Políticas e Análise de Risco na Segurança de Informação

Mestrado em Cibersegurança e Informática Forense

Valsabor S.A.

Gil Aguilar, 2210512

Gonçalo Vicente, 2210510

Pedro Santos, 2210636

Leiria, *janeiro de 2022*

Esta página foi intencionalmente deixada em branco

Resumo

O presente documento descreve um documento orientador que permite o desenvolvimento gradual do nível de segurança da Valsabor S.A. no âmbito da unidade curricular de Políticas e Análise de Risco na Segurança de Informação pertencente ao mestrado em Cibersegurança e Informática Forense.

Este relatório encontra-se dividido em nove capítulos que apresentam todo o processo de planeamento, construção e desenvolvimento do respetivo documento.

No primeiro capítulo é abordado a caraterização do ambiente empresarial, nomeadamente a estrutura empresarial, localização e ramos de atividades; principais parceiros de negócio; estrutura de administração empresarial e enquadramento da empresa com o mundo digital.

No segundo capítulo existe referência à arquitetura do sistema de informação nomeadamente as principais unidades de negócio e respetivos processos e atividades; principais aplicações utilizadas; tecnologias utilizadas e localização dos ativos tecnológicos.

No terceiro capítulo são abordadas atividades críticas da organização.

Na parte quatro deste documento existe a identificação do responsável de segurança e equipas de segurança, nomeadamente a localização da organização de segurança; funções e responsabilidades; competências necessárias para os colaboradores; catálogo de serviços da organização de segurança e aplicações essenciais no contexto *governance* para a segurança da informação.

No capítulo cinco, existe um estabelecimento de metodologias de análise de risco, particularmente a metodologia de análise de risco utilizada; vulnerabilidades associadas aos serviços e ameaças a que se encontram expostas e probabilidade de concretização e impacto das ameaças.

No sexto capítulo, aborda-se as políticas de segurança da informação da organização abordando especificamente 4 diferentes normas: ambiente e segurança da informação; mitigação de riscos do negócio; gestão de ativos e classificação de informação.

No sétimo capítulo é enunciado o desenho e implementação da arquitetura e segurança perimétrica.

No oitavo capítulo recorre-se ao estabelecimento de conformidades com legislação e normas aplicáveis, subdividindo entre identificar a legislação aplicável e regulatórios a que está sujeita e normas ou certificações relevantes e aplicáveis ao setor.

Por fim é abordada a política de uso aceitável nomeadamente os pressupostos da Política de Uso Aceitável adequada aos recursos TI.

Palavras-chave: *Cibersegurança, gestão de ativos, mitigação de riscos, políticas de segurança*

Esta página foi intencionalmente deixada em branco

Abstract

This document describes a guiding document that allows the gradual development of the security level of Valsabor S.A. within the curricular unit of Policies and Risk Analysis in Information Security belonging to the Masters in Cybersecurity and Forensic Informatics.

This report is divided into nine chapters that present the entire process of planning, building, and developing the respective document.

The first chapter addresses the characterization of the business environment, namely the business structure, location, and branches of activities, main business partners, business administration structure and framing the company with the digital world.

In the second chapter there is a reference to the architecture of the information system, namely the main business units and respective processes and activities, main applications used, technologies used and location of technological assets.

The third chapter addresses critical activities of the organization.

In part four of this document, there is the identification of the responsible for security and security teams, namely the location of the security organization, roles, and responsibilities, needed skills for employees, catalog of security organization services and essential applications in the governance context for information security.

In chapter five, there is an establishment of risk analysis methodologies, particularly the risk analysis methodology used; vulnerabilities associated with the services and threats to which they are exposed, and probability of materialization and impact of the threats.

The sixth chapter addresses the organization's information security policies, specifically addressing 4 different standards: environment and information security, business risk mitigation, asset management and information classification.

The seventh chapter outlines the design and implementation of the architecture and perimeter security.

The eighth chapter refers to the establishment of conformity with applicable legislation and standards, subdividing between identifying the applicable legislation and regulations to which it is subject and relevant standards or certifications applicable to the sector.

Finally, the ninth chapter addresses the acceptable use policy is addressed, namely the assumptions of the Acceptable Use Policy appropriate to IT resources.

***Keywords*:** *Cibersecurity*, *assets management*, *risk mitigation*, *security policies*

Esta página foi intencionalmente deixada em branco

Lista de Figuras

Esta página foi intencionalmente deixada em branco

Lista de Tabelas

Esta página foi intencionalmente deixada em branco

Lista de acrónimos

UPS - *Uninterruptible Power Supply*

BYOD - *Bring Your Own Device*

ERP – *European Recycling Platform*

RFID – *Radio-Frequency IDentification*

SWOT – *Strengths, Weaknesses, Opportunities e Threats*

CIA – Confidentiality, Integrity, Availability

DoS – *Denial of Service*

IDS – *Intrusion Detection System*

IPS – *Intrusion Protection System*

TLS – *Transport Layer Security*

IP – *Internet Protocol*

ASAE – Autoridade de Segurança Alimentar e Económica

CNCS – Centro Nacional de Cibersegurança

QNRCS – Quadro Nacional de Referência para a Cibersegurança

GAP - *Good Agricultural Practices*

VPN – *Virtual Private Network*

RGP – Regulamento Geral de Proteção de Dados

HTTP – *Hypertext Transfer Protocol*

URL – *Uniform Resource Locator*

Esta página foi intencionalmente deixada em branco

Índice

1. Caracterização do ambiente empresarial

1.1. Estrutura empresarial, localização e ramos de atividade

O ValGrupo é um grupo de empresas centrado na produção animal (suínos, bovinos e aves) e no abate, transformação e comercialização de produtos alimentares.

O presente projeto incidirá na empresa onde se encontra a sede do grupo, ValSabor, que é a empresa responsável pelo abate e transformação de carne. A ValSabor é localizada em Alcanede, concelho de Santarém, e possui cerca de 400 colaboradores nas instalações da sede, e cerca de 1100 no total de todas as empresas.

1.2. Principais parceiros de negócio

No que toca aos principais parceiros de negócio da ValSabor, temos quase todo o mercado nacional, nomeadamente a SONAE, Jerónimo Martins, Intermarché, que como podemos ver, são conhecidas cadeias de supermercados retalhistas a nível nacional.

A nível de mercados internacionais, a ValSabor está presente em França e Angola, com filiais com o seu nome, dando assim a sua marca.

Através da Agrupalto - Agrupamento de Produtores Agropecuários, empresa na qual Valgrupo detém 50% de ações [5] e que conquistou vários prémios, entre os quais o Porco Diamante, que distingue o melhor produtor em Portugal, foi iniciado a exportação de carne de porco para a China [1]. Esta operaçãto recorreu à compra de um matadouro em Reguengos de Monsaraz para trabalhar, exclusivamente, para o mercado chinês. Um investimento de quatro milhões de euros, a que se juntam mais seis milhões para transformar a Maporal, até ao final de 2020, na maior unidade de abate nacional, havendo previsões de investidores que antecipam que exportações atingissem os 200 milhões de euros em 2020. [2]

1.3. Estrutura de administração empresarial

A estrutura empresarial da ValSabor consiste na divisão por departamentos como o de Qualidade, Informático, Contabilidade, Recursos Humanos, entre outros, tendo cada um, um Chefe de Departamento e os respetivos funcionários. Na figura 1, é possível visualizar o organograma da empresa ValSabor, demonstrado a administração da empresa bem como os diferentes departamentos e quem são os chefes de departamento.

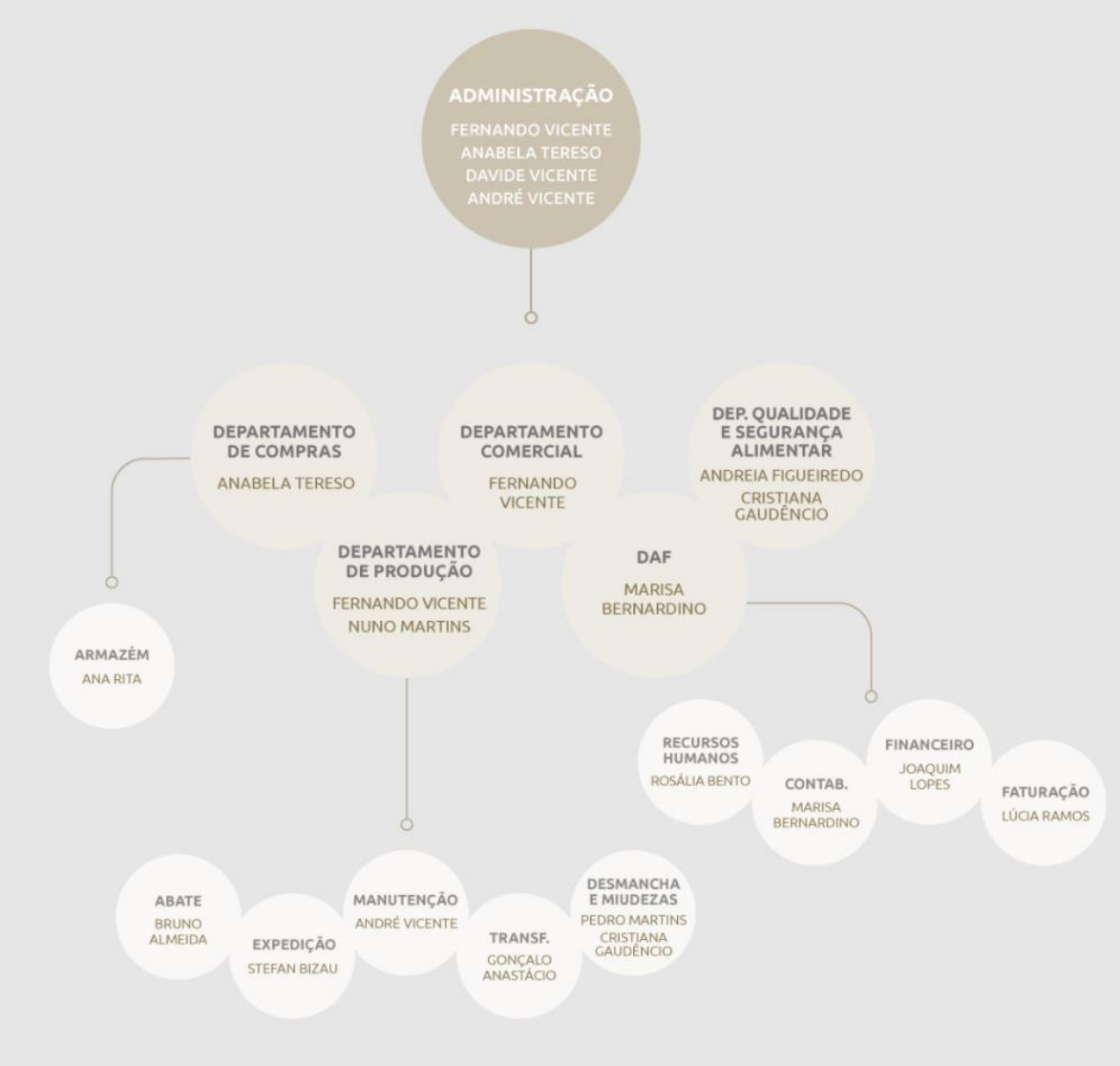

Figura 1 - Organograma da Valsabor Fonte: [3]

O presidente da ValGrupo é o CEO da ValSabor, o Senhor Fernando Vicente.

