Daniela Filipa Dinis Silva

ANÁLISE DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Estudo de Caso de uma Empresa do Setor dos Transportes Rodoviários de Mercadorias e Armazenagem

Trabalho de Projeto submetido como requisito parcial para obtenção do grau de **Mestre em Gestão de Sistemas de Informação**

Orientador (Professor Doutor, José Manuel Gaivéo, ESCE/IPS)

janeiro de 2021

Dedicatória

"Cruz
Que este livro galante,
ante
Teus olhos, lembre um dia,
Quem to oferece nesta
Festa
De anos e de alegria.

Pequeno ele é e modesto.
Mesto
Quase sempre e tristonho;
Não roubará, no entanto,
Quanto
Tens de ilusão e sonho.

Aquela, que hás de agora,
Hora
Tirar (sem percebê-lo),
Das que em teus anos verdes
Perdes;
Não perderás ao lê-lo.

Lê com vagar. Repara
Para
A beleza do verso;
Vê como o vate ardente
Sente
O mundo tão diverso!...

Mas, que não te entristeças;
Nessas
Linhas, não há verdade.
Vive sempre a florida
Vida
Entre a felicidade".

Mário de Andrade

Dedico este trabalho à minha mãe *Rosa e à avó Francelina.*
São a minha motivação!

Agradecimentos

A realização deste trabalho apenas foi possível com o contributo de diversas pessoas que direta ou indiretamente me acompanharam nesta jornada. Desta forma, são todas merecedoras das minhas palavras de apreço e gratidão.

Expresso aqui o meu profundo agradecimento ao meu orientador, Professor Doutor José Manuel Gaivéo, pelo seu rigor e sabedoria, pela sua flexibilidade e prontidão que sempre demonstrou durante este percurso. Todas as suas revisões textuais, toda a bibliografia disponibilizada e todas as palavras de incentivo foram fulcrais para que as minhas ideias passassem do papel para o terreno e fossem exequíveis.

Agradeço, também, ao diretor geral da TMS, Henrique Elvas Martins, por ter autorizado que desenvolvesse o meu projeto na empresa e por ter contribuído de forma ativa para o mesmo respondendo a algumas perguntas que sustentam a parte prática.

Aos colaboradores da TMS, em especial à Cláudia Silva e à Patrícia Cardoso, que se mostraram sempre disponíveis para participar no projeto, preenchendo e devolvendo o questionário que também suporta a parte prática.

Ao Marco Freitas pelas conversas motivadoras e de incentivo durante todo o processo.

Á Marta Costa, começou colega mas depressa se tornou amiga, conselheira e companheira neste percurso. As suas palavras de incentivo e motivação, de amizade e preocupação foram fundamentais.

Ao Emmanuel Teixeira, pelo companheirismo, pela união, pela paciência, pelo amor e pelo carinho sempre demonstrado em todos os momentos.

Á minha estimada família, o meu muito obrigada pela ajuda, pela motivação pelo carinho e pelos olhares de orgulho que vos deixo ao entregar este trabalho.

O meu sincero obrigado a todos os intervenientes.

Índice

Índice de Tabelas

Índice de Figuras

Siglas e Abreviaturas

ASTRE - Associação de Transportes Europeus – Rede Europeia de Distribuição

CAE – Classificação Portuguesa das Atividades Económicas

CMR - *Convention on the Contract for the International Carriage of Goods by Road*

DRP - *Disaster Recovery Planning*

ERP – *Enterprise Resource Planning*

ID - *Identify*

IDC - *International Data Corporation*

IEC – *International Electrotechinal Commission*

INE – Instituto Nacional de Estatística

ISO- *International Organization for Strandardization*

ITRM - Inquérito ao Transporte Rodoviário de Mercadorias

NFC – *Near Field Communication*

SI – Sistemas de Informação

SGSI – Sistema de Gestão de Segurança da Informação

TI – Tecnologias de Informação

TIC – Tecnologias da Informação e da Comunicação

NAS – *Network Attached Storag*

Resumo

A introdução dos Sistemas de Informação (SI) e das Tecnologias de Informação (TI) traduz-se num conjunto de desafios e exigências com que as organizações se vêm confrontadas e cujas respostas dependem da cultura organizacional e das pessoas que as constituem.

A informação tem, hoje em dia, um papel fundamental nas organizações, espera-se que esta seja a fonte do funcionamento tático, estratégico e operacional, gerando vantagem competitiva nos mercados. A sua crescente importância conduziu a um problema, antigamente a partilha de informação apenas se registava por iterações pessoais, contudo, agora existem elementos como pessoas, processos, ambientes e tecnologias que podem contribuir para sérios problemas de segurança da informação nas empresas e influenciar diretamente no seu crescimento. É difícil e complexo controlar todos estes elementos mas existem práticas de segurança de informação que garantem que a informação certa esteja disponível no tempo certo, para que a pessoa certa possa tomar a decisão estratégica adequada.

Neste trabalho, a empresa escolhida pertence ao setor dos transportes rodoviários de mercadorias e armazenagem e o estudo de caso baseia-se na análise dos seus vários departamentos relativamente aos processos e procedimentos existentes sobre segurança da informação aliada à perceção da postura da empresa sobre a problemática abordada.

A gestão da segurança da informação da empresa apresenta algumas falhas. Desta forma, seria vantajoso a elaboração de um conjunto de políticas e regulamentos que uniformizem todo o processo e contribuam para a segurança dos dados da empresa.

Palavras-chave: Sistemas de Informação, Informação, Segurança, Transportes rodoviários de mercadorias e armazenagem

Abstract

The introduction of Information Systems (IS) and Information Technologies (IT) translates into a set of challenges and demands that organizations are faced with and whose responses depend on the organizational culture and the people that constitute them.

Information nowadays has a fundamental role in organizations, it is expected that this is the source of the tactical, strategic and operational functioning, generating competitive advantage in the markets. Its growing importance has led to a problem, in the past information sharing was only registered through personal iterations, however, there are now elements such as people, processes, environments and technologies that can contribute to serious information security problems in companies and directly influence its growth. Controlling all these elements is difficult and complex, but there are information security practices that ensure that the right information is available at the right time, so that the right person can make the right strategic decision.

In this essay, the chosen company belongs to the road transport of goods and storage sector and the case study is based on the analysis of its various departments in relation to the existing processes and procedures regarding information security combined with the perception of the company's posture on the problematic addressed.

The management of the company's information security has some flaws. Thus, it would be advantageous to develop a set of policies and regulations that would standardize the entire process and contribute to the security of the company's data.

Keyword: Information Systems, Information, Security, Road transport of goods and storage

1 Introdução

A informação representa um dos ativos mais importantes e poderosos para as organizações sendo responsável pelo processo de decisão organizacional e como tal este necessita de um adequado volume de informação preveniente de diversas fontes cujos elementos estão interligados numa rede de conexões sustentada por uma economia global.

Segundo Gaiveo, (2008) as preocupações com a segurança dos SI crescem exponencialmente com os efeitos da globalização nas sociedades, as organizações apostam cada vez mais em vias de comunicação digital, o que acarreta riscos que comprometem a confidencialidade, integridade e disponibilidade da informação, estes riscos devem ser analisados e controlados através de mecanismos de proteção adequados para garantir a segurança da informação e de todo o SI.

Os gestores de topo têm um papel fundamental na gestão da segurança da informação nas organizações, são eles que garantem a continuidade do negócio através de uma gestão ativa da segurança dos seus dados. Definem estratégias, métodos, ações e ferramentas a implementar para que os funcionários e partes interessadas percebam a importância das suas ações em todo o SI.

Desta forma, é importante que os gestores encarregues desta missão tenham profundos conhecimentos sobre a problemática abordada de modo a conseguir alinhar toda a organização no objetivo comum.

1.1 Objetivos

O presente estudo foi realizado no âmbito do Mestrado em Gestão de Sistemas de Informação, da Escola Superior de Ciências Empresariais do Instituto Politécnico de Setúbal, sendo objeto de avaliação de final do curso.

Este trabalho tem como principal objetivo o estudo da gestão da segurança da informação de uma empresa do setor dos transportes rodoviários de mercadorias e armazenagem. Pretende-se analisar todos os seus processos e procedimentos internos relativamente à proteção dos seus dados juntamente com a perceção da postura da organização sobre a problemática abordada.

Como objetivos específicos, este estudo irá analisar quais as principais falhas existentes na empresa relativamente à segurança da informação, perceber qual o motivo da sua existência, analisar se existe forma de as solucionar e propor soluções para os

problemas encontrados tendo por base as recomendações existentes nos *standards* internacionais sobre gestão da segurança da informação.

1.2 Metodologia

De acordo com os objetivos definidos foi necessário optar por uma metodologia de investigação que mais se adequa-se à problemática abordada e à realidade na qual iria ser estudada.

Freixo, (2010) e Fortin, (2009) afirmam que as metodologias de investigação estão assentes num conjunto de meios que permitem realizar a investigação; enquanto, o método é uma forma de selecionar a técnica e a forma de avaliar alternativas para a ação científica. Esta diferenciação indicia que numa metodologia pode recorrer -se à utilização de vários métodos.

Neste trabalho, optou-se pelo método de investigação qualitativo, segundo Fortin, (2009) este método consiste na criação de modos ou de tendências e visa fornecer uma descrição e uma compreensão alargada de um fenómeno, segundo este paradigma qualitativo, "... os fenómenos são únicos e não previsíveis e os esforços são orientados para a compreensão total do fenómeno estudado." Assim sendo, e como a gestão da segurança da informação contempla várias perspetivas dentro do contexto organizacional, foi necessário escolher um método que ajudasse a obter uma compreensão total e absoluta do fenómeno em análise.

O estudo foi realizado tendo do base uma empresa pertencente ao setor dos transportes rodoviários de mercadorias e armazenagem, ou seja, uma realidade e um contexto especifico da vida real, assim sendo, optou-se pelo estudo de caso como metodologia de investigação, segundo Yin, (1989), esta metodologia é uma inquirição empírica que investiga um fenómeno dentro de um contexto da vida real, quando o limiar entre o fenómeno e o contexto não é claramente evidente e onde múltiplas fontes de evidência são utilizadas. Esta perspetiva de Yin é reforçada por Mazzotti, (2006) que menciona que esta metodologia caracteriza-se por interesse em casos únicos e não pelos métodos de investigação.

Como técnica de recolha de dados, e considerando a complexidade do fenómeno em estudo, optou-se numa primeira fase pela observação participativa e posteriormente pelo inquérito por questionário para analisar o ambiente organizacional e as ações dos colaboradores da empresa sobre a segurança da informação, contando também com o

recurso à entrevista estruturada ao diretor geral para perceber a visão da empresa relativamente à problemática abordada.

1.3 Estrutura da Dissertação

De forma a conseguir atingir os objetivos propostos este trabalho encontra-se dividido em nove capítulos, o 1º capítulo faz um resumo sobre o enquadramento do trabalho, referindo a problemática, os objetivos, a metodologia e a sua estrutura .

O capítulo 2 apresenta uma seleção da literatura sobre a importância da informação e dos sistemas de informação para as organizações, fazendo referência à necessidade da gestão destes elementos em contexto organizacional. Aborda, também, as políticas e os mecanismos de proteção como forma de garantir a segurança da informação contribuindo para o alinhamento desta com a estratégia organizacional.

No capítulo 3 é apresentada uma breve descrição do setor de atividade em estudo juntamente com a referência da importância dos SI para a sua sobrevivência.

O capítulo 4 apresenta a empresa alvo de estudo, a sua cultura, missão, visão, e valores. Mencionando, também, o seu organograma e a analise da maturidade digital da empresa.

No capítulo 5 está mencionado o estudo de caso nomeadamente quais as técnicas de recolha de dados utilizadas e a sua explicação.

Surge o capítulo 6, onde se analisam os dados considerados relevantes para o estudo e resultantes das técnicas de recolha de dados aplicadas.

No capítulo 7 apresenta-se um conjunto de soluções e perspetivas de trabalho futuro que a organização deverá aplicar e desenvolver para eliminar ou mitigar as falhas encontradas ao nível da gestão da segurança da informação.

O capítulo 8 apresenta uma recomendação final auxiliando a organização no alinhamento da gestão da segurança da informação com a estratégia organizacional.

Por fim, o capítulo 9 é a conclusão, no qual será realizado um resumo de todo o trabalho desenvolvido em conjunto com a importância das soluções encontradas tendo em conta as falhas existentes na organização relativamente à gestão de segurança da informação.

2 Enquadramento Teórico

Neste capítulo, procura-se analisar a posição de vários autores sobre a importância da problemática em estudo – gestão da segurança da informação.

Qual o papel da informação e dos sistemas de informação para a sobrevivência das organizações e de que modo a segurança dos dados pode influenciar o negócio e a envolvência externa das organizações nos mercados concorrentes.

Quais as diretrizes que devem ser seguidas pelos gestores de topo para garantir a confidencialidade, integridade e disponibilidade da informação.

Pretende-se sintetizar quais os principais requisitos e modelos de gestão a ter em conta para garantir um Sistema de Gestão de Segurança da Informação (SGSI) eficiente, dando especial relevância às políticas e mecanismos de proteção da segurança da informação como meios de garantir a segurança dos dados das organizações.

Por último, faz-se a ligação entre o alinhamento da segurança da informação das organizações com a sua estratégia organizacional, mencionando a importância do papel dos gestores de topo e das chefias para atingir este objetivo.

2.1 Informação

Os dados constituem observações individuais, estando na base da comunicação humana, das mensagens textuais, das interrogações eletrónicas e nos instrumentos científicos de medição de fenómenos. O objetivo da recolha e análise dos dados é gerar informações úteis e para que estas tenham credibilidade é preciso reunir, analisar e compreender os dados (Waltz, 1998).

A informação consiste em conjuntos organizados de dados de forma a colocá-los num determinado contexto para subsequente pesquisa e análise, esta uma vez analisada e compreendida, transforma-se em conhecimento.

"Na atualidade, o mundo vive na era da informação, exigindo das organizações uma gestão estratégica eficiente, a qual pode ser facilitada pela utilização de recursos inteligentes oferecidos pelas TI e pelos SI" (López, 2014, p.25). A autora acrescenta ainda que a informação é, hoje em dia, um dos "motores da atividade humana" e que se apresenta como recurso estratégico sob a ótica de vantagem competitiva. Possui valor, pois está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros e tecnológicos.

"Sociedade da informação pode assim ser definida, como uma forma de desenvolvimento social e económico capaz de conduzir à criação de conhecimento e à satisfação das necessidades dos cidadãos e das organizações" (Fernandes *et al,* 2007, p.459)

O desenvolvimento e a crescente evolução das organizações está no resultado da evolução do conhecimento e da informação.

"Porém, as informações geram custos de obtenção e de processamento, o que implica a necessidade de se analisar a relação custo – benefício de se ter ou não uma determinada informação" (López, 2014, p.41).

Segundo Rodrigues, (2002) o valor da informação varia consoante os fatores de influência e uso da sua interpretação.

2.2 Sistemas de Informação

Encontramo-nos numa sociedade que favorece cada vez mais a informação, como sendo esta uma das principais preocupações. Assim, nas organizações existe a necessidade de garantir uma adequada infraestrutura para a sua recolha, armazenamento, processamento, representação e distribuição, o que obriga a que uma parcela apreciável do esforço da organização seja orientada para estas preocupações (López, 2014).

Segundo Gaivéo, (2008) um sistema tem a finalidade de suportar todos os processos de negócio de uma organização, sendo o termo processo definido como "... um conjunto relacionado de tarefas ou atividades que usam pessoas, informação e outros recursos para criar valor para os seus clientes internos e externos.".

Outros autores definem os sistemas de informação como sendo mecanismos de apoio à gestão, desenvolvidos com base na tecnologia de informação e com suporte da informática para funcionarem como condutores das informações que visam facilitar, agilizar e otimizar o processo decisório nas organizações (Pereira *et al*, 1997).

Gill, (1999) considera que os sistemas de informação compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros agregados segundo uma sequência lógica para o processamento dos dados e a correspondente tradução em informações.

"Todas as organizações, desde a sua constituição produzem, no seu funcionamento normal, informação que se traduzem no seu SI" (López, 2014, p.40).

Para dar resposta ao meio envolvente os SI têm todo um processo de transformação e desenvolvimento associado para que depois seja possível dar respostas ás atividades de toda a organização.

2.3 Segurança da Informação

A ISO/IEC 27000 (2014), define informação como um ativo que tem valor para uma organização e que requer proteção adequada, independentemente da forma ou meio de armazenamento, processamento e/ou transmissão. Define também o conceito de segurança como a tentativa de minimizar a vulnerabilidade de valores e recursos, entendendo-se, neste domínio, por vulnerabilidade o atributo de qualquer situação a partir da qual terceiros podem penetrar num SI informatizado sem qualquer autorização no sentido de tirar proveito do seu conteúdo ou das suas características.

"Segurança significa a existência de capacidade para se tomarem medidas preventivas que, se não forem suficientemente capazes para evitar as ocorrências indesejadas, maliciosas ou inesperadas, pelo menos prevejam ações a serem tomadas que minimizem as mesmas" (Mamede, 2006, p.3).

Ou seja, isso significa identificar os elementos mais fracos do sistema que se pretende seguro e desenhar soluções adequadas, que tenham em consideração os riscos e os custos associados à proteção de dados.

A informação é o principal ativo das empresas e está sob constante risco. O custo da sua integridade qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente.

"O acesso à informação em tempo oportuno e em termos físicos permite a criação de estratégias organizacionais gerando vantagens competitivas de penetração nos mercados ou mesmo de comparação de estratégias" (López, 2014, p.41).

De acordo com o ISO/IEC 27001 (2013) a análise da segurança da informação baseia-se em três conceitos principais: Confidencialidade, integridade e disponibilidade.

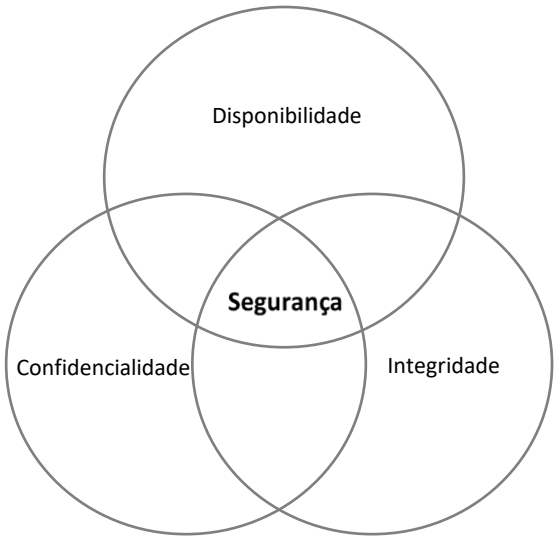


Figura 1 - Desafio da segurança da informação

(Adaptado de Pfleeger e Pfleeger (2003))

A confidencialidade está relacionada com a prevenção da utilização não autorizada de informação. A integridade está relacionada com a prevenção da modificação não autorizada da informação. E por fim a disponibilidade está relacionada com a prevenção da retenção não autorizada de informação ou recursos.

Estes conceitos estão relacionados, respetivamente, com a quantidade e natureza da informação que deve ser restringida, a credibilidade das fontes e o grau de certeza de que a informação é realmente a verdadeira e a possibilidade de utilização da informação no tempo e local requerido pelos utilizadores.

"O propósito de segurança da informação é proteger a informação de uma grande variedade de ameaças, assegurando a continuidade do negócio através da minimização dos danos causados neste por incidentes de segurança e da maximização do retorno dos investimentos e das oportunidades de negócio" (Gaiveo 2008, p.120).

Segundo Carneiro, (2009) cada vez mais os gestores de topo das organizações manifestam preocupações relativamente ao normal funcionamento dos SI na eventualidade da existência de um acidente que afetasse a confidencialidade, integridade e disponibilidade da informação. Sabendo que um acidente não é completamente evitável, é necessário garantir " ... a continuidade das atividades das empresas, minimizando os prejuízos, prevenindo e reduzindo o impacto dos incidentes de segurança e definindo padrões que permitam a análise e avaliação do SI".

2.4 Gestão da Segurança da Informação

A segurança da informação concretiza-se com um SGSI, que abarca o agrupamento dos ativos de negócio (pessoas, equipamentos, edifícios, material auxiliar, informação, entre outros) que sejam identificados como essenciais para o normal desenvolvimento do negócio, proporcionando a sua gestão de acordo com o estipulado nas normas e políticas vigentes.

A ISO/IEC 27001 (2013) define a gestão de segurança da informação, como um processo de gestão estruturado que permite garantir os principais requisitos de segurança da informação.

O SGSI é uma parte do sistema geral de gestão, baseando-se numa abordagem ao risco do negócio, para estabelecer, implementar, operar, monitorar, rever, manter e melhorar a segurança da informação. (ISO/IEC 27000, 2018).

Para facilitar os gestores de topo na gestão dos processos do SGSI a norma ISO/IEC 27001, 2013 indica o modelo, baseado no ciclo de melhoria contínua, PDCA (*Plan-Do-Check-Act*).

No modelo, as atividades iniciais são as de planeamento, na fase "*Plan*", passando para as de execução, na fase "*Do*", as de verificação, na fase "*Check*", e por último as atividades de melhoria, na fase "Act". Esse ciclo é repetido sucessivamente para que a cada novo ciclo, o sistema seja melhorado (figura 2).

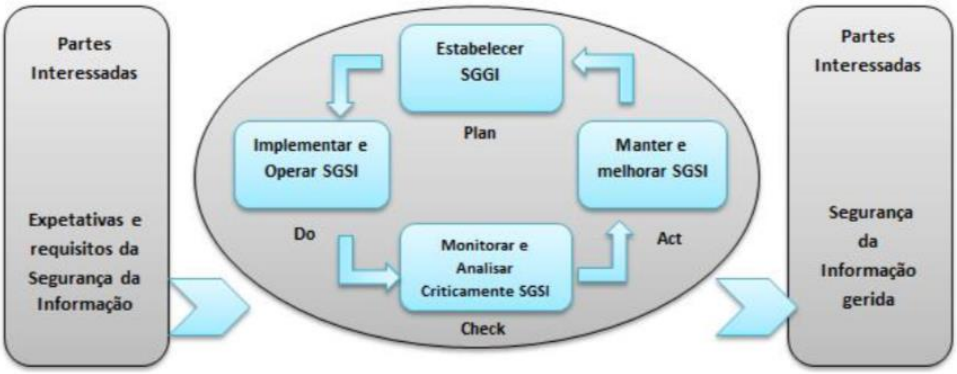


Figura 2 - Modelo PDCA aplicado aos processos do SGSI

(Adaptado de ISO/IEC 27000, 2014))

Fases do modelo PDCA:

a) *Plan* (Planear): estabelecer a política de segurança da informação, os objetivos, processos e procedimentos do SGSI;

b) *Do* (Fazer): implementar e operacionalizar a política, os procedimentos, controlos e processos do SGSI;

c) *Check* (Verificar): monitorizar, analisar criticamente, realizar auditorias e medir o desempenho dos processos;

d) *Act* (Agir): manter e melhorar, por meio de ações corretivas e preventivas, o SGSI visando seu contínuo aperfeiçoamento.

A aplicação do ciclo de desenvolvimento de melhoria continua, conhecido como modelo PDCA, serve para se obter padronização e indicadores de controlo na elaboração de políticas de segurança (Sequesseque, 2017).

Como forma de aplicar políticas de segurança e garantir a conformidade com a gestão, existe um conjunto de normas internacionais que são utilizadas para a Gestão de Segurança da Informação e fornecem uma estrutura para a sua implantação (Lemos *et al,* 2016).

Assim sendo, a ISO/IEC 27001 tem o objetivo de garantir a eficácia do SGSI, sustentando o nível de segurança definido pelos membros participantes do mesmo e gerindo a segurança da informação conforme os riscos de negócio, de modo geral serve de critério de conformidade para as auditorias e é a única utilizada como documento para a obtenção de certificação em SGSI.

Enquanto que a ISO/IEC 27002 é um código de práticas para a gestão de segurança da informação, ou seja, é um guia de boas práticas em SI para a implantação dos controlos do Anexo A da norma ISO/IEC 27001.

2.5 Políticas de Segurança da Informação e Mecanismos de Proteção

As políticas são linhas orientadoras quanto à proteção de dados e de recursos e devem indicar situações e/ou entidades de quem o sistema tem de estar protegido, (Carneiro, 2009). Ou seja, para criar sistemas seguros necessitamos de utilizar mecanismos de proteção, Mamede, (2006) acrescenta que a segurança tem a ver com a proteção de bens, o que significa que estes têm de ser conhecidos, bem como o seu respetivo valor. Os tipos de ações a implementar por parte dos gestores de topo são influenciadas por este conhecimento.

Zúquete, (2006) afirma que as políticas de segurança definem o foco da segurança e o que deve ser garantido com a sua utilização, enquanto que os mecanismos de segurança correspondem às tecnologias/mecanismos utilizadas para colocar em prática essas mesmas políticas, em suma, são os instrumentos de operacionalização destes documentos, sendo de elevado valor a sua adequação à mudança das características do sistema.

Segundo a norma ISO/IEC 27000 (2014) as políticas de segurança da informação têm como principal objetivo proporcionar diretivas de gestão e suporte para a segurança da informação, Barman, (2002) reforça a ideia mencionando que estas políticas não são diretrizes ou standards, nem procedimentos ou controlos, descrevem assim a segurança em termos genéricos, não específicos.

Para Carneiro, (2009) os conceitos de confidencialidade, integridade e disponibilidade e a sua operacionalização " ... devem ser transformados em componentes da cultura organizacional" em contexto de política de segurança.

Assim sendo, deverá existir um documento que suporte toda a política de segurança da informação, esse documento deverá ser do "... conhecimento de todos os colaboradores da organização, constando nele o comprometimento da gestão, a definição do que se entende por segurança da informação, a descrição das políticas, a definição das responsabilidades pela segurança da informação e ainda as referências a documentação de suporte, procurando obter-se a colaboração do maior número possível de pessoas" (Gaivéo, 2008, p.127).

A política de segurança da informação deve assim providenciar o comprometimento da gestão e o adequado suporte às atividades essenciais à segurança da informação.

2.6 Alinhamento da Segurança da Informação com a Estratégia Organizacional

A segurança de uma organização deve ser analisada num contexto alargado, tomando-se em consideração todas as diferentes perspetivas como, por exemplo, dados, operações, aplicações e acesso físico, entre muitas outras. Este processo é algo que envolve todas as pessoas da organização e não apenas um grupo restrito. Desta forma é possível verificar-se a amplitude e a multidisciplinariedade da segurança organizacional, tentando-se concertar todas as vertentes que contribuem para a sua implementação (Mamede, 2006).

Os responsáveis de segurança das organizações não podem olhar apenas para questões associadas à segurança física, sem conhecer o negócio da organização e não podem tomar medidas preventivas sem procedimentos de controlo e auditoria. Para facilitar o processo de implementação de segurança também é necessário conhecer o alinhamento dos SI e das TI com a organização e com a sua estratégia, ou seja, implica conhecer a sua missão, os seus recursos e processos, os seus clientes e concorrentes, os problemas com que se depara, os pontos fortes e as oportunidades de negócio, envolvendo todos os membros da organização na sua construção (Gaivéo, 2008).

O alinhamento organizacional está diretamente relacionado com uma adequada estrutura organizacional, integrando atividades de negócio com o SI e com as TIC sendo que a informação tem um papel fundamental, enquanto recurso, de conduzir este alinhamento (Anunciação & Zorrinho, 2006).

As empresas devem considerar que as suas ações não são independentes, são relações "... cruzadas entre os diversos componentes do meio envolvente que condicionam as análises, as formulações e as implementações de estratégias" (Carneiro, 2009, p.9).

É necessário que os responsáveis da organização reflitam sobre essa sensibilização, sobre a importância da segurança da informação do topo para baixo, na estrutura organizacional.

A tomada de consciência é o primeiro passo para o sucesso do processo de segurança. Toda a organização tem que estar alinhada para conseguir atingir objetivos comuns.

3 Caracterização do Setor de Atividade – Transportes Rodoviários de Mercadorias e Armazenagem

Segundo ePortugal.gov.pt, (2020) o setor dos transportes rodoviários de mercadorias e armazenagem (H)[1] contempla o transporte rodoviário de mercadorias, local ou de longa distância, por meio de camiões ou veículos similares, contempla, também, a armazenagem, sendo ela constituída por um conjunto de funções de receção, carregamento, arrumação, e conservação de matérias primas, produtos acabados ou semiacabados.

O transporte rodoviário continua a ser o meio privilegiado de transporte de passageiros e mercadorias na Europa. Em termos económicos, o transporte rodoviário é o meio principal de transporte de mercadorias e representa a maior parte do volume de tráfego do transporte terrestre no território da União Europeia; nas últimas décadas tem registado um crescimento contínuo (Comissão Europeia, 2014).

Segundo o relatório de Estatísticas dos Transportes e Comunicações do Instituto Nacional de Estatística (INE) referente a 2018, o número de empresas no setor de Transportes e Armazenagem (secção H da Classificação Portuguesa das Atividades Económicas (CAE)) situou-se em 25,1 mil, mais 9,7% que no ano anterior.

Apesar do aumento de empresas o volume de negócios do setor registou um abrandamento do seu ritmo de crescimento (6,7% em 2018 comparativamente com 10,7% no ano anterior), ascendendo a um total de 21,8 mil milhões de euros.

Relativamente ás mercadorias transportadas, os resultados do Inquérito ao Transporte Rodoviário de Mercadorias (ITRM), para o ano de 2018, evidenciaram um ligeiro aumento de 0,1%, 6,1% em 2017 para 157,8 milhões de toneladas.

Estas variações registadas no transporte rodoviário de mercadorias, tanto em peso como em volume, deveram- se ao transporte internacional, com aumento de 1,0% em toneladas (24,9 milhões) e diminuição de 5,9% em toneladas-km (22,1 mil milhões).

O transporte nacional decresceu 0,1% (em peso e volume), representando 84,2% do total de toneladas transportadas menos 0,2 pontos percentuais.

O aumento no transporte internacional deveu-se ao crescimento no transporte por conta de outrem, mais 0,8% para 23,1 milhões de toneladas, dado que representou 92,6% do total de movimento.

[1] (H) Classificação de acordo com o quadro do setor disponibilizado pelo Banco de Portugal

A principal mercadoria carregada em Portugal foi - Outros produtos minerais - que representou mais de 10% do total (10,5%, 0,82 milhões de toneladas). Os - Produtos da agricultura - foram o grupo mais descarregado, com 12,6% do total (1,12 milhões de toneladas).

Por países, Espanha continuou a ser a principal origem e destino do transporte com, respetivamente, 72,0% e 66,0% da carga movimentada.

3.1 A Importância dos Sistemas de Informação para o Setor

A logística gere os recursos materiais, financeiros e humanos, desde a compra e entrada de materiais, passando pelo planeamento de produção, o armazenamento, o transporte, até à distribuição dos produtos, controlando as operações e gestão de informações (Alvarenga & Novaes, 2000).

Assim sendo, é necessário que exista um sistema de gestão que integre todas estas componentes da logística e as agregue num mesmo conceito. A gestão da cadeia de abastecimento desempenha este papel, segundo Croxton, Garcia, lambert & Rogers (2001), é a integração dos principais processos de negócio, do cliente final ao fornecedor de produtos, serviços ou informação, que adiciona valor para os clientes e outras partes interessadas, *Council of Supply Chain Management Profissionals* (CSCMP, 2010) reforça esta definição dizendo que a gestão da Cadeia de Abastecimento envolve a coordenação e a procura de colaboração entre parceiros de cadeia ou do canal de distribuição, sejam eles fornecedores, intermediários, prestadores de serviços logísticos ou clientes.

O setor em estudo faz parte da cadeia de abastecimento logística, desempenha a função de armazenagem e transporte integrando dois dos principais processos de negócio levando os produtos desde do fornecedor ate ao cliente final.

Uma gestão eficiente da cadeia de abastecimento possibilita retirar vantagem competitiva por parte das empresas que operam neste sistema e criar as condições necessárias para promover o valor percebido do cliente. Para atingir estes objetivos é necessário controlar o produto/bem durante todo o processo desde a origem até ao destino final. Portal Gestão, (2015) menciona que existem dois tipos de fluxos a ter em consideração fluxos físicos e os fluxos de informação, sendo que o primeiro representa a parte visível da cadeia de abastecimento, transformação, armazenagem e transporte de produto e o segundo permite coordenar toda a cadeia de abastecimento.

Como referido por Bowersox & Closs, (1996), foram sistematizados seis princípios que a informação deverá incorporar quando se concebem ou avaliam sistemas logísticos: disponibilidade, exatidão, oportunidade, gestão por exceção, flexibilidade e formato adequado. Por disponibilidade entende-se informação pronta e consistente, de rápido acesso e atual, para possibilitar respostas rápidas. A informação deve ser precisa, correta e fidedigna, o que contribui para a redução de incerteza. Também deverá ser oportuna, e procurar reduzir, tanto quanto possível, o intervalo de tempo entre o momento em que determinada atividade física acontece até que esta se tornar visível para o SI. Segundo Rodrigues, (2013) no que respeita à gestão por exceção, a informação deverá contribuir para alertar sobre situações problemáticas, encomendas de quantidades fora do habitual, produtos com pouco ou nenhum stock, expedições atrasadas, ou oportunidades de melhoria de serviço ou de redução de custos, a informação deve, ainda, ser flexível, capaz de satisfazer as necessidades dos utilizadores e os requisitos dos clientes. Por último, deverá apresentar-se com formato adequado, contendo informação para os fins a que se destina, na sequência, estrutura e suporte adequados, facilitando a consulta e a tomada de decisão dos gestores.

A grande força para incrementar os níveis de desempenho no ramo da logística é o uso das tecnologias de informação, uma vez que estas são capazes de fornecer as informações fiáveis no momento certo para tomar a decisão certa pelo motivo certo, e, portanto, promover resultados económicos, níveis de satisfação do cliente e de operacionalização dos recursos disponíveis (Bowersox & Closs, 1996).

A disponibilidade das TIC e dos SI vêm facilitar a integração da informação ao longo da cadeia de abastecimento. Neste contexto, é reconhecida a importância dos sistemas que permitem aumentar a produtividade e promover a redução de erros.

A implementação de SI, possibilita o acesso a informação relevante e fiável, promovendo a melhoria de grande parte dos processos logísticos e tornando-os mais ágeis.

4 Caracterização da Organização

A TMS – Transportes e Logística S.A é uma pequena média empresa inserida no setor dos Transportes rodoviários de mercadorias e armazenagem fundada em 1967.

Esta empresa tem como principal atividade o transporte rodoviário de mercadorias sendo que também presta serviços de armazenagem, parqueamento e lavagens de veículos pesados (TMS, 2019).

A sede da empresa está localizada no Montijo, o Logipark[2], sendo que esta conta ainda com uma unidade de armazenagem a norte de Portugal, mais concretamente na zona industrial da Maia.

Ao longo dos anos a empresa foi estabelecendo parcerias a nível europeu, integrando o grupo ASTRE (Associação de Transportes Europeus – Rede Europeia de Distribuição).

É constituída, atualmente, por 80 trabalhadores: 3 administradores, 1 diretor geral, 1 diretor financeiro, 1 diretor de operações, 13 administrativos, 4 operadores de armazém, 2 mecânicos e 55 motoristas.

4.1 Cultura, Missão, Visão e Valores

A TMS tem como principal missão a eficiência do serviço prestado ao cliente: "Contribuir para uma maior eficiência dos nossos clientes assegurando uma prestação de serviços de qualidade, planeada e executada segundo rigorosos padrões de segurança, de acordo com as especificações do cliente" (TMS, 2019)

Existe o propósito criar maior riqueza e responder com experiência e competência aos novos desafios que o mercado coloca, esta é a visão que a empresa assume como sua e o motivo pelo qual estabelece os seus objetivos (TMS, 2019)

No que diz respeito à sua atividade diária, a empresa rege-se pelos seguintes valores: "Desenvolver políticas internas que contribuam para o aumento da segurança rodoviária e para minimizar o impacto negativo da atividade e no meio ambiente" (TMS, 2019).

Relativamente à cultura organizacional esta empresa é uma organização que adota uma cultura familiar. Em todos os departamentos existe um membro da família Martins

[2] Complexo logístico da TMS composto pela oficina, o edifício principal dos escritórios, o armazém, local de lavagem de viaturas, bomba de combustível, parque e portaria.

que coordena e chefia as atividades diárias e são eles que compõem a administração da empresa.

4.2 Organograma

Na figura 3 está representada a estrutura organizacional da TMS. No topo, nível hierárquico superior, temos a administração, seguindo da direção geral. Entidades às quais os restantes departamentos deveram responder relativamente às suas atividades diárias.

No que diz respeito às suas áreas funcionais a TMS encontra-se departamentalizada da seguinte forma: Direção Financeira, Direção Comercial e Direção Operacional**.** Sendo que cada uma delas agrega um conjunto de responsabilidades e competências necessárias à sobrevivência da atividade da empresa.

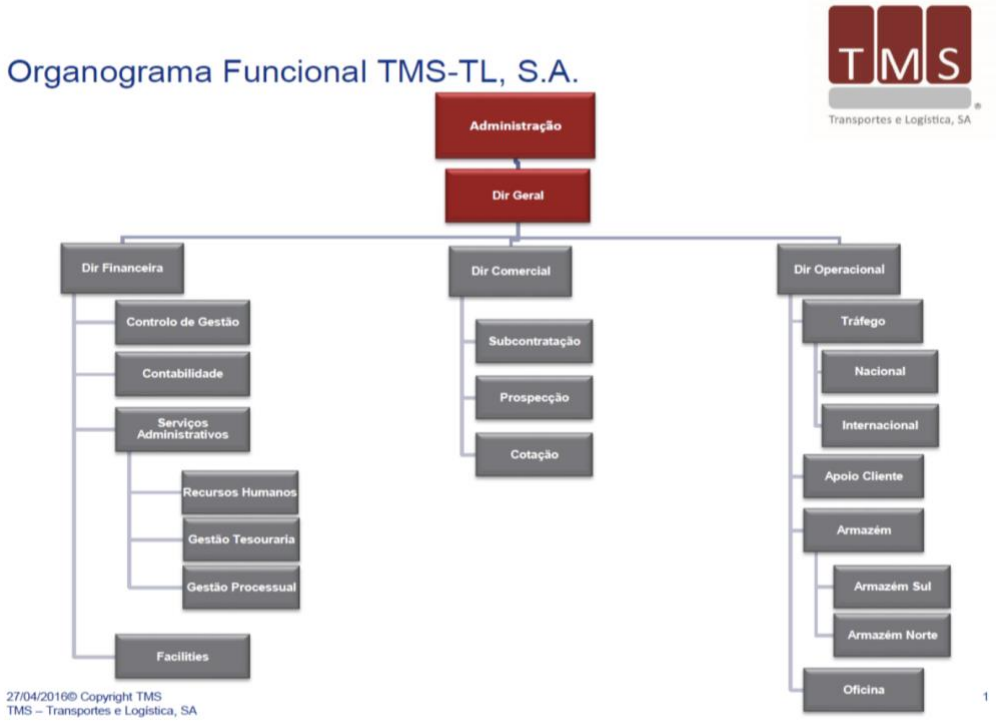


Figura 3- Organograma da TMS – Transportes e Logística, S.A

(Adaptado dos estatutos da TMS – Transportes e Logística S.A)

4.3 Maturidade Digital

A atividade dos transportes rodoviários de mercadorias e armazenagem gera imensa informação em formato papel, informação legal resultante dos vários movimentos de carga e descarga de mercadorias e armazenagem.

A TMS encontra-se numa fase inicial de maturidade digital, segundo a IDC[3] (*International Data Corporation*), alguns dos seus processos estão informatizados, porém existe ainda documentação em formato físico. A gestão da informação, gerada nos vários departamentos é efetuada através de um ERP (*Enterprise Resource Planning*) e a sua relação com os clientes é feita através de e-mail e contactos telefónicos.

Relativamente à infraestrutura, a sua ligação à internet é feita através de cabo e as máquinas estão ligadas em rede.

A empresa não adota nenhuma metodologia para a gestão das suas tarefas diárias, apenas se auxilia com o conjunto de aplicações do *Microsoft Office*[4] para a realização das suas tarefas.

[3] Consultoria internacional especializada em maturidade digital.

[4] Conjunto de aplicativos que contem programas como processador de texto, folha de calculo, bases de dados, apresentação gráfica e gestor de emails.

5 Estudo de Caso

Para que um conhecimento possa ser considerado científico, torna-se necessário identificar as operações mentais e técnicas que possibilitam a sua verificação. Ou, em outras palavras determinar o método que possibilitou chegar a esse conhecimento (Gil, 1989).

Para começar a formular a problemática, e tendo em conta os objetivos do presente trabalho, solicitou-se à empresa que autoriza-se a observação das atividades operacionais durante o período laboral. Segundo Pocinho, (2012, p.27) "Os estudos observacionais caracterizam-se pela inexistência de manipulações de intervenções diretas sobre a amostra limitando-se à observação dos indivíduos do estudo e das suas características"

O objetivo desta observação consistiu em analisar os comportamentos dos colaboradores da empresa durante o desempenho das suas atividades diárias relativamente ao tratamento da informação com a qual trabalham e consequentemente ao comprometimento da sua segurança. É nesta fase da observação que se recolhe ou reúne concretamente as informações encontradas junto das pessoas ou unidades de observação incluídas na amostra.

Foram analisados todos os departamentos e todos os colaboradores que integram o sistema de informação da empresa. Um estudo descritivo é aquele que ambiciona apenas estimar parâmetros de uma população, não necessita de elaboração de hipóteses de estudo pois trata-se apenas de uma "fotografia" da situação (Pocinho, 2012).

Esta etapa durou cerca de dois meses e possibilitou a descoberta de algumas falhas ao nível da gestão da segurança da informação, comportamentos heterogéneos dos colaboradores sobre métodos de trabalho, negligência em algumas ações do dia-a-dia que afetavam direta e indiretamente a segurança da informação da empresa.

Desta forma, foi necessário explorar, analisar e comprovar estas falhas recorrendo a técnicas de recolha de dados adequadas.

A maioria das pesquisas em SI não se baseiam na objetividade das ciências exatas mas em abordagens subjetivas que procuram compreender como os fatos tecnológicos são concebidos na consciência das pessoas e dos grupos sociais.

5.1 Técnicas de Recolha de Dados

O presente estudo é caracterizado pela utilização de duas técnicas de recolha de dados, o inquérito por questionário e a entrevista.

O inquérito por questionário realizado teve como objetivo estudar os processos e procedimentos de cada departamento funcional da TMS relativamente à segurança da informação. Enquanto que a entrevista pretende analisar a postura da empresa relativamente à mesma.

A conceção e a implementação de um questionário é um processo cujo objetivo é a recolha de informação temática válida e fiável, obtida a partir das respostas individuais dadas a um conjunto de questões por um grupo representativo de inquiridos, em torno das quais se produzem conclusões passíveis de serem generalizadas ao universo da população em estudo (Thayer-Hart, Dykema, Elver, Schaeffer & Strevenson, 2010).

Segundo, Quivy & Campenhoudt, (2017) os métodos de entrevista distinguem-se pela aplicação dos processos fundamentais de comunicação e de interação humana. Este tipo de processos permite ao investigador retirar da entrevista uma reflexão muito mais completa do fenómeno em análise.

5.2 Questionário

Relativamente ao inquérito por questionário, a população-alvo de estudo são os trabalhadores da TMS quem têm acesso ao SI da empresa.

Apenas serão considerados os trabalhadores que de forma direta modificam, alteram ou carregam informação no SI. Não considerando os trabalhadores que apenas têm acesso físico, ou seja, têm os meios necessários para mas não efetuam nenhuma interação com o SI.

Assim sendo, pode-se considerar um universo de 13 trabalhadores. Repartidos da seguinte forma: 1 diretor financeiro, 1 diretor operacional, 2 comerciais, 3 gestores de tráfego e 6 administrativos.

5.2.1 Elaboração do Questionário

Realizou-se, apenas, um questionário (ANEXO I) para toda a população-alvo não se sentiu a necessidade de criar diferentes questionários visto que a amostra é homogénea.

O questionário foi entregue presencialmente e recolhido da mesma forma.

Para a elaboração do mesmo foram colocadas questões de escolha única, escolha múltipla e de classificação (valores entre 1 e 6).

Colocou-se uma nota prévia sobre a definição teórica de segurança de informação para que o inquirido tivesse plena consciência sobre a temática abordada.

O questionário encontra-se estruturado em 6 grupos distintos:

Grupo I – (Caracterização do público alvo) define o departamento que o indivíduo exerce funções e há quanto tempo as exerce. Este grupo apresenta 2 questões.

Grupo II – (Questões gerais sobre processos e procedimentos internos) procura perceber se cada inquirido tem o seu próprio computador ou se existe partilha do mesmo. Se possuí acesso ao sistema de informação da empresa ou se o acesso é partilhado e releva se o indivíduo tem correio eletrónico da empresa. Neste grupo, também é possível verificar como é deixada a sessão do computador quando se ausenta do seu local de trabalho. Este grupo apresenta 8 questões.

Grupo III – (Procedimentos relativamente à utilização de passwords) destina-se essencialmente a verificar se existe password de acesso aos computadores e ao sistema de informação da empresa e se essa mesma password é partilhada ou individual. Também procura verificar quais os métodos utilizados pelos trabalhadores para memorizar as suas passwords. E por fim, o grupo III aborda algumas questões sobre as passwords bancárias, se são individuais ou partilhadas e os motivos dessa partilha, fazendo referência aos processos que os inquiridos utilizam para guardar as passwords confidenciais. Este grupo apresenta 11 questões.

Grupo IV – (Segurança da informação confidencial da empresa) neste grupo é possível perceber que tipo de informação confidencial os inquiridos utilizam para a realização das suas tarefas do dia-a-dia e em que formato está guardada. Procurou-se classificar a facilidade de acesso à informação em formato papel e entender como se acede à informação guardada em formato digital. Este grupo apresenta 6 questões.

Grupo V – (Impressão de documentos através do sistema informático) destina-se essencialmente a verificar se a impressão da documentação é efetuada em modo privado, quais as atitudes do inquirido quando não encontra a documentação impressa e como é que procede quando encontra documentação que não é sua. Este grupo apresenta 6 questões.

Grupo VI – (Questões gerais sobre a segurança do sistema informático) procura a perceção dos indivíduos, segundo a sua perspetiva, relativamente á violação da segurança do sistema informático, o grau de segurança do mesmo e a importância deste último para o desempenho das funções diárias do inquirido. Este grupo apresenta 3 questões.

5.3 Entrevista

Foi realizada uma entrevista estruturada ao diretor geral da TMS dia 22 de Outubro de 2019. A qual durou cerca de 30 minutos e teve lugar nos escritórios da empresa. O principal objetivo foi a identificação da visão da empresa relativamente à segurança dos seus dados. Se adota normas, regras, regulamentos e/ou procedimentos para garantir a segurança da informação e como efetua o seu controlo.

5.3.1 Elaboração da Entrevista

A entrevista (ANEXO II) apresenta 9 grupos distintos. O grupo I pretende sintetizar a postura da empresa relativamente à segurança da informação, grupo II procura verificar a facilidade de acesso físico ao sistema de informação, grupo III aborda algumas questões sobre a rede da empresa e o método de acesso à internet, grupo IV esclarece como é efetuado o acesso, proteção, manutenção e assistência ao servidor da empresa, grupo V demonstra como é elaborado todo o processo de gestão das cópias de segurança, grupo VI procura demonstrar como é efetuada a gestão de acessos ao sistema de informação da empresa, grupo VII pretende verificar como é efetuado e controlado o acesso físico ao edifício principal da empresa, grupo VIII como no grupo anterior, pretende-se verificar como é efetuado e controlado o acesso físico contudo de um modo mais abrangente, o complexo logístico da TMS, e por fim o grupo IX procura demonstrar como é efetuada a segurança do perímetro do logipark, quem a efetua e como efetua, quais as restrições e/ou exceções existentes ou não à entrada de pessoas no complexo logístico.

6 Análise de Resultados

O objetivo da investigação é responder à pergunta de partida, neste caso, como é realizada a gestão da segurança da informação numa empresa do setor dos transportes rodoviários de mercadorias e armazenagem. Para esse efeito, formula-se hipóteses e procede-se às observações que elas exigem. Trata-se de verificar se os resultados observados correspondem aos resultados esperados.

Neste capítulo, o objetivo é fazer uma análise dos dados obtidos através da aplicação das técnicas de recolha de dados descritas anteriormente. No entanto, apenas se apresenta de forma exaustiva os dados com relevância suficiente para o estudo desenvolvido, todos os outros, foram devidamente analisados, contudo, como não serão tidos em consideração.

Poderá ser consultado no Anexo III os dados resultantes do questionário que sofreram uma sumarização e um tratamento estatístico adequado. É importante referir que a amostra estudada é pequena, apenas 13 pessoas, e alguns resultados esperados do questionário não se concretizaram na realidade.

6.1 Análise do Questionário

As questões pertencentes ao grupo I do questionário caracterizam os inquiridos, a maioria das respostas obtidas são relacionadas com colaboradores pertencentes ao departamento operacional da empresa (46%), figura 4. De um modo geral, os inquiridos desempenham funções na TMS entre 5, 10 ou mais anos, 23% e 31% respetivamente, como se pode comprovar na figura 5.

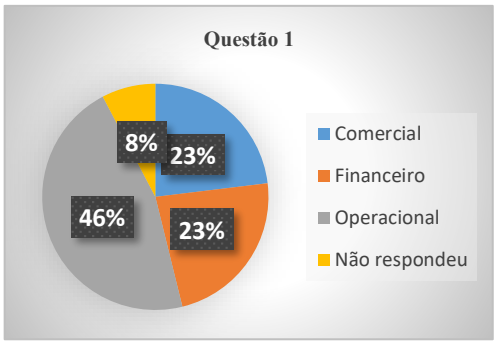


Figura 4 – Grupo I - Em que departamento se insere a sua função?

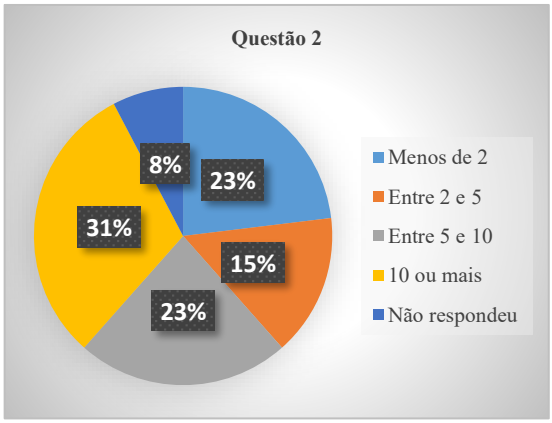


Figura 5 – Grupo I – Há quantos anos desempenha funções na TMS?

Todos os 13 inquiridos têm atribuído um computador para utilização individual, segundo as respostas apuradas à questão 3 do grupo II do questionário. Apesar da maioria não partilhar o seu computador com os restantes colegas existe 38% (5 colaboradores) que partilham, figura 6. Contudo, desses 38%, 80% (4 colaboradores) partilha com mais um colega, figura 7.

O motivo pelo qual existe esta partilha deve-se ao facto de existir substituições durante os períodos de ausência dos colaboradores, consultar a tabela 1.

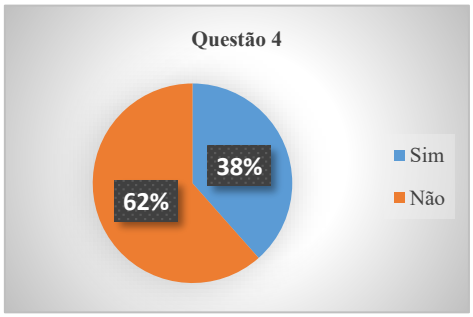


Figura 6 – Grupo II – Partilha o seu computador de trabalho com algum/alguns colega/s?

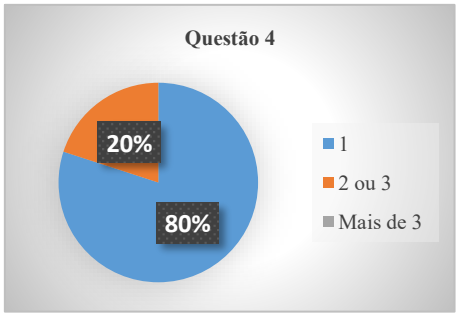


Figura 7 - Grupo II – Se partilha, com quantas pessoas?

Respostas
Quando estou de férias ou de baixa
Férias
Férias/Ausências
No caso de férias
Quando estou de férias

Tabela 1 - Grupo II - Em que circunstância partilha o seu computador de trabalho?

Os resultados obtidos à questão 5 do questionário demonstram que a amostra estudada cumpre os requisitos definidos à priori, todos os colaboradores inquiridos têm acesso ao sistema informático da empresa, tabela 2.

	Respostas
Sim	13
Não	0

Tabela 2 – Grupo II – Possui acesso ao sistema informático da empresa?

- **Gestão de Passwords**

Relativamente à atribuição de *passwords* de acesso ao sistema de informação organizacional, pela análise da questão 13 verificamos que a atribuição de *passwords* não segue um padrão, 54% das *passwords* são escolhidas pelo colaborador e os restantes 46% são atribuídas pela empresa, figura 8.

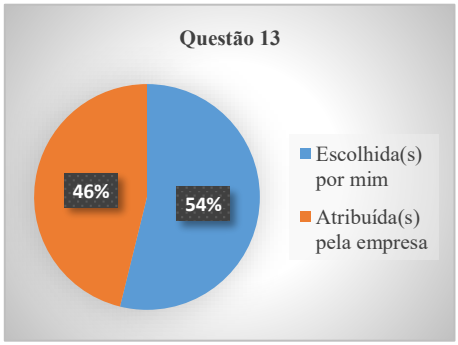


Figura 8 - Grupo III - As passwords são atribuídas pela empresa ou escolhidas por si?

A questão 14 revela que que as *passwords* utilizadas na empresa não são individuais e intransmissíveis, 77% dos inquiridos partilha a *password* com colegas do trabalho, figura 9. Dos 13 inquiridos, 10 partilham a sua *password* e dos que partilham 70% fá-lo com 2 ou 3 colegas de trabalho, figura 10.

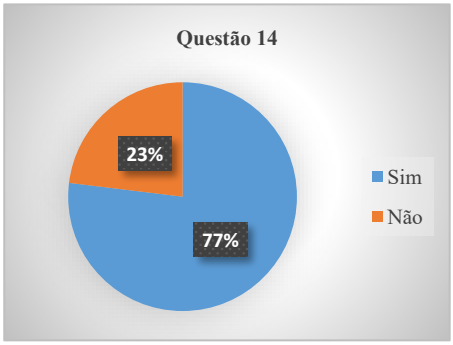


Figura 9 – Grupo III - Partilha a password com colegas de trabalho?

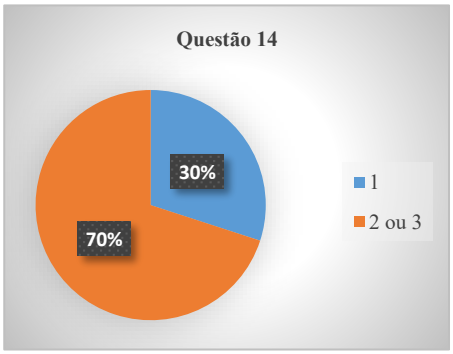


Figura 10 – Grupo III – Com quantas pessoas partilha a password?

Os motivos pelos quais as *passwords* são partilhadas estão mencionados na tabela 3, apesar de termos 3 respostas nulas, 4 colaboradores em 10 partilham devido à falta de licenças por utilizador individual e 3 colaboradores em 10 partilham devido aos períodos de ausência, nomeadamente férias dos colegas.

Respostas	
Quando estou de férias	1
Quando estou de férias ou doente	1
É password de departamento	1
licenças	1
Férias	1
O mesmo departamento	1
O utilizador é partilhado	1
Não respondeu	3

Tabela 3 - Grupo III - Motivo da partilha de passwords

O principal objetivo de existir *password* passa por individualizar um acesso à informação contida num determinado local, desta forma, apenas a pessoa titular da informação poderá aceder. O princípio base do uso de *passwords* não é aplicado pela empresa.

A empresa não consegue controlar quem modifica, atualiza ou apaga informação contida no sistema de informação. A segurança da informação fica comprometida.

- **Passwords bancárias**

O questionário realizado aos colaboradores da TMS coloca algumas questões relativamente ao uso de *passwords* nas contas bancárias da empresa. Desta forma, foi possível perceber que apenas 3 pessoas, 23% da amostra, tem acesso às contas bancárias da empresa através de *password*, figura 11. Contudo, as que têm acesso todas elas partilham a *password* entre si, figura 12.

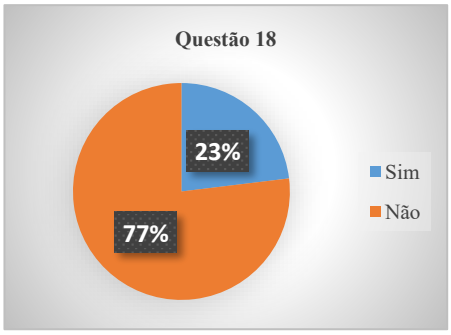


Figura 11 - Grupo III - Tem acesso às contas bancárias da empresa?

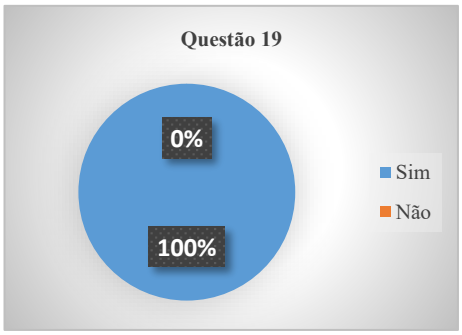


Figura 12 - Grupo III - A password de acesso ás contas bancárias é partilhada?

Quando se pergunta aos inquiridos qual o motivo da partilha das *passwords*, respondem que a empresa definiu este procedimento devido ao utilizador de acesso às contas bancárias ser os mesmos para todos os colaboradores, tabela 4. No entanto, conseguiu-se apurar que este acesso apenas é restrito e não total, tabela 5.

	Respostas
Qual o motivo da partilha?	O utilizador do site do banco é partilhado (No departamento)
	Método incutido pela empresa
	Não respondeu

Tabela 4 – Grupo III - Qual o motivo da partilha de passwords bancárias?

	Resposta
Acesso total ás contas	
Acesso restrito	3
Apenas consulta	

Tabela 5 - Grupo III - Qual o tipo de acesso concedido através das passwords bancárias?

Relativamente às *passwords* de acesso a informação confidencial, como é o caso das *passwords* de acesso às contas bancárias, verificamos que a empresa não adota nenhum método para proteger este tipo de informação, tão sensível e vital para a empresa.

A empresa não consegue controlar os acessos à informação contida nas contas bancárias nem rastrear o que cada colaborador fez nas mesmas.

- **Gestão da impressão de documentação**

Verificamos que toda a amostra estudada, 13 colaboradores, têm acesso à impressão de documentação através do sistema informático da empresa, figura 13.

Contudo, concluímos que desses 13 colaboradores 9 (69%) não efetuam a impressão de documentação em modo privado e a restante parcela divide-se, entre partilha em privado e ausência de padrão para o seu comportamento relativamente a este procedimento interno, figura 14.

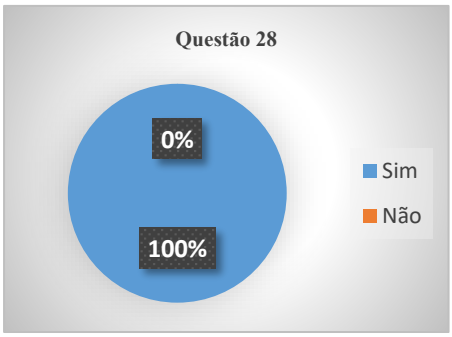


Figura 13 - Grupo V - Possui acesso à impressão de documentação?

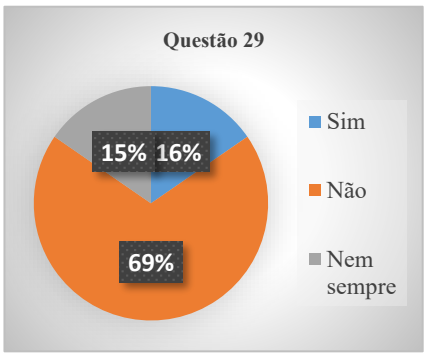
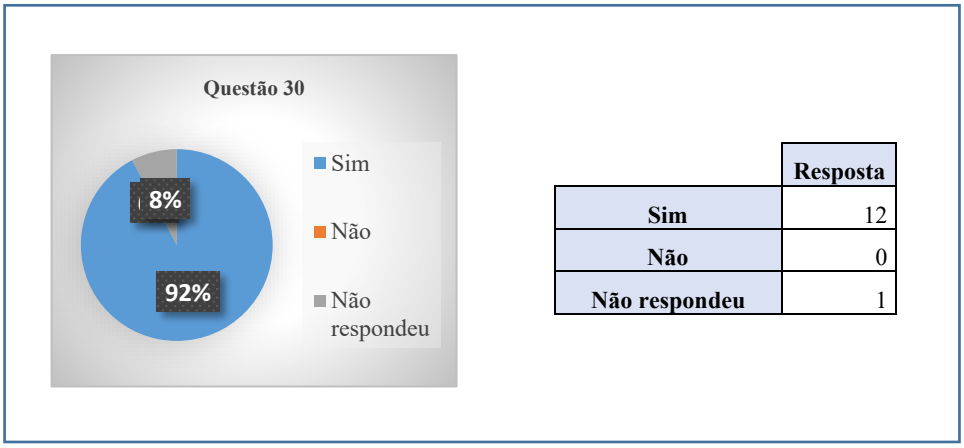


Figura 14 - Grupo V - A impressão é efetuada em modo privado?

Os inquiridos foram questionados relativamente ao método utilizado para a recolha da documentação na impressora, foi possível apurar que quase toda a amostra estudada (12 colaboradores) saí do seu local de trabalho e dirige-se à impressora para ir buscar os seus documentos, figura 15.



	Resposta
Sim	12
Não	0
Não respondeu	1

Figura 15 - Grupo V - Depois de imprimir saí do local de trabalho e vai buscar a impressão?

Desta forma, tendo uma percentagem tão significativa de colaboradores que não imprime em privado (figura 14) faz com que a informação contida nas impressões fica à mercê de qualquer colaborador ou não colaborador que passe no local, desde do momento que se dá o OK para imprimir até ao momento que efetivamente o colaborador chega ao local, podendo, assim, esta informação ser consultada e/ou destruída por pessoal não autorizado.

Foi necessário perceber que ações tomam os colaboradores quando não encontram a sua documentação no tabuleiro da impressora, tabela 6.

	Resposta
Pergunta aos colegas se alguém encontrou o documento em questão	11
Tenta encontrar o documento	8
Imprime novamente	6
Verificar se ainda aguarda impressão	6
Nunca aconteceu	
Outra	

Tabela 6 - Que atitude toma quando não encontra os documentos que mandou imprimir na impressora?

Importa referir que esta pergunta 31 do questionário é de escolha múltipla, o mesmo inquirido poderá responder todas as opções, se aplicável, no entanto a tabela 6 espelha as ações tomadas pelos colaboradores da empresa.

Grande parte da amostra em estudo pergunta aos colegas se alguém encontrou o documento (11 respostas) ou tentam encontrar a impressão (8 respostas). Como nenhum inquirido selecionou a opção ”Nunca aconteceu”, podemos concluir que é recorrente que aconteça o desaparecimento de documentos da impressora da empresa.

Foi importante perceber se os colaboradores encontram documentação que não seja a sua no tabuleiro da impressora partilhada da empresa, concluímos que 92% (12 colaboradores) dos inquiridos respondeu que já encontrou documentos que não lhe pertenciam, figura 16.

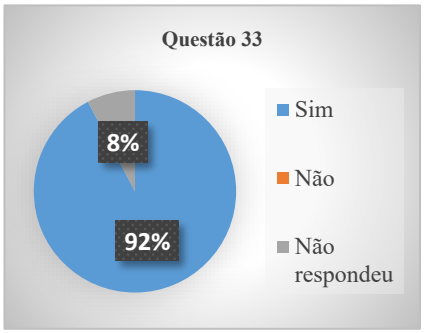


Figura 16 - Grupo V - Já encontrou documentos que não os seus na impressora partilhada da empresa?

Perante a situação descrita acima, questionou-se qual a atitude que o inquirido toma para tentar solucionar a situação. A questão imposta é de escolha múltipla, podendo cada inquiridos responder a várias opções. Dos 92% que responderam que encontraram documentação alheia, 63% deixa os documentos junto à impressora, apenas uma pequena parcela (37% dos inquiridos), tenta encontrar o proprietário da documentação perdida, até lá a informação fica num local de fácil acesso.

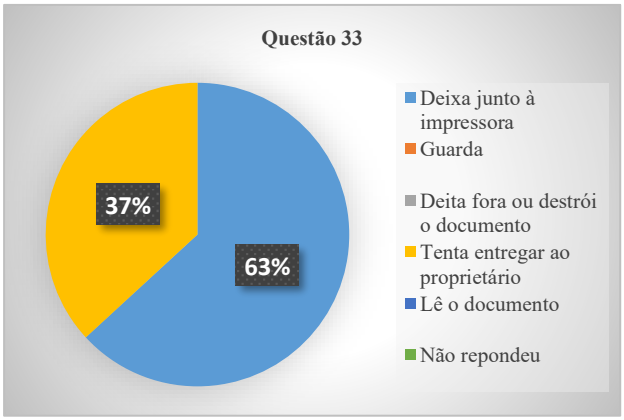


Figura 17 - Quando encontra documentação que não a sua na impressora partilha, que atitude toma?

Não existem processos e/ou procedimentos implementados pela empresa para controlar e mitigar este tipo de problemas que tão frequentemente ocorrem, cada colaborador delibera a ação que tomar perante determinada situação.

6.2 Análise da Entrevista

- **Políticas, normas, regulamentos, regras e/ ou procedimentos relativamente à segurança da Informação**

A entrevista ao diretor geral da TMS possibilitou retirar algumas conclusões sobre como é efetuada a gestão da segurança da informação na empresa.

As primeiras perguntas centraram-se na perceção da postura da gestão de topo sobre o tema em estudo, nesse sentido, questionou-se o diretor geral se considerava a informação um dos ativos da empresa, o mesmo respondeu que sim, definindo-a como muito importante para o negócio, considerando, também, necessário a implementação de medidas para a proteger, passado a cita-lo "... a informação é importante! Alguma é confidencial e outra crítica à atividade da empresa. Pelo que deverá ser protegida*",* contudo, quando lhe perguntamos se a empresa dispõe de algum tipo de política para garantir a segurança da informação, o mesmo responde de forma confusa dizendo que "... existem de forma não estruturada".

Podemos concluir que não existe políticas, normas, regulamentos, regras e/ou procedimentos relativamente à segurança da informação.

Desta forma, a empresa não tem como assegurar a segurança da sua informação nem consegue controlar as ações dos seus colaboradores relativamente à proteção dos seus dados.

- **Acesso ao sistema de informação da empresa – Atividades proibidas**

Relativamente aos locais onde existe acesso ao sistema de informação da empresa questionamos o diretor geral sobre as atividades que são proibidas, o mesmo responde indicando que as únicas atividades que estão proibidas são fumar e instalar/desinstalar software. Quando se pergunta de que forma essas atividades estão proibidas, o diretor geral responde: "senso comum". Ou seja, nem as atividades descritas como proibidas estão efetivamente proibidas, não existe nenhuma política que o indique e que o faça ser cumprido.

A empresa incorre sérios riscos não tendo esta salvaguarda para a proteção da sua informação, desta forma, os colaboradores poderão tomar determinadas ações que ponham em risco a confidencialidade, integridade e disponibilidade da informação contida no sistema da empresa.

- **Gestão das cópias de segurança**

Foram realizadas um conjunto de questões sobre gestão das cópias de segurança da empresa, pela sua importância para a continuidade do negócio.

Sabemos que a empresa realiza as cópias de segurança seguindo o seguinte método: *Backups*[5] incrementais diariamente e completos semanalmente. Para o efeito, conta com um responsável externo para a gestão das cópias de segurança.

Existe um contrato celebrado com a empresa externa que assegura o armazenamento e periodicidade das cópias de segurança incluindo toda a manutenção do equipamento afeto à realização das mesmas. Optaram por armazenar todos os *backups* num servidor NAS[6] colocado num local remoto, seguindo o método indicado anteriormente, backups incrementais diariamente e completos semanalmente.

De acordo com os procedimentos adotados pela empresa em conjunto com o seu fornecedor externo, percebemos pela análise à resposta da pergunta 42 da entrevista que alguns pontos do contrato não estão a ser cumpridos.

O diretor geral indicou que a gestão ineficiente das cópias de segurança deu origem a um incidente muito grave de perda total de informação de gestão, referente a um ano comercial da empresa. Numa escala de 1 a 6, onde 6 é elevado e 1 baixo, o diretor classificou como 6 a gravidade da situação.

Diariamente, numa empresa, é gerado um fluxo de informação muito elevado sendo imperativo a realização eficaz de cópias de segurança para garantir que este ativo esteja a ser salvaguardado, dada a sua importância para a continuidade do negócio. Para tal, a gestão das cópias de segurança também deverá ser controlada pelas partes interessadas.

- **Controlo de acessos físicos ao sistema de informação**

O Grupo VII da entrevista permite perceber como é efetuado o controlo de acesso físico ao edifício principal da TMS, o escritório[7].

[5] Termo inglês que significa cópias de segurança. Frequentemente utilizado em informática para indicar a existência de cópias de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.
[6] Servidor de armazenamento conectado em rede
[7] Edifício onde ocorre toda a atividade administrativa, financeira e operacional da empresa. Contém as salas da administração e das restantes chefias, bem como o

Conclui-se que existe controlo e registo de entradas e saídas através de um sistema de cartão magnético com um ID individual por colaborador.

Nesta parte da entrevista questionou-se, também, se a empresa labora em horário noturno ao qual o diretor geral respondeu que sim. Assim sendo, perguntou-se se os trabalhadores têm acesso ao escritório durante o horário noturno, e o diretor geral disse que apenas o responsável de armazém. Quando se pergunta qual a finalidade deste acesso o mesmo informa que é apenas para fotocopiar documentação resultante da atividade noturna no armazém.

No horário noturno não é possível controlar o acesso à informação. Portanto, a empresa incorre sérios riscos ao consentir que este procedimento continue a ser praticado, ou seja, o colaborador tem livre acesso a todas as salas, secretárias, computadores, equipamento e documentação, sendo que não está ninguém na empresa durante este período para conseguir controlar quais as atividades que o funcionário efetivamente realiza.

Desta forma, é urgente encontrar um processo alternativo para conseguir assegurara a confidencialidade, integridade e disponibilidade da informação da empresa.

Outra questão que se colocou ao diretor geral foi o facto da existência de empresas de outsourcing ou fornecedores externos que frequentem o perímetro do edifício principal, o Logipark.

As respostas às questões 79, 80 e 81 da entrevista indicam que existe esta frequência de entidades externas à empresa, nomeadamente, empresa de limpeza, controlo de pragas, manutenção e gestão das TIC e que de um modo geral é uma frequência diária.

Quando perguntamos se estas empresas têm um acesso privilegiado, o diretor geral diz que apenas algumas das quais a empresa de " ... limpeza que tem acesso total a todo o edifício além de ter chave da empresa para limpar aos fins-de-semana" e a empresa de "... manutenção que tem acesso parcial, apenas a algum equipamento informático e sempre ou quase sempre em dias de semana".

Controlar os acessos físicos ao sistema de informação dentro da organização é importante mas controlar o acesso físico ao sistema da informação a terceiros, a fornecedores e entidades externas à empresa é mandatário.

---

armazém, ponte de ligação entre a atividade de armazenagem e a atividade de distribuição desempenhada pela empresa.

As intenções, as ações, as consultas de informação realizadas por terceiros, sem controle, pode dar origem a graves problemas para a empresa, desde perda de informação como ainda fuga de informação para empresas concorrentes.

7 Soluções e Perspetivas de Trabalho Futuro

A TMS – Transportes e Logística, S.A foi alvo de estudo do presente trabalho com o intuito de analisar como é efetuada a gestão da segurança da informação dentro da organização.

A aplicação das técnicas de recolha de dados possibilitou a identificação de alguns problemas e questões relativamente à proteção da informação da empresa. Desta forma, propõe-se algumas soluções e perspetivas de trabalho futuro com o intuito de solucionar ou mitigar os problemas encontrados para que a empresa consiga assegurar a confidencialidade, integridade e disponibilidade da sua informação e desta forma protege-la de eventuais incidentes ou ameaças existentes.

7.1 Gestão de Passwords

Um dos problemas encontrados foi a gestão de *passwords*, na empresa todos os colaborares têm uma *password* atribuída para iniciar sessão no sistema de informação, contudo, as *passwords* não são individuais nem intransmissíveis. Opta-se pela atribuição de *passwords*, por parte da empresa, nos casos em que o utilizador da sessão é partilhado com outros colaboradores e quando não o é, o próprio pode escolher a sua *password.* Questões como controlar quem modificar, atualiza, apaga ou insere informação, ou apenas garantir que o colaborador que acede à informação tem permissão para tal ficam postas em causa devido à prática adotada pela empresa.

Relativamente às *passwords* de acesso a informação confidencial, *passwords* de acesso às contas bancárias, a empresa adota procedimentos descuidados, visto que permite que os colaboradores não tenham uma *password* individual para consultar e efetuar as operações permitidas, os utilizadores partilham a *password* entre si. Assim sendo, a empresa não tem como controlar quem consulta, quando consulta e para que finalidade o faz.

A criação e gestão das *passwords* deverá estar claramente definida, especificado qual o circuito a seguir e as autorizações necessárias para a criação de um perfil de utilizador com a respetiva senha. Segundo Mamede (2006), deverá estar indicado um conjunto de recomendações aos utilizadores sobre como efetuar a escolha de senhas, quais os prazos de validade, quais as formas de escolha e quais os mecanismos de auditoria das mesmas que irão implementar na organização.

O recurso a este método de autenticação permite determinar um conjunto de informação sobre o utilizador, nomeadamente segundo Stallings, (2000), determinar se o utilizador tem autorização para aceder ao sistema, determinar os privilégios daquele utilizador no sistema e permitir a utilização de controlo de acesso discricionário.

No seguimento do exposto e atendendo que os métodos adotados pela empresa não garantem a confidencialidade, integridade e disponibilidade da informação, existe a necessidade de criar um método que alinhe os seus processos e procedimentos relativamente à gestão das *passwords* com as diretrizes da segurança da informação de modo a salvaguarda-la, minimizando, assim, eventuais incidentes.

A ISO/IEC 27002 (2013) recomenda que um sistema de gestão das *passwords* seja interativo e que garanta a qualidade das *passwords*. Sabendo que a empresa não tem políticas, normas, regulamentos, regras ou procedimentos relativamente à gestão de *passwords* elaborou-se uma política de *passwords* para ajudar a empresa a fazer a gestão deste tema, consultar ANEXO IV.

O documento foi elaborado tendo as recomendações do controlo A.9.4.3 disponível no ANEXO A da ISO/IEC 27001 (2013), e, posteriormente, à consulta da sua aplicabilidade na ISO/IEC 27002 (2013), sendo utilizado apenas como forma de orientação para a solução final e não a sua aplicabilidade na íntegra.

7.1.1 Sugestão de Trabalho Futuro - Gestão de Passwords

Para que a política de *passwords* elabora seja aplicável é necessário eliminar os motivos pelos quais os colaboradores utilizam a mesma *password*.

Assim sendo, sugere-se que exista um utilizador individual para cada colaborador da empresa, e não um utilizador por área funcional. Será necessário investir em licenças individuais para o uso do ERP – Microsoft Dynamics NAV.

Sugere-se, ainda, que seja efetuada uma gestão das substituições, em caso de ausências. Ou seja, analisar dentro da empresa quem tem capacidade para substituir, mapear os acessos dentro do ERP necessários para que aconteça essa substituição e quando efetivamente for necessário basta atribuir o conjunto de acessos definido ao colaborador que irá substituir. Desta forma, não é necessário utilizar uma *password* de outro colega para realizar as funções atribuídas.

7.2 Gestão de Impressão de Documentação

Os procedimentos adotados pela empresa para a impressão de documentações não são homogéneos. Cada colaborador delibera a ação a tomar mediante determinado cenário. Nem todos imprimem da mesma forma, a opção da impressão em privado é opcional e apenas uma pequena minoria opta por este método.

Atendendo ao mencionado acima é normal que no tabuleiro da impressora exista, recorrentemente, documentação esquecida e sem "dono" evidente, pois quando se executa a ação de imprimir e se por algum motivo se esquece de ir buscar a impressão a informação contida no documento irá ficar exposta, irá ficar acessível para que qualquer outro colaborador ou não colaborador tenha acesso.

A inexistência de políticas, normas, regulamentos, regras ou procedimentos relativamente à gestão de impressão de documentação fomenta que exista comportamentos dispares, por exemplo, quando os colaboradores encontram documentação que não a sua no tabuleiro da impressora uns tentam encontrar o proprietário mas a restante parcela deixa a documentação no mesmo local.

Todos os pontos mencionados não contribuem para uma gestão eficiente da segurança da informação da empresa, uma das diretrizes da segurança da informação é completamente posta em causa, a confidencialidade.

Os documentos impressos contêm informação de todo o tipo, pode parecer inofensivo mas abordam-se questões como quem é que eventualmente pode aceder, com que intuito e para que finalidade.

Em qualquer programa de segurança da informação organizacional, as pessoas serão sempre entendidas como o elo mais fraco a não ser que as políticas, a formação, as competências e as tecnologias sejam devidamente utilizadas para evitar que as pessoas, acidental ou intencionalmente, danifiquem ou percam informação (Whitman & Mattord, 2005)

Assim sendo, e como forma de solucionar esta problemática, redigiu-se uma política de impressão para que a empresa adote nas suas funções do dia-a-dia, consultar o ANEXO V.

7.2.1 Sugestão de Trabalho Futuro - Gestão de Impressão de Documentação

Recomendamos que no futuro, em conjunto com a política de impressão desenvolvida, seja implementado um sistema de identificação *Near Field Communication* – NFC[8] - para impressão dos documentos.

Este sistema consiste num leitor, com a tecnologia NFC incorporada, que é instalado na impressora da empresa e que identifica cada colaborador e desbloqueia a impressão que pretende imprimir com o auxilio de um cartão que o identifica. Os ficheiros a imprimir serão enviados para a impressora mas ficam em espera até que o colaborador proprietário os liberte.

Este sistema preserva a confidencialidade da informação contida nos documentos e ajuda a empresa no controlo e na gestão da impressão de documentação.

7.3 Restrições ao Sistema de Informação - Hardware e Software

As políticas, normas, regulamentos, regras e/ou procedimentos são instruções claras que fornecem as orientações de comportamento do colaborador para proteger a informação, e é um elemento fundamental no desenvolvimento de controlos efetivos para contra-atacar as possíveis ameaças à segurança.

No conjunto dos ativos que constituem o sistema de informação de uma empresa estão o *software* e o *hardware*, pois é através destes que os dados são processados e armazenados de modo a gerar informações úteis para a atividade da empresa. Como tal, necessitam de ser protegidos.

Considerando a análise da entrevista ao diretor geral foi possível perceber que existe ausência de instruções claras para o manuseamento destes ativos de informação.

Mamede, (2006) menciona que provavelmente o maior problema para a segurança física dos sistemas é o próprio utilizador, já que se este falhar nas diligências para proteger fisicamente os dispositivos de computação á sua disposição, praticamente todos os controlos implementados se tornam ineficazes.

A ISO/IEC 27001 (2013) indica que para garantir a integridade do sistema operacional é necessário implementar procedimentos para controlar a instalação de *software* nas organizações sendo obrigatória a existência de regras que regulem esta

[8] Padrão de comunicação sem fios, de curto alcance, desenvolvido para fazer uma comunicação simples e intuitiva entre dois equipamentos eletrónicos.

instalação por parte dos utilizadores juntamente com a necessidade de proteção dos equipamentos para a continuidade das atividades da organização.

Desta forma, e como forma de solucionar a ausência de restrições à utilização de *software* e *hardware* da empresa, elaboramos uma política que menciona as principais atividades que estão proibidas para preservação do sistema de informação da empresa, consultar o ANEXO VI.

O documento foi elaborado tendo em conta os controlos A.11.2.4, A.11.2.5, A.12.5.1 e A.12.6.2 disponível no ANEXO A da ISO/IEC 27001 (2013), e posteriormente à consulta da sua aplicabilidade na ISO/IEC 27002 (2013), sendo utilizados apenas como forma de orientação para a solução final e não a sua aplicabilidade na íntegra.

7.3.1 Sugestão de trabalho futuro - Restrições ao Sistema de Informação - Hardware e Software

A política que foi elaborada apenas é vantajosa para a empresa se os colaboradores efetivamente a utilizarem e a respeitarem de forma exemplar. Todas as políticas, normas, regulamentos, regras e/ou procedimentos que sejam implementados terão de ser controlados, só desta forma os gestores de topo conseguem garantir que estão a ser cumpridos os prepósitos para os quais os procedimentos foram desenvolvidos anteriormente.

Tendo em conta a solução encontrada para o problema abordado e fazendo referencia ao exposto acima, recomendamos que a empresa selecione um ou mais colaboradores aleatoriamente, de seis em seis meses, e verifique o conteúdo instalado na sua máquina, fazendo referência ao definido na política relativamente ás restrições de utilização de software.

7.4 Gestão das Cópias de Segurança

A empresa optou pelo *outsourcing* [9] para fazer a gestão das cópias de segurança dos seus dados. A opção por esta forma de gestão é bastante vantajosa para as organizações, estão a depositar a responsabilidade das cópias de segurança em quem

[9] Processo usado por uma empresa no qual outra organização é contratada para desenvolver uma certa área da empresa.

realmente é especializado em fazê-lo, nesta perspetiva, sobra tempo e disponibilidade para os gestores de topo dedicarem a outras funções.

A confiança depositada nestas empresas está sempre salvaguardada por condições contratuais, acordadas à priori, por ambas as partes, que garantem o armazenamento, periodicidade e manutenção do equipamento afeto ás cópias de segurança.

Segundo Hintzbergen, Hintzbergen, Smulers e Hans (2018) o propósito de fazer *backups* é manter a integridade e disponibilidade da informação e das instalações computacionais, e sabendo que apenas se consegue avaliar um sistema de gestão de cópias de segurança quando efetivamente se necessita de fazer a recuperação dos dados é necessário criar mecanismos e soluções que deem respostas quando existe esta necessidade.

Sabemos que a segurança está relacionada com a capacidade de recuperação após um incidente. E esta capacidade representa não só disponibilidade de dados mas também do tempo que se despende para conseguir repor uma situação estável e integra de funcionamento (Mamede, 2006).

Ou seja, recuperação e prevenção são os elementos chave para se conseguir um bom sistema de gestão de copias de segurança.

Tendo em conta a informação obtida através da entrevista ao diretor geral da TMS foi possível verificar que o elemento prevenção não está a ser cumprido pela empresa contratada para realizar a gestão das cópias de segurança, pois foi possível existir perda de informação de gestão referente a um ano comercial.

Existindo um contrato, existindo pagamento de um serviço, este tipo de incidentes não podem acontecer, perda de informação para um empresa pode significar o seu encerramento, pode destruir o que demorou anos a construir, mesmo existindo uma recuperação relativamente rápida.

A informação cria vantagem competitiva se estiver correta e atual, estando a passar por uma fase de recuperação não cumpre o seu prepósito e deixa a empresa numa situação de vulnerabilidade perante o mercado da concorrência.

7.4.1 Sugestão de Trabalho Futuro – Gestão de Cópias de Segurança

Num futuro, aconselhamos à organização que esteja mais envolvida com a empresa de gestão de cópias de segurança, sendo esta empresa ou uma outra, que controle e verifique se o contrato está a ser cumprido e quais os planos e procedimentos que têm

definidos caso volte a existir algum incidente semelhante. Propomos que este seguimento seja efetuado por um responsável interno, dando o *feedback* posteriormente ao diretor geral.

O controlo A.15.2.1 da ISO/IEC 27002 (2013) diz que as organizações devem monitorizar, rever e auditar regularmente a prestação de serviços dos fornecedores, assegurando que os termos e as condições sobre segurança da informação dos contratos estão sendo atendidos, e que os incidentes e problemas de segurança da informação estão sendo geridos adequadamente. O controlo A.15.2.2 da ISO/IEC 27002 (2013) acrescenta ainda que as alterações nos serviços de fornecedores devem ser geridas levando em conta a criticidade da informação, dos sistemas e dos processos envolvidos da empresa, e levando em conta uma reavaliação dos riscos.

Nem todo o incidente é um incidente de segurança. Então, deve ser feita uma avaliação do incidente para determinar se realmente há um incidente desta natureza.

Recorrendo ás indicações dos controlos A.16.1.5 e A.16.1.6 constante da ISO/IEC 27002 (2013) propomos que a organização defina procedimentos de recolha de provas e documentação das mesmas após a ocorrência de um incidente para poder adquirir conhecimento para ajuda a reduzir o impacto ou a probabilidade de ocorrência de incidentes futuros .

Pensar de forma antecipada sobre a continuidade dos processos de trabalho é essencial para a organização. Segundo Hintzbergen, *et al* (2018, p.183) "o prepósito da gestão da continuidade dos negócios é prevenir que as atividades da empresa sejam interrompidas, proteger processos críticos das consequências de grandes perturbações nos sistemas de informação e permitir uma rápida recuperação".

Desta forma e tendo em conta os acontecimentos ocorridos na TMS aconselhamos a elaboração de um DRP (*Disaster Recovery Planning*). O objetivo deste plano é minimizar as consequências de um desastre e tomar medidas necessárias para garantir que funcionários , ativos e processos do negócio estejam disponíveis novamente dentro de um tempo aceitável, ou seja, uma recuperação imediata após um desastre.

7.5 Controlo de Acessos Físicos ao Sistema de Informação

A segurança física é parte da segurança da informação, pois todos os ativos do negócio também devem ser fisicamente protegidos.

Segundo Carneiro, (2009) o principal objetivo da segurança física é garantir a proteção dos SI quanto ás suas dimensões físicas e no que se refere a todos os seus componentes.

O autor define os seguintes objetivos da segurança física:

Segurança Física	Objetivos
Do pessoal	Reduzir os riscos devidos a erros humanos, roubo, fraudes e/ou má utilização dos recursos existentes
Do equipamento	Proteger o hardware computacional, outros equipamentos, as suas interligações e o fornecimento de energia
Das instalações	Requisitos da localização e estrutura dos edifícios destinados aos centros de informática de forma a garantir um nível de segurança adequado

Tabela 7 - Objetivos de segurança física

(Adaptado Carneiro (2009))

Analisando a entrevista ao diretor geral da TMS foi possível verificar que ao nível da segurança física do SI existem alguns procedimentos internos que não cumprem os principais objetivos da mesma, livre circulação de pessoal com acesso total ao edifício da empresa, durante o horário noturno e livre circulação de fornecedores externos a todo o logipark, durante a semana e aos fins-de-semana.

Todas as ações que são tomadas por parte do pessoal afeto à TMS podem ter ou não implicações na segurança da informação da empresa basta um ato intencional ou um erro humano para comprometer o SI da empresa.

Desta forma é recomendável que a TMS analise todas as situações que prevejam possíveis ameaças à segurança da informação e defina uma estratégia para mitigar os riscos relativamente à segurança física do seu SI.

7.5.1 Sugestão de Trabalho Futuro - Controlo de Acesso Físicos ao Sistema de Informação

O controlo A.11.1.1 presente na ISO/IEC 27002 (2013) menciona que os parâmetros de segurança devem ser definidos e usados para proteger áreas que contêm informações confidenciais ou críticas e instalações de processamento de informação. A segurança física para escritórios, salas e instalações deve ser projetada e aplicada, segundo o controlo A.11.1.3 também constante na ISO/IEC 27002 (2013).

No seguimento destas diretrizes, recomenda-se, que no imediato, a empresa anule o motivo pelo qual o seu funcionário tem acesso total ao edifico onde está concentrado todo o sistema de informação.

Sabendo que este acesso é cedido porque o responsável de armazém necessita da fotocopiadora para tratar a documentação necessária e resultante das cargas/descargas noturnas, sugerimos que a empresa instale uma impressora no armazém, barrando o acesso do edifício ao colaborador, através do sistema de controlo de acessos já utilizado pela empresa (ver questões 57 a 59 da entrevista, ANEXO II). Esta última recomendação está diretamente ligada ao controlo A.11.1.2 presente na ISO/IEC 27002 (2013) que diz que as áreas seguras devem ser protegidas por controles de entrada apropriados para garantir que apenas o pessoal autorizado tenha acesso permitido.

Outra questão que verificámos é a externalização de serviços. Os acessos dados a estes colaboradores externos têm de ser fortemente condicionados na medida que não incapacitem a realização das funções contratadas mas que evitem, ao máximo, a possibilidade de serem executadas ações que possam comprometer a segurança dos dados da empresa. Segundo Mamede (2006) devem de existir contratos com clausulas muito especificas onde estejam discriminadas as condições de acesso, as formas de controlo e os mecanismos de auditoria.

O controlo A.15.1.1 presente na ISO/IEC 27002 (2013) faz referência que um dos requisitos da segurança da informação é mitigar os riscos associados ao acesso dos fornecedores aos ativos da organização, acessos esses que deverão ser sempre acordados e documentados.

Uma medida que deverá ser garantida pela empresa é a de que nenhum colaborador externo pode deambular sozinho pelas instalações, principalmente sem identificação visível. O ideal é sempre que chega alguém, se houver autorização para essa mesma pessoa poder entrar, ser acompanhada desde esse momento por alguém da segurança ou vir o contacto respetivo busca-lo à zona de receção e depois trazê-la.

Os gestores de topo têm que se consciencializar de que por muito que reúnam esforços para conseguir uma organização segura, relativamente a ataques externos, essa segurança será nula se não tiver sido previsto como combater esses ataques, (Carneiro, 2009).

Atendendo ao exposto, deixamos uma recomendação à empresa para que no futuro consiga ter total controlo pela segurança física do seu SI. Sugerimos que seja elaborada uma política de segurança para acessos físicos atendendo às recomendações

constantes nas ISO/IEC 27001 (2013), ISO/IEC 27002 (2013), seguindo os critérios dos controlos do ANEXO A da ISO/IEC 27001 (2013).

Segundo Mamede (2006) os elementos importantes a considerar para a elaboração do documento são os métodos de acesso físico, os procedimentos para autorização, modificações e negações de acessos, restrições de acesso baseadas no estatuto de cada pessoa, horas de operação, pontos de contacto para o acesso e procedimentos para manipulação de incidentes.

"A segurança física constitui-se como um imenso componente de qualquer política de segurança... e quando se fala de acesso físico, não é apenas ao edifício da organização, mas também, de forma mais particular, a qualquer área dentro deste" (Mamede 2006, p.55).

8 Recomendação Final

O conjunto de soluções e recomendações descrito no capítulo anterior resolve os problemas encontrados no imediato e auxilia a empresa a definir o rumo a seguir para garantir a segurança dos seus dados, contudo, da análise da entrevista ao diretor geral da TMS foi possível verificar um problemas comum a todos os outros, todos os processos e procedimentos implementados na empresa não têm nenhum documento base que os clarifique ou que os faça ser cumpridos. Cada colaborador toma as suas próprias decisões perante determinada situação ou problema, o questionário passado aos mesmos clarifica esta realidade.

Na gíria da empresa fala-se de senso comum, como sendo este o responsável pelas ações de todos dentro da organização, no entanto, quando existe um acidente que comprometa a segurança da informação, o senso comum não ajuda, apenas é um obstáculo para apurar culpados, resolver a situação e evitar que a mesma não se repita.

Um acidente não é completamente evitável mas é necessário que se garanta a continuidade das atividades da empresa, minimizando os prejuízos e reduzindo o impacto dos incidentes de segurança (Carneiro, 2009).

Para garantir a continuação das atividades da empresa e evitar eventuais acidentes recomenda-se que a empresa elabore uma política de segurança da informação atendendo ás recomendações das ISO/IEC 27001 (2013) e ISO/IEC 27002 (2013), sabendo que estes documentos são genéricos a aplicabilidade dos mesmo não dispensa uma análise do contexto organizacional onde irão ser aplicados.

ISO/IEC 27002 (2013) orienta que convém que a direção estabeleça uma clara orientação da política, alinhada com os objetivos de negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

Barman, (2002) diz que antes de ser escrita a política de segurança torna-se necessário determinar quais os objetivos gerais nomeadamente que atividades de negocio devem ser protegidas e se essa proteção deve atender apenas a fluxos de dados ou aos SI, referindo que o primeiro passo é determinar o que deve ser protegido e porquê.

A política deve ser escrita de acordo com os requisitos do negócio, bem como pelas leis e regulamentos que a empresa se rege para o exercício das suas funções, a mesma deverá ser aprovada pelo conselho de administração e publicada para todo o pessoal interno e todos os parceiros externos. Deverá existir um programa de consciencialização,

bem estruturado, para assegurar o sucesso da sua implementação (Hintzbergen *et al*, 2018).

ISO/IEC 27002 (2013) estabelece que as políticas de segurança da informação devem ser revistas em intervalos planeados ou se ocorrerem mudanças significativas na organização a fim de assegurar a sua contínua conformidade adequação e eficácia. A política deverá ter um responsável que tenha a função de a desenvolver, rever e avaliar.

Em suma a politica de segurança da informação deverá providenciar o comprometimento da gestão e o adequado suporte ás atividades essenciais à segurança da informação (Gaivéo, 2008).

9 Conclusão

A informação é um elemento essencial, possibilita a execução das atividades operacionais, mas, antes de tudo, é um recurso crítico para a definição da estratégia organizacional tendo impacto direto na continuidade do negócio e na sua credibilidade. Devido à sua importância necessita de ser adequadamente protegida.

O propósito de segurança da informação é proteger a informação de uma grande variedade de ameaças, assegurando a continuidade da atividade através da minimização dos danos causados por incidentes de segurança.

A conceção de um projeto de segurança da informação numa organização deve estar suportado por um SGSI que precisa ser planeado e organizado, implementado, mantido e monitorado. Sendo que essa responsabilidade cabe aos profissionais de TI e gestores de topo das organizações, estes não podem olhar apenas para questões associadas à segurança física, sem conhecer o negócio da organização e não podem tomar medidas preventivas sem procedimentos de controlo e auditoria.

Ou seja, para facilitar todo o SGSI é necessário fazer o alinhamento do SI e das TI com a organização e com a sua estratégia e cultura organizacional.

A empresa escolhida para este estudo pertence ao setor dos transportes rodoviários de mercadorias e armazenagem que é caracterizado pela necessidade de tratamento de grandes fluxos de informação para conseguir coordenar toda a atividade da cadeia de abastecimento dando origem ao aumento do valor percebido dos seus clientes.

Sabendo que a grande força para incrementar os níveis de desempenho no ramo da logística é o uso das tecnologias de informação, uma vez que estas são capazes de fornecer informações fiáveis e, portanto, promover resultados económicos positivos, níveis de satisfação do cliente e de operacionalização dos recursos disponíveis sentiu-se a necessidade de perceber como é efetuada a gestão da segurança da informação no setor tendo como exemplo o estudo de caso da TMS – Transportes & Logística, S.A.

Para a observação e descrição da situação atual da empresa, as opções metodológicas adotadas foram a observação participativa numa fase inicial seguindo-se, posteriormente, o questionário passado aos colaboradores, tendo como objetivo a análise dos processos e procedimentos existentes relativamente à segurança da informação, numa ultima fase realizou-se uma entrevista estruturada ao diretor geral da TMS que teve como foco principal perceber a postura e a visão da organização sobre a temática abordada.

Depois de toda a informação recolhida e devidamente tratada e analisada foi possível encontrar com conjunto de falhas ao nível da gestão da segurança da informação, nomeadamente ausência de gestão de passwords, ausência de gestão da impressão de documentação, ausência de políticas, normas, regulamentos e procedimentos relativamente à segurança da informação, ausência de restrições de acesso ao sistema de informação da empresa, gestão ineficiente das cópias de segurança e ausência de controlo de acesso físico ao sistema de informação da empresa.

Reunidos todos os problemas encontrados, elaborou-se um conjunto de soluções que a empresa deverá implementar para anular alguns dos seus principais problemas, nomeadamente, política de passwords, política de impressão e política de utilização de hardware e software. Para complementar estas soluções deixamos um conjunto de recomendações para trabalho futuro que a empresa deverá realizar, uns de forma a conseguir implementar as soluções apresentadas outros para fomentar a adoção de melhores práticas relativamente à segurança da informação.

Por último, deixamos uma recomendação final com o intuito de alinhar a cultura e a estratégia organizacional da empresa com a gestão da segurança da informação, sugerimos que seja elaborada e implementada um política de segurança da informação. É expectável que este documento elimine o senso comum da gíria da empresa, que atribua responsabilidades e sanções, que indique o que deve ser protegido e porquê, que seja escrita de acordo com os requisitos do negócio e do setor em que se insere, deverá ser aprovada e comunicada a toda a comunidade e, por último, deverá ter um responsável que a desenvolva, reveja e avalie, em suma, deverá alinhar a empresa num objetivo comum, a proteção da informação presente no seu sistema de informação.

Uma gestão da segurança da informação eficaz potencia a criação de organizações autónomas, sem medos e com capacidade de resposta a eventuais incidentes de segurança. Sabendo a importância da informação, hoje em dia, a adoção de boas práticas de gestão potencia a diferenciação destas empresas nos seus setores e define estratégias organizacionais mais eficientes.

Bibliografia

A

Almeida, W. (2020, maio, 29). T.I em foco: Conceitos Básicos de Segurança da Informação. Retirado de https://blog.grancursosonline.com.br/conceitos-basicos-de-seguranca-da-informacao/

Alvarenga, A.C. & Novaes, A.G. (2000). Logística Aplicada: suprimento e distribuição física. 3ª Edição. São Paulo: Edgard Blucher

Amaro, A. (2005) Consciência e cultura do risco nas organizações. Torritorium : Revista da Associação Portuguesa de riscos, prevenção e segurança. 5-9

Anunciação, P. & Zorrinho, C. (2006). Urbanismo Organizacional – Como gerir o choque tecnológico nas empresas: Edições Sílabo

B

Backup Systems. (2020). Rick vs Benefits of Outsourcing Backups. Retirado de http://www.backup-systems.co.uk/blog/risk-vs-benefits-of-outsourcing-backup

Barman, S. (2002). Writing Information Security Policies: New Riders Publishing

Bastos, E. (2015, fevereiro,13). O que é a gestão da cadeia de abastecimento?. Portal Gestão. Retirado de https://www.portal-gestao.com/artigos/7617-o-que-%C3%A9-a-gest%C3%A3o-da-cadeia-de-abastecimento.html

Bowersox, D.J. & Closs, D.J. (1996). Logistical Management: The Integrated Supply Chain Process: McGraw-Hill.

Brother Industries. (2020). Soluções de segurança na impressão. Retirado de https://www.brother.pt/solucoes-empresariais/seguranca-impressao

Brother Industries. (2020). Solução avançada de SecurePrint+. Retirado de https://www.brother.pt/solucoes-empresariais/seguranca-impressao/secureprint-plus

C

Carneiro, A. (2009). Auditoria e Controlo de Sistemas de Informação. 1ª Edição. Lisboa: FCA – Editora Informática

Comissão Europeia. (2014). Compreender as políticas da União Europeia: Transportes. Luxemburgo

Council of Supply Chain Management Professionals. (2020). About CSCMP: Definitions. Retirado de http://cscmp.org/aboutcscmp/definitions.asp

Croxton, K.L., Garcia-Dastugue, S.J., Lambert, D.M., & Rogers, D.S. (2001). The supply chain management processes. The International Journal of Logistics Management, 12: 13-36.

Cunha A. (2016). NFC (Near Field Communication) – Aplicações e uso. O portal Embarcados. Retirado de https://www.embarcados.com.br/nfc-near-field-communication/

E

ePortugal.gov.pt. (2020). Espaço empresa – Categorias de atividade. Retirado de https://eportugal.gov.pt/categorias-de-actividade/transporte-armazenam

ESL - Excelência em sistemas logísticos. (2020). A importância na cadeia de transportes. Retirado de https://transporteenegocios.eslsistemas.com.br/a-importancia-da-informacao-na-cadeia-de-transportes/

F

Fernandes, J.P., Correia, M. & Antunes, M. (2007). A terminologia e a sociedade da informação in José Dias Coelho (coordenador), Sociedade da Informação – O percurso português. Edições Sílabo. 457-472

Freixo, M. (2010). Metodologia Cientifica: Fundamentos Métodos e Técnicas. 2ª Edição. Lisboa: Instituto Piaget.

G

Gaivéo, J. M. (2008). As Pessoas nos Sistemas de Gestão da Segurança da Informação. Tese de Doutoramento em Informática, Universidade Aberta

Gil, A. C. (1968). Métodos e Técnica de Pesquisa Social. São Paulo: Editora Atlas, S.A

H

Haguette, T. M. (1997). Metodologias Quantitativas na Sociologia. Petrópolis: Vozes

Hintzbergen, J.; Hintzbergen, K.; Smulers, A.; & Hans, B. (2018) Fundamentos da Segurança da Informação – com base na ISO27001 e na ISO27002, Brasport

I

INE. (2019). Estatísticas dos Transportes e Comunicações. Lisboa: Edição de 2019

ISO/IEC (2013). ISO/IEC 27001 - Information technology – Security techniques – Information Security Management Systems - Requirements. International Standard Organization

ISO/IEC (2014). ISO/IEC 27000 - Information security management systems - Overview and vocabulary. International Standard Organization.

ISO/IEC (2018). ISO/IEC 27000 – Information technology - security techniques – Information security management systems - Overview and vocabulary. International Standard Organization

L

Lemos, C.S., Andrade, C.A.B. (2016) Entregar, Servir e Suportar um SGSI. Revista Científica da FASETE. Faculdade JK - Especialização em Gestão de TI na Administração Publica, 2, 206-232

López, Yanai. (2014). Sistemas de Informação para gestão. Lisboa: Escolar Editora

M

Macedