipamentos, a confusão causada dentro da própria estrutura do programa nuclear iraniana teve igualmente

repercussões devastadoras, levando a um atraso significativo nas operações de enriquecimento (Dine 2016).

Contudo, quando o Stuxnet se torna público e as vulnerabilidades que permitem a sua propagação começam a ser corrigidas através de atualizações, a sua existência torna-se praticamente obsoleta. Além disso, a intervenção dos técnicos do programa nuclear e os recursos investidos, fizeram com que estes equipamentos fossem rapidamente substituídos, recuperando facilmente o controlo das operações a quando da sua descoberta (Falliere, Murchu e Chien 2011).

A maior lição que se pode tirar do Stuxnet, não são os objetivos alcançados, mas sim a sua própria existência. Conforme foi explicado anteriormente, os recursos humanos e financeiros necessários para a sua criação são tão elevados que não estão disponíveis para hackers individuais, grupos de hackers, organizações criminosas ou mesmo a generalidade das nações. Desta forma, a generalidade dos autores referidos anteriormente, acreditam que tenham estado envolvidos na sua criação e distribuição, uma ou mais nações poderosas. Contudo não passa de uma especulação.

Além da questão dos recursos para o seu desenvolvimento, é essencial levar em consideração que o vírus foi introduzido manualmente numa instalação secreta, fortemente guardada e com procedimentos para salvaguardar a sua cibersegurança. O uso de uma arma desta natureza numa instalação tão protegida é sem dúvida um dos maiores feitos do Stuxnet e levanta fortes preocupações internacionais sobre o uso destas armas altamente avançadas (Dine 2016).

Atualmente, existe um novo desafio pós-Stuxnet, a divulgação do código utilizado. Este é hoje em dia vendido como *open-source* no mercado negro. O estudo deste vírus, mostrou que o ataque a ICS pode efetivamente causar danos no mundo real, tornando-se uma arma apetecível por quem pretenda disseminar este tipo de ataques. Assim, usando este código como *template*, é possível a uma organização com recursos (contudo uma fração do custo total do seu desenvolvimento) criar uma nova arma, tirando partido de ultras vulnerabilidades ou das mesmas, em sistemas ainda não utilizados (Dine 2016).

2.6. AVALIAÇÃO DE CIBERSEGURANÇA

2.6.1. AWWA E O GUIA

A Amercican Water Works Association (AWWA) é uma associação internacional sem fins lucrativos que tem como objetivo o estudo e educação das matérias relacionadas com a Gestão da Água. Esta foi fundada em 1881, sendo atualmente a maior do mundo no seu sector, contando com mais 51.000 membros (AWWA 2019).

Uma vez que se dedica a uma visão holística da gestão deste sector crítico, os seus membros representam um grande espectro da sociedade, como sendo entidades de sector público e privado, gestão de água para consumo humano e águas residuais, juristas e advogados ambientais, cientistas, académicos, associações e grupos civis, fabricantes de tecnologias, entre outros (AWWA 2019).

Uma vez que esta associação está intimamente relacionada com a pesquisa para a proteção da água e na garantia da sua qualidade e acesso, é natural que tenha focado a sua atenção nos assuntos relacionados com os ICS, nomeadamente a sua proteção.

Desta forma, surge em 2014 a primeira versão do "*Water Sector Cybersecurity Risk Managment Guidance*", tendo sido lançada em Abril de 2019 a sua 3ª edição.

De forma a conseguir a adoção dos conceitos de cibersegurança a um sector crítico, a AWWA iniciou em Fevereiro de 2013 o projeto de criar um guia para auxiliar a implementação deste nos ICS do sector (West Yost Associates 2019).

Para tal, foi elaborado um estudo detalhado, tendo por base o "Cybersecurity Framework" da organização americana National Institute of Standards and Technology (NIST). Este é um documento de referência a nível mundial, onde se inclui conjuntos de normas, metodologias e procedimentos que permitem o alinhamento entre as políticas, a tecnologia e as organizações na procura de redução dos riscos relacionados com a cibersegurança. Assim foi criado o Water Sector Cybersecurity Risk Management Guidance (AWWA Guidance), com o intuito de ser uma ferramenta para o apoio dos gestores das entidades gestoras do sector da Água (West Yost Associates 2019).

Pela análise do Guia (West Yost Associates, 2019), podemos considerar que esta é caracterizada por ter uma metodologia consistente para a identificação de fragilidades e a

recomendação de ações para a redução das vulnerabilidades para o caso de ciberataques, tendo por base as recomendações das normas ANSI/AWWA "G430: Security Practices for Operations and Management" e "EO 13636". Assim, foi criada uma lista de recomendações para aumentar a cibersegurança das organizações do sector e uma ferramenta online para a sua avaliação.

Além do apoio aos responsáveis pela cibersegurança nas organizações, este tem também o intuito do *call to action* de toda a organização, sendo transversal desde os seus trabalhadores e áreas, dando especial atenção ao papel dos gestores de topo.

Deve ser destacado que neste documento é possível também consultar-se uma ligação entre as diversas recomendações e os requisitos das normas em vigor (aplicável aos EUA), bem como a sugestão de diversas medidas de controlo.

Para a criação das questões apresentadas neste trabalho, foram analisadas cada uma das recomendações presentes deste guia, tendo-se posteriormente gerado o "QUESTIONÁRIO SOBRE PRÁTICAS DE CIBERSEGURANÇA NOS ICS" (**Anexo I**). De um modo geral, estas questões apenas por sofreram pequenas alterações e adaptações.

A secção "7 - Data Security" foi retirado do questionário, uma vez que, as questões relacionadas os Dados Pessoais e com a Arquitetura e Segurança das Redes e Sistemas de Informação que os utilizam, já estão muito bem definidos pelo Regulamento (UE) 2016/679 e pela Resolução do Conselho de Ministros n.º 41/2018.

De seguida é apresentada a tabela com sintetização das questões utilizadas:

Sessão	Quantidade
Governação e Gestão do Risco	5
Continuidade de negócio e recuperação de desastres	4
Endurecimento dos Servidores e das Workstation	7
Controlo de Acessos	11
Segurança das Aplicações	6
Encriptação	5
Arquitetura, Telecomunicações e Segurança da Rede	9
Segurança Física dos ICS	4
Acordos com entidades externas	3
Segurança da Operação	2
Engenharia Orientada para a Cibersegurança	2
Educação	7
Papel dos Trabalhadores	2
Total	76

2.6.2. TECNOLOGIAS DE SUPORTE À PLATAFORMA

Para o desenvolvimento desta plataforma, optou-se por utilizar 4 tecnologias, sendo estas direcionadas para a produção de conteúdos nas diversas camadas abordadas, nomeadamente a de Apresentação, a de Lógica e a de Dados. Tendo por base a obra de Robin Nixon (Nixon 2012), são apresentadas de seguida estas 4 tecnologias:

A. HTML

A *Hyper Text Markup Language* (HTML) surge nos anos 80 como forma de partilha de informação no mundo académico. Baseou-se no uso de etiquetas para a formatação dos conteúdos tendo por de trás a lógica de cliente-servidor, passando a utilizar browsers para aceder a repositórios e descarregar os conteúdos solicitados. É ainda hoje a base das páginas de Internet, servindo de plataforma a outras tecnologias, tendo sido gradualmente atualizado como forma a responder aos constantes desafios e avanças tecnológicos.

B. CSS

O *Cascading Style Sheets* (CSS) é uma linguagem criada para ser utilizada junto de conteúdos HTML. Esta tem como função a definição de estilos a serem utilizados, permitindo a separação deste do restante conteúdo. Esta funcionalidade ganha ainda mais relevância com a possibilidade de links para fora da própria página, facilitando a troca de formatações, bem como a sua reutilização e o uso em múltiplos projetos.

C. PHP

Criado em 1994, esta linguagem script gratuita foi desenvolvida para funcionar do lado do servidor, sendo esta embutida no HTML de uma determinada página. Esta permite a geração de conteúdos dinâmicos, sendo disponibilizados apenas os dados necessários para os request efetuados, sendo então apresentados ao utilizador.

D. MySQL

O MySQL foi criado nos meados dos anos 90, sendo um dos primeiros Open-Source de *Relational Database Management System* (RDMS) a ser criado. Este tem como base a *Structured Query Language* (SQL), tendo sido adicionada a esta, uma camada de interface que permite entre outras coisas, o controlo das bases de dados e a conectividade com outras linguagens e ferramentas, por exemplo PHP.

CAPÍTULO 3

ARQUITETURA DO SISTEMA

3.1. VISÃO GERAL

Para a implementação desta plataforma, foi utilizado o modelo de Cliente-Servidor através da Internet de forma a criar uma aplicação distribuída. Assim, os dados e a aplicação estão alojados num servidor online, sendo o acesso a este possível através de qualquer browser com acesso à internet.

Este conceito baseia-se na separação de funcionalidade e recursos entre os interfaces, os servidores e as bases de dados. Cabe assim ao servidor a gestão dos acessos aos conteúdos e a relação entre as requisições dos utilizadores e o sistema (**Figura 14**).

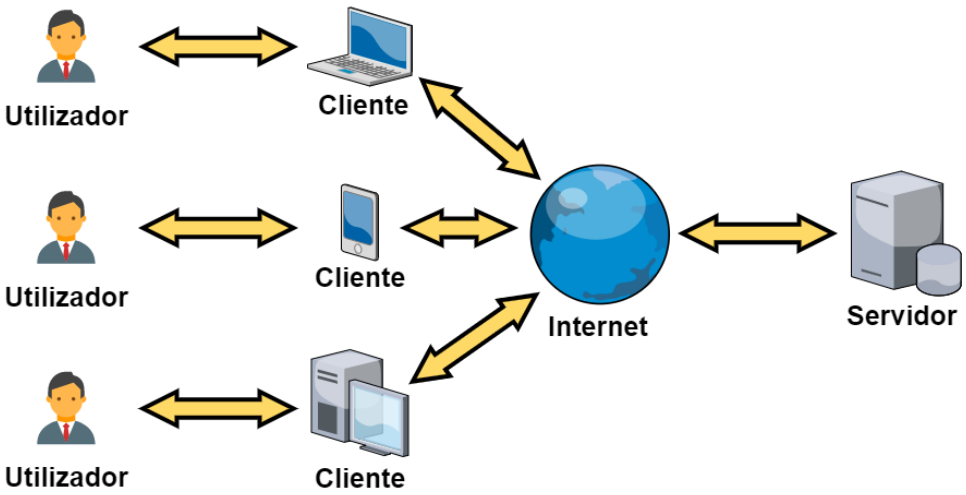


Figura 14 - Arquitetura Cliente-Servidor através da Internet

Conforme foi referido anteriormente, o funcionamento desta plataforma baseia-se num modelo dividido em 3 camadas:

A. Camada de Apresentação - Esta camada faz a ligação do utilizador com a plataforma e é criada tendo por base HTML e CSS. A utilização da versão 5, a mais recente à data, do HTML em conjunto com as capacidades de personalização do CSS, permite que esta seja *Responsive Web Design* (RWD), ou seja, tem a possibilidade de se adaptar a qualquer dispositivo utilizado pelo utilizador.

B. Camada Lógica - Esta camada tem como funcionalidade a gestão da interface, dotando-a da "inteligência" que posteriormente é usada para a geração dos conteúdos (como por exemplo, nas informações estatísticas geradas), as interações dinâmicas com que o utilizador interage e a ligação com a base de dados. Neste caso, é utilizada a versão mais recente do PHP, a 7.3.

C. Camada de Dados - Através do uso de MySQL 5.6, é feita a gestão da base de dados utilizada. Neste são armazenadas todas as informações, como por exemplo as referentes aos utilizadores ou os resultados dos questionários.

De seguida é apresentado um diagrama com as camadas descritas anteriormente (**Figura 15**).

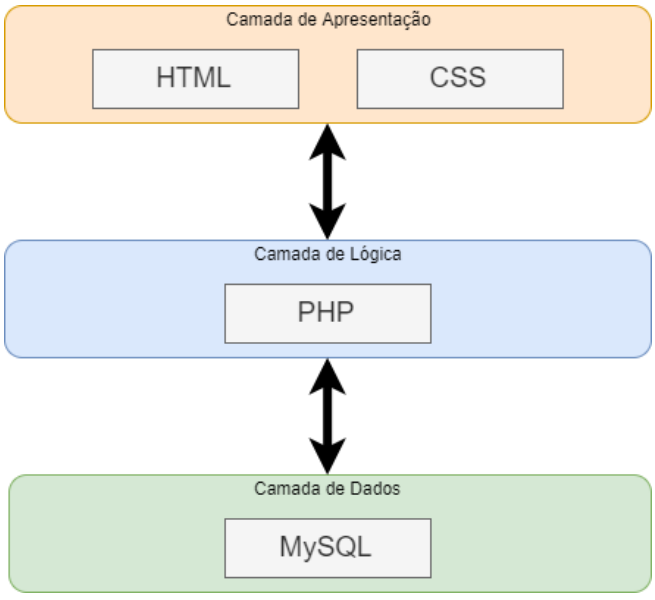


Figura 15 - Camada de Apresentação, Lógica e Dados

3.2. MODELO DE DOMÍNIO

O funcionamento da plataforma será baseado na existência de uma interface central onde os utilizadores poderão desempenhar diversas funções, como sendo:

- Preenchimento do questionário sobre o ICS das suas organizações;

- Aceder às medidas de controlo sugeridas;

- Consultar os resultados das estatísticas;

- Consultar e interagir com os conteúdos inseridos pelos Utilizadores.

No modelo seguinte, podemos ver os principais componentes da plataforma e a forma com interagem entre si (**Figura 16**).

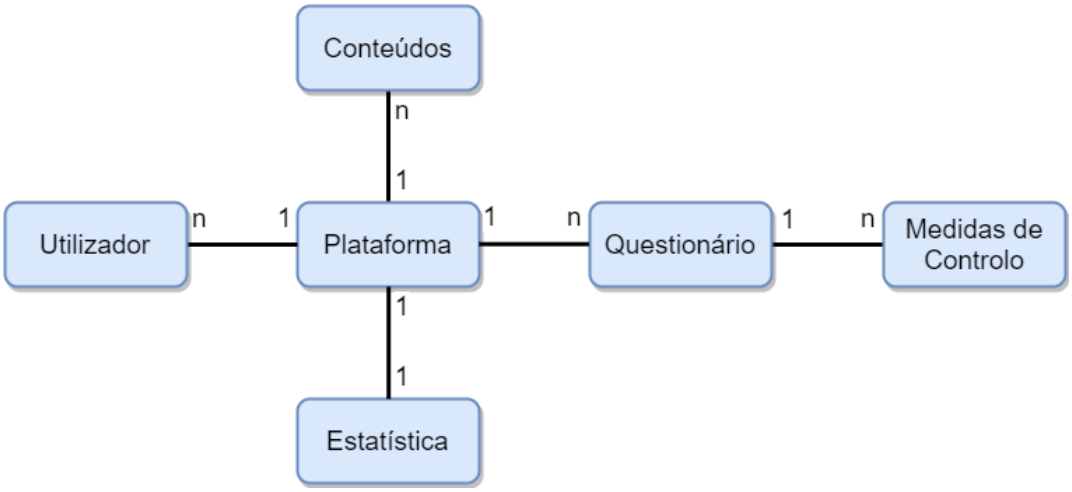


Figura 16 - Modelo do Domínio

3.3. USE CASES

Nesta secção, vão ser apresentados os principais casos de uso do sistema, bem como as funções e privilégios dos diversos utilizadores.

3.3.1. ATORES

Para o acesso ao *Front-End*, é necessário que os utilizadores estejam autorizados. Para tal, estes podem inscrever-se como visitantes na plataforma, sendo necessária autorização para inscrição para níveis superior. Foram criados 5 tipos de utilizadores, sendo identificados pelo seu Nível, sendo atribuído ao utilizador com menores privilégios, o 1 e ao utilizador com maiores privilégios, o 5. Foi definido que os privilégios são herdados para os níveis superiores, ou seja, um determinado nível tem um conjunto de atribuições, mais todas têm as dos níveis anteriores.

Na **Figura 17** é possível ver a representação dos diversos tipos de utilizadores.

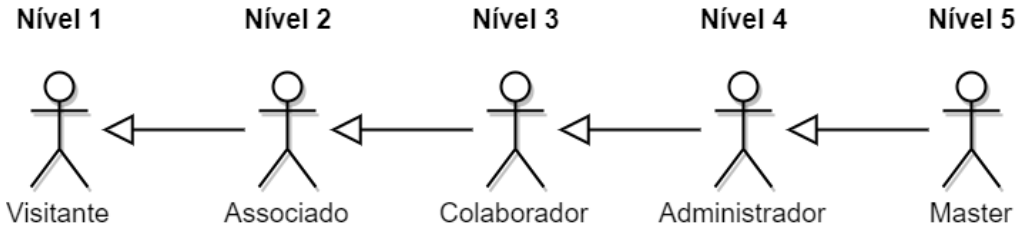


Figura 17 - Atores da plataforma

3.3.2. CASOS DE USO

São apresentados de seguida os 5 casos de usos para os atores da plataforma.

3.3.2.1. VISITANTE

Este Visitante (Nível 1) corresponde ao mais baixo do projeto, sendo o atribuído a todos os utilizadores aquando da entrada no site. Este nível permite a visualização de conteúdo abertos, nomeadamente notícias e publicações partilhadas por utilizadores com mais privilégios. Contudo, este não pode adicionar os seus próprios conteúdos, nem comentar os “posts” existentes.

Além destes conteúdos, também existe a possibilidade de visualização das estatísticas dos dados existentes na plataforma, nomeadamente os gráficos referentes aos níveis médios das respostas dos utilizadores.

Todos os Visitantes têm à sua disposição a ferramenta para a criação de um novo utilizador, podendo, através de *form* própria, carregar os seus dados (mediante convite) e passar a ter credenciais de acesso. Ao ser feito o login, este vai assumir um novo nível, deixando de ser Visitante e passando a ter novas funcionalidades.

Na imagem seguinte encontra-se a representação gráfica deste Caso de Uso (**Figura 18**).

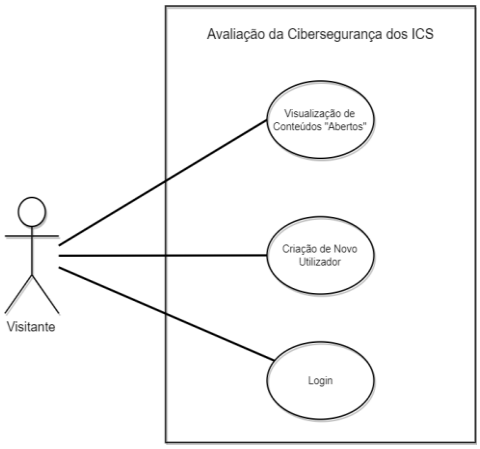


Figura 18 - Caso de Uso: Visitante

3.3.2.2. ASSOCIADO

O Associado é o nível mais baixo (Nível 2) dentro dos utilizadores registados e corresponde à generalidade dos mesmos. Este é concebido para ser o principal “alvo” da plataforma, sendo o principal responsável pelo preenchimento dos Questionários.

Como foi referido anteriormente, este vai herdar todas as permissões do Visitante, sendo que acrescenta a possibilidade do preenchimento do questionário e a possibilidade de comentar os conteúdos colocados por outros utilizadores.

Na imagem seguinte encontra-se a representação gráfica deste Caso de Uso (**Figura 19**).

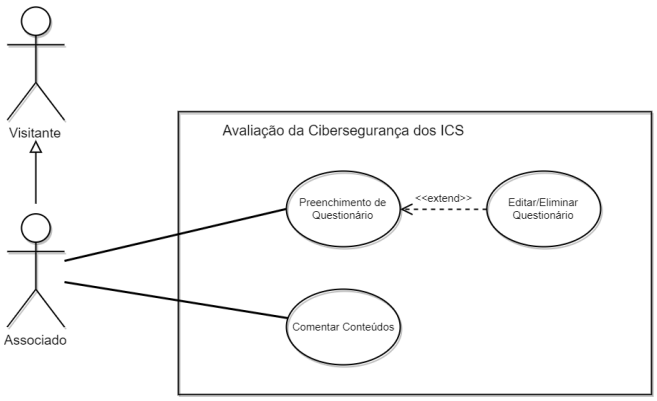


Figura 19 - Caso de Uso: Associado

3.3.2.3. COLABORADOR

O Colaborador (Nível 3) tem como função aumentar o valor da plataforma, permitindo o acrescento de informação relevante para o mesmo. Assim, a principal diferença entre este e o colaborar é a possibilidade de acrescentar conteúdo para todos os utilizadores. Este por sua vez podem ser editados ou eliminados por parte do seu autor.

Na imagem seguinte encontra-se a representação gráfica deste Caso de Uso (**Figura 20**).

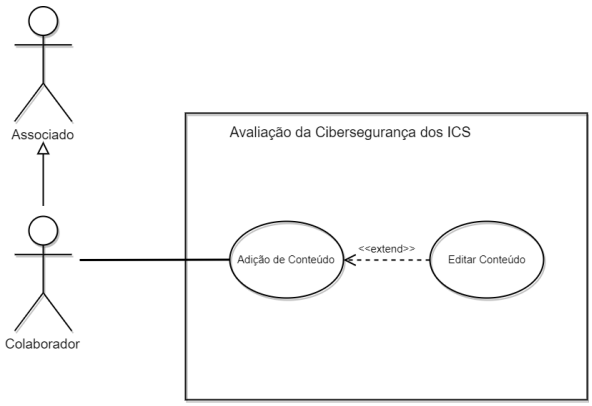


Figura 20 - Caso de Uso: Colaborador

3.3.2.4. ADMINISTRADOR

O Administrador tem o nível mais elevado de todos os utilizadores (Nível 4), sendo apenas ultrapassado pelo responsável pela plataforma. Como o próprio nome indica, este tem como função a gestão dos conteúdos colocados pelos utilizadores e dos questionários respondidos.

Este será desempenhado por especialistas da área, de forma a serem capazes de detetar falhas e incoerências técnicas nos conteúdos, podendo proceder a alguma alteração pontual, desativação da sua publicação ou mesmo a sua eliminação. Após a confirmação dos conteúdos, este deve validá-los de forma a ficarem online.

Além desta tarefa, também cabe a estes a criação de convites para os níveis anteriores, devendo para tal gerar um Código e transmiti-lo ao utilizador.

Na imagem seguinte encontra-se a representação gráfica deste Caso de Uso (**Figura 21**).

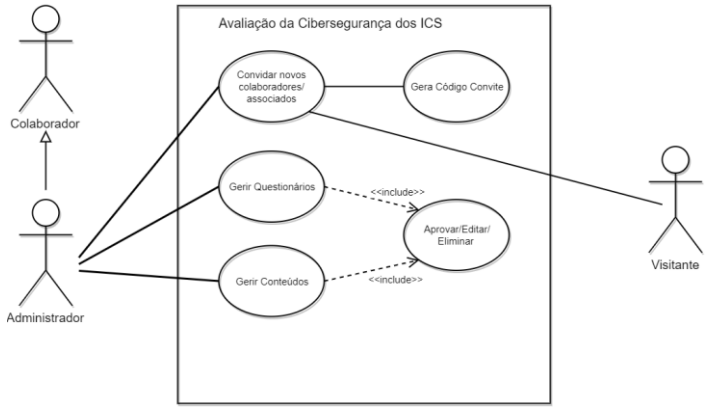


Figura 21 - Caso de Uso: Administrador

3.3.2.5. MASTER

O Master é utilizador com o maior nível de (Nível 5). Este tem como função a gestão da plataforma, bem como as funções de gestão dos utilizadores. Além da resolução dos problemas relacionados com as funcionalidades da plataforma, cabe a este a criação dos Administradores.

Uma vez que o Master é responsável pela manutenção da plataforma, espera-se deste menos ações relacionadas com os conteúdos e mais com o questionário em si (de acordo com os feedbacks e cooperação dos restantes utilizadores) e o seu correto funcionamento.

Outra funcionalidade importante do Master é a possibilidade de consulta e análise do Log do sistema. Neste, é possível a consulta de grande parte das ações importantes do sistema, como sendo a criação de convites ou a adição de questionário.

Na imagem seguinte encontra-se a representação gráfica deste Caso de Uso (**Figura 22**).

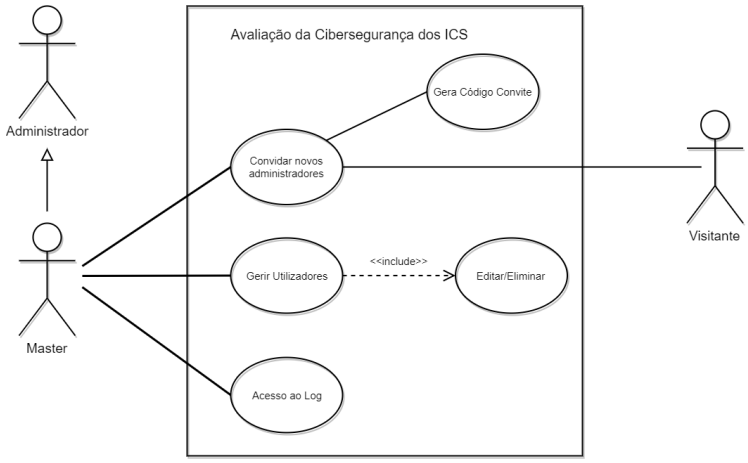


Figura 22 - Caso de Uso: Master

3.4. MODELO DE DADOS

Conforme foi referido anteriormente, os dados da plataforma são guardados numa base de dados, gerida por MySQL, sendo a interação com esta feita através de PHP. De forma a serem organizados os dados, dentro desta foram criadas diversas tabelas para as várias funcionalidades.

Na **Figura 23** podemos ver o diagrama relacional do modelo de dados definida para este projeto. Neste é possível verem-se 7 tabelas, sendo as mesmas explicadas de seguida

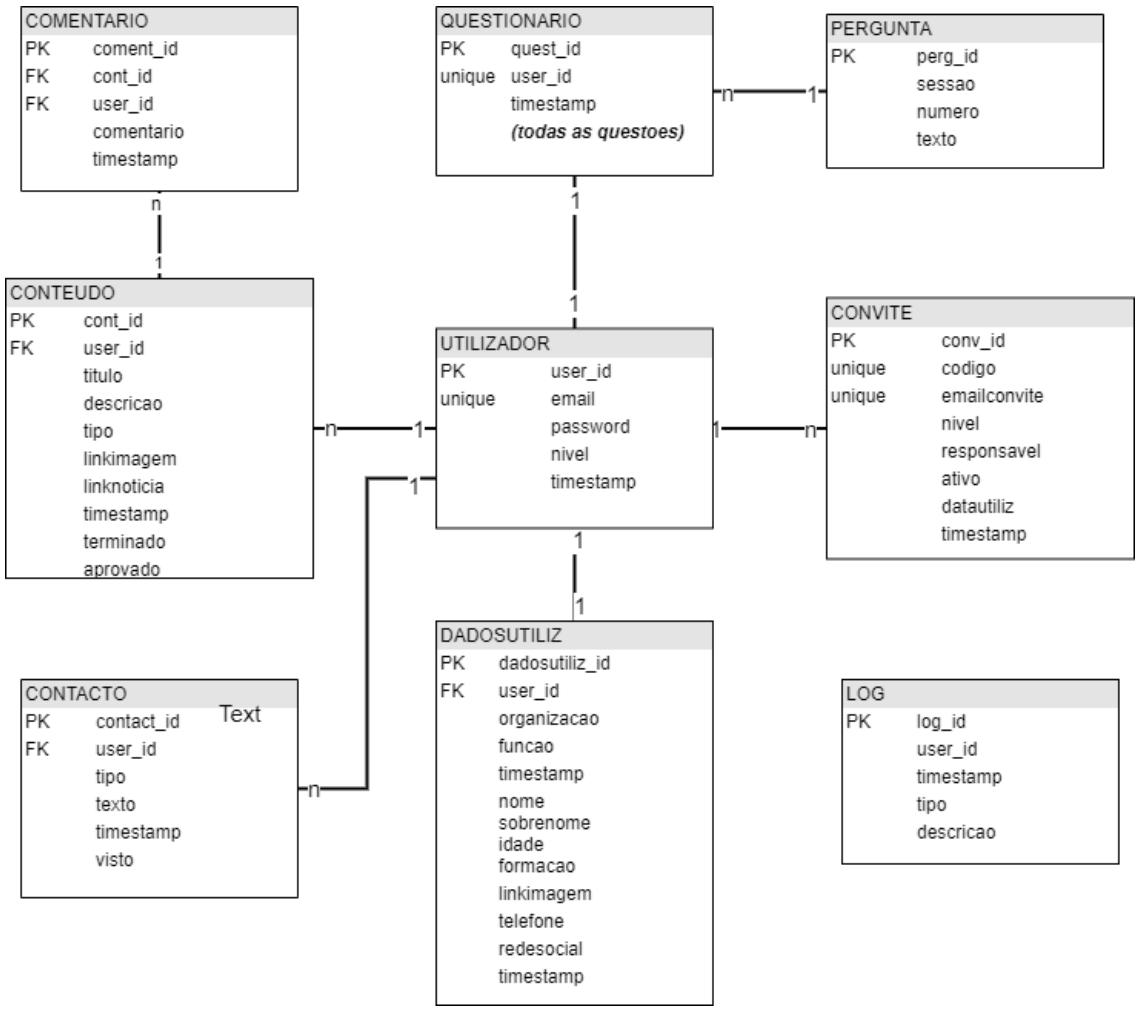


Figura 23 - Diagrama relacional do modelo de dados

3.4.1. TABELA: UTILIZADOR

Esta tabela encontra-se no meio do modelo, uma vez que as funcionalidades da plataforma estão diretamente ligadas às operações dos utilizadores. Por exemplo, nesta tabela, encontramos dados relativos ao *username* e ao nível, essenciais para a validação de dos acessos ou para a apresentação dos responsáveis por determinadas ações. Além destes, encontram-se também campos para a colocação do email e para o *timestamp*. Este último existe em todas as tabelas e tem a importante função de permitir a monitorização e controlo da introdução dos dados.

3.4.2. TABELA: DADOSUTILIZ

Esta tabela corresponde a “Dados do Utilizador” e tem como função o armazenamento dos dados introduzidos pelo utilizador para a sua própria caracterização. Estes dados são o nome, a organização e o contacto. Há também um campo para a ligação de uma imagem online que o utilizador pretenda. Além disso poderá também colocar uma ligação a uma rede social profissional.

3.4.3. TABELA: CONVITE

A tabela Convite tem como funcionalidade armazenar os códigos criados pelos utilizadores de topo para permitir o registo de um visitante. Ao ser gerado um novo convite, é automaticamente adicionado à tabela qual o email do futuro utilizador registado. Desta forma, ao ser criado um novo utilizador, tem que ser selecionada na tabela a informação que vai confirmar a autorização. Além destes campos, esta tabela também tem um conjunto para a identificação que o convite ainda está ativo e em que data foi ativado.

3.4.4. TABELA: QUESTIONARIO

Esta tabela tem como funcionalidade o armazenamento das respostas dos utilizadores aos seus questionários. Embora desempenhe uma importante função na plataforma, a tabela em si é relativamente simples, sendo a grande maioria dos campos as respostas e apenas outros dois referentes ao *timestamp* e ao ID do utilizador.

No modelo relacional da **Figura 23** não se encontram a totalidade dos campos das respostas por uma questão de gestão de espaço.

3.4.5. TABELA: PERGUNTAS

Esta tabela corresponde às “Perguntas” que vão ser apresentadas no questionário. Estas foram codificadas de forma a serem ligadas às respostas dadas e introduzidas na tabela anterior. Além do id, esta tabela tem como campos o código da pergunta, o seu grupo e o texto.

3.4.6. TABELA: CONVITE

A tabela Convite tem como funcionalidade armazenar os códigos criados pelos utilizadores de topo para permitir o registo de um visitante. Ao ser gerado um novo convite, é automaticamente adicionado à tabela qual o email do futuro utilizador registado. Desta forma, ao ser criado um novo utilizador, tem de ser selecionado na tabela a informação que vai confirmar a autorização. Além destes campos, esta tabela também tem um conjunto para a identificação se o convite ainda está ativo e em que data foi ativado.

3.4.7. TABELA: CONTEUDO

Esta tabela tem como finalidade o armazenamento dos diversos conteúdos gerados pelos utilizadores para sem exibidos na *frontpage* da plataforma. Este são pequenos cartões com informações relevantes sobre as temáticas abordadas na plataforma. Com os campos desta tabela temos o conjunto relativo ao conteúdo em si, como o título, a descrição e o tipo. Além destes, temos também outros campos que permitem a colocação de links para notícias/páginas externas com relação ao conteúdo, bem como a possibilidade de colocação de uma pequena imagem online. Por fim, existem mais 3 campos com informações do sistema sobre o *timestamp* da criação, se o mesmo está pronto a ser disponibilizado e a validação por parte de um Administrador.

3.4.8. TABELA: LOG

Esta tabela é muitíssimo importante, uma vez que permite ao Master ter o conhecimento sobre os eventos do sistema. Desta forma, sempre que o sistema gerar um acontecimento importante, além do visualizado pelo utilizador, é também inserida uma string com a descrição, o originador, o *timestamp* e o tipo de evento.

3.4.9. TABELA: COMENTARIO

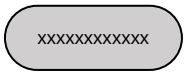
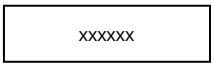
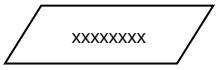
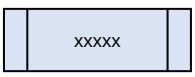
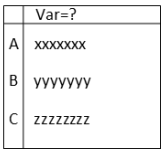
Esta tabela tem como função o armazenamento dos dados criados a um conteúdo. Esta é organizada de forma simples, havendo apenas a relação entre o utilizador que criou o comentário e qual o comentário a que se destina. Além disso apenas possui o campo de *timestamp*.

3.4.10. TABELA: CONTACTO

Esta tabela é tem como função o armazenamento das mensagens enviadas entre os utilizadores e o Master. Além de existirem campos para o ID das mensagens, existem também outros dados simples como o username do emissor, o seu conteúdo e o *timestamp*. Além destes, também existe um campo para o tipo (como forma de organizar a tipologia de contacto) e outro campo para a indicação de que se é ou não uma mensagem nova, identificado com o Visto.

3.5. FLUXOGRAMAS DOS MODELOS LÓGICOS

Para a demostração do funcionamento pretendido da plataforma, foram criados fluxogramas com os diferentes modelos lógicos para os principais processos. Para tal foi adaptada a norma ISO 5807, sendo o significado dos diversos elementos descritos de seguida:

Forma	Nome	Significado
	Terminal	Inicio ou fim de um processo ou subprocesso. Pode haver mais de um início e/ou fim, devendo estes estar identificados por diferentes condições.
	Decisão	Decisão booleana (sim ou não) de uma condição definida no próprio elemento. Caso a condição necessite de uma formulação mais complexa, deverá ser utilizada uma nota.
	Evento	Evento no processo, podendo representar diversas situações como por exemplo a apresentação de mensagens, resultado de operações com inputs ou eventos.
	Operação	Representa uma operação de introdução de input e/ou onde é produzido um output.
	Subprocesso	Indica a existência de um subprocesso que é descrito num fluxograma próprio. Este pode ser corrido mais que uma vez. Poderá ter mais que uma saída (por exemplo com diferentes estados booleanos) estando estas identificadas nos fluxos de saídas por variáveis.
	Escolha Múltipla	Este elemento simboliza escolha múltipla, tendo um funcionamento semelhante ao “CASE” em programação. Neste caso, uma condição pode ter vários resultados associados sendo este atribuído a uma variável. O valor da variável vai condicionar qual o fluxo de saída.
 XXXXXX	Tabela da Base de Dados	Tabela utilizada da base de dados, sendo o seu nome indicado na legenda inferior.

	Fluxo	Indica a direção que o processo deve tomar.
	Fluxo com Dependência	Este fluxo deverá ser utilizado quando existe uma condição associada, existindo normalmente múltiplas saídas de um elemento para destinos (por exemplo saídas de Subprocessos). Deverá ser indicado com clareza a condição que distingue cada um dos fluxos.
	Entrada de Dados	Indica a entrada de dados que um elemento tem por origem de uma operação (por exemplo introdução em uma base de dados)
	Saída de Dados	Indica a saída de dados de um elemento de forma a ser utilizado por outra operação (por exemplo leitura de dados de uma base de dados)

De forma a compreender-se o funcionamento geral da plataforma, foi criado um modelo lógico com os principais processos (**Figura 24**). De forma a simplificar a mesma, não foram colocadas todas as interações no mesmo fluxograma, tendo sido estes separados em subprocessos. Assim podemos considerar que a plataforma funciona através de um Login de um utilizador com as suas credenciais de acesso, sendo depois direcionado para a página principal. De acordo com o seu nível, são carregados nesta os conteúdos e as estatísticas, bem como a barra de navegação. Após isso, a opção do utilizador faz com que seja desencadeado um processo. De seguida é demonstrada a lógica para cada um destes.

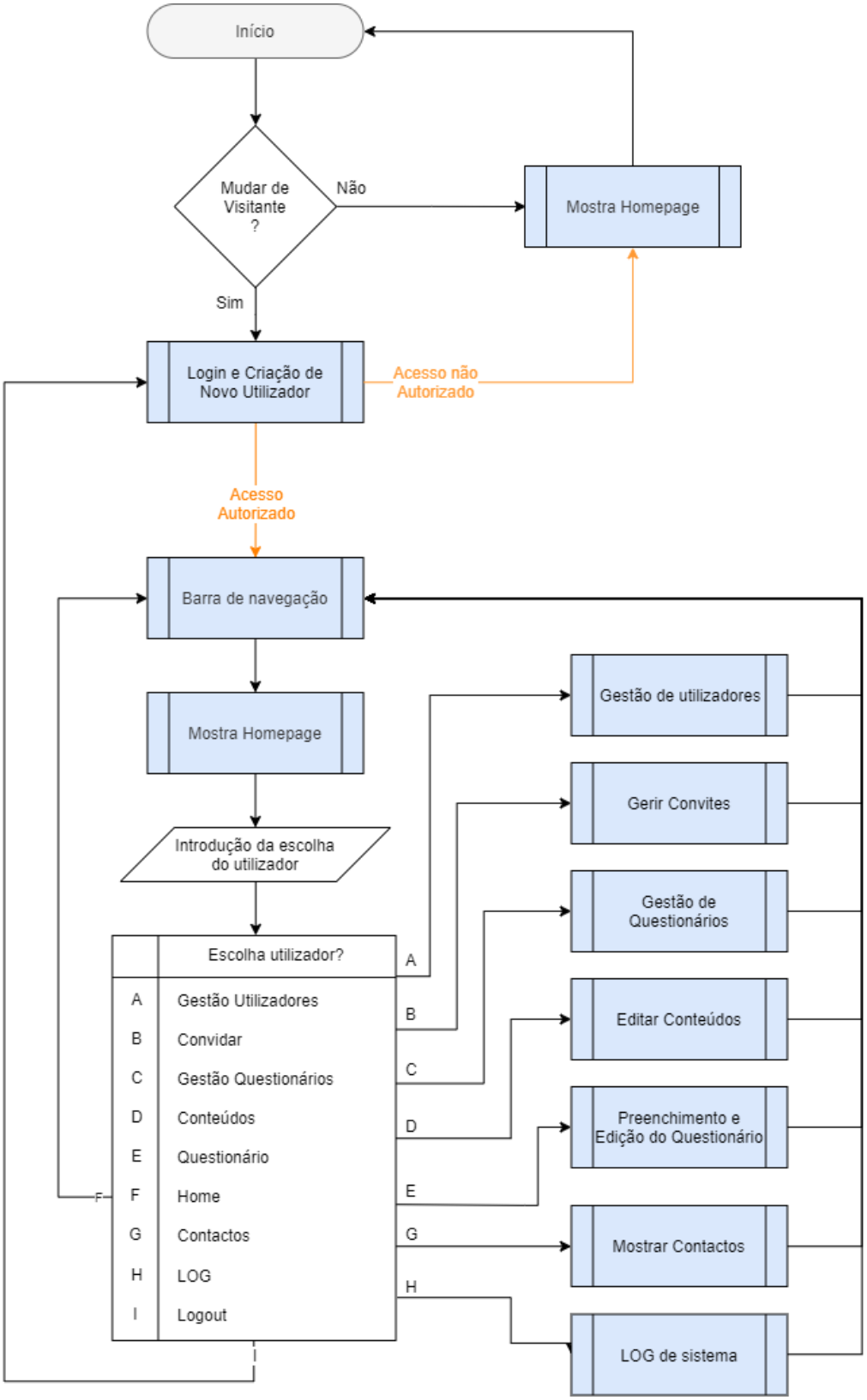


Figura 24 - Modelo lógico da plataforma

3.5.1. SUBPROCESSO: LOGIN E CRIAÇÃO DE NOVO UTILIZADOR

Neste subprocesso foram agrupadas as funções de criação de um novo utilizador e de Login na plataforma. Este pode ser analisado de seguida, na **Figura 25**.

De acordo com o especificado nas secções anteriores, pretende-se que um visitante possa fazer um novo registo ou utilizar as suas credenciais para aceder à plataforma. Para tal é mostrado uma *form* que vai permitir que o visitante coloque os seus dados, tendo de introduzir o seu código de nível para serem validados os níveis superiores. Para tal, será feita uma consulta à BD através da tabela CONVITES. Caso tudo esteja de acordo, então o utilizador é criado, sendo adicionada a informação na tabela UTILIZADORES. É também introduzido na tabela LOG informações sobre este evento.

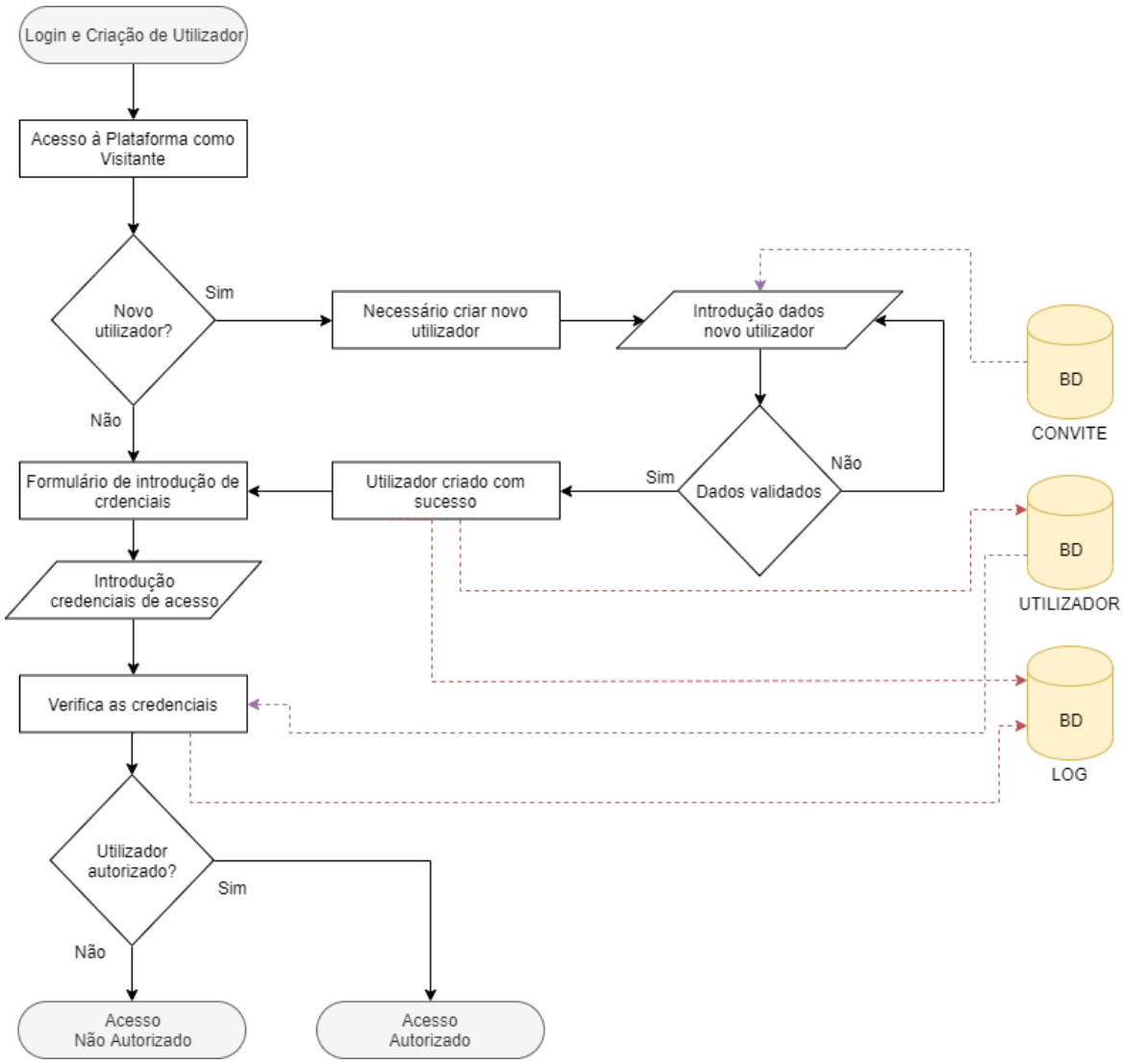


Figura 25 - Modelo lógico: Criação de Utilizador e Login

Após ter um utilizador criado, o visitante pode proceder à introdução dos dados através das suas credenciais de acesso. Para tal, é utilizado PHP para comparar os dados introduzidos com os existentes na tabela UTILIZADORES. Caso seja igual, o *username* e o nível (entre outros dados) são guardados como variáveis de sessão para continuarem a ser utilizados na plataforma até que seja efetuado o *Logout* ou que seja fechado o browser.

Este subprocesso tem duas saídas, uma para os utilizadores autorizados e outra para os não autorizados.

3.5.2. SUBPROCESSO: MOSTRA HOMEPAGE

Este subprocesso tem como função gerar a home page da plataforma que devido ao uso de PHP, será diferente consoante o nível o utilizador (**Figura 26**). Este começa por fazer diversos tipos de verificação de nível para ver quais os ícons que cada utilizador irá ver.

No caso dos utilizadores mais baixos, estes apenas vêm as estatísticas e os conteúdos sem que tenham acesso a nenhum ícon de edição ou gestão. Os utilizadores que se encontrem entre o nível 3 e 4 já terão algumas destas opções, sendo que só o nível 5 tem a opção de gestão do utilizador e visualiza as últim as entradas no LOG.

O primeiro bloco a aparecer na home page são as estatísticas da Plataforma. Aqui será possível visualizar-se a médias das diversas secções do questionário dadas pelo total das organizações participantes. Todos os dados estatísticos apresentados têm os seus conteúdos calculados com base na tabela QUESTIONARIOS e são gerados por cada vez que é carregada a página.

O segundo bloco a ser visualizado são os conteúdos. Estes são apresentados como cartas de informação, podendo o utilizador filtrá-los com as ferramentas disponibilizadas. Os dados carregados são lidos na tabela CONTEUDOS.

O terceiro bloco a ser gerado é a lista dos últimos 20 eventos (apenas disponível para o Master), sendo para tal carregados os dados existentes na tabela “LOG”. Neste existe a possibilidade de transitar para a lista completa de Logs dos eventos do sistema.

Em todos os casos, são utilizados outros subprocessos para explicar as operações que se sucedem. Após a geração destas informações, existe um espaço final reservado a informações diversas visualizáveis por todos.

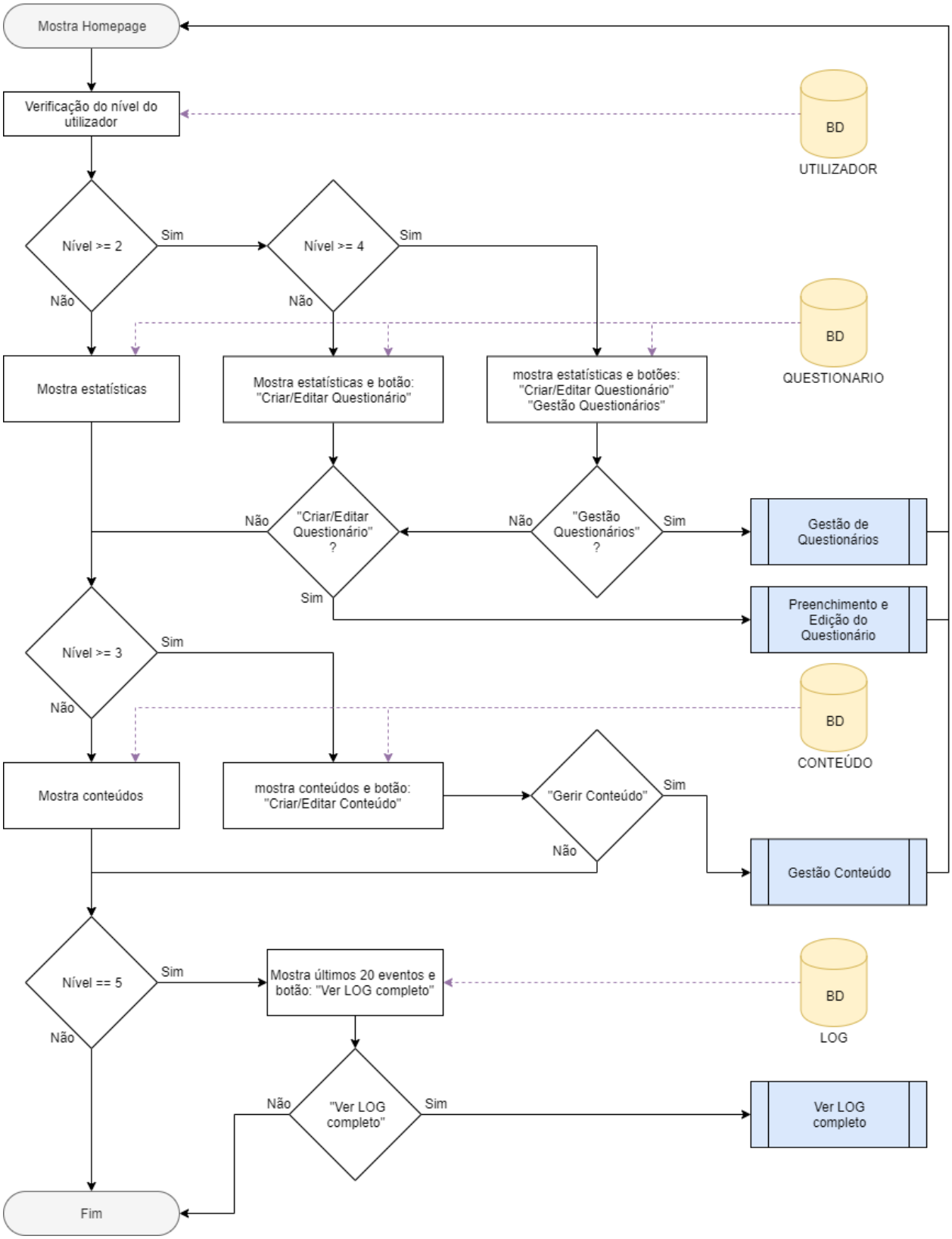


Figura 26 - Modelo lógico: Mostra home page

3.5.3. SUBPROCESSO: BARRA DE NAVEGAÇÃO

Qualquer página da plataforma tem no seu cimo a barra de navegação. Esta, dependendo do nível do utilizador, permite o acesso às principais funcionalidades disponíveis. Através da leitura do nível do utilizador, na tabela UTILIZADOR, é utilizado o conceito de herança de forma a não existir repetição de código. Na **Figura 27** pode ver-se o subprocesso.

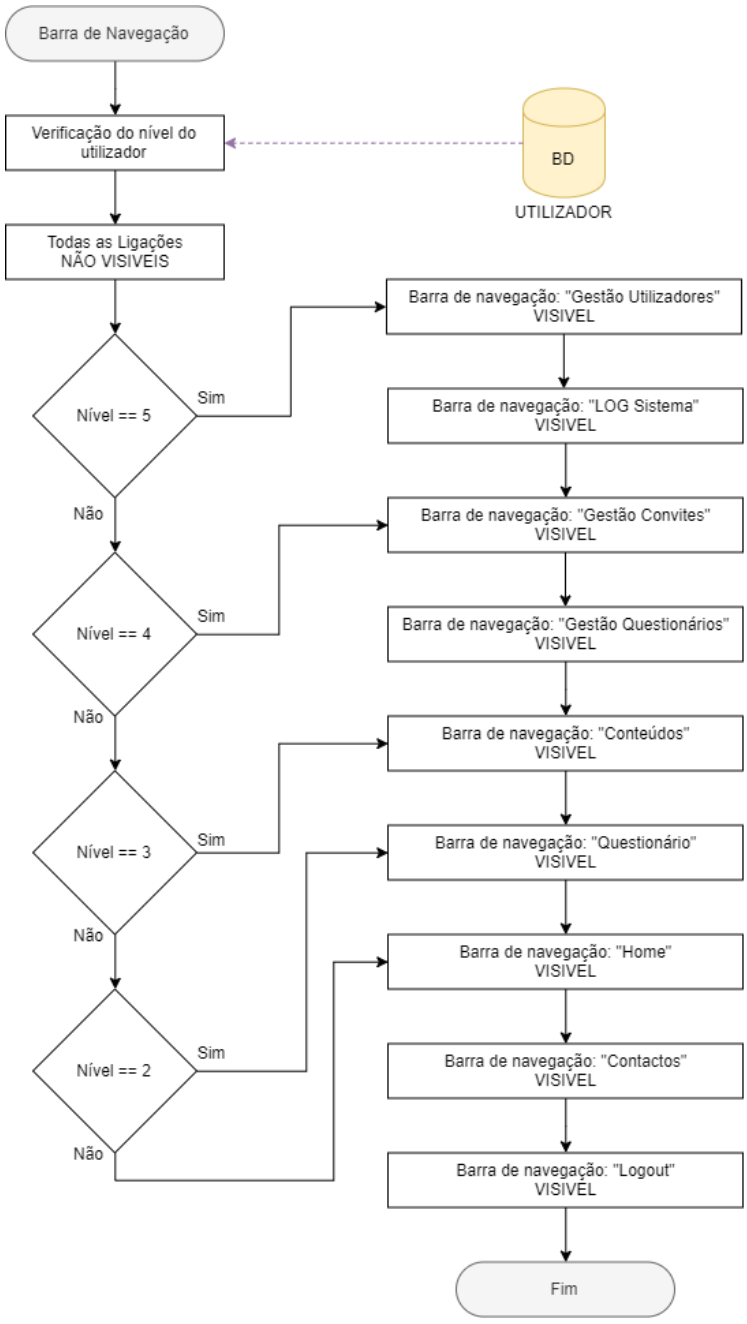


Figura 27 - Modelo lógico: Barra de Navegação

3.5.4. SUBPROCESSO: GESTÃO UTILIZADORES

Neste subprocesso (**Figura 28**) é possível fazer-se a Gestão dos Utilizadores, podendo de forma simples proceder à alteração e eliminação destes. De forma a aumentar a segurança, este inicia o seu código pela confirmação do nível do utilizador. Isto impede a introdução manual do URL de uma página para que um utilizador não autorizado tenha acesso a informação ou comandos indevidos. Neste caso, independentemente da forma como se chegou à página de Gestão de Utilizadores, apenas os que têm nível 5 podem proceder a alterações.

Ao ser carregada a página referente a este subprocesso, é gerada uma lista com todos os utilizadores, aparecendo as informações de nome, nível e email, seguidas do ícon de edição, reset de password e eliminação.

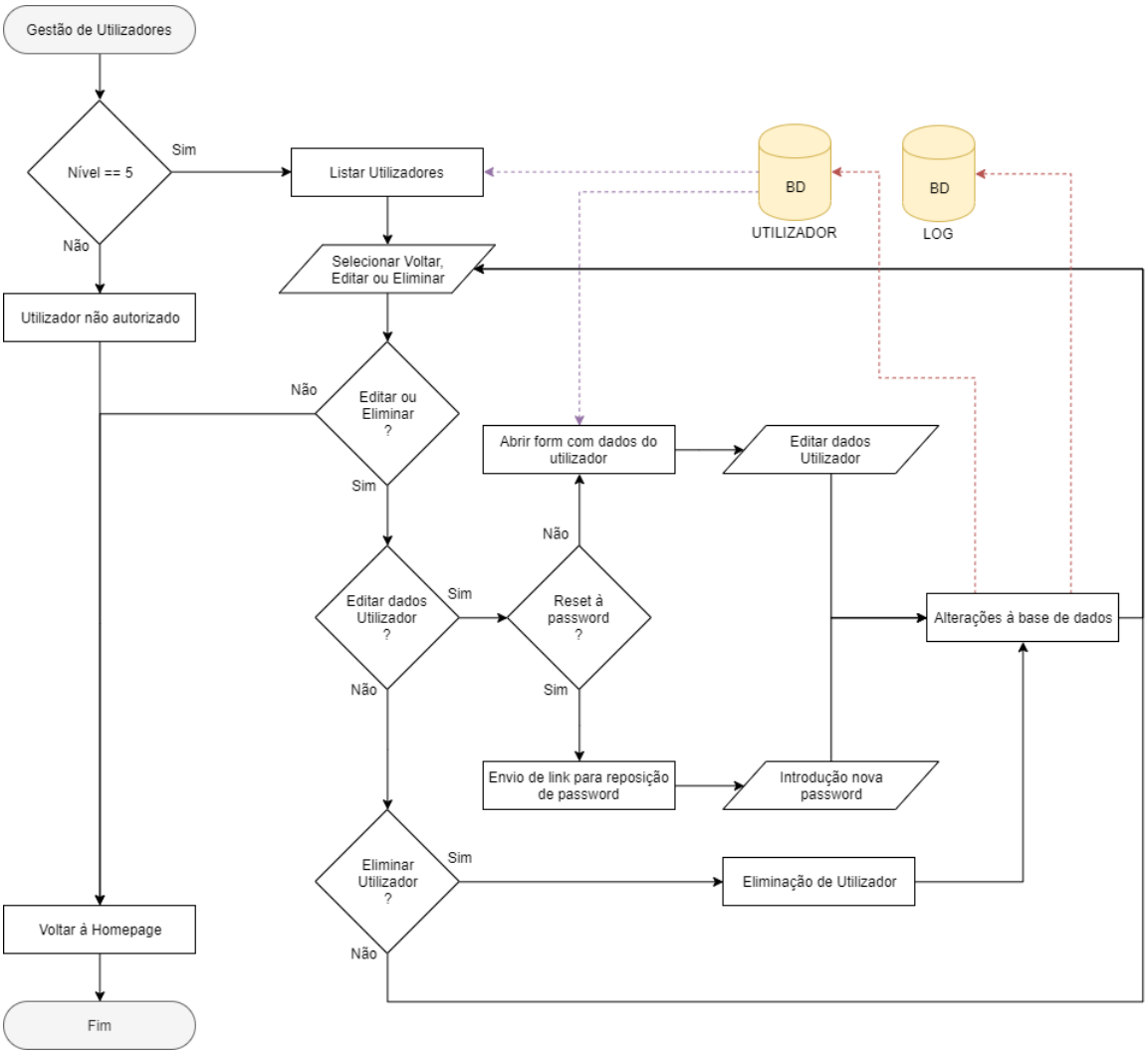


Figura 28 - Modelo lógico: Gestão de Utilizadores

Na edição, deverá surgir um *form* com os campos pré-preenchidos com o guardado na tabela UTILIZADOR, podendo estes serem alterados aí. O administrador deverá, após proceder às alterações, confirmar ou cancelar as mesmas.

A solicitação de reset da password, deverá ser feita pelo menu de contactos, sendo enviada uma mensagem predefinida para o efeito, não sendo necessário para tal fazer login com o utilizador. O reset à password será feito de forma a respeitar a privacidade do utilizador, não sendo esta exibida em lado nenhum do sistema. Assim, ao ser submetido um comando de reset, esta será substituída temporariamente por uma aleatória (gerada pelo sistema), sendo posteriormente enviada para o email registado pelo utilizador.

A eliminação de um utilizador será feita através da seleção do botão correspondente, sendo depois aberto um *form* com os dados do utilizador e os botões para confirmar ou anular a eliminação.

Todas as três ações anteriores, além de desencadearem interações com as respetivas tabelas da BD, irão também acrescentar entradas eventos no LOG do sistema.

3.5.5. SUBPROCESSO: GERIR CONVITES

À semelhança do subprocesso anterior, este também necessita de validação do nível do utilizador antes de ser possível aceder à Gestão de Convites (**Figura 29**), sendo que neste caso, o utilizador tem de ser no mínimo nível 4.

Caso o utilizador seja um Administrador, então o PHP irá apenas gerar uma lista com os convites feitos pelo próprio. Aí será possível, através da utilização de ícons, editar ou eliminar o convite. Caso seja o Master, então serão listados todos os Convites existentes no sistema. Nos dados exibidos, poderão ser visualizados não apenas as informações dos destinatários, mas também se o convite já foi usado e quando o foi.

Além destas opções, ambos os tipos de utilizadores têm à sua disposição a possibilidade de criar um novo convite, sendo este adicionado a tabela CONVITE.

Todas as operações de edição, eliminação e criação de convites vão gerar eventos que serão adicionados à tabela de LOG.

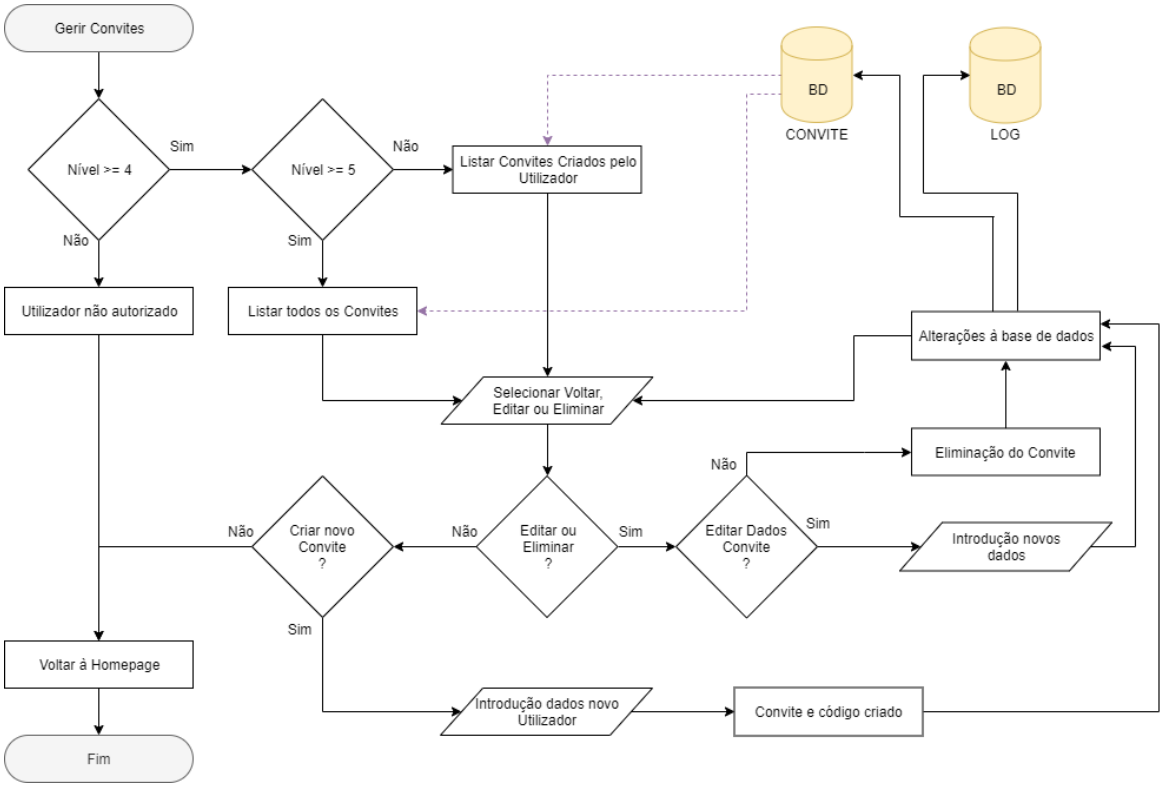


Figura 29 - Modelo lógico: Gerir Convite

3.5.6. SUBPROCESSO: GESTÃO DE QUESTIONÁRIOS

Para a Gestão de Questionários, foi criado o subprocesso representado na **Figura 30**. Mais uma vez neste existe a validação do nível do utilizador, estando vedado o acesso aos níveis 4 e 5.

Para esta gestão, é gerada primeiramente a lista de todos os questionários efetuados, sendo colocado junto destes os ícons de edição e eliminação. Para tal, são listados todos os elementos da tabela QUESTIONARIO. No caso de se optar pela eliminação, esta é feita através da retirada da entrada pretendida da tabela QUESTIONARIO, ao mesmo tempo que é criada uma nova entrada na tabela LOG

No caso de ser editado, a lógica a seguir-se será descrita no ponto seguinte.

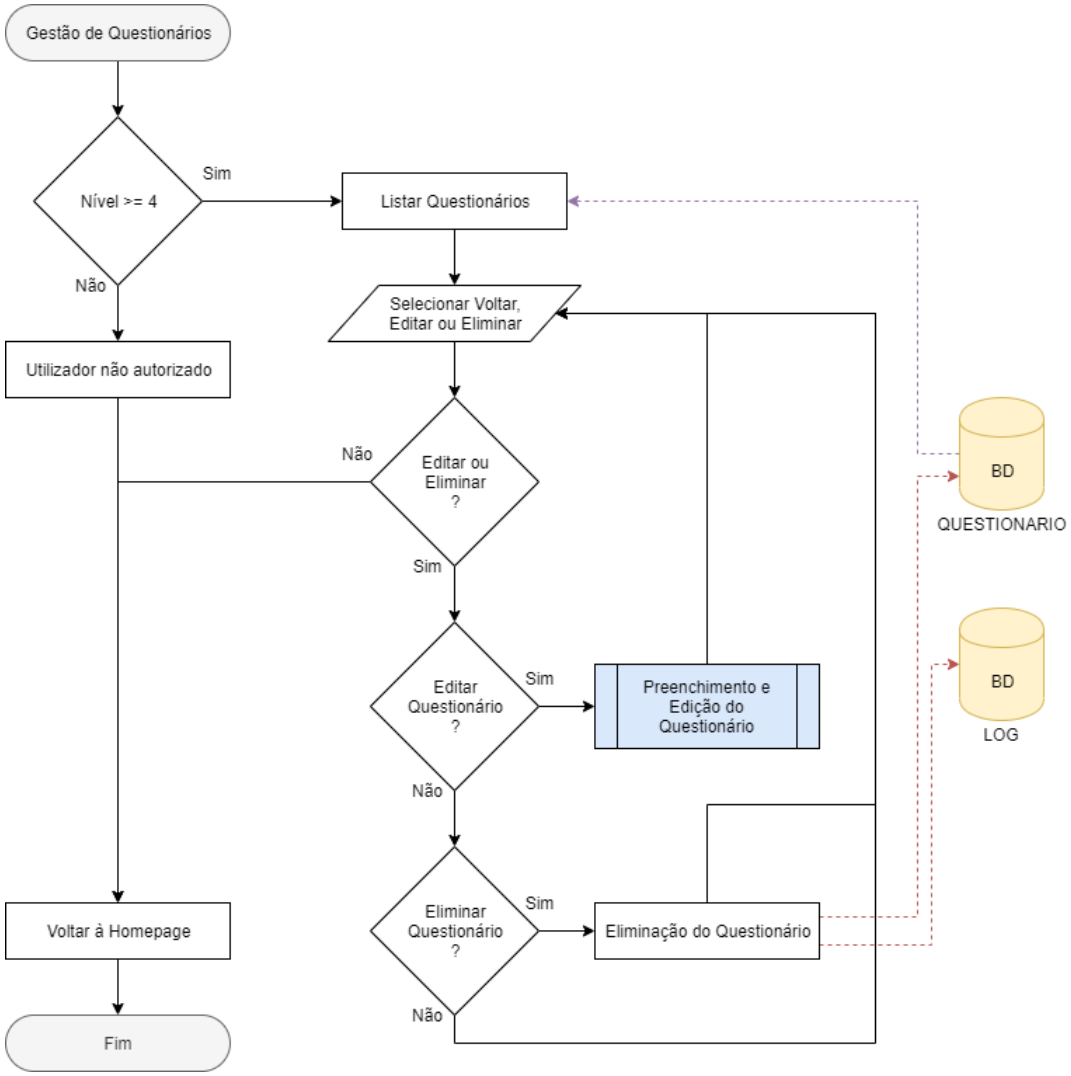


Figura 30 - Modelo lógico: Gestão de Questionários

3.5.7. SUBPROCESSO: PREENCHIMENTO E EDIÇÃO DE QUESTINÁRIOS

Conforme é apresentado na **Figura 31**, após a verificação do nível do utilizador, caso este seja superior a 2, torna-se possível o preenchimento do questionário. Para tal, o sistema irá consultar a tabela QUESTIONARIO pela existência de um já preenchido. Caso exista, o *form* apresentado será previamente preenchido, caso contrário, este será apresentado em branco.

Quando terminado, será verificado pelo sistema para ver se está corretamente preenchido. Caso não esteja, o utilizador poderá proceder às alterações necessárias. Caso esteja correto e o utilizador pretenda dar por terminado o preenchimento, os dados são carregados na tabela QUESTIONARIO.

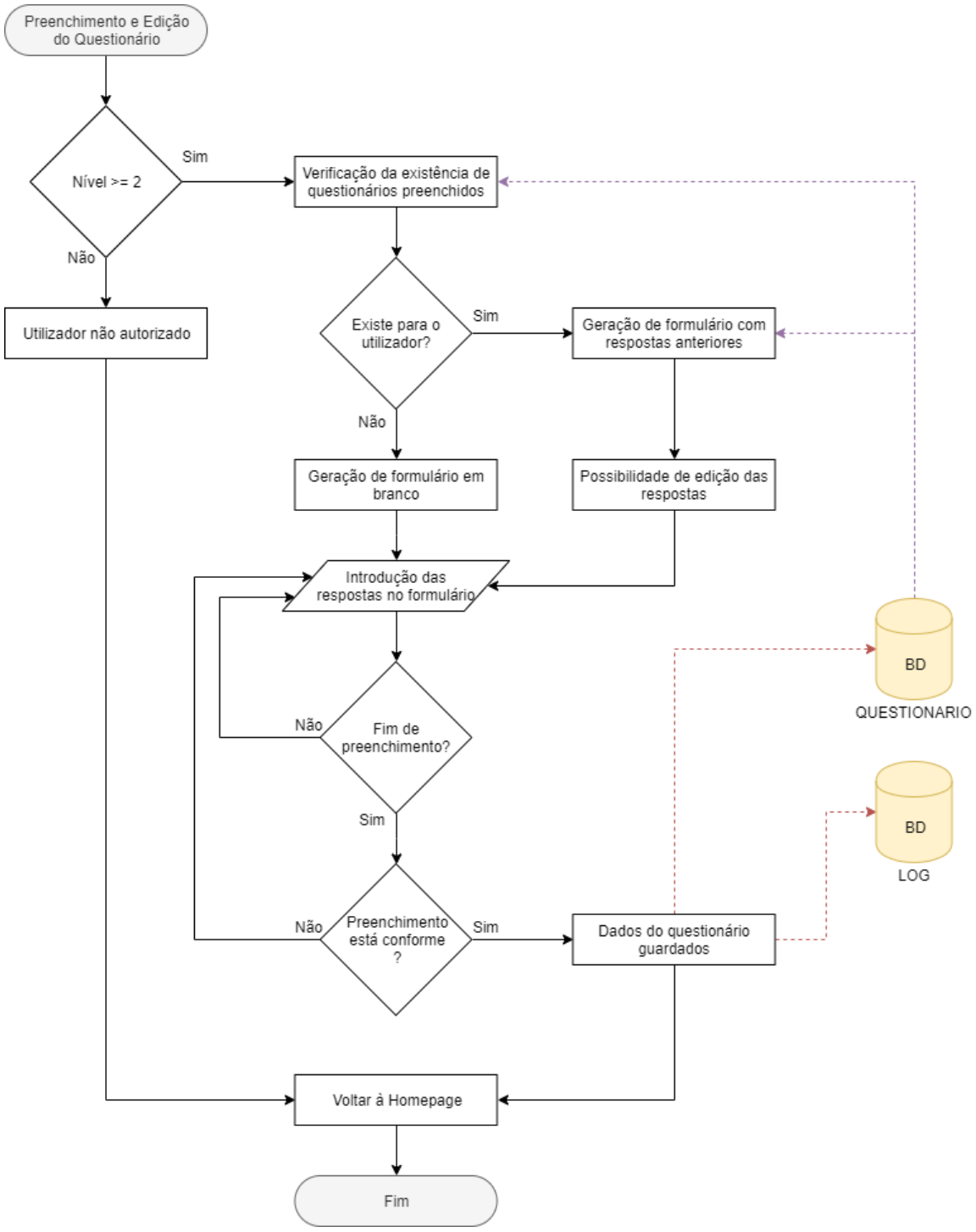


Figura 31 - Modelo lógico: Gestão de Questionários

3.5.8. SUBPROCESSO: GESTÃO CONTEÚDO

Os conteúdos permitem dar algo mais ao utilizador após o preenchimento do questionário. Não sendo objetivo da plataforma a criação de uma rede social, esta opção introduz uma capacidade de comunicação entre os membros da plataforma (**Figura 32**).

Desta forma, à exceção do visitante, todos os utilizadores podem aceder e comentar os conteúdos publicados. Estes são introduzidos na tabela COMENTARIO. À semelhança de outros subprocessos, os eventos também são carregados em LOG.

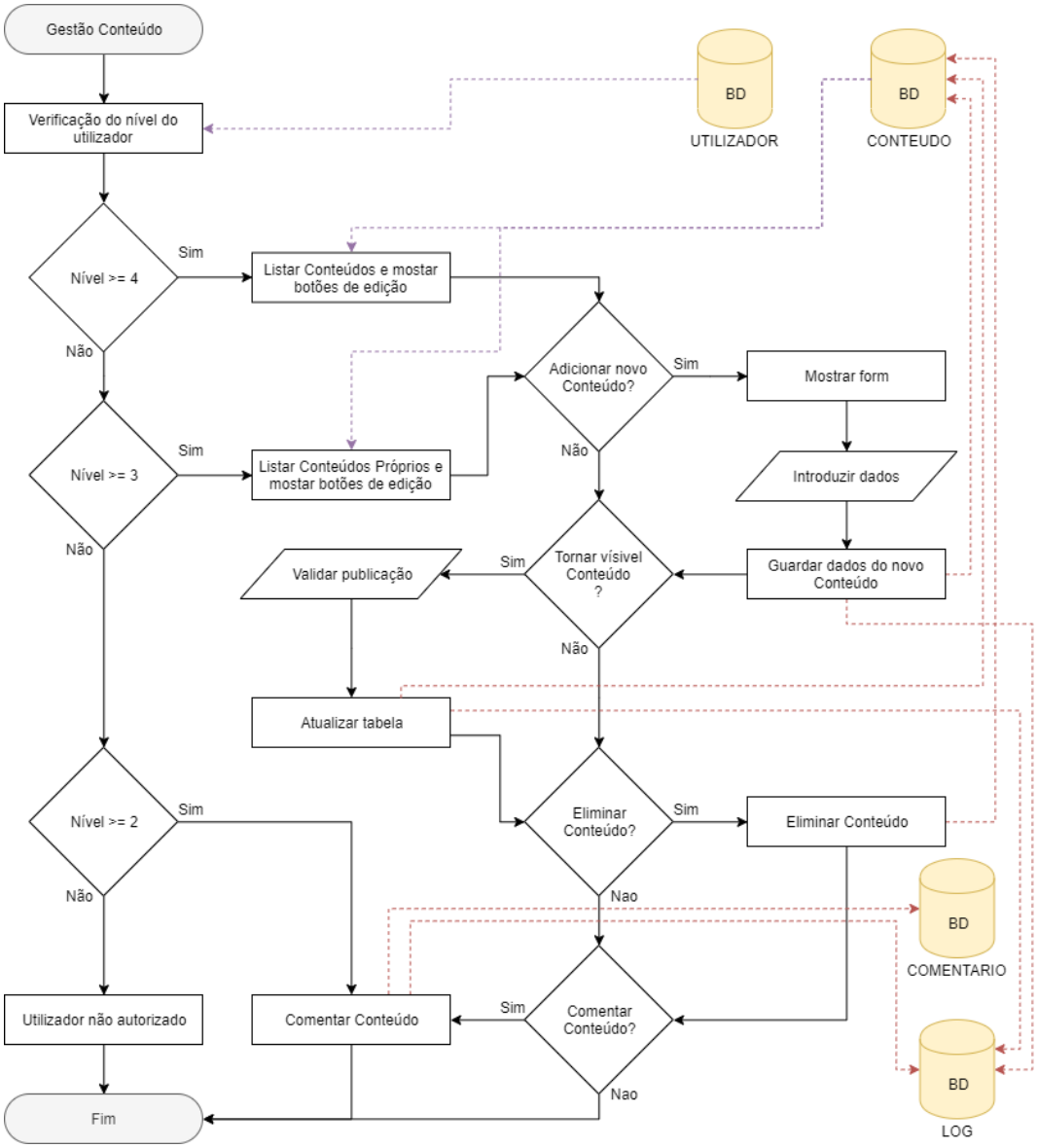


Figura 32 - Modelo lógico: Gestão de Conteúdo

3.5.9. SUBPROCESSO: MOSTRAR CONTACTO

Este subprocesso permite que qualquer utilizador da plataforma envie uma mensagem para o Master, nomeadamente as mensagens de apoio técnico. Desta forma foi criada uma estrutura muito simples que se baseia num campo de texto e num *droplist* para escolha do tipo contacto.

Após a introdução dos dados, os campos são enviados para a tabela CONTACTO, bem como é criado um evento na tabela LOG.

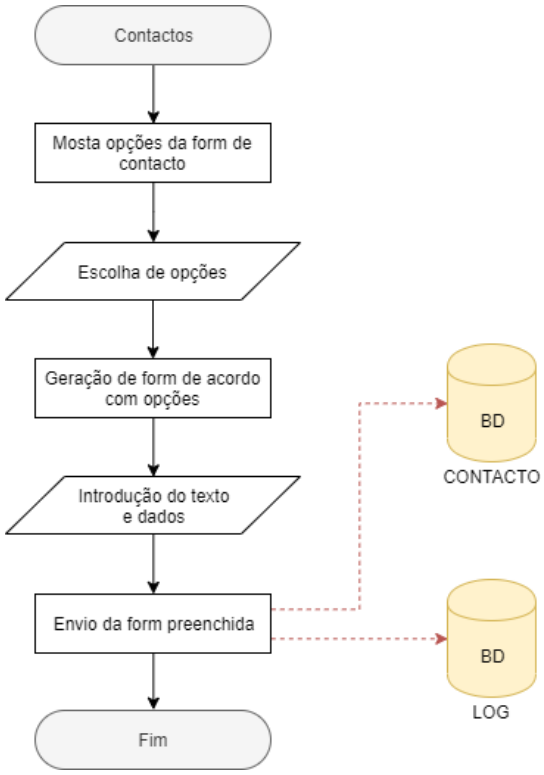


Figura 33 - Modelo lógico: Contactos

3.5.10. SUBPROCESSO: LOG DE SISTEMA

Este último modelo lógico apenas está disponível para o Master (nível 5), baseando-se na geração de uma lista com todas as entradas da tabela LOG. O utilizador terá à sua disposição um conjunto de filtros para mostrar apenas os de eventos que pretende ver, nomeadamente ao nível de tipo, nome de utilizador ou data.

De seguida na **Figura 34** podemos ver o fluxograma referente a este subprocesso.

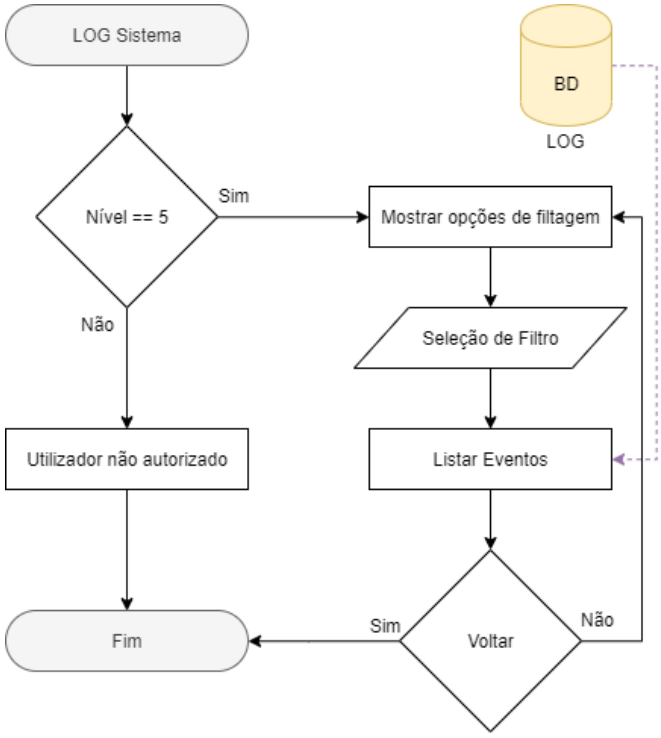


Figura 34 - Modelo lógico: LOG Sistema

CAPÍTULO 4

PROTÓTIPO APLICACIONAL

4.1. ESQUEMA NAVEGACIONAL

De acordo com o definido no capítulo anterior, foi desenvolvido um Protótipo Aplicacional para com o objetivo de criar uma ferramenta para auxiliar a aplicação das medidas de segurança identificadas.

Este tem como objetivo mostrar o funcionamento geral do site, bem como disponibilizar as questões. No Protótipo não irão estar disponíveis todos os elementos e funcionalidades que seriam de esperar numa versão em produção.

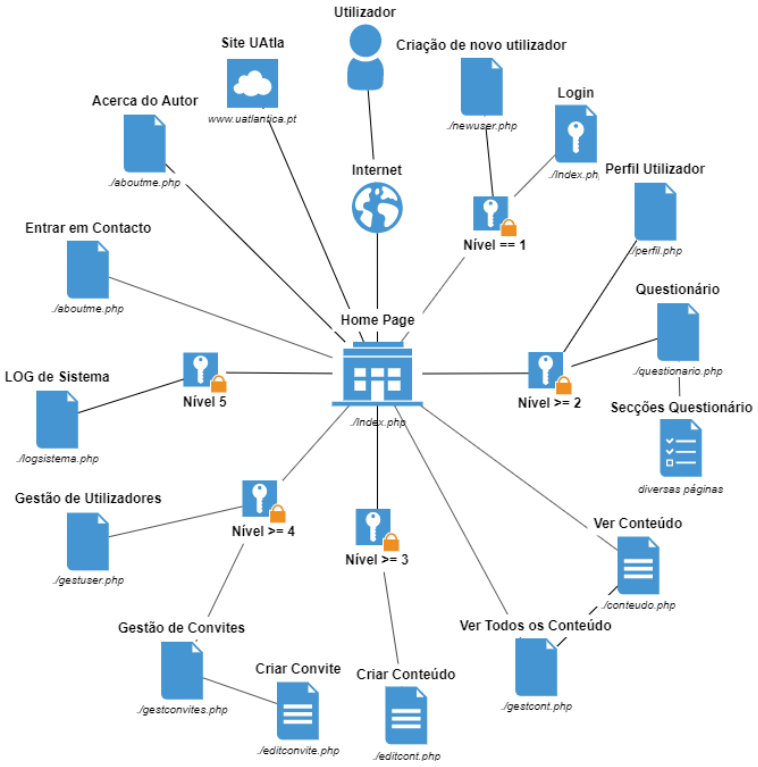


Figura 35 - Esquema Navegacional da plataforma

Na **Figura 35** podemos visualizar o esquema de navegacional do protótipo, sendo identificados apenas os componentes que foram implementados. Conforme se pode ver, toda a plataforma está centralizada numa página principal, onde existe a opção para navegar para as restantes.

Esta navegação baseia-se numa barra de topo que permite aceder a qualquer conteúdo que o Utilizador esteja autorizado, ou seja, apenas tem disponíveis os conteúdos que estão validados para o seu nível. Esta barra é incluída em cada página, estado o seu código no ficheiro `barratopo.php`.

No fundo de todas as páginas, encontra-se uma ligação a informações sobre a plataforma e o seu criador (`aboutme.php`) e à página institucional da Universidade Atlântica, estando ambos os códigos alocados no ficheiro `rodape.php`. Além das informações disponibilizadas nesta área, esta tem também como função, demonstrar a possibilidade da existência de um espaço para estes. Na **Figura 36** podemos ver em cima a barra de navegação para um utilizador não registado, no meio a mesma barra para um utilizador registado de nível 5 e por fim, no fundo, podemos ver o rodapé.

Figura 36 - Barra de navegação e rodapé

4.2. DETALHES DE INTERFACE

Neste subcapítulo irão ser apresentados em detalhe os principais elementos criados para o funcionamento da plataforma. Estes são representados pelo nome a negrito que se encontra na **Figura 35**.

4.2.1. HOME PAGE (INDEX.PHP)

Tal como as restantes páginas, esta foi criada em HTML usando como mecanismo lógico o PHP e como ligação ao armazenamento de dados o MySQL. Nela, encontra-se o corpo central de todo o protótipo, sendo que é remetido sempre que se pretende aceder a outros conteúdos. O corpo da página está dividido em 3 secções, sendo a primeira designada de “Conteúdos”, a segunda de “Grau de Implementação das Medidas de Controlo” e a terceira de “Últimos Eventos”.

A primeira secção tem como intuito a criação de um espaço em que os níveis 3 e superiores possam publicar informações úteis aos utilizadores sobre temas referentes aos ICS. Aqui, são apresentadas as últimas 5 introduções, havendo a possibilidade de aceder à página de visualização do total de conteúdos ativos (`gestcont.php`). Na **Figura 37** podemos observar esta página para o utilizador Nível 5 com a secção de conteúdos.

A segunda componente tem como objetivo mostrar os resultados do questionário preenchido. Nesta é apresentado um gráfico de barras horizontais para cada secção, sendo assim apresentada a média de cada uma. No topo, à direita, existe a indicação da média total da implementação das medidas de controlo. Aqui existe também um botão que permite a ligação ao questionário.

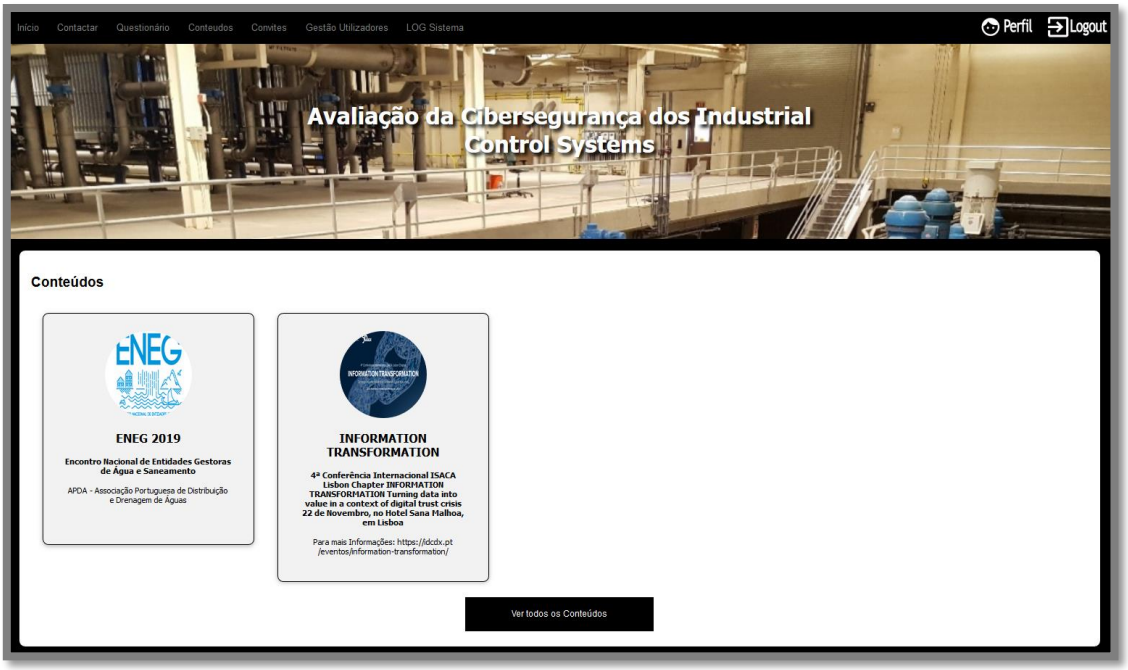


Figura 37 - Home page com secção de “Conteúdos”.

Figura 38 - Secção de "Grau de Implementação das Medidas de Controlo" (no cimo) e "Últimos Eventos" (em baixo)

Para a geração do gráfico, foi utilizada uma função disponibilizada pela Google, denominada Google Charts. Esta componente externa, permite a personalização dos gráficos de forma simples, permitindo a sua fácil integração. Esta secção é apresentada na **Figura 38** (no cimo)**.**

A última secção está limitada ao utilizador de nível 5 e apresenta os últimos principais eventos registados na plataforma. Este permite ao responsável perceber o funcionamento da mesma sem que tenha de ir consultar a página específica de Log de Sistema. Pode ser visualizado na **Figura 38** (em baixo).

Conforme se pode ver na **Figura 37**, no topo do ecrã existe ligação para a edição de Perfil de Utilizador e de Logout. Ambas as funções serão descritas de mais à frente neste capítulo.

4.2.2. NOVO UTIILIZADOR (NEWUSER.PHP)

Para se aceder à plataforma, os utilizadores interessados deverão proceder à sua inscrição na mesma. Para tal necessitam de ter um convite, sendo este gerado pelos níveis superiores a 4. Após a receção do email com as credenciais, o utilizador acede à página de Novo Utilizador (`newuser.php`) e preenche os dados solicitados.

Além dos correspondentes aos seus dados, o utilizador dever introduzir o email, nível e código iguais aos do email, uma vez que a criação apenas é possível se estes forem iguais aos existentes na tabela `convite`. Além destas, a plataforma também verifica se o nome de utilizador e email são únicos, não permitindo o avanço caso estes já existam na tabela `utilizador`.

Aquando da criação de um novo utilizador, além de ser feita uma nova entrada na tabela `utilizador` com os dados deste, são também introduzidos na tabela `questionario` e `perfil` entradas apenas com o *id* do utilizador, sendo os restantes dados a *null*, de forma a serem atualizados mais tarde.

Na **Figura 39** pode-se ver a página de criação de Novo Utilizador.

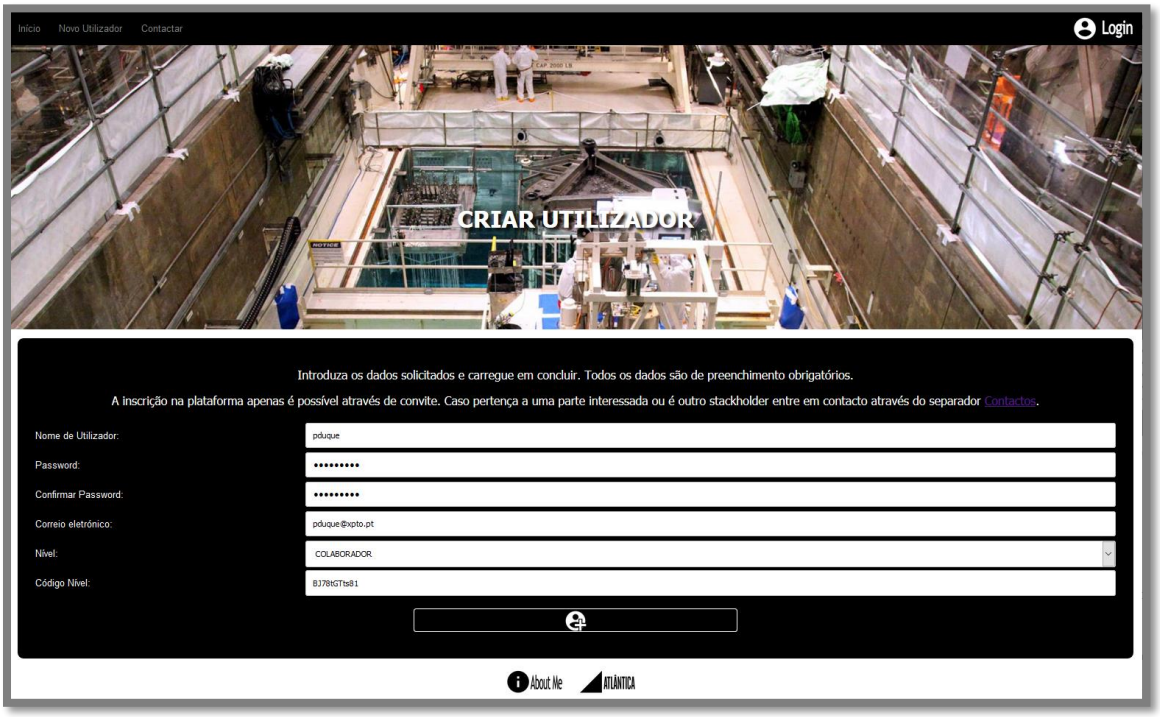


Figura 39 - Ecrã Criação de Novo Utilizador

4.2.3. CONTACTAR (CONTACTOS.PHP)

A qualquer altura da utilização da plataforma, é possível ao utilizador enviar uma comunicação ao responsável da plataforma. De forma a facilitar o contacto, foram gerados modelos que devem ser respeitados, sendo os mesmo escolhidos de um *dropdown menu*. Esta funcionalidade encontra-se na página `contactos.php` e pode ser observada na **Figura 40.**

O envio da comunicação é feito através de SMTP da conta QuestSegICS@gmail.com, tendo sido para tal utilizada uma função disponibilizada pela plataforma InfinityFree.

Figura 40 - Ecrã Entrar em Contacto

4.2.4. LOGIN (LOGIN.PHP)

Conforme se pode ver na barra mostrada na **Figura 36**, quando o utilizador não está autenticado, este tem a opção de proceder à sua autenticação. Esta é feita através de página própria, sendo esta conseguida através de uma forma que compara os dados introduzidos com os existentes na tabela `utilizadores` da base de dados. Os mecanismos de segurança

Figura 41 - Ecrã de Login

associados a esta operação serão detalhados no Subcapítulo 4.3. De seguida é apresentada a **Figura 41** onde se pode ver o ecrã de autenticação.

4.2.5. PERFIL DE UTILIZADOR (`INDEX.PHP`)

De forma a caracterizar o utilizador, foi criada uma página para o efeito, designada de `perfil.php`. Nesta, além dos dados pessoais do utilizador, são pedidas algumas informações para a caracterização da sua organização.

Nesta fase da plataforma, estes dados ainda não são utilizados para análise estatística, mas permitiram num desenvolvimento futuro, a aplicação de ferramentas de correlação de dados, por exemplo, entre a dimensão e os resultados obtidos.

Além destes, existe espaço para a inserção de uma ligação para uma imagem que identifique o utilizador. Da mesma forma, esta funcionalidade será útil numa fase posterior, onde serão colocadas algumas características de interação social entre os utilizadores.

Na **Figura 42** é possível visualizar-se esta Página.

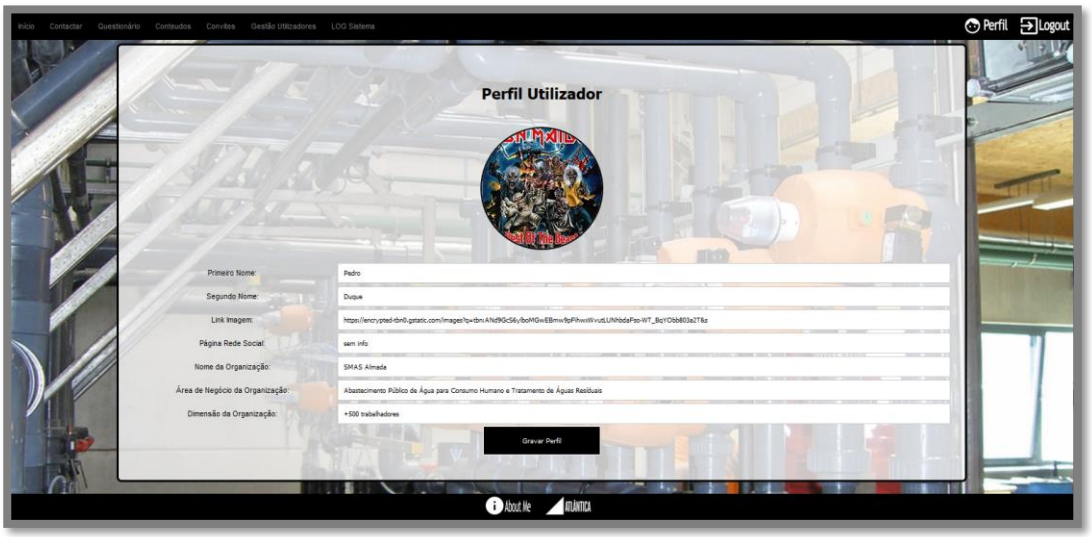


Figura 42 - Ecrã Perfil de Utilizador

4.2.6. QUESTIONÁRIO

Este conjunto de páginas são o ponto principal desta plataforma, uma vez que servem de "Checklist" de medidas de Cibersegurança a implementar na organização. Conforme se pode ver na **Figura 43**, existem ao total 13 secções que deverão ser avaliadas pelo utilizador, sendo estas:

Secção 1 - Governação e Gestão do Risco
Secção 2 - Continuidade de Negócio e Recuperação de Desastres
Secção 3 - Fortalecimento da Segurança dos Servidores e das Workstations
Secção 4 - Controlo de Acessos
Secção 5 - Segurança das Aplicações
Secção 6 - Encriptação
Secção 7 - Arquitetura, Telecomunicações e Segurança da Rede
Secção 8 - Segurança Física dos ICS
Secção 9 - Acordos com Entidades Externas
Secção 10 - Segurança da Operação
Secção 11 - Engenharia Orientada para a Cybersegurança
Secção 12 - Educação
Secção 13 - Papel dos Trabalhadores

Em cada uma destas existe um número variado de perguntas, sendo ao total 76. Estas são respondidas através de um input tipo *slider*, onde o utilizador deve escolher entre 0%, 25%, 50%, 75% ou 100% de grau de implementação de cada. Sempre que termina o preenchimento de uma página, este deve selecionar o botão “Inserir Resultados” e passar para a seguinte.

Uma vez que este questionário pretende funcionar não só como uma ferramenta de avaliação, mas também como uma ferramenta de apoio à implementação destas medidas, as respostas podem sempre ser revistas, sendo a mudança destas natural ao longo da evolução dos sistemas e das organizações. Todas os estes dados são armazenados na tabela `questionario` correspondendo a cada linha, uma resposta de um utilizador.

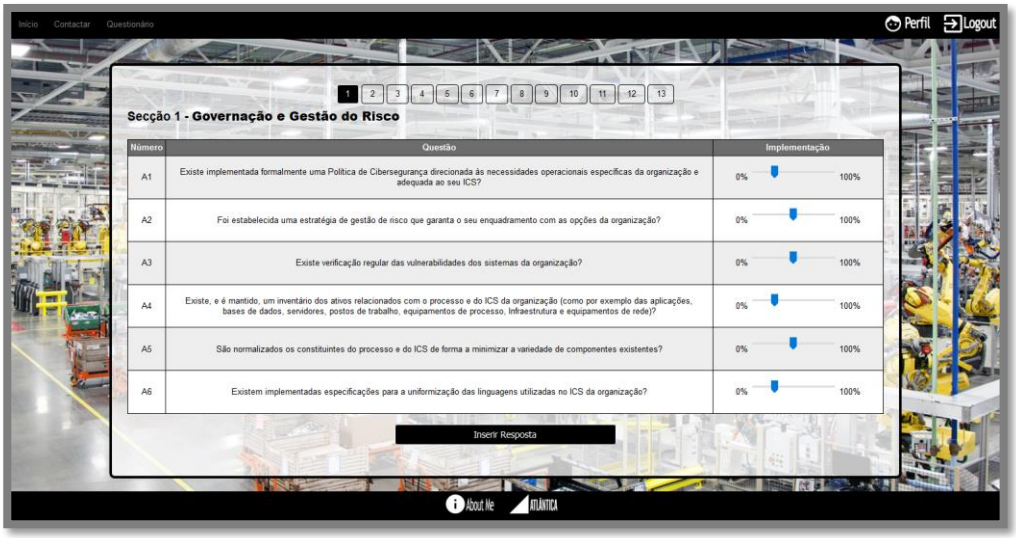


Figura 43 - Ecrã Preenchimento de Questionário

4.2.7. VER CONTEÚDO E CRIAR CONTEÚDO (`GESTCONT.PHP` E `EDITCONT.PHP`)

Conforme foi referido anteriormente, a plataforma permite a publicação de “conteúdos” relevantes para os interessados em ICS. Para tal foi criado um conjunto de páginas que permitem a publicação, a edição e a navegação nestes elementos, sendo as opções limitadas aos níveis dos utilizadores e se são ou não o criador dos mesmos. Na **Figura 44** é possível a ver-se o menu de gestão das mesmas (página `gestcont.php`) que utiliza a tabela `conteudo` para ler os elementos criados.

Figura 44 - Ecrã Gestão de Conteúdos

4.2.8. GESTÃO DE CONVITES (GESTCONVITES.PHP E EDITCONVITE.PHP)

Conforme foi referido anteriormente, o acesso à plataforma apenas é possível para utilizadores registados e para tal é necessária a existência de um convite. Este é criado no menu de gestão da página `gestconvites.php` por um utilizador com nível igual ou superior a 4, sendo introduzido um email, o nível pretendido e um código de validação. O código é gerado aleatoriamente, através de uma função criada para o efeito, podendo este ser personalizado e introduzido pelo administrador (**Figura 45**).

À semelhança do Contacto, ao ser selecionado um novo convite e serem validados os dados introduzidos, o sistema envia automaticamente um email para o endereço especificado com os dados necessários à criação de um novo utilizador.

Figura 45 - Ecrã Criação de Convite

Uma vez criado um convite, a tabela `convite` é novamente atualizada de forma a desativar o código, não podendo este ser utilizado novamente. Além desta funcionalidade, foi definido que apenas é possível eliminar os convites que ainda não foram ativados, sendo que os que já foram ativados, permanecem visíveis para consulta neste menu.

4.2.9. GESTÃO DE UTILIZADORES (GESTUSER.PHP)

De forma a serem geridos os utilizadores, foi criado um menu onde é possível aos utilizadores com nível igual ou superior a 4, fazer a gestão dos mesmos. Foram criados alguns mecanismos de gestão, tais como o utilizador não poder modificar as suas próprias definições ou os administradores não se poderem eliminar entre eles. Além da opção de eliminar, é também possível aos administradores bloquearem o acesso a utilizadores, ficando estes temporariamente impossibilitados de aceder ao site. Em ambos os casos, as ações são inseridas nos eventos do sistema.

Nesta página, é também possível proceder à criação de novo utilizador, através do ícone disponível para o efeito. Na **Figura 46** é possível ver o menu de Gestão de Utilizador.

Figura 46 - Ecrã Gestão de Utilizadores

4.2.10. LOG DE SISTEMA (LOGSISTEMA.PHP)

Conforme foi referido anteriormente, todas as principais ações efetuadas pelos utilizadores criam entradas na tabela `log` da base de dados. Aqui é possível filtrar os eventos pelo seu tipo, facilitando a monitorização do funcionamento da plataforma (**Figura 47**).

Às ações realizadas na plataforma (por exemplo criar utilizador ou eliminar convite) são acrescidas de uma *tab* com o resumo das ações efetuadas, nomeadamente, com a descrição, o *timestamp* e o seu responsável. Esta tab é então introduzida na tabela `log`.

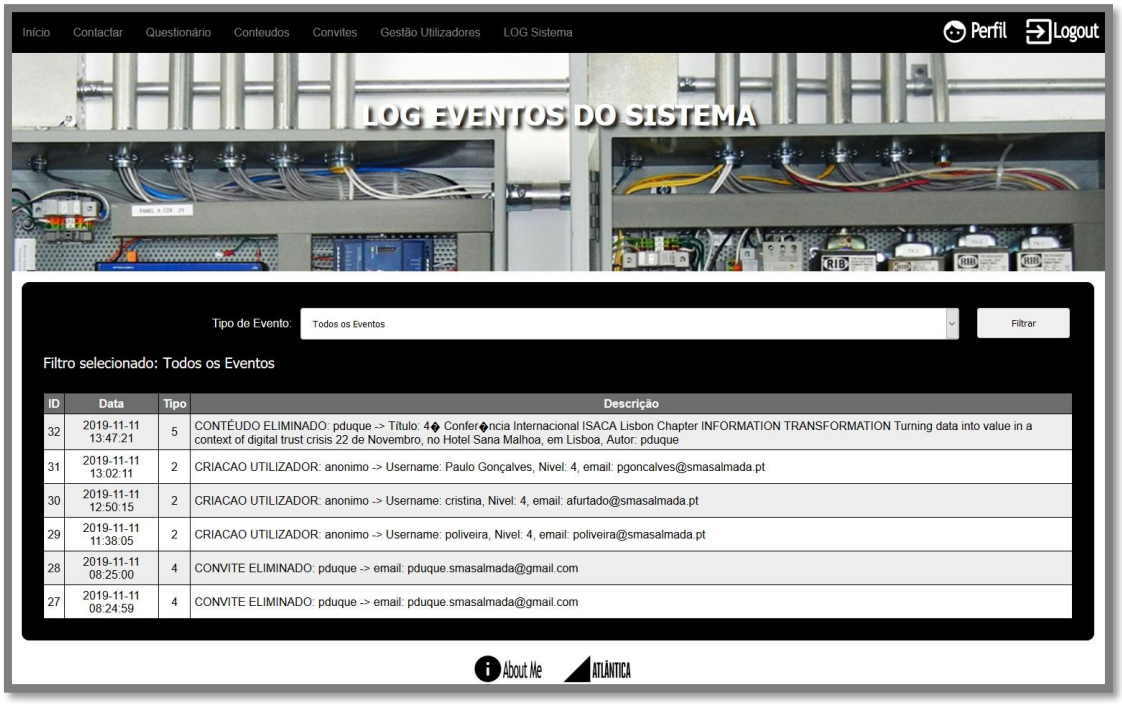


Figura 47 - Ecrã LOG de Sistema

4.3. OPÇÕES DE IMPLEMENTAÇÃO

Para o funcionamento da plataforma é necessário que sejam tomadas diversas decisões, quer em termos de funcionamento, quer ao nível da segurança. Assim, neste subcapítulo serão abordadas algumas das decisões tomadas para a criação e operacionalização desta.

4.3.1. ALOJAMENTO DA PLATAFORMA

Para a disponibilização online, foi necessária a escolha de uma plataforma gratuita que suportasse tanto o alojamento dos ficheiros das bases de dados, ao mesmo tempo que permitisse o uso de PHP e de HTML5. A resposta a estas necessidades foi a escolha da plataforma InfinityFree, optando-se pelo url http://questionarioics.epizy.com/.

4.3.2. DESIGN E CSS

Embora exista na internet um grande número de templates para a construção de páginas em html tendo como base o uso de bibliotecas de CSS, foi opção do autor a construção na integra destes elementos. Assim, foi criado o ficheiro `style.php` onde foi colocada a maioria do estilo, sendo estes compartilhados entre as diversas páginas da plataforma.

4.3.3. SQL INJECTION

De forma a aumentar a proteção contra este tipo de ataque, foram implementados mecanismos para o limitar. Uma das técnicas utilizadas foi o uso de *Prepared Statement* sempre que existe a introdução de dados por parte do utilizador. Desta feita, é usado um filtro sobre o tipo de dados introduzidos, garantido que os mesmos respeitam o que está previamente esperado.

Além disso foi também usado outro nível de proteção, o uso de *mysqli_real_escape_string* para a remoção de caracteres que podiam ser usados para a introdução de comandos maliciosos.

4.3.4. CREDENCIAIS DE ACESSO

Para o acesso à plataforma, é necessário que o utilizador esteja registado na mesma. Assim, é necessário coincidir vários dados entre os introduzidos e os armazenados na base de dados para a criação de novo utilizador, sendo depois necessária a introdução das credenciais para o login.

Após a autenticação do utilizador, é guardado o seu nível numa variável de sessão de forma a poder ser utilizado enquanto o browser se mantiver aberto. Desta forma, antes da execução do código de cada página e do seu carregamento a partir do servidor, é testado sempre qual o seu nível. Desta forma, caso seja acedido o url através de introdução direta no browser, esta não irá funcionar, ficando assim salvaguardado o acesso indevido.

4.3.5. ARMAZENAMENTO DE DADOS

A privacidade é atualmente uma das grandes preocupações quando se fala de gestão de dados. Desta forma, os dados são armazenados em bases de dados protegidas por password, sendo as ferramentas necessárias à sua gestão, disponibilizada pela própria plataforma InfiniyFree. De forma a aumentar a proteção, o acesso a esta é também dependente do uso de credenciais.

Em termos de encriptação, apenas se optou por aplicar esta no armazenamento das passwords de acesso. Esta decisão foi tomada por forma a respeitar a privacidade dos utilizadores, garantindo assim que mesmo durante as ações de desenvolvimento e manutenção da plataforma, a sua privacidade é assegurada. A técnica utilizada foi o comando *password_hash()*, sendo a password introduzida encriptada através do algoritmo standard do HTML5.

CAPÍTULO 5

VALIDAÇÃO

5.1. TESTES POR PERFIL DE UTILIZADOR

Para a realização dos testes do protótipo optou-se por disponibilizar o mesmo a especialistas tanto da área da informática como dos processos industriais de instalações suportados por ICS. Decidiu-se pela criação de dois grupos baseados nas áreas de especialidade para o agrupamento dos resultados, dando a todos os utilizadores o mesmo nível de acesso, Administrador. De seguida é esquematizada a metodologia adotada:

1º Contacto Telefónico

Contacto telefónico com os especialistas para os convidar a participar nos testes, tendo sido dada uma breve explicação sobre a plataforma e os objetivos do teste.

2º Criação de Convite

Criação na plataforma do convite para os utilizadores com o seu e-mail, códigos e níveis. Para o e-mail optou-se, sempre que possível, pelo uso de e-mail profissional de forma a aumentar a credibilidade dos utilizadores perante terceiros. Por sua vez, os códigos foram gerados aleatoriamente e o nível foi igual para todos, optando-se pelo "Administrador" equivalendo a nível 4.

3º Envio Convite

Optou-se por não enviar o convite diretamente pela plataforma devido à necessidade de personalização do texto e de envio de anexo. Assim, foram enviadas as credenciais, o texto explicativo do projeto e o documento de avaliação pelo e-mail QuestSegICS@gmail.com.

4º Teste da Plataforma

Coube aos especialistas o dever de testar as funcionalidades da plataforma, dando especial ênfase às medidas propostas no questionário e sua aplicabilidade. Desta forma, estes não deveriam analisar se as medidas estavam ou não implementadas em determinada organização, mas sim, através da sua experiência, verificar se as mesmas tinham lógica e se poderiam ser avaliadas numa situação real.

5º Avaliação

Conforme foi referido, foi enviado aos especialistas um questionário para avaliação da plataforma. O questionário encontra-se disponível no Anexo 2 e está dividido em 5 secções que serão explicadas no subcapítulo seguintes.

6º Envio Avaliação

Após a conclusão do preenchimento da avaliação, o especialista envia-a de volta para o email do autor do trabalho.

7º Análise das Avaliações

Tendo por base a análise das avaliações recebidas, foram elaboradas tabelas para a compilação e análise dos dados.

Na tabela seguinte estão os perfis e a caracterização dos diversos especialistas convidados para participar na avaliação do protótipo:

Especialista	Perfil	Experiência	Data Teste	Respond?
1	Informática	33 anos	11/11/2019	Sim
2	ICS	21 anos	11/11/2019	Sim
3	ICS	17 anos	11/11/2019	Sim
4	Informática	-	-	Não
5	Informática	30 anos	13/11/2019	Sim
6	ICS	17 anos	12/11/2019	Sim
7	Informática	-	-	Não
8	ICS	15 anos	13/11/2019	Sim
9	Informática	14 anos	12/11/2019	Sim

5.2. PREENCHIMENTO E AVALIAÇÃO DE QUESTIONÁRIOS INDIVIDUAIS

O questionário foi estruturado em 5 secções, sendo estas descritas de seguida:

a) Caracterização do Convidado e Perfil do Utilizador
Nesta secção pretendeu-se recolher alguns dados relativos à identificação do especialista convidado, nomeadamente o seu perfil e os anos de experiência que detém na área.

b) Avaliação da Interface
Nesta secção pretende-se avaliar as questões relacionadas com a interface da plataforma, tendo sido questionadas as opiniões relativas a características como aspeto, intuítividade facilidade de navegação e a organização dos conteúdos.

c) Avaliação de Medidas de Controlo
Esta secção tem como objetivo avaliar as medidas propostas para aumentar a segurança dos ICS. Nesta era esperado que os especialistas analisassem questões como a aplicabilidade das medidas, a potencial eficiência, a adequação às organizações e a sua atualidade face aos riscos.

d) Considerações Finais
Nesta secção pretendia-se a recolha de opiniões qualitativas sobre a plataforma, tendo sido elaboradas perguntas de resposta aberta, relativas ao protótipo e ao conceito do projeto em termos da sua utilidade enquanto ferramenta para aumentar a Cibersegurança dos ICS.

Em termos de concretização de respostas, obteve-se 77,78% de retorno, tendo sido convidados 9 especialistas e tendo sido recebido em tempo útil 7 questionários de avaliação. De seguida são apresentadas três tabelas com os resultados obtidos nas três últimas secções referidas anteriormente nas alíneas b), c) e d).

5.2.1. AVALIAÇÃO DA INTERFACE

Os resultados obtidos estão descritos na tabela seguinte, tendo sido retirados os utilizadores que não entregaram os questionários em tempo útil.

Especialista	Facilidade de navegação	Intuitividade	Aspeto atraente	Características Modernas	Organização dos Conteúdos	Média
1	4	4	4	4	4	4,00
2	5	5	5	5	-	5,00
3	5	4	3	4	4	4,00
4	-	-	-	-	-	-
5	3	2	4	4	5	3,60
6	4	4	3	4	4	3,80
7	-	-	-	-	-	-
8	4	5	5	5	4	4,60
9	4	3	3	3	4	3,40
Média	4,14	3,86	3,86	4,14	4,17	

A partir destes dados, foram elaborados os gráficos (**Figura 48**) onde é possível verificar-se a avaliação positiva dos tópicos questionados. Destacam-se a característica "**Organização dos Conteúdos**" que obteve uma apreciação média de 4,17% como melhor resultado e a "**Intuitividade**" o "**Aspeto Atraente**", ambas com 3,86 o valor mais baixo.

Tem que ser levado em consideração que as respostas do Especialista 1 encontra-se "deturpada" por não ter respondido ao campo Organização dos Conteúdos, uma vez que considera que "Não consegue avaliar".

A média total destas componentes foi avaliada em **4,03** considerando-se um resultado satisfatório.

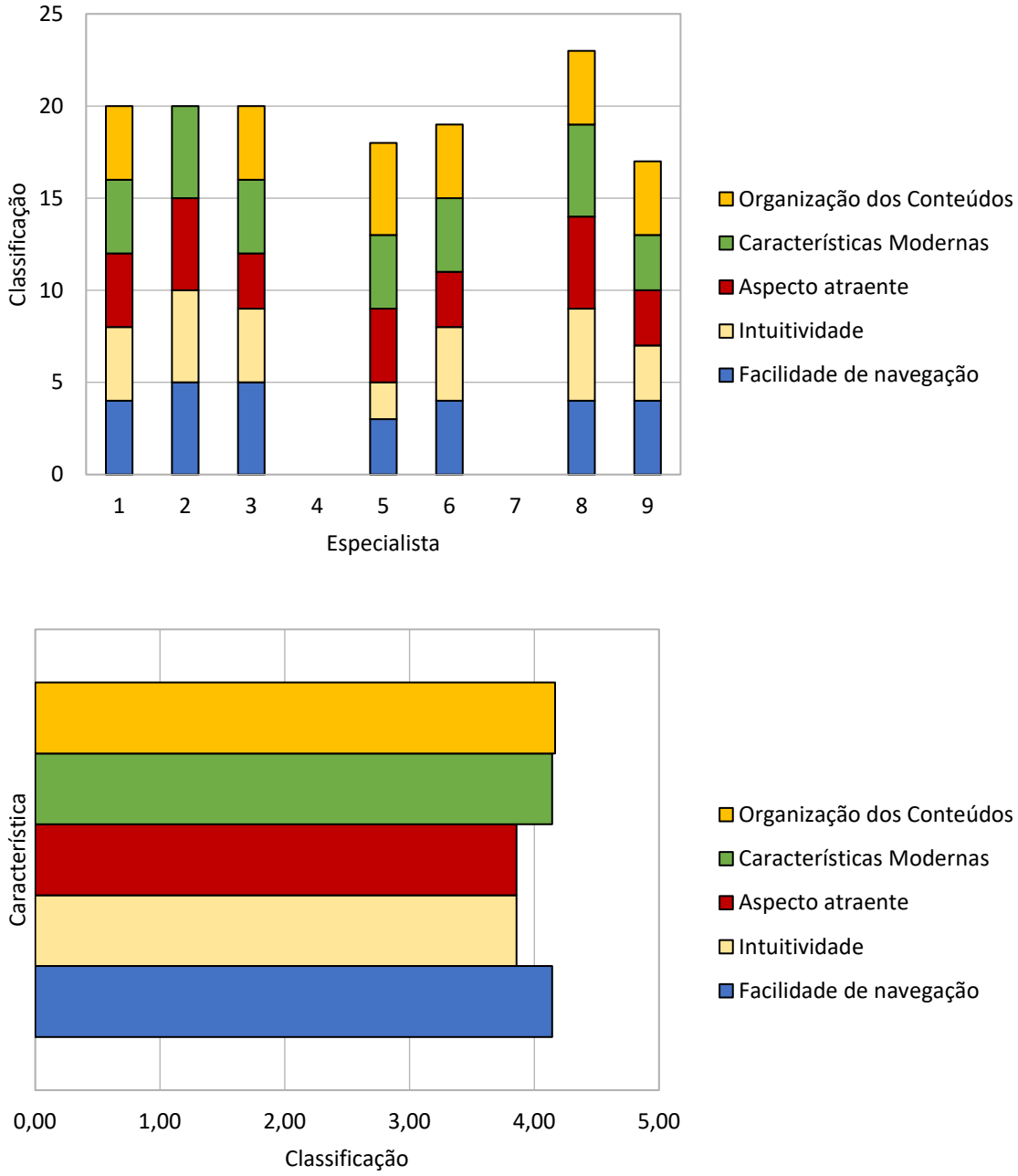


Figura 48 - Representação gráfica dos resultados da Avaliação do Interface

5.2.2. AVALIAÇÃO DAS MEDIDAS DE CONTROLO

À semelhança do ponto anterior, os resultados obtidos estão descritos na tabela seguinte, tendo também sido retirados os utilizadores que não entregaram os questionários em tempo útil.

Especialista	São aplicáveis?	São eficientes?	Estão atualizadas aos riscos atuais?	Englobam as necessidades da organização?	Ajudam a implementar as medidas?	Média
1	5	5	5	4	4	4,60
2	5	4	5	5	5	4,80
3	4	4	4	5	5	4,40
4	-	-	-	-	-	-
5	4	4	3	3	5	3,80
6	4	4	4	4	4	4,00
7	-	-	-	-	-	-
8	5	5	5	5	4	4,80
9	4	4	4	4	4	4,00
Média	4,43	4,29	4,29	4,29	4,43	

A partir destes dados, foram elaborados os gráficos (**Figura 49**) onde, à semelhança do ponto anterior, também é possível verificar-se a avaliação positiva dos tópicos questionados. Embora em todos existam resultados bastante satisfatórios, destacam-se as características "**São aplicáveis?**" e "**Ajudam a implementar as medidas?**" que obtiveram uma apreciação média de 4,43 como melhor resultado e as restantes características com 4,29 como valor mais baixo.

De notar que o Especialista 1, com funções num ICS, considera que não pode avaliar a eficiência com grande grau de confiança por considerar que a avaliação necessita grande grau de conhecimento informático.

Também o mesmo utilizador considera que a implementação da avaliação das medidas é especialmente útil para a utilização com *checklist* de apoio à implementação das mesmas.

A média total destas componentes foi avaliada em **4,34** considerando-se um resultado satisfatório.

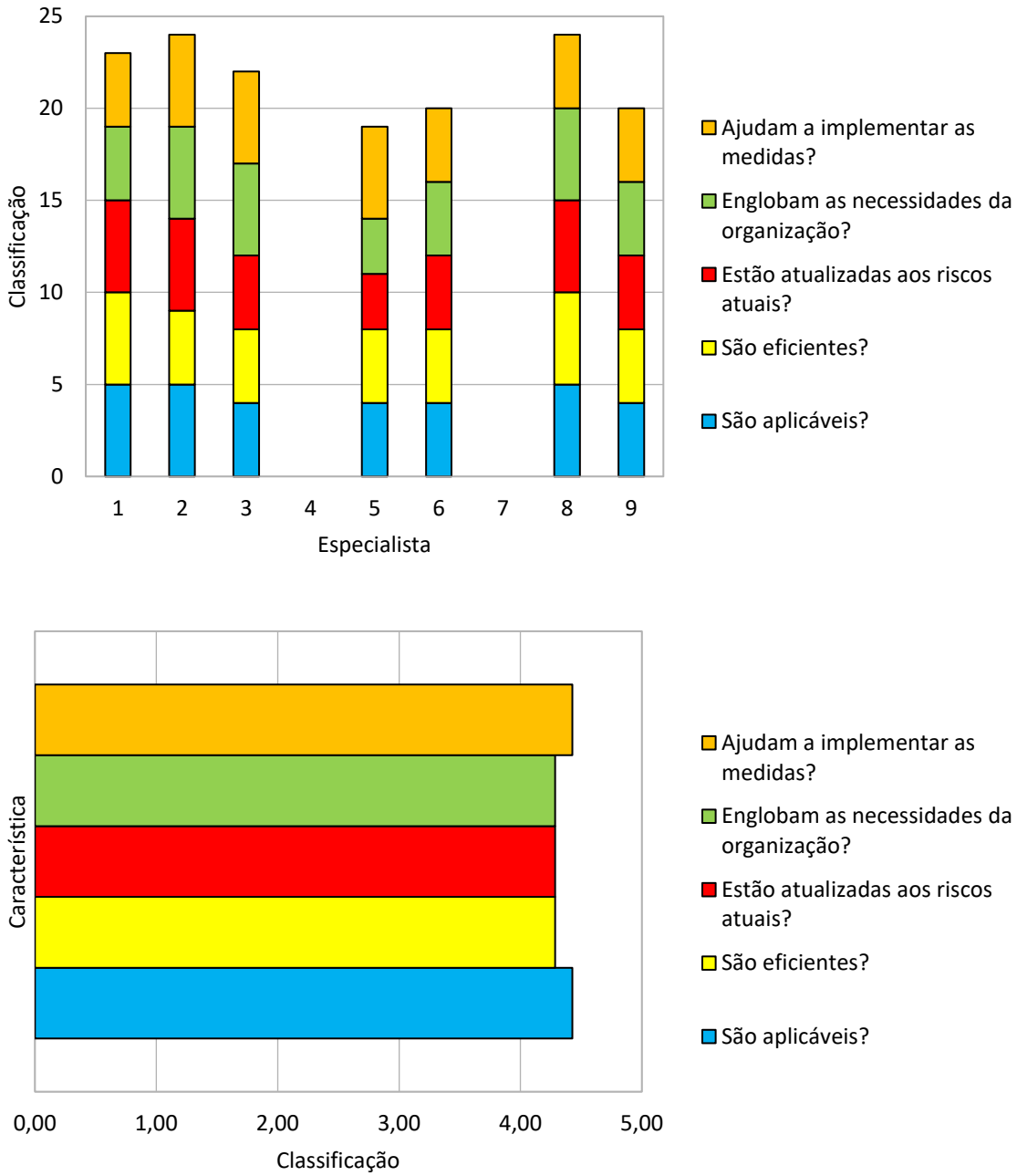


Figura 49 - Representação gráfica dos resultados das Medidas de Controlo

5.2.3. AVALIAÇÃO GLOBAL

Em termos de avaliação global do protótipo, foram em geral apreciações positivas, tendo contudo, sido feitos alguns comentários construtivos que permitiram a melhoria do protótipo nas fases seguintes.

De seguida encontra-se a compilação das respostas dos especialistas. Uma vez que as respostas são abertas, estas foram uniformizadas pelos seus conteúdos, evitando assim a repetição das mesmas. Criou-se o grupo das apreciações positivas e o grupo das apreciações negativas.

Uma vez que neste campo eram esperadas respostas qualitativas, não serão levadas em consideração as respostas quantitativas recebidas, uma vez que estas serão analisadas no último ponto deste capítulo.

a) Considera útil a existência de uma plataforma para o apoio à implementação de medidas para o aumento da cibersegurança dos ICS?

Apreciações Positivas	Apreciações Negativas
- A plataforma é importante para a organização em todas as áreas, ainda mais importante nos ICS porque as consequências poderão ser mais graves. - Se implementada, poderá ser bastante útil por ir aumentar a *awareness* para o problema que os responsáveis das diversas vertentes das ICS têm em relação à Cibersegurança. - Poderá ser um apoio muito importante o para as empresas como forma de resposta ao crescente número de ataques.	- Algumas questões a rever de pormenor a resolver.

b) Considera que as medidas de controle avaliadas no questionário correspondem à necessidade de cibersegurança dos ICS, nomeadamente, das Infraestruturas Críticas?

Apreciações Positivas	Apreciações Negativas
- Considera que uma vez que as organizações ainda não estão preparadas para a Cibersegurança dos ICS, o questionário vai permitir às organizações entenderem as suas fragilidades. - Considera que as medidas referidas, quando implementadas, vão reduzir o risco de ciberataques, uma vez que contribuem para o aumento da cibersegurança.	- Sem o tempo necessário para uma avaliação mais cuidada. - Necessidade de implementação prática das medidas para uma melhor avaliação.

c) Pontos positivos e negativos do protótipo?

Apreciações Positivas	Apreciações Negativas
- Existência das medidas de controlo. - Interface simples e atraente, facilitando o acesso e sendo percetível para *non-experts*. - Interface visualmente interessante. - O questionário é abrangente e completo nas diversas vertentes da Cibersegurança. - Conceito inovador.	- Poderiam existir mais funcionalidades na secção de conteúdos. - Em algumas questões, constam termos específicos em inglês que não são conhecidos pelos utilizadores não especialistas em informática (ex: Whitlisting, patches, ciberwarness, ciberhigiene, bootleneks, default, etc.). - Alguns problemas de compatibilidade com os caracteres no browser tornam difícil perceber alguns textos.

	- Necessidade de ligação das questões a resultados práticos. - No questionário, ao terminar uma secção, deveria passar para o seguinte. - No questionário, deveria aparecer o valor escolhido com a barra ou as mesmas terem legendas. - Cores demasiado escuras.

d) O que acrescentaria ao protótipo?

- Comentários aos resultados com sugestão de caminhos a seguir e soluções para os problemas identificados.
- Mais conteúdos informativos.
- Legenda das siglas técnicas do questionário (ex: VPN, ICS, IT, ftp).
- Algumas questões da navegação entre conteúdos deviam ser melhoradas (ex. abertura de página sem ser no inicio, mas sim no conteúdo que se estava a consultar; melhoria de navegação entre secções do questionário; no contacto, simplificar a escolha de assunto).
- Deviam ser acrescentados pedidos de confirmação de ações (ex. eliminação de conteúdos).
- Garantir que os links externos do rodapé são abertos em novo separador.
- Melhorar a utilização do Perfil de Utilizador.
- Para aumentar a segurança, não se deve descriminar se é o user ou pass que estão errados no login.
- Existência de funções para execução de teste prático demonstrativo das funcionalidades.

e) Avaliação global do protótipo?

- Em geral entre o bom e o muito bom com bastante utilidade.
- Com algumas "questões" a rever, mas de pormenor.
- A ser implementado, irá aumentar a *awareness* para o problema que os responsáveis das diversas vertentes das ICS têm em relação à Cibersegurança.

De forma a ser possível avaliar a plataforma em valores absolutos, os especialistas foram também questionados sobre a sua avaliação global do projeto, balizando os resultados entre 1 e 5, tendo sido obtido o valor final de **4,00**. De seguida na **Figura 50** podemos ver o gráfico com estes resultados.

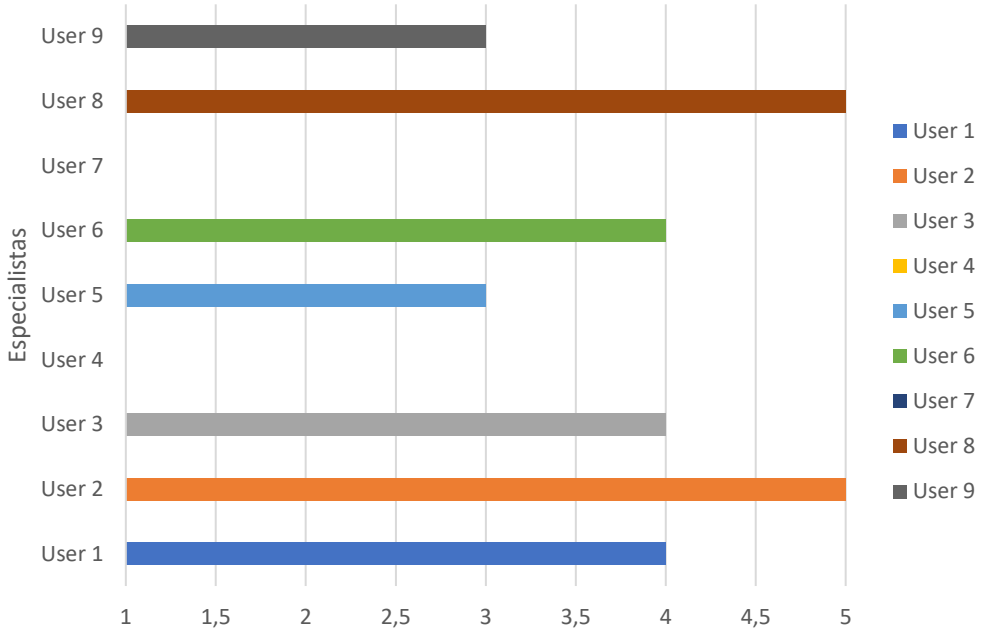


Figura 50 - Representação gráfica dos resultados da Avaliação das Medidas de Controlo

5.2.4. CONSLUSÕES DOS RESULTADOS OBTIDOS

Embora sendo o valor global obtido elevado e assim como a generalidade das considerações são positivas, considera-se que o resultado esteja um pouco enviesado pela dimensão da amostra, pelos perfis dos utilizadores não serem especialistas em Cibersegurança de ICS e representarem um universo pequeno de organizações. Contudo, podemos tirar algumas conclusões das opiniões dos participantes neste teste, transformando-os em tarefas a desempenhar como forma de melhorar a plataforma:

- Será necessário que sejam feitas algumas alterações ao nível da navegação, facilitando-a entre conteúdos e seleção de opções;

- Deverão ser colocadas mais opções, nomeadamente na página do Questionário e dos Conteúdos;

- Deverão ser acrescentadas ferramentas para que, após a realização do questionário, o utilizador possa continuar a aumentar a Cibersegurança do ICS.

- Deverá ser alterado o uso de siglas durante a plataforma ou acrescentado o seu significado em separador próprio;

- O Código da plataforma deverá ser revisto de forma a corrigir alguns erros detetados pelos utilizadores;

CAPÍTULO 6

CONCLUSÕES

Este trabalho foi criado tendo como questão principal a:

"Necessidade da criação de uma ferramenta online para a auxiliar na implementação e avaliação do ICS de uma determinada organização."

Para ser alcançada a resolução desta questão, foram formulados 4 objetivos intermédios. O cumprimento destes, permite não apenas a avaliação do projeto, mas principalmente, o encaminhamento destes, servindo de guia.

Em relação ao O1 "**Identificar os principais fatores que contribuem para a ciber(in)segurança dos sistemas ICS**" foi desenvolvido no 2º Capítulo, no ponto 2.3.3 "Vulnerabilidades utilizadas por ataques comuns", um levantamento sobre estes fatores. Assim, este ponto é considerado como cumprido.

No seguimento do anterior, o objetivo O2 "**Identificar boas práticas ao nível da Cibersegurança (física/lógica)**" pretende dar resposta as vulnerabilidades apresentadas previamente.Como vimos, na secção 3.6 "Avaliação de Cibersegurança" foi criada uma listagem completa com as práticas identificadas pela "*Cybersecurity Framework*" da *National Institute of Standards and Technology* (NIST) referentes às questões da cibersegurança das organizações com ICS. Esta pode ser analisada no Anexo I intitulado "Questionário Sobre Práticas de Cibersegurança nos ICS". Pelas evidências referidas anteriormente, considera-se que o objetivo foi cumprido.

Na formulação do objetivo O3 "**Definir a arquitetura do sistema visando a instanciação de um protótipo**" definiu-se que fosse definido o funcionamento da ferramenta para identificar a questões relacionadas com os ICS das organizações. Para tal, foi criado todo o Capítulo 3, onde a Arquitetura do Sistema foi definida e explicada. Desta forma, considera-se que foi cumprido o objetivo.

Por fim, O4 "**Criar uma ferramenta web para avaliação das questões de segurança de um ICS existente na organização**" estipulava que a ferramenta esquematizada anteriormente deveria funcionar online através de uma página web. Assim, foi desenvolvida a plataforma "Avaliação da Cibersegurança dos Industrial Control Systems" disponível no url http://questionarioics.epizy.com. À semelhança dos objetivos anteriores, também este foi cumprido.

Conforme se pôde ler anteriormente, todos os 4 objetivos foram cumpridos, podendo desta forma considerar-se que a questão que esteve por trás da criação deste trabalho ficou solucionada. Chega-se a esta conclusão pois, no final deste trabalho, existe uma plataforma online que permite apoiar um responsável por um ICS na implementação de medidas para melhorar a cibersegurança da sua instalação e a organização.

Para a validação deste trabalho foram contactados especialistas, tando de informática como de instalações com ICS que produziram críticas construtivas sobre o mesmo. Destes foi possível retirar um conjunto de informações que não só permitiram corrigir erros e problemas no imediato, como serviram de mote para a definição dos trabalhos futuros.

De acordo com o sugerido pelos especialistas e com as espectativas do próprio autor da plataforma, a continuação do desenvolvimento deste trabalho devia ser em 2 eixos independentes.

No primeiro, deveria ser melhorada a ferramenta de avaliação, sendo adicionadas ferramentas para a elaboração de uma Avaliação de Riscos e outra para acompanhar a implementação das medidas. Ambas as melhorias permitiriam focar mais nas características de cada ICS e respetiva organização, tornando a implementação das medidas mais eficiente, ao mesmo tempo que, permitiria um melhor acompanhamento das mesmas.

O segundo eixo que deveria ser levado em consideração como trabalho futuro é o aumento das opções Sociais. Embora não seja intenção criar uma rede social, a implementação de algumas das características destas seria uma mais valia. Questões como a partilha de conteúdos em diversas redes sociais, a comunicação entre utilizadores ou a possibilidade de discussão de temas entre utilizadores são algumas das opções válidas que aumentariam o potencial do projeto.

Considerando que o autor do projeto assume este é apenas uma ferramenta académica, sem intenção de o tornar online após a conclusão deste trabalho, os trabalhos futuros propostos

enquadram-se na ótica de continuação dos estudos, ou seja, num ciclo superior como um Mestrado ou Pós-graduação. Neste caso, além de toda a revisão teórica que teria de ser feita, deveriam ser implementadas estas medidas ao mesmo tempo que deveria ser alargado o leque de participantes na avaliação do “novo protótipo”.

REFERÊNCIAS

Ackerman, Pascal. *Industrial Cybersecurity.* Birmingham: Packt Publishing, 2017.

AWWA. *About Us.* 2019.

Ayllon, Nelly. *PROFIBUS vs PROFINET - Comparison and Migration Strategies.* 2. Scottsdale: PI North America, 2016.

Bartman , Tom, e Kevin Carson. “Securing Communications for SCADA and Critical Industrial Systems.” *Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions*, 2018.

Butterworth, Jim. “Threat Vectors.” *Handbook SCADA/Control Systems Security*, 2013: 57-68.

CSE-Semaphore. *Remote Automation and Monitoring: PLC or RTU?* Sheffield, 2010.

Curran, Mark, e Brian Shirk. *Basics of Fiber Optics.* Allen, Texas: Amphenol Fiber Systems International, 2015.

Dine, Alexandra Van. “Project on Nuclear Issues.” Em *A Collection of Papers from 2016 Nuclear Scholas Initiative and PONI Conference Series*, de Mark Cancian, 101-114. ashington: CSIS, 2016.

Falliere, Nicolas, Liam O Murchu, e Eric Chien. *W32.Stuxnet Dossier - v1.4.* Symantec Security Response, 2011.

Filali-Yachou, Said. “HMI/ SCADA standards in the design of data center interfaces: A network operations center case study.” *DYNA 82* (Universidad Nacional de Colombia), 2015: 180-186.

Goldsmith, Andrea. *Wireless Communications.* Cambridge : Cambridge University Press, 2005.

Grami, Ali. *Introduction to Digital Communications.* Londres: Elsevier, 2016.

Gruhn, Paul. “Human Machine Interface (HMI) Design: The Good, The Bad, and The Ugly (and what makes them so).” Houston, TX, USA: ICS Triplex, 2011. 1 - 10.

Hayden, Ernie, Michael Assante, e Tim Conway. *An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity.* USA: SANS™ Institute, 2014.

Hollifield, Bill, Dana Oliver, Ian Nimmo, e Eddie Habibi. *The High Performance HMI Handbook.* 1ª. Houston, TX, USA: PAS, 2008.

James Powell, P. *Profibus and Modbus: a comparison.* Karlsruhe: Siemens, 2013.

Knapp, Eric D., e Joel Thomas Langill. *Industrial Network Security.* 2ª. Editado por Samani Raj . Waltham: Elsevier, 2015.

Kott, Alexander, e Edward J.M. Colbert. *Cyber-security of SCADA and Other Industrial Control Systems.* Springer, 2016.

Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum* 50 (03 2013): 48 - 53.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, e Juraj Malcho. *Stuxnet Under the Microscope.* ESET, 2010.

Nixon, Robin. *Learning PHP, MySQL, JavaScript and CSS. 2*ª. Editado por Andy Oram. Sebastopol, California: O'Reilly Media, Inc., 2012.

Ozdemi, Engin, e Mevlut Karacor. "Mobile phone based SCADA for industrial automation." *ISA Transactions* 45 (1 2006): 67-75.

PROFIBUS, Nutzerorganisation;. *PROFINET System Description - Technology and Application.* Karlsruhe: PROFIBUS & PROFINET International, 2014.

Rouse, Margaret. *TechTarget.com.* 2017. https://searchsecurity.techtarget.com/definition/worm (acedido em 07 de 10 de 2019).

SCME, Southwest Center for Microsystems Education. *Introduction to Transducers, Sensors and Actuators.* Albuquerque, USA: University of New Mexico, 2011.

Siemens. "Step 2000 Basis Of PLC." Em *PLCs*, 4-7. Georgia, EUA: Siemens, 2000.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, e Adam Hahn. *Guide to Industrial Control Systems (ICS) Security.* 2. USA: NIST, 2015.

Susman, Gerald I., e Roger D. Evered. "An Assessment of the Scientific Merits of Action Research." *Administrative Science Quarterly*, 1978: 582-603.

Temprana, E., et al. "Overcoming Kerr-induced capacity limit in optical fiber transmission." *Science*, 2015: 1445-1448.

Thomas, George. "Introduction to Modbus Serial and Modbus TCP." *The Extension - A Technical Supplement to Control Network*, Setembro de 2008.

Turc, Traian. "Using WEB Services in SCADA Applications." *8th international Condeferen Interdisciplinarityin Engineering, INTER-ENG 2014, 9-10 October 2014.* Tirgu-Mures, Romenia: Procedia Technology, 2014. 584-590.

Ubiquiti. “Ubiquiti Networks.” *Air-Fiber 11fx.* s.d. https://www.ui.com/airfiber/airfiber-11fx/ (acedido em 02 de 05 de 2019).

Ujvarosi, Alexandru. “Evolution of SCADA Systems.” *Bulletin of the Transilvania University of Braşov* 9, nº 1 (2016): 63 - 68.

Weiss, Joe. “Water/Waster Control System Cyber security.” Em *Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems*. Applied Control Solutions, 2016.

West Yost Associates. *Water Sector Cybersecurity Risk Managment Guidance.* 3ª. American Water Works Association, 2019.

ANEXO I - QUESTIONÁRIO SOBRE PRÁTICAS DE CIBERSEGURANÇA NOS ICS

1. Governação e Gestão do Risco

1.1 - Existe implementada formalmente uma Política de Cibersegurança direcionada às necessidades operacionais específicas da organização e adequada ao seu ICS?

1.2 - Foi estabelecida uma estratégia de gestão de risco que garanta o seu enquadramento com as opções da organização?

1.3 - Existe verificação regular das vulnerabilidades dos sistemas da organização?

1.4 - Existe e é mantido, um inventário dos ativos relacionados com o processo e do ICS da organização (como por exemplo as aplicações, bases de dados, servidores, postos de trabalho, equipamentos de processo, Infraestrutura e equipamentos de rede)?

1.5 - São normalizados os constituintes do processo e do ICS de forma a minimizar a variedade de componentes existentes?

1.6 - Existem implementadas especificações para a uniformização das linguagens utilizadas no ICS da organização?

2. Continuidade de negócio e recuperação de desastres

2.1 - Existe um Plano de Continuidade de Negócios/ Recuperação de Desastres adequado ao ICS incluindo, por exemplo, uma equipe de Gestão de Crises, redundância de equipamentos ou sistemas, possibilidade de funcionamento manual como *bypass* ao sistema, capacidade de recuperação ou trabalho *offline?*

2.2 - Nos Plano de Continuidade de Negócios da empresa estão incluídos os procedimentos, responsabilidades e contactos relacionados com os ICS?

2.3 - Existe na organização um ou mais softwares para a criação de backups e gestão dos softwares utilizados no ICS, nomeadamente, para o registo das alterações efetuadas?

2.4 - Os backups e as metodologias de recuperação são testadas regulamente?

3. Fortalecimento da Segurança dos Servidores e das Workstation

3.1 - Está implementada uma *whitelisting* para as aplicações que são autorizadas a correr em cada computador ou posto de trabalho?

3.2 - Os contratos de manutenção dos softwares HMI, bem como a aplicação de *patches* para a atualização de anti-virus, anti-malwares e dos sistemas operativos estão de acordo com o definido pelo fabricante?

3.3 - Existe implementado um ou mais programas para gerir a implementação de *patches* e verificações periódicas destas vulnerabilidades?

34 - Existe um ou mais programas para a gestão das alterações efetuadas às aplicações, equipamentos e infraestruturas?

3.5 - Quando não necessário, as contas de administradores locais, de convidados e *default* dos Sistemas Operativos são desativados. As contas de administrador têm os seus nomes de login diferentes das default?

3.6 - Quando não essencial e por sistema, as portas USB, os leitores de CD/DVD e outros interfaces locais foram desativadas dos postos de trabalho e terminais?

3.7 - Quando ativos as interfaces locais, foram desativados os sistemas de auto-run dos dispositivos conectados?

4. Controlo de Acessos

4.1 - Existem medidas de proteção para acesso às instalações e equipamentos?

4.2 - É necessário uso de aplicações para aceder a funções chave do sistema?

4.3 - O acesso à ligação entre o ICS e exterior é controlada, nomeadamente, a troca de ficheiros, atualizações e servidores externos?

4.4 - É possível utilizar o sistema em offline ou isolado para a aplicação de atualizações ou instalação de novos componentes?

4.5 - Estão identificados os privilégios necessários para acesso de entidades externas, dando o mínimo acesso possível a este tipo de utilizadores?

4.6 - O acesso por parte de entidades externas necessita que o acesso seja iniciado manualmente?

4.7 - Está garantido um sistema seguro de acesso aos diversos equipamentos?

4.8 - É utilizada tecnologia VPN para garantir a proteção da informação nos acessos externos?

4.9 - No acesso pelo exterior da organização, são utilizados multi-fatores de autenticação, principalmente no acesso a informação e funções sensíveis?

4.10 - No acesso remoto estão limitados aos privilégios ao mínimo necessário?

4.11 - Os portáteis com acesso à rede ICS são usados apenas para este fim? Todas as portas e interfaces não necessários, estão desativados e o software não necessário foi removido?

5. Segurança das Aplicações

5.1 - Os utilizadores que interagem com o ICS da organização utilizam credenciais únicas e têm apenas os privilégios necessários para a realização das suas funções?

5.2 - Existem procedimentos para a criação de passwords seguras (tipo de caracteres, cumprimentos e regras semânticas), renovação de passwords e bloqueio automático de utilizadores por excesso de tentativa de acesso?

5.3 - São separadas as funções de administrador e de utilizador, não permitindo que utilizadores que não estejam a executar funções de administração estejam com estes privilégios ativos?

5.4 - Existem regras definidas para obrigar à criação de credenciais de acesso distintas para as aplicações do ICS e do IT da organização?

5.5 - Existem implementado sistemas de auditoria de controlo e monitorização de acesso ao sistema e das suas modificações?

5.6 - Existe implementado um sistema agregado de auditoria e monitorização dos eventos de rede, aplicações e restante sistema?

6. Encriptação

6.1 - As infraestruturas de rede, computadores, dispositivos móveis, dispositivos de armazenamento e equipamentos tem os seus dados encriptados de forma a minimizar o acesso aos seus dados em caso de roubo?

6.2 - As comunicações em fios são encriptadas sempre que possível, independentemente da tecnologia utilizada?

6.3 - As comunicações com fios sobre infraestruturas partilhadas são encriptadas através do uso de VPN?

6.4 - É utilizada a encriptação mais forte disponível, para os equipamentos existentes nos componentes do ICS e é especificada qual a encriptação necessária para os novos equipamentos?

6.5 - As bases de dados e repositório utilizados para os dados recolhidos no ICS são encriptados?

7. Arquitetura, Telecomunicações e Segurança da Rede

7.1 - Na rede existe implementada algum tipo *Application Layer Firewall* (controlo de input e output) ou *Statefull Firewall* (firewall com filtragem dinâmica de pacotes)?

7.2 - Existe na rede algum Sistema de Deteção de Intrusão (IDS) para deteção, alarme e/ou bloqueio de acessos não autorizados?

7.3 - Existe implementado algum sistema que permita em tempo real a monitorização dos eventos de segurança e anomalias dos equipamentos do ICS?

7.4 - Existe na organização, separação física (infraestrutura) da rede de comunicações e/ou lógica (IP subnets ou VLans) principalmente ao nível dos equipamentos/sistemas partilhados?

7.5 - Existe implementada regras de segurança ao nível das portas das interfaces dos equipamentos e as infraestruturas de rede?

7.6 - Foram analisados os riscos e os benefícios para o ICS da decisão do seu isolamento às redes exteriores e à internet?

7.7 - A arquitetura do ICS e a seleção dos seus componentes foi desenvolvida de forma a garantir a continuidade da sua operação mesmo com falhas de comunicação ou isolamento de partes do sistema?

7.8 - Existe sistema de monitorização e análise do sistema de forma a interpretar e avaliar o seu funcionamento, garantido assim a identificação de "*bootlenecks*" e outros entraves à sua performance e segurança?

7.9 - A documentação da arquitetura da rede do ICS existe e é revista periodicamente, nomeadamente as questões relacionadas com os seus limites e as ligações da mesma com a rede IT da organização?

8. Segurança Física dos ICS

8.1 - Os equipamentos da infraestrutura de rede não utilizados têm acesso limitado e controlado e estão desabilitadas as interfaces não utilizadas?

8.2 - Os canais de comunicação utilizados nos componentes estão protegidos de alterações não autorizadas?

8.3 - O acesso às salas de controlo, aos data centers, aos bastidores e aos racks têm controlo de acessos e está fechado por defeito?

8.4 - A alteração de componentes dos computadores dos postos de trabalho, bem como a introdução de dispositivos amovíveis nos mesmos, está bloqueado por sistemas físicos?

9. Acordos com entidades externas

9.1 - Estão identificadas todas as entidades externas que são necessárias à implementação, operação e manutenção do ICS, havendo contratos formais com estes? Nestes contratos estão definidos os tempos de resposta e as responsabilidades de cada entidade?

9.2 - Existe o cuidado de limitar o número de entidades externas contratadas com acesso ao ICS?

9.3 - Existem acordos escritos com as entidades e pessoas externas à organização para a sua responsabilização, confidencialidade e resposta a emergência?

10. Segurança da Operação

10.1 - Estão claramente definidas as fronteiras entre as funções de negócio e as do ICS, estando bloqueado neste todos os acessos externos (email, internet, ftp…) deste último?

10.2 - Estão implementadas medidas de controlo operacional nos dispositivos móveis e portáteis?

11. Engenharia Orientada para a Cybersegurança

11.1 - Existe análise de consequência e impactos de diversos cenários, priorizando-os de acordo com a sua severidade?

11.2 - O sistema foi desenhado e implementado de forma a minimizar os potenciais danos e consequências de um ataque?

11.3 - Existem controlos adicionais no sistema para além dos habituais em IT?

11.4 - O sistema foi desenhado de forma a garantir a simplificação e otimizando a operacionalidade?

11.5 - Existe planeamento para a resiliência do sistema, melhorando as ações de resposta e a recuperação?

11.6 - Há preocupação em controlar a distribuição de informações referentes à construção do ICS, diminuindo as distribuições não autorizadas?

11.7 - Os processos de aquisição, bem como as suas clausulas técnicas, são controlados?

11.8 - Existem sistemas para controlar a interdependência do sistema?

11.9 - É fomentada e mantida uma cultura de ciberawarness e ciberhigiéne para os trabalhadores, colaboradores externos e visitantes?

11.10 - Existe um inventário completos dos ativos do ICS, nomeadamente do hardware, software e firmware utilizado?

12. Educação

12.1 - Foi criado e está implementado um programa/plano de formação e sensibilização para a ciberawarness e ciberhigiene, que inclua a Engenharia Social?

12.2 - O programa/plano de formação e sensibilização foi criado com base na ligação entre a camada IT da organização e o seu ICS, tendo como suporte as melhores práticas e os procedimentos e normas implementados?

12.3 - Existe formação básica de redes (com e sem fios) para os técnicos com responsabilidades de manutenção e operação do ICS?

12.4 - A organização participa em encontros e parcerias com outras entidades do setor, garantido assim a partilha de informação e conhecimento em matérias de cibersegurança?

12.5 - Estão identificadas quais as certificações adequadas à organização (tanto ao nível operacional como ao nível estratégico) e aos seus funcionários, bem como os requeridos aos seus colaboradores externos?

12.6 - Existe um plano de treino e/ou simulacro que abranja todos os trabalhadores e colaboradores externos de forma a prepará-los para as ameaças e riscos com que se deparem?

12.7 - É promovida a partilha de informação relacionada com a cibersegurança dentro da organização?

13. Papel dos Trabalhadores

13.1 - Está implementado um procedimento junto dos trabalhadores e dos colaboradores externos para a identificação das suas necessidades de formação e treino, bem como, a identificação dos seus *background*?

13.2 - Foi dado a conhecer e foi subscrito pelos trabalhadores da organização, o compromisso o cumprimento dos procedimentos de Cibersegurança?

ANEXO II - QUESTIONÁRIOS INDIVIDUAIS DE AVALIAÇÃO

1 - Caracterização do Convidado

Dados da sua caracterização

Nome:		Função Profissional:	☐ Especialista Informático ☐ Responsável ICS
Email:			
Data:		Anos em Função:	

2 - Perfil do Utilizador

Dados utilizados durante o teste do protótipo

Username:		Nível:	
Data de Teste:			

3 - Avaliação Interface

Como classifica o protótipo em termos de aspecto e funcionalidade

	1	2	3	4	5	Notas
Facilidade de navegação						
Intuitividade						
Aspecto atraente						
Caracteristicas modernas						
Organização dos conteúdos						

4 - Avaliação de Medidas de Controlo

Como classifica as medidas propostas para o aumento de segurança do ICS

	1	2	3	4	5	Notas
São aplicáveis?						
São eficientes?						
Estão atualizadas aos riscos atuais?						
Englobam as necessidades da organização?						
Ajudam a implementar as medidas?						

5 - Considerações Finais

Como classifica o protótipo e o conceito do projecto

Considera útil a existencia de uma plataforma para o apoio à implementação de medidas para o aumento da cibersegurança dos ICS?	
Considera que as medidas de controle avaliadas no questionário correspondem às necessidade de cibersegurança dos ICS, nomeadamente, das Infraestruturas Críticas?	
Avaliação global do protótipo	
Pontos positivos e negativos do protótipo	
O que acrescentaria ao protótipo?	

	1	2	3	4	5
Avaliação global do protótipo					