A empresa recorre a outsourcing, uma vez que utilizam serviços prestados por outras empresas. Neste caso, o outsourcing pode ser confundido com insourcing, uma vez que as empresas recorridas para as prestações de serviços supracitadas, pertencem ao ValGrupo

(grupo de empresas onde se insere a ValSabor). Na figura 2 é possível visualizar todo o ciclo de atividade do grupo demonstrando assim todo o processo de negócio do grupo.

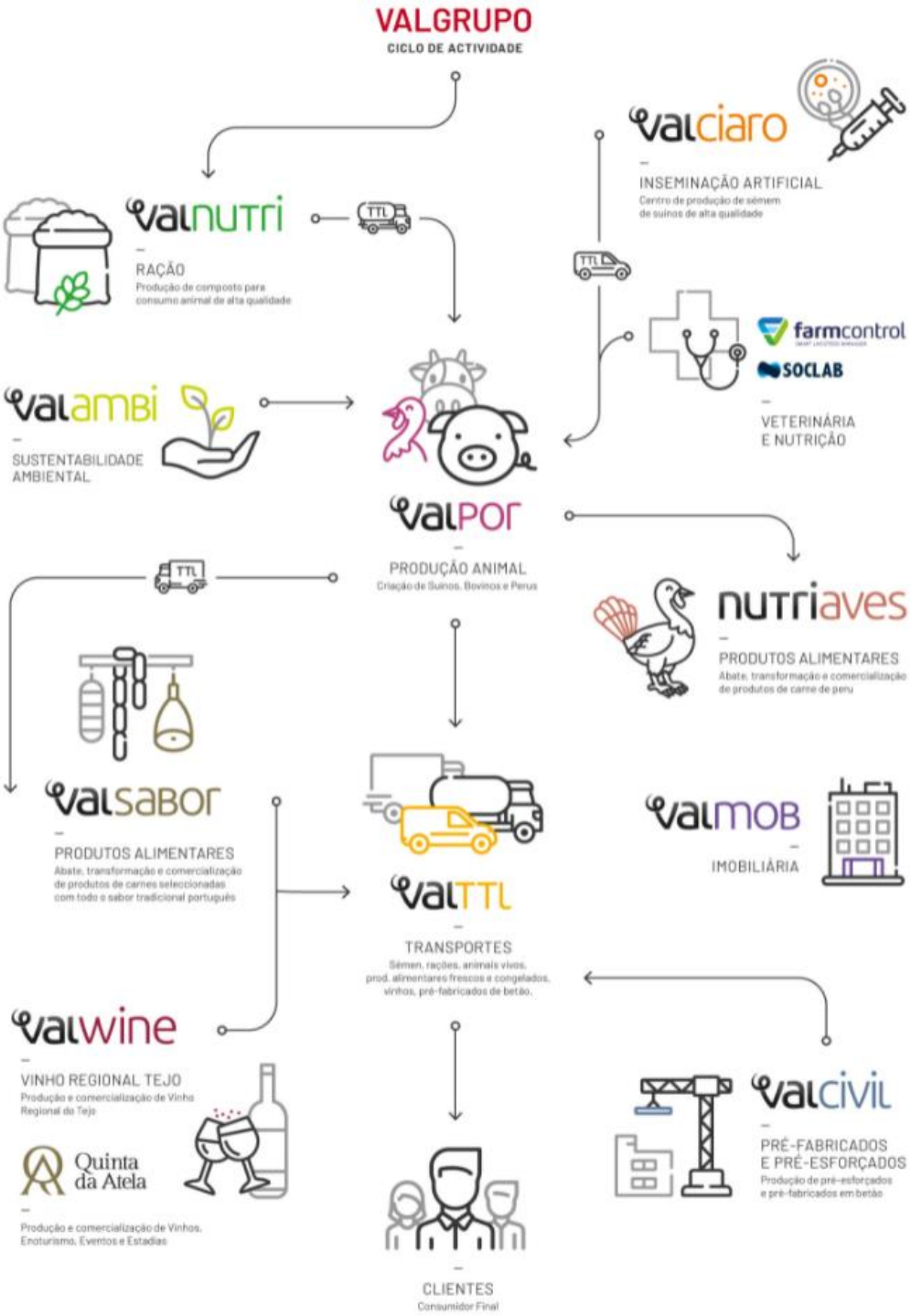

Figura 2 - Ciclo de atividade ValGrupo Fonte: [4]

1.4. Enquadramento da empresa com o mundo digital

A nível tecnológico a empresa Valsabor está a fazer grandes esforços financeiros para estar ao mais alto nível das empresas nacionais [6] [7]. Através de um sistema inovador de processo de abate, existem máquinas extremamente rigorosas, que não permitem falhas, possuindo um excecional controlo de níveis de CO2, de modo a efetuar um abate quase indolor para os animais.

A empresa possui sistemas de controlos de acesso físicos suportados pela certificação da ISO 22000, que está relacionada com gestão de segurança alimentar [8], assim como um Datacenter interno onde estão alocados vários tipos de servidores (Windows Server 12 e Linux), bem como servidores na *cloud* de Altice Portugal.

2. Arquitetura do Sistema de Informação

2.1. Principais unidades de negócio e respetivos processos e atividades

Localizada na freguesia de Alcanede encontra-se a ValSabor, a sede do grupo de empresas que compõe o ValGrupo. A ValSabor dedica-se ao abate, transformação e comercialização de suínos e outros produtos alimentares transformados. Possui uma moderna linha de abate que permite o abate de 300 suínos por hora e 350 para desmancha [9].

Para além da sede ValSabor, o ValGrupo é constituído por mais 31 empresas, sendo que 8 delas são comparticipadas e as restantes 23 empresas estão distribuídas em grupos, empregando total de 935 colaboradores diretos e 160 indiretos. A nível de frota o grupo apresenta 190 viaturas. Através das 220 explorações agropecuárias existentes, são produzidos, anualmente, 1 100 000 suínos, 500 bovinos, 600 000 perus alimentados por 430 000 toneladas de ração produzidas em empresas próprias, movimentando um volume de negócios de cerca de 556 milhões de euros. Na infografia seguinte, é possível visualizar todas estas informações.

Figura 3 - Valgrupo – Como somos! [4]

Assim, iremos de seguida descrever cada um dos grupos de empresas associadas ao grupo.

A ValPor é a entidade e imagem de marca responsável pela produção de animais (suínos, bovinos, aves), e representa um conjunto de 12 empresas que acompanha todo o ciclo produtivo dos animais. Produz cerca de 115.000 toneladas de carne de suíno por ano (1.350.000 suínos), 140 toneladas de carne de bovino por ano (500 bovinos) e 8400 toneladas de carne de peru por ano (700.000 perus) [10].

A ValTTL é a empresa responsável pela distribuição de todos os produtos e matérias-primas das empresas do grupo, contando com uma frota moderna superior a 200 viaturas (ligeiras e pesadas). Toda a frota é monitorizada por GPS e as manutenções são feitas em oficinas próprias [11].

A ValNutri é a entidade que representa 7 empresas que servem e garantem a qualidade da alimentação dos animais do grupo através da criação de rações seguindo fórmulas especificas para um melhor resultado no animal [12].

A ValCiaro é a empresa que se dedica à inseminação artificial de suínos sendo o primeiro centro existente em Portugal, registando uma produção de 330.000 doses por ano [13].

A ValCivil é uma empresa que produz pré-fabricados e pré-esforçados em betão para a construção civil [14].

A ValMob é a entidade que atua no setor imobiliário, a unidade negócio onde são geridos os investimentos imobiliários do grupo, sendo constituída por 2 empresas [15].

A ValAmbi é a empresa que se encarrega de enquadrar o grupo numa perspetiva de proteção e preservação ambiental. Para isso faz o tratamento de resíduos através de uma ETAR própria e rege-se pelo lema "Reutilizar, Reciclar e Reduzir" [16].

A NutriAves é a empresa que se dedica ao abate e transformação de perus tendo como capacidade o abate de 1.000 por hora e desmancha de 600 [17].

ValWine é a marca dos vinhos que o grupo reserva e seleciona das vinhas da Quinta da Atela [18].

Relativamente a empresas participadas existem as empresas associadas ao grupo InterSuínos como o caso MAPORAL, que se dedica ao abate e transformação de suínos, possuindo uma linha de abate e desmancha de mais de 200 por hora, e a AGPMEAT que tem como objetivo a exportação de carne portuguesa para o mercado internacional, nomeadamente França, Angola e China [19].

A empresa possui ainda um *datacenter* no edifício da sede sendo composto por 5 *switch* de rede, uma firewall, um router e 5 servidores. Este *datacenter* tem como função dar suporte a todas as empresas do grupo bem como empresas comparticipadas nomeadamente a nível de ERP, domínio e sistema de backups. Assim, todo o processo de assistência informática em todo o grupo é dado pela equipa de IT instalada na ValSabor bem como assistência de empresas subcontratadas para questões mais especificas.

Na infografia presente na imagem 4, é possível ter uma precessão das empresas associadas a cada grupo de empresa.

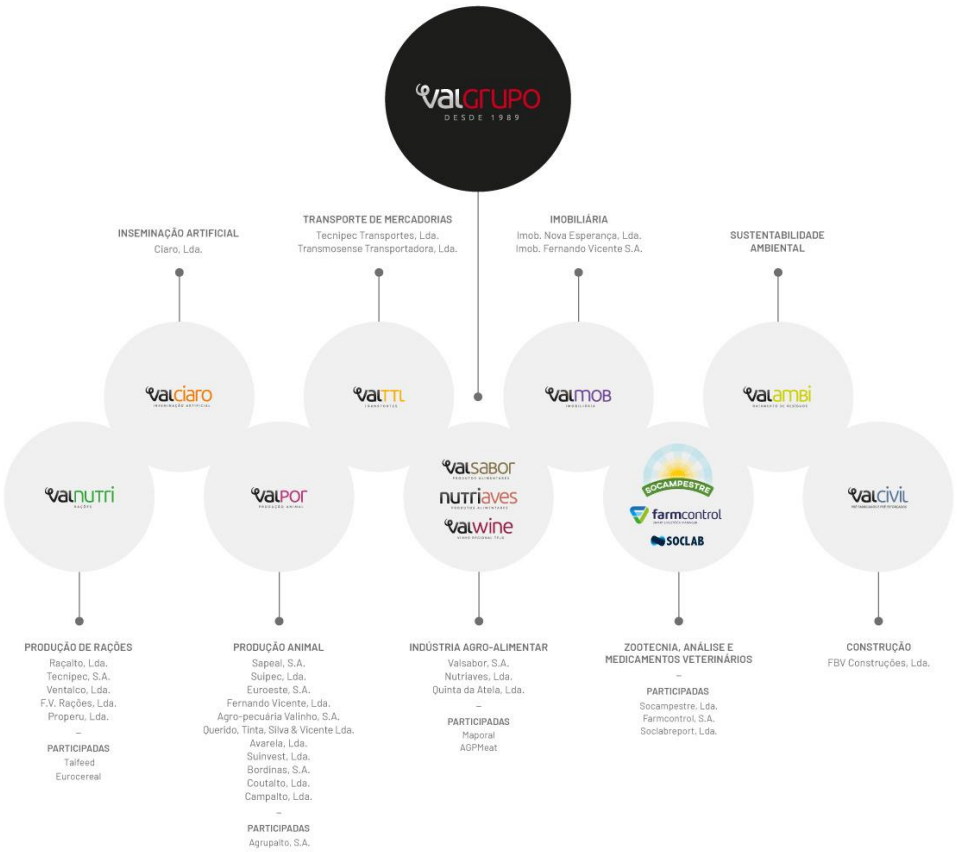

Figura 4 – Infografia ValGrupo Fonte: [4]

2.2. Principais aplicações utilizadas

No que toca a aplicações e software, o principal software desenvolvido pela empresa são o "ValGrupo – Gestão Pecuária" e o "ValGrupo – Gestão". O portal "ValGrupo – Gestão Pecuária" que permite realizar novas encomendas, fazer pedidos de assistência ao departamento de informática, consultar receitas, funções administrativas, entre outras funcionalidades. Relativamente ao portal "ValGrupo – Gestão" existe a possibilidade de fazer movimentos associados a animais como integrações entre custos e animais utilizando o ERP utilizado pelo grupo.

A nível de *softwares* generalistas, a empresa utiliza "*EticaData*", um ERP que permite realizar faturações e guias de transporte e aplicação "SAP", utilizando os módulos de "*Touch*" e "*Piking*" que permite realizar o *picking* de códigos de barras no processamento de encomendas.

2.3. Tecnologias utilizadas

A nível de sistemas operativos utilizados recorre ao Windows Server 12 e Windows 10 Pro, assim como dois servidores com o sistema operativo Linux SUSE, associados ao *SAP IANA*.

A empresa possui um sistema de comunicação através de email havendo diferentes domínios, dependendo da empresa em que o funcionário está inserido, sendo esse serviço disponibilizado pela empresa de comunicações Altice Portugal.

O sistema de armazenamento funciona à base de servidores e de uma *NAS* (dispositivo de armazenamento ligado a uma rede que possibilita o armazenamento e a recuperação de dados de um local centralizado).

2.4. Localização dos ativos tecnológicos

Os ativos tecnológicos e de informação da empresa encontram-se *on premises*, nomeadamente os servidores que suportam toda infraestrutura do grupo e *backups* armazenados na *NAS*.

Na infraestrutura tecnológica e informática da ValSabor, estão armazenados todos os servidores e backups das diferentes empresas que compõe a ValGrupo.

3. Atividades críticas da organização

Tendo em conta a quantidade de empresas que compõe o ValGrupo, ao longo deste trabalho iremos debruçarmo-nos em estabelecer políticas de segurança apenas para a empresa onde se encontra a sede do grupo. Nesse caso, será a empresa Valsabor que irá ter grande parte da nossa atenção ao longo deste relatório.

Como foi explicado nos capítulos anteriores, a empresa Valsabor dedica-se ao abate e transformação de carne. Assim sendo, uma das atividades críticas da organização é a tecnológica linha de abate que possuem. As máquinas que incorporam esta linha de abate altamente tecnológica são extremamente rigorosas e não permitem falhas. Neste sentido, esta linha de abate é fundamental para a organização, uma vez que problemas nesta linha podem causar atrasos e constrangimentos neste processo, originando atrasos indesejáveis em todo o processo de distribuição do produto final aos clientes.

Relativamente aos ativos da organização é necessário proteger os documentos pessoais dos funcionários que são entregues ao departamento de Gestão de Recursos Humanos (GRH). Uma das políticas da empresa, é a atribuição de um smartphone a todos os funcionários para contactar com outros funcionários ou entidades externas. Estes

equipamentos também são um dos ativos que se deve proteger, uma vez que são equipamentos que podem conter informações importantes acerca do negócio, com uma maior ou menor importância dependendo da área em que o colaborador se encontra inserido.

Os *laptops* ou *desktops* atribuídos a determinados funcionários devem também ser alvo de proteção uma vez que é um instrumento de trabalho com acesso à rede interna da empresa, sendo uma fonte de propagação de *software* nocivo.

Para os funcionários que necessitam de conduzir um carro da empresa, é atribuído um cartão RFID [20] que permite ativar a ignição dos veículos e o acesso às bombas de combustível. Este cartão, é um ativo bastante importante que deve ser protegido, uma vez que o acesso a este cartão por pessoas não autorizadas pode permitir um uso indevido de veículos da organização.

Por fim, um ativo bastante importante é o *datacenter* da empresa, onde se encontram alojados os diversos servidores que dão suporte a todo o grupo, nomeadamente ERP. Pelos diversos edifícios, existem espalhados bastidores, existindo controlos de acesso em algumas das portas que dão acesso a esses locais, porém existem outros que devem ser protegidos uma vez que um acesso indevido pode causar danos graves à organização. Além disso, deve também ser definido quem é necessário contactar em caso de necessidade para abrir essas portas através de uma chave RFID.

4. Identificação do responsável de segurança e equipas de segurança

Apesar de o grupo não possuir um departamento de segurança da informação atualmente, recomenda-se a criação de um. Até então, todas as questões relacionadas com a segurança da informação estão direcionadas para o departamento de IT, porém e tendo em conta a carga de trabalho diária, em virtude da gestão informática de todas as empresas detidas na totalidade pelo grupo bem como as empresas comparticipadas, a que estão sujeitos, questões relacionadas com a segurança da informação acabam por ser descuradas.

4.1. Localização da organização de segurança

Tendo em conta a dimensão do grupo (cerca de 1100 colaboradores espalhados por diversas empresas), justifica-se a criação de um gabinete de segurança interno na empresa. Assim, este gabinete situar-se à na empresa sede do grupo, Valsabor, S.A., em Alcanede. Esta opção é tomada com base em a Valsabor, S.A. ser a empresa sede do grupo, a empresa que emprega uma maior quantidade de funcionários e onde a infraestrutura é mais critica de

proteção uma vez que funciona nesta empresa o maior matadouro de todo o grupo e que realiza um maior número de abates por dia.

4.2. Funções e responsabilidades

Relativamente ao gabinete de segurança a ser criado, este irá ser um SOC (*Security Operation Center*), sendo, neste caso um SOC Multifunções. Assim sendo, além de possuírem uma instalação dedicada irão estar operacionais durante 16/5, agirão de forma reativa e pró-ativa e providencia também serviços de operação e manutenção de redes ou sistemas da informação, sendo uma forma de minimizar os custos associados a duas equipas distintas.

De acordo com o Quadro Nacional de Referência para a Cibersegurança [22], serviços reativos são a reação a incidentes, nomeadamente alertas e avisos, resposta a incidentes ocorridos (análise, resposta, suporte e coordenação), gestão de vulnerabilidades e gestão de artefactos ao nível de análise, resposta e coordenação. Relativamente a serviços pró-ativos, estes enquadram-se em campanhas de sensibilização aos colaboradores, acompanhamento e esclarecimento de dúvidas relacionadas com o uso da tecnologia, auditorias e avaliações de segurança de forma a garantir uma melhoria continua, configuração e manutenção de ferramentas de segurança, aplicações e infraestrutura, desenvolvimento e aplicação de ferramentas de segurança bem como serviços de deteção de intrusão. No documento supracitado, é também referido que deverá existir operacionais num contexto de 24/7, porém no contexto da empresa não se aplica, uma vez que existem apenas 2 turnos de 8 horas durante os dias semanais. Neste sentido, é apenas necessário o suporte neste período de tempo.

4.3. Competências necessárias para os colaboradores

Relativamente ao responsável pelo gabinete de segurança, o CISO (*Chief Information Security Officer*), deverá ser uma pessoa com elevados conhecimentos sobre os processos chave da organização uma vez que terá uma responsabilidade transversal a todo o grupo. Assim sendo, o CISO, deverá conseguir transcrever os objetivos da organização em requisitos da segurança da informação, devendo ser, por este motivo, um bom comunicador. Nesse sentido, o CISO deverá assegurar e manter a estratégia da segurança da informação sendo para tal necessário implementar boas práticas que se devem utilizar, desenvolver e implementar políticas, processos e procedimentos da segurança da informação. A necessidade de conhecimento sobre a legislação e regulamentação especifica para o setor da atividade agropecuária bem como conhecimentos ao nível da segurança da informação, nomeadamente a ISO/IEC 27001 e o Regulamento Geral de Proteção de Dados Pessoais. A dinamização de ações de sensibilização junto dos diversos colaboradores também é uma função atribuída ao CISO [22].

Juntamente com o CISO, irá estar uma equipa composta por mais 4 colaboradores a operarem em conjuntos de 2 elementos em turnos de 8 horas. Num processo de recrutamento a ter em conta, irá dar-se privilégios a colaboradores que possuam, pelo menos, o título de Licenciado, nomeadamente em Engenharia Informática ou Informática de Gestão que possuam características mais direcionadas para as redes informática, garantindo que tenham conhecimento ao nível da cibersegurança e de tipo de políticas que se podem implementar de forma a aumentar a segurança em todo o parque informático da instituição. Este processo de seleção, irá ser direcionado para dois elementos com 5 ou 6 anos de experiência e para dois elementos com pouco ou nenhum nível de experiência, de forma que os colaboradores mais experientes possam vir a dar formação aos menos experientes procurando desde cedo traçar um caminho de sucesso profissional e constituir uma equipa bastante forte num médio prazo.

4.4. Catálogo de serviços da organização de segurança

No que diz respeito aos catálogos de serviços da organização de segurança, existem a necessidade de perceber, tanto nas *firewalls* internas da empresa, como na *firewall* da operadora Altice Portugal, quais as portas de rede que se encontram a permitir a entrada de pedidos e porque que necessidade existe. Assim sendo, é importante perceber o que ainda está a ser utilizado e qual a sua finalidade, bem como os portos de rede que já não necessitam de permitir esta entrada. Um ponto a ter em conta é a existência de uma dupla *firewall*, uma externa ao grupo que se encontra ao cuidado da Altice Portugal e onde a equipa de segurança da informação não tem possibilidade de aplicar configurações, porém na *firewall* interna existe a necessidade de uma configuração minuciosa de forma a ter uma maior segurança.

Uma outra questão importante, é perceber que equipamentos existem na rede, bem como perceber se são equipamentos da empresa ou pessoais dos colaboradores, fazer a catalogação de endereços MAC [22], *serial numbers* [23] e começar a preparar uma aplicação de forma a fazer a rastreabilidade dos equipamentos, ou seja, qual a data de receção que um utilizador recebe um equipamento, quando o devolve ao departamento de IT e quais as razões, para onde é atribuído de seguida. Todas estas pequenas informações não se encontram devidamente documentadas o que dificulta uma ação de pesquisa através de um mecanismo de logs.

Uma questão que é bastante importante é a política de *backups* que se encontra implementada bem como a de reposição de *backups*. Apesar de já estar a ser documentada uma política de *backups*, não existe documentação sobre tal nem quais os procedimentos necessários tomar de forma a repor os *backups* existentes em caso de necessidade urgente. Neste sentido, deve estar devidamente documentado todos os passos necessários de forma que qualquer elemento da equipa de segurança da informação consiga fazê-lo com a maior brevidade possível e com o mínimo de constrangimentos. Um passo importante é replicar os

backups existentes que são guardados no servidor localizado na sede do grupo na *cloud* que se encontra na empresa Altice Portugal, sendo mais uma garantia de segurança dos dados em caso de existência de uma catástrofe ambiental, uma vez que a empresa pode estar sujeita tendo em conta proximidade com a Nazaré e pela zona da Serra de Aire e Candeeiros onde se encontra.

Questões como a sensibilização dos utilizadores dos portais internos do grupo, ou seja, duas aplicações web e uma aplicação mobile, bem como utilizadores de programas como o Eticadata, SAP, entre outros, procurem utilizar palavras-passe minimamente seguras (utilização de maiúsculas, minúsculas, números e carateres expeciais) bem como uma introdução gradual de um sistema de gestão de passwords para aumentar a segurança das empresas associadas ao grupo. Esta questão irá ficar a cargo do CISO, que irá, de uma forma gradual fomentar estas boas práticas nos utilizadores.

A cargo do CISO, ficará também ações de formação com núcleos específicos de colaboradores com vista a implementar boas práticas de segurança da informação, não só ao nível de passwords, mas também com cuidados a ter com emails de spam que possam não ter sido catalogados como tal e cheguem assim ao utilizador final. Neste caso, é importante saber classificar esse email como tal e reportar esse caso à equipa de segurança da informação de forma a procurar melhorar para evitar que tal se verifique novamente no futuro.

4.5. Aplicações essenciais no contexto *governance* para a segurança de informação

No contexto da empresa, existem 4 aplicações fundamentais no contexto da *governance* para a segurança da informação. Nesse sentido podemos classificar tanto o ERP da empresa, o "Eticadata" como a aplicação mais importante de toda a empresa, uma vez que é nessa aplicação que são lançados todas faturas e guias de remessa da empresa, movimentos contabilísticos bem como um processamento de salários de todos os colaboradores. Para esta aplicação, existe, no *datacenter* da empresa, um servidor dedicado para tal. É um servidor exclusivo que possui um sistema de redundância de alimentação, sendo alimentado por duas fontes de alimentação diferentes bem como suportado por uma UPS [24] de última geração que é suportada por dois *packs* de bateria que estão acoplados.

Uma outra aplicação de extrema importância é o programa SAP. Este programa encontra-se em serviço no matadouro existente, tanto no processo de abate como nos processos de desmancha e expedição bem como as encomendas que chegam pelos diferentes vendedores que a empresa possui chegam à sede através do lançamento nesta aplicação. Falhas nesta aplicação são bastante graves uma vez que, sem saber as encomendas para os dias seguintes, não é possível fazer o planeamento dos suínos que são necessários abater, quais os novos suínos que devem ser mudados para as engordas que, entretanto, ficaram livres bem como os diferentes tipos de rações que são necessárias entregar nas diversas

engordas que forneceram animais. Além desta situação, sem o pleno funcionamento desta aplicação o sistema de abate não funciona, uma vez que é controlado através de opções existentes nesta aplicação. Sem que o abate ocorra corretamente, é influenciado todo o processo de desmancha e expedição não permitindo que as encomendas cheguem ao cliente final nas datas previstas.

A nível interno do grupo existem duas plataformas web, que se encontram a ser mantidas e desenvolvidas novas funcionalidades pela equipa de desenvolvimento da Valsabor, S.A., que suportam tanto os movimentos de planeamentos de entregas de ração nas diversas explorações agropecuárias bem como uma outra plataforma onde se realizam os fechos de engorda bem como todos os movimentos associados a mudanças de explorações de produção de leitões como para mudanças diretamente para o matadouro.

Assim sendo, o portal "ValGrupo – Gestão Pecuária", é um portal que se encontra disponível no *url* portal.valgrupo.pt e é um pequeno portal desenvolvido com o auxílio de *WordPress* [25] e que realiza inserções diretamente no ERP "Eticadata". Neste portal, são feitos todos os planeamentos de entregas de rações para todas as explorações do grupo (explorações de perus, suínos ou bovinos). Todos estes planeamentos são feitos localmente na fábrica de rações do Carregado, a F.V. Rações, pertencente à ValNutri.

Um outro portal existente e de extrema importância é o portal ValGrupo - Gestão, disponível no *url*, gestao.valgrupo.pt, e é uma aplicação desenvolvida com o auxílio da framework *Laravel* [26], porém neste momento encontra-se a ser desenvolvida recorrendo também à framework *VueJS* [27], transformando-o num website híbrido. Este portal tem como objetivo ser o único portal que todo o grupo irá utilizar, desde o momento de lançar compras, associar equipamentos a utilizadores ou até mesmo registo da qualidade da carne durante o processo de transformação. Atualmente, a principal funcionalidade deste portal é no planeamento de mudanças de animais entre diferentes explorações agropecuárias ou mesmo para os diversos matadouros. Aqui, os responsáveis das explorações, quando os animais chegam a objetivos definidos fazem um pedido de requisição da quantidade de animais que se encontram disponíveis para retirar de um determinado pavilhão. Consoante as necessidades, a equipa responsável pelo planeamento associada à ValPor, faz a mudança necessária. Estes planeamentos são feitos localmente na ValSabor em Alcanede, porém todos os pedidos de requisição são feitos geograficamente por todo o Portugal continental, nas cerca de 500 explorações que fornecem o grupo.

5. Estabelecimento de metodologias de análise de Risco

De modo a podermos realizar uma análise de risco, vamos ter de definir primeiro a metodologia de análise de risco, baseada na identificação de vulnerabilidades e ameaças, e avaliação do impacto dos principais ativos da empresa.

O objetivo principal da análise de risco passa por salientar quais os ativos que constituem maior impacto na empresa no caso de alguma ameaça associada a eles se verifiquem, de modo a dar uma visão geral dos aspetos que devem ser melhorados, e quais é que devem ser priorizados.

5.1. Metodologia de Análise de Risco utilizada

A metodologia de análise utilizada será baseada em análises qualitativas dos riscos, através da utilização de escalas para classificar os riscos, tendo em conta os aspetos supracitados. Para cada uma das ameaças, será atribuído um nível de severidade de potenciais impactos (Baixo, Médio e Alto) assim como a probabilidade da ocorrência das mesmas ameaças. Esta metodologia é indicada pelo Quadro Nacional de Referência para a Cibersegurança [21].

5.2. Vulnerabilidades associadas aos serviços e ameaças a que se encontram expostas

Segundo o Quadro Nacional de Referência para a Cibersegurança (QNRCS) [21], antes de avaliarmos as possíveis vulnerabilidades, existe a necessidade de identificar as ameaças que podem criar impactos negativos aos ativos e serviços críticos descritos no ponto 3 - Atividades críticas da organização.

As ameaças podem ser de origem natural ou humana, e podem ser acidentais ou deliberadas, e, tendo em conta os ativos descritos no ponto 3 - Atividades críticas da organização, selecionámos cinco grupos de ativos.

Algumas ameaças aos seguintes ativos são:

Linha de abate tecnológica e inovadora

- Acesso físico, de modo a destabilizar o funcionamento manual da linha de abate (acesso indevido por alguém que não pertença à equipa e que queira prejudicar a empresa, ou até mesmo alguém de dentro que, descontente com a empresa, a queira prejudicar).

- Acesso informático, de modo a destabilizar o funcionamento algorítmico e tecnológico da linha de abate (um atacante informático que aceda a qualquer código do software da máquina, e que altere ou remova código que faça a linha de abate funcionar normalmente).

Smartphones e *laptops* atribuídos aos funcionários

- Roubo físico, uma vez que um telemóvel e um *laptop* são objetos físicos e portáteis que podem ser roubados por alguém.
- Roubo de informação, uma vez que um telemóvel e um laptop são dispositivos com acesso à internet, podem ser invadidos por um atacante que queira obter alguma informação sobre a empresa, de modo a conseguir obter alguma vantagem ou conteúdo que possa prejudicar a empresa.

Cartão RIFD para viatura da empresa

- Roubo do cartão, assim como um telemóvel ou *laptop*, estes cartões são físicos e portáteis, e como tal, podem ser roubados por alguém.
- Clonagem do cartão, uma vez que aquando da sua utilização, podem ser capturados dados referentes a acesso ao dispositivo, ou neste caso à viatura da empresa, e através de um chip, podem ser colocados esses dados e a viatura passa a estar comprometida, uma vez que pode ser acedida não só por quem possui o cartão RFID, mas também por quem executou a clonagem.

Datacenter

- Acesso informático, uma vez que pode ser invadido informaticamente por um atacante que queira prejudicar a empresa, destruindo os dados ou pedindo um resgate pelo retorno dos dados.
- Destruição/danificação do *datacenter*, que sem um backup apropriado, irá causar um grande atraso à empresa.

Vistas as ameaças, vamos então analisar as vulnerabilidades associadas a estes serviços. Segundo o QNRCS [21], as vulnerabilidades podem estar associadas à organização, processos e procedimentos, rotinas de gestão, colaboradores, ambientes físicos, configuração dos sistemas de informação, hardware, software e equipamento de rede e dependência com partes externas interessadas.

Assim sendo, podemos atribuir as possíveis vulnerabilidades aos ativos:

Linha de abate tecnológica e inovadora

- Processos e Procedimentos – a má explicação dos procedimentos para o correto funcionamento da linha de abate pode resultar num dano à mesma, e, por conseguinte, afetar a empresa
- Rotinas de Gestão – definir rotinas de gestão de todos os aspetos da linha de abate é fundamental para o seu bom funcionamento

- Ambientes físicos – convém que a linha de abate esteja situada numa sala com tecnologia suficientemente eficaz contra desastres naturais que ocorram, como sismos ou inundações
- Configuração dos sistemas de informação – o software relacionado com a linha de abate deve ser bem configurado para evitar ataques informáticos

Smatphones e *Laptops* atribuídos aos funcionários

- Processos e procedimentos – o mau uso dos dispositivos (acesso a sites indevidos, instalação de aplicações indevidas) pode resultar em danos para a empresa, uma vez que podem expor o dispositivo a ataques informáticos, e como tal, existirem processos de verificação de integridade dos dispositivos é fundamental.
- Configuração dos sistemas de informação – como é óbvio que os dispositivos devem estar devidamente configurados principalmente em questões de segurança, como a utilização de mecanismos como 2FA (2 *factor authentication*) [28] e um gestor de passwords [29], assim como uma boa *firewall* [30] e um bom antivírus [31], por exemplo.

Cartão RIFD para viatura da empresa

- Configuração dos sistemas de informação – relativamente aos cartões RIFD, existe a possibilidade de serem clonados com certos dispositivos se estes forem mal configurados, como a não implementação de um mecanismo de cifragem de dados.

Datacenter

- Ambientes físicos – no caso da ocorrência de um terramoto ou inundação, um *datacenter* num local onde possam ocorrer esse tipo de desastres naturais, e sem as condições de segurança "física" necessárias, corre o risco de ser danificado.
- Configuração dos sistemas de informação – a má configuração do *datacenter* pode levar à existência de vulnerabilidades no software que possam ser exploradas por atacantes informáticos.

5.3. Probabilidade de concretização e impacto das ameaças

De seguida, vamos calcular o impacto que cada ameaça representa no caso de se concretizar, assim como a probabilidade da mesma acontecer. Assim, ao lerem este tópico, a administração da empresa pode ter uma noção dos aspetos a melhorar.

Linha de abate tecnológica e inovadora

- **Acesso físico** – a empresa possui um eficiente sistema de acessos físicos, com possibilidade de uma entrada e uma saída nas instalações, por dia, por funcionário, logo esta ameaça tem BAIXA probabilidade de acontecer.

- **Acesso informático** – o departamento de informática da empresa é um dos mais debilitados, tendo a empresa poucos recursos humanos na área da segurança informática. Tendo isso em conta, e o facto de ainda não terem existido ataques informáticos à linha de abate, esta ameaça tem MÉDIA probabilidade de acontecer.
- No que toca ao **impacto** que os riscos associados a este ativo, caso se concretizem, podemos classificar o impacto como ALTO, uma vez que esta nova linha de abate tecnológica e inovadora é o principal instrumento/ferramenta que difere a empresa dos concorrentes, e que assegura a principal fonte de rendimento da empresa.

Smatphones e *laptops* atribuídos aos funcionários

- **Roubo físico** – esta ameaça depende muito do comportamento que os funcionários que possuem quer os smartphones, quer os *laptops*, tem no seu dia a dia, mas regra geral, espera-se que não ocorram roubos destes dispositivos, logo esta ameaça tem BAIXA probabilidade de acontecer.
- **Roubo de informação** – como referido anteriormente, o departamento de informática da empresa não está muito desenvolvido, nem existem formações aos funcionários sobre como devem proteger os seus dispositivos, logo esta ameaça tem MÉDIA probabilidade de acontecer.
- No que toca ao **impacto** que os riscos associados a este ativo, caso se concretizem, podemos classificar o impacto como MÉDIO, uma vez que cada funcionário pertence a um departamento, e não à totalidade dos mesmos da empresa, logo o impacto sobre a descoberta de informação num dispositivo de um funcionário não é tão preocupante como se fosse no caso do CEO da empresa ou de um chefe de departamento.

Cartão RIFD para viatura da empresa

- **Roubo do cartão** – igualmente ao roubo físico de smartphones e laptops, esta ameaça depende muito do comportamento que os funcionários que possuem estes cartões têm no seu dia a dia, mas regra geral, espera-se que não ocorram roubos deste tipo de dispositivo, logo esta ameaça tem BAIXA probabilidade de acontecer.
- **Clonagem do cartão** – novamente, como já foi referido, o departamento de informática da empresa é dos mais debilitados, não tendo estes dispositivos a configuração necessária para evitar este tipo de ataque (clonagem remota). Diferente do roubo de informação no tópico anterior, aqui é algo que os funcionários não podem evitar ou controlar, ao contrário dos *smartphones* e *laptops*, que podem ter certos cuidados com a sua utilização.
- No que toca ao **impacto** que os riscos associados a este ativo, caso se concretizem, podemos classificar o impacto como BAIXO, uma vez que a única situação que aconteceria, seria a perda das viaturas. Seria uma perda financeira, mas não teria grande impacto no que toca à integridade base da empresa, ou seja, esta não ficaria exposta a impactos igualmente comparados a exposição ou roubo de informações que possam prejudicar a empresa no caso de se tornarem públicas ou sejam entregues a concorrentes diretos da empresa.

Datacenter

- **Acesso informático** – novamente, como já foi referido, o departamento de informática da empresa é dos mais debilitados, por isso a probabilidade de um ataque ao *datacenter* classificada como MÉDIA, uma vez que ainda não ocorreram ataques informáticos ao mesmo.
- **Destruição/danificação do *datacenter*** – tendo em conta a região onde o *datacenter* se encontra (Alcanede, Santarém), não é uma área nem muito próxima do mar, nem com grande atividade sísmica, como o Algarve, para causar um terramoto, logo, a probabilidade desta ameaça eventualmente se realizar é BAIXA.
- No que toca ao **impacto** que os riscos associados a este ativo, caso se concretizem, podemos classificar o impacto como ALTO, uma vez que o *datacenter* é o local onde estão concentrados os sistemas computacionais da empresa, como os sistemas de comunicação, armazenamento, entre outros, o impacto que a interrupção das funcionalidades do *datacenter* provocaria na empresa, seria elevado.

De modo a compreender o "valor" de cada classificação, apresentamos de seguida três tabelas com o significado de cada atribuição quer ao impacto que um ativo ameaçado/atacado pode causar na organização, quer a probabilidade de tal acontecer.

IMPACTO	
Baixo	Impacto classificado como Baixo é aquele que, no caso de acontecer, causa danos mínimos na organização, facilmente reparáveis.
Médio	Impacto classificado como Médio é aquele que, no caso de acontecer, causam danos que podem atrasar o funcionamento da organização.
Alto	Impacto classificado como Alto é aquele que, no caso de acontecer, causa danos críticos (podem até ser irreversíveis) na organização, que condicionam drasticamente o funcionamento da organização.

Tabela 1 - Classificação do Impacto negativo de uma ameaça a ativo

PROBABILIDADE	
Baixa	Probabilidade classificada como Baixa é referente à junção de uma ameaça que nunca aconteceu e que a organização tem mecanismos adequados de proteção contra a ameaça em questão.
Média	Probabilidade classificada como Média é referente à junção de uma ameaça que nunca aconteceu, mas que a organização não tem mecanismos adequados de proteção contra a ameaça em questão, ou vice-versa (a ameaça já aconteceu sob a forma de ataque, mas, entretanto, a organização já adotou mecanismos de proteção contra a ameaça em questão).
Alta	Probabilidade classificada como Alta é referente à junção de uma ameaça que já aconteceu e que a organização não tem mecanismos adequados de proteção contra a ameaça em questão.

Tabela 2 - Classificação da probabilidade de concretização de uma ameaça a um ativo

		IMPACTO		
		Baixo	Médio	Alto
PROBABILIDADE	ALTA			
	MÉDIA			
	BAIXA			

Tabela 3 - Tabela de Criticidade (Impacto x Probabilidade)

Esta última tabela representa a criticidade de uma ameaça baseada na combinação entre o impacto que pode vir a provocar e probabilidade de acontecer. Esta tabela deve ser também utilizada para priorizar quais as ameaças que devem ser combatidas primeiro e quais os ativos que devem ser primeiramente protegidos.

6. Política de segurança de informação da organização

Tendo em conta a análise de risco que contempla as vulnerabilidades e ameaças associadas aos principais ativos da ValSabor, foi criada uma política de segurança de informação com quatro normas.

Cada uma das normas abrange temas como uma política de segurança macro para dar a entender o ambiente da segurança da informação (política de segurança macro), mitigação/controlo dos riscos do negócio, gestão dos ativos e classificação de informação.

De salientar que todas estas normas são resultado da informação, que temos sobre a ValSabor, referente aos principais ativos e funcionamento da organização e as recomendações dadas pelo Quadro Nacional de Referência para a Cibersegurança [21] e Roteiro para Capacidades Mínimas de Cibersegurança [32].

6.1. Norma n.º 1 – Ambiente de segurança da informação

1 – Antes de tudo, a organização deve efetuar uma análise SWOT [33] em relação à segurança da informação para perceber quais os seus pontos fortes (*Strengths* - possivelmente sistemas ou mecanismo eficientes que possui), os seus pontos fracos (*Weaknesses* – a falta de um departamento de segurança da informação, no caso da ValSabor), as oportunidades (*Opportunities* – oportunidades que tenha de melhorar a segurança da informação) e Ameaças (*Threads* – como as ameaças provenientes dos ativos em análise no presente documento).

2 – A missão e objetivos da segurança da informação é garantir a tríade CIA que se baseia em garantir a confidencialidade da informação, que consiste na proteção da informação contra acessos não autorizados, a integridade da informação, que previne a informação de ser alterada ou eliminada por pessoas não autorizadas a tal, e a disponibilidade da informação, que consiste na disponibilidade da informação a "tempo e horas" a pessoas autorizadas.

3 – Para além dos objetivos referidos no ponto anterior, a organização deve procurar saber mitigar o impacto de possíveis incidentes (norma n.º 2), gerir os ativos que possui (norma n.º 3) de modo a poder priorizar a segurança/proteção dos ativos e serviços mais críticos para o bom funcionamento da organização, e classificar a informação com que a organização trabalha (norma n.º 4).

6.2. Norma n.º 2 – Mitigação de riscos do negócio

1 – A organização deve adquirir no mínimo dois UPS e implementá-los nos dois ativos em análise mais importantes (Datacenter e Sistema tecnológico e inovador de abate) uma vez que são os principais para a atividade crítica da organização.

2 – Relativamente aos *laptops* e *smartphones*, deve ser dada uma formação aos funcionários da organização, no âmbito de os sensibilizar às boas práticas quer de utilização dos dispositivos (como navegar na internet de forma segura e sem comprometer o dispositivo), quer de segurança (boas práticas relacionadas a *passwords* ou utilização de *2FA – 2 Factor Authentication* [28] nas suas contas de redes sociais, correio eletrónico, entre outros).

3 – A organização deve ter contratos com terceiros, nomeadamente: operadoras de comunicações para evitar ataques de negação de serviços (*DoS*) através de serviços ou *software*, ou mitigar o impacto no caso de um desses ataques, sob a forma de possuírem um contacto de uma operadora que resolva a situação o mais rapidamente possível; empresas de manutenção de *hardware* e *software* de modo a realizar periodicamente uma análise de bom funcionamento dos ativos físicos e lógicos da organização; empresas de distribuição de

eletricidade, como a EDP, para no caso de interrupção da mesma, a organização consiga retomar as suas atividades o mais rapidamente possível.

4 – A organização deve implementar mecanismos de deteção (*IDS*), de modo a tentar prever a ocorrência de um ataque o mais rápido possível e alertar entidades competentes que possam resolver a situação, assim como configurar mecanismos de proteção (*IPS*) como uma firewall que bloqueie o tráfico de dados para *IPs* e portos específicas.

5 – Para complementar o ponto anterior, a organização deve adotar certos protocolos para cada estado em que a informação se encontra, como o uso do protocolo *TLS* para dados em transporte numa comunicação; realizar análises dos cabeçalhos dos pacotes de rede para detetar possíveis anomalias que levem a ataques ou que de alguma forma possam vir a representar um impacto negativo na organização e restringir o uso de interfaces externas para o funcionamento da organização, uma vez que tudo o que é exterior ao ambiente/rede da organização, esta não tem controlo do que se possa circular e dos perigos que podem representar.

6 – A mitigação dos riscos deve ser baseada e priorizada consoante a análise de risco, sobre os ativos em questão, que contempla as vulnerabilidades correspondentes às ameaças que cada ativo pode levantar, probabilidade dessas mesmas ameaças se concretizarem e o impacto que o acontecimento dessas ameaças teria na organização.

7 – A organização deve realizar uma análise de vulnerabilidades a cada 3 meses, de modo a identificar vulnerabilidades existentes, recorrendo à sua identificação para posterior atuação e mitigação das mesmas.

8 – A organização deve desenvolver um mecanismo de contenção em caso de incidente que suspenda o acesso à internet (para evitar que *malware* [34] entre no sistema), bloquear contas temporariamente até o incidente estar resolvido (para que estas não sirvam como ferramenta ou fonte de dados para o atacante), fechar portos de comunicação (como o porto 22 que é responsável por ligações remotas a um dispositivo), entre outras coisas.

9 – Complementando o ponto anterior, a organização deve adquirir uma equipa de segurança informática, pronta a erradicar um ataque, removendo o *malware* [34] utilizado no ataque, aplicando atualizações de segurança e restaurando as cópias de segurança necessárias. Tudo isto antes do término do mecanismo de contenção, para evitar que o ataque se espalhe para além da rede da organização em questão.

6.3. Norma n.º 3 – Gestão de ativos

1 – Aquando da aquisição ou criação de um ativo por parte da organização, este deve ser inventariado. Se a organização não possuir ainda esse inventário, este deve ser criado o mais rapidamente possível.

2 – A inventariação deve conter para *laptops* e *smartphones* o endereço *IP*, número de série e a quem pertence o dispositivo; para os cartões RFID a quem pertence o cartão; e

para a tecnológica e inovadora linha de abate, e *datacenter*, deve ser guardado o nome e departamento associado aos funcionários que interagem com estes ativos.

3 – A inventariação deve ser atualizada a cada 6 meses.

4 – Para além dos ativos físicos, deve ser feita a inventariação das aplicações e sistemas que a organização utiliza (ativos lógicos).

5 – Os ativos devem ser classificados conforme a sua criticidade para a atividade da organização, e tendo em conta a classificação atribuída à informação com que os ativos trabalham.

6 – Os ativos que suportam os serviços críticos da empresa também devem ser inventariados, e classificados como críticos, tendo em conta a sua importância.

6.4. Norma n.º 4 – Classificação de informação

1 – A organização deve implementar um sistema que classifica toda a informação que esta possuir como normal ou confidencial, de modo a poder tratar cada um desses tipos de informação de forma diferente. A informação que será classificada como confidencial é informação que pode de alguma forma prejudicar a organização em caso de fuga de informação ou má uso da mesma (informação que seja necessária para o bom funcionamento da organização).

2 – A organização deve implementar um sistema que classifica o correio eletrónico dos membros da mesma como normal ou maligno.

3 – A organização deve ter em especial atenção o transporte de informação classificada como confidencial, devendo esta ser transportada apenas por um responsável de transporte, elegido pelo CEO da organização.

4 – A organização deve criar um departamento que se dedique ao tratamento da informação, nomeadamente a informação classificada como confidencial, de modo a ser avaliada antes de ser entregue aos funcionários que irão trabalhar com a mesma.

5 – A informação classificada como confidencial ser armazenada num servidor onde seja aplicada mais segurança que o normal, uma vez de se tratar de informação sensível da organização.

6 – No final do ciclo de vida de informação classificada como confidencial, esta deve ser destruída com um fragmentador de papel, no caso de se apresentar nesse formato, e se algum servidor ou disco externo deixar de ser utilizado e contiver informação desse tipo de classificação, deve ser utilizada uma máquina que destrua metal.

7. Desenho e implementação da arquitetura e segurança perimétrica

No desenho da arquitetura e segurança perimétrica, decidimos dividir a Valsabor em 4 zonas principais de segurança, sendo elas o *datacenter*, a linha de abate, a frota de veículos e os escritórios.

Em primeiro lugar temos o *datacenter* que é um ativo com uma grande importância para a organização. São estes servidores do *datacenter* que suportam não só a Valsabor como todas as outras organizações de todo o grupo, dando acesso à maioria dos serviços essenciais para o funcionamento da organização. O *datacenter* tem também um UPS de última geração alimentado por duas potentes baterias, que tem como objetivo mitigar possíveis falhas na energia, tentando assim manter os servidores sempre disponíveis, até que o gerador existente consiga suportar a energia para os diversos edifícios.

Logo abaixo temos, uma zona de segurança relacionada com a principal atividade da empresa que é o abate e a transformação de carne. Esta linha de abate está ligada a um dashboard onde são apresentados os dados recolhidos da linha de abate e que está diretamente ligada ao *datacenter*. Para a linha de abate também está ligado um UPS, que, tal como no *datacenter*, tem como objetivo mitigar possíveis falhas na energia, tentando neste caso manter as máquinas desta linha sempre ativas.

Outra zona de segurança é também a frota de veículos, uma vez que alguns funcionários têm acesso a um cartão RFID que permite terem acesso aos veículos da empresa e também às bombas de combustível.

Por fim temos, também, uma zona bastante importante que são os escritórios da organização, onde é tratada toda a logística e parte informática. Os computadores do escritório estão diretamente ligados ao *switch* que têm ligação ao *router* permitindo assim existir uma conexão à *internet*.

Como podemos verificar todas as zonas acabam por ter uma ligação direta ou indireta ao *router* que permite a ligação à *internet*. Esta ligação está protegida através de uma *Firewall* que faz a filtragem do tráfego e evita a exposição da organização a protocolos de comunicação desnecessários ou perigosos.

Para além da *firewall*, é também usado um IDS que permite que a filtragem seja também feita com base numa base de dados podendo assim analisar o conteúdo do tráfego e detetar e bloquear padrões de ataques conhecidos.

Na figura 4, podemos visualizar um desenho da arquitetura de rede da organização.*Figura 5*

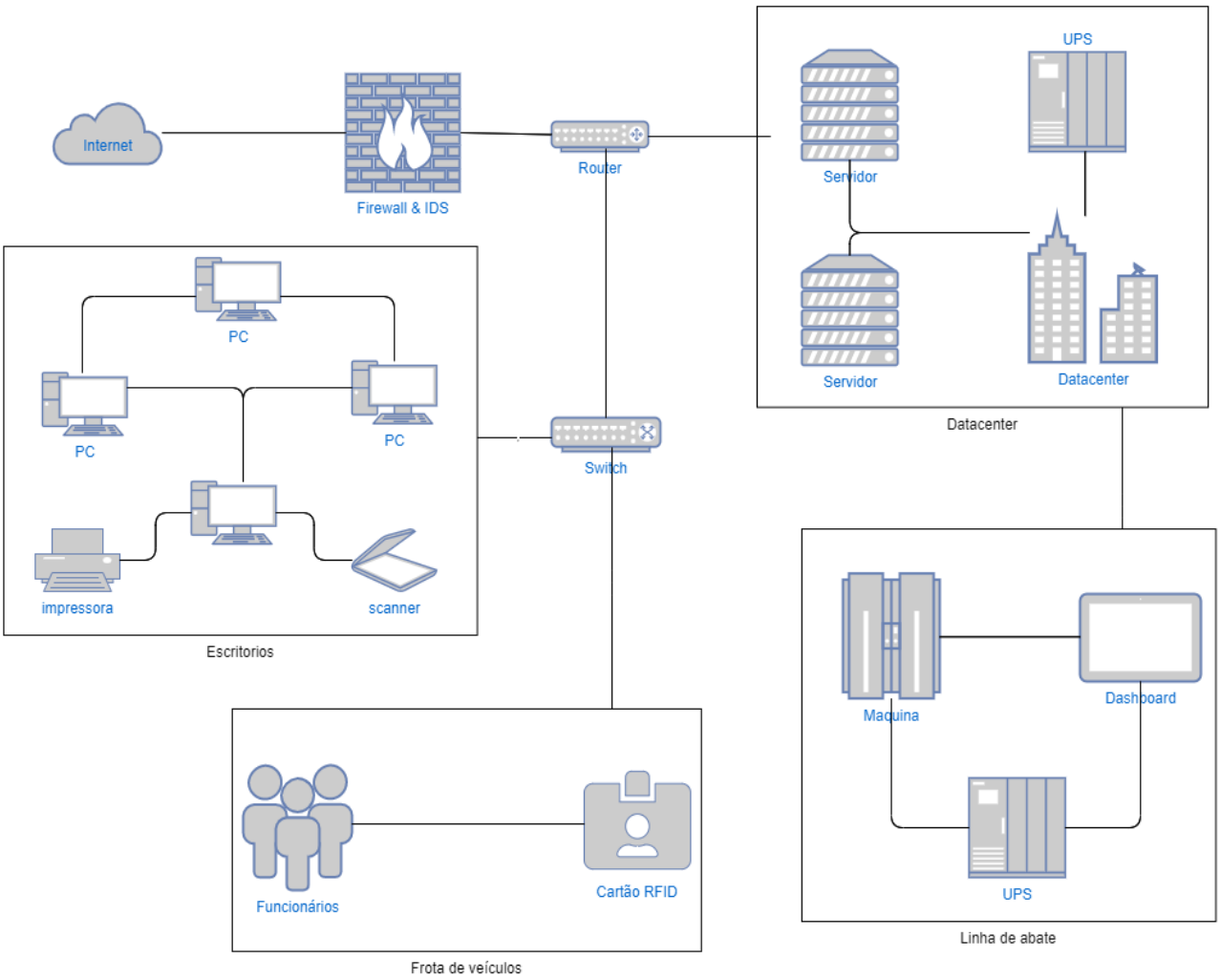

Figura 5 - Desenho da arquitetura de rede da organização

8. Estabelecimento de conformidade com legislação e normas aplicáveis

8.1. Identificar a legislação aplicável e os quadros legais e regulatórios a que está sujeita

Existem duas entidades responsáveis pela legislação e por todo o regulamento aplicável ao setor animal e alimentar.

Relativamente ao bem-estar animal existe o Manual do Bem-Estar Animal [35], desenvolvido pela Direção Geral de Alimentação e Veterinária em cooperação com a Confederação dos Agricultores de Portugal. Este manual contempla toda a legislação aplicável a cada caso e em relação a 5 espécies animais (Bovinos, Caprinos/Ovinos, Suínos, Galinhas Poedeiras e Frangos) como também relativamente ao seu transporte.

A ASAE tem como objetivo a "fiscalização e prevenção do cumprimento da seguinte legislação reguladora do exercício das atividades económicas em sentido amplo, nos setores alimentar e não alimentar, bem como a avaliação e comunicação dos riscos na cadeia alimentar, sendo o organismo nacional de ligação com as suas entidades congéneres, ao nível europeu e internacional."

A legislação pela qual a ASAE fiscaliza e toma as suas medidas está presente no Diário da República.

8.2. Normas ou certificações relevantes e aplicáveis ao setor

A Valsabor é uma empresa focada no abate e transformação de carne, podendo assim dividir-se em tom mais geral em dois tipos de certificações e normas que podem ser relevantes para este contexto. Em primeiro, ao nível do Bem-estar Animal, ou seja, a forma como os animais são tratados e em que condições são criados que indiretamente pode estar ligado, em segundo, ao nível da qualidade dos alimentos que são produzidos.

As certificações associadas ajudam as empresas a se destacarem no mercado, dando aos consumidores credibilidade e confiança na qualidade dos seus produtos.

Em relação ao bem-estar animal, uma certificação bastante relevante e reconhecida a nível europeu, é a *WelFairTM*, é uma certificação baseada em dois projetos já existentes e onde foram desenvolvidos sistemas de avaliação e controle do bem-estar dos animais em explorações, pontos de venda e matadouros como é o caso da Valsabor. Esta certificação tem a validade de 3 anos.

Em relação certificações e normas relevantes para o setor alimentar, existem:

- ISO 22000 – Sistema reconhecido internacionalmente e desenvolvido para assegurar a segurança alimentar de forma sistemática em cada etapa da cadeia de abastecimento.
- BRC Global Standard – Dá à empresa uma garantida de qualidade, segurança e responsabilidade. Atua ao nível dos produtos, do seu embalamento e de como são armazenados e distribuídos.
- FSSC 22000 – Norma reconhecida internacionalmente que visa ajudar as empresas a proteger as suas marcas e salvaguardar a saúde publica.
- SQF – Abrange todo o ciclo de fornecimento, o seu objetivo é garantir um sistema de qualidade, segurança alimentar e controle de documentos. Esta certificação está dividida em 3 níveis.
- IFS Food – Certificação globalmente conhecida que contribui para melhorar a imagem da marca, aumentar a confiança dos consumidores e aumentar as oportunidades de mercado.
- Global GAP – Promove a segurança ao nível da agricultura, pecuária e aquacultura. O cumprimento desta norma também indica que os produtos são criados de forma sustentável.

Neste momento o ValGrupo possui duas empresas com certificados alimentares.

A Nutriaves que possuí a certificação *IFS FOOD* – "Esta certificação, reconhecida a nível internacional, veio representar uma garantia adicional da qualidade dos produtos Nutriaves e nos processos alimentares, construindo mais confiança aos consumidores." [36].

A Valsabor possui até 2024 a certificação ISO 22000 – "Com o objetivo de minimizar os riscos alimentares e aumentar a confiança dos consumidores cada vez mais conscientes no que se refere à segurança e qualidade dos alimentos, este esquema de certificação, que incorpora a norma ISO 22000 promove o contínuo cumprimento dos requisitos legais aplicáveis ao nível da segurança alimentar, possibilitando o reconhecimento das empresas num mercado mais amplo e exigente" [8].

A Maporal encontra-se certificada, pela SGS, de acordo com a Norma NP EN ISO 22000:2005, desde abril de 2010, o que reflete a preocupação da empresa em garantir que todos os processos inerentes à sua atividade contribuam para a obtenção de produtos finais seguros no momento do consumo [38].

9. Política de Uso Aceitável (PUA)

A política de uso aceitável é um documento que define como é que os recursos de IT de uma organização podem e devem ser utilizados com o objetivo de proteger os sistemas contra acessos não autorizados, danos, perdas, abusos e roubo.

Esta política deve ser cumprida por todos os que tenham algum contacto com a empresa, sejam eles funcionários, parceiros ou convidados.

Estas políticas de uso aceitável pretendem ser um primeiro passo para que todos os colaboradores estejam cientes da sua responsabilidade ao usar os recursos de TI da ValSabor de forma legal, ética e profissional.

9.1. Pressupostos da Política de Uso Aceitável adequada aos recursos TI

9.1.1. Papéis e Responsabilidades

1 - A organização tem o dever de facultar o equipamento necessário para o bom desempenho dos funcionários, dar-lhes formações para que estes possam desempenhar bem as suas tarefas e defender os direitos dos trabalhadores.

2 – O funcionário compromete-se a cumprir todas as regras de higiene, segurança e ambientais, assim como não prejudicar propositadamente a organização em termos informáticos.

9.1.2. Manutenção dos postos de trabalho e ambiente de trabalho

1 – Os funcionários devem executar uma limpeza periódica do posto de trabalho, mantendo os locais limpos, uma vez que a acumulação de resíduos pode danificar alguns dispositivos.

2 – Não comer nos locais de trabalho. Os funcionários devem recorrer à cantina e ao bar para tomar as refeições. Isto porque um derrame acidental de líquidos em dispositivos informáticos, pode danificá-los.

3 – Os funcionários devem ter em atenção o manuseamento dos cabos de rede, uma vez que o mau manuseamento dos mesmos pode causar embaraço e confusão na sua disposição, e posteriormente, utilização.

9.1.3. Correta utilização do correio eletrónico para uso profissional

1 – Os funcionários não devem utilizar o mail profissional para registo/uso em aplicações e websites externos.

2 – Os funcionários devem apenas aceder ao correio eletrónico profissional nas instalações da organização, ou através do uso de uma VPN para acesso ao mesmo quando o funcionário não se encontrar nas instalações da organização.

3 – O endereço de correio eletrónico é baseado no primeiro e último nome do funcionário, e é-lhe atribuído aquando da contratação do mesmo.

4 – Os funcionários devem sempre verificar atentamente o conteúdo e teor dos mails que receberem, uma vez que existem formas de contornar os mecanismos de deteção e proteção de intrusão.

5 – As passwords dos correios eletrónicos tem de possuir pelo menos 8 caracteres, 1 número, 1 caracter especial e uma letra maiúscula.

9.1.4. Comportamento adequado na navegação na Internet

1 – Os funcionários devem ter atenção aos links antes de os abrir, uma vez que um link pode estar disfarçado e redirecionar o utilizador para outro website que possa descarregar *malware* na máquina do funcionário. Em caso de dúvida utilizar ferramentas como virustotal.com [37] para saber se o *URL* é ou não confiável.

2 – Os funcionários devem ter em atenção o protocolo de comunicação utilizado pelos websites que visitam durante o tempo de trabalho, uma vez que websites com protocolo de comunicação *HTTP* não cifram mensagens / informação que neles circula.

3 – Qualquer password que os funcionários utilizem quer internamente, quer externamente à rede, nunca devem ser armazenados no browser. Devem então recorrer a um gestor de passwords.

9.1.5. Utilização de dispositivos em contexto BYOD

1 – Todos os smartphones dos funcionários não se podem ligar à rede informática da organização, uma vez que podem ser alvo de um ataque e depois contaminam a rede da mesma.

2 – Não é recomendado o uso de portáteis pessoais por parte dos funcionários, uma vez que a organização fornece todo o equipamento necessário para o bom desempenho das tarefas de cada funcionário. Se os funcionários optarem pelo uso de equipamento pessoal, este deve passar por uma análise rápida sempre que acedem à rede da organização.

3 – Outros dispositivos pessoais com endereços IP e que utilizem protocolos de comunicação, como *smartwatches*, *hearphones* ou colunas *Bluetooth* são expressamente proibidos.

9.1.6. Instalação e utilização de software aplicacional

1 – Qualquer software que seja instalado por um funcionário, deve passar por uma breve análise do departamento de segurança da informação, para avaliar a sua confiabilidade.

2 – O uso de software não fidedigno ou malicioso e não aprovado pelo departamento de segurança da informação pode levar ao despedimento direto do funcionário.

9.1.7. Respeito pelos princípios de ética e pela privacidade e proteção de dados pessoais

1 – Assegurar que os dados pessoais dos funcionários e dos clientes são tratados de acordo com a legislação nacional e com o regulamento geral de proteção de dados (RGPD).

2 – Os funcionários não devem guardar documentos profissionais que contenham informações pessoais ou sensíveis, em dispositivos pessoais, relacionados com a organização.

3 – Os funcionários devem trabalhar/utilizar a informação sensível a que possam ter acesso apenas para os fins a que a mesma foi destinada.

4 – Os funcionários não podem criar, transmitir, apresentar ou publicar qualquer informação sensível, com o objetivo de denegrir a imagem ou prejudicar a organização ou qualquer outro funcionário.

9.1.8. Trabalho remoto ou teletrabalho

1 – Em caso de doença ou indisponibilidade de comparecer no local físico de trabalho, os funcionários podem optar por trabalhar em teletrabalho. Como é óbvio, a

justificação tem de ser plausível e confirmada por uma outra entidade (como um médico, por exemplo).

2 – A não justificação ou fraca justificação da recorrência ao teletrabalho leva ao despedimento direto do funcionário.

3 – Aquando da recorrência a teletrabalho, os funcionários devem recorrer ao uso da VPN da organização, de modo à sua monitorização quer de trabalho desenvolvido, quer de *websites* ou aplicações que o funcionário possa estar a recorrer.

9.1.9. Administração do parque informático e do acesso aos recursos em rede

1 – Os administradores do departamento de informática da organização devem ter em atenção às atualizações que possam surgir nos softwares utilizados pelos funcionários e no *firmware* dos dispositivos como servidores e *end-points* da organização.

2 – Aquando da entrada de um funcionário na organização, a este é-lhe concedida uma conta de utilizador, mas baseada no privilégio mínimo, ou seja, apenas terão acesso a todos os recursos da rede, os funcionários que possuam uma conta com privilégios de administrador.

3 – Os administradores do departamento de informática devem proceder à realização de *backups* periódicos de toda a informação fundamental para o bom funcionamento continuo da organização.

Referências

[1] "AGRUPALTO PRESENTE NO PROJETO DA COMISSÃO EUROPEIA," [Online]. Available: www.valgrupo.pt.

[2] R. Silva, "Revolução na suinicultura. Alentejo vai acolher maior unidade nacional de abate," 22 10 2019. [Online]. Available: rr.sapo.pt.

[3] "Valsabor," [Online]. Available: valsabor.pt.

[4] "ValGrupo," [Online]. Available: valgrupo.pt.

[5] "AQUISIÇÃO DA INTERSUÍNOS PELA EUROESTE POTENCIA ATIVIDADE EXPORTADORA PARA ÁSIA E AMÉRICA," [Online]. Available: www.valgrupo.pt.

[6] "VALSABOR INVESTE MAIS DE 15 MILHÕES NA UNIDADE PRODUTIVA DE ALCANEDE," [Online]. Available: www.valgrupo.pt.

[7] J. Baptista, "Valgrupo anuncia investimentos de 38 milhões de euros em nova fábrica de rações e novo matadouro," [Online]. Available: www.maisribatejo.sapo.pt. [Acedido em 21 10 2020].

[8] "VALSABOR OBTÉM A CERTIFICAÇÃO ISO 22000," [Online]. Available: www.valgrupo.pt.

[9] "Valsabor," [Online]. Available: www.valgrupo.pt.

[10] "ValPor," [Online]. Available: www.valgrupo.pt.

[11] "ValTTL," [Online]. Available: www.valgrupo.pt.

[12] "ValNutri," [Online]. Available: www.valgrupo.pt.

[13] "ValCiaro," [Online]. Available: www.valgrupo.pt.

[14] "ValCivil," [Online]. Available: www.valgrupo.pt.

[15] "ValMob," [Online]. Available: www.valgrupo.pt.

[16] “ValAmbi,” [Online]. Available: www.valgrupo.pt.

[17] “Nutriaves,” [Online]. Available: www.valgrupo.pt.

[18] “ValWine,” [Online]. Available: www.valgrupo.pt.

[19] “Empresas Participadas,” [Online]. Available: www.valgrupo.pt.

[20] “O que é RFID ?,” [Online]. Available: www.ncontrol.com.pt.

[21] “Quadro Nacional,” [Online]. Available: www.cncs.gov.pt.

[22] L. Kovacs, “O que é endereço MAC?,” [Online]. Available: www.tecnoblog.net.

[23] “Número de série,” [Online]. Available: www.techlib.wiki.

[24] “CONCEITOS SOBRE UPS,” [Online]. Available: www.tecnicontrol.pt.

[25] “WordPress,” [Online]. Available: pt.wordpress.org.

[26] “Laravel,” [Online]. Available: laravel.com.

[27] “VueJS,” [Online]. Available: vuejs.org.

[28] E. Griffith, “Two-Factor Authentication: Who Has It and How to Set It Up,” [Online]. Available: www.pcmag.com. [Acedido em 27 04 2021].

[29] R. Silva, “Gestor de passwords: o que é e para que serve?,” 28 09 2016. [Online]. Available: www.i-tecnico.pt.

[30] “O que é firewall? - Conceito, tipos e arquiteturas,” [Online]. Available: www.infowester.com. [Acedido em 19 02 2013].

[31] “O que é um antivírus?,” [Online]. Available: www.eset.com.

[32] “Roteiro para Capacidades Mínimas de Cibersegurança,” [Online]. Available: www.cncs.gov.pt.

[33] C. Casarotto, “Aprenda o que é análise SWOT, ou análise FOFA, e saiba como fazer uma análise estratégica do seu negócio,” 20 12 2019. [Online]. Available: rockcontent.com.

[34] “O que é malware? Como malwares funcionam e como se livrar deles,” [Online]. Available: www.avg.com.

[35] “Manuais de Bem-Estar Animal,” [Online]. Available: www.dgadr.gov.pt.

[36] “CERTIFICAÇÃO IFS FOOD - NUTRIAVES,” [Online]. Available: www.valgrupo.pt.

[37] “VirusTotal,” [Online]. Available: www.virustotal.com.

[38] “Certificações,” [Online]. Available: www.maporal.com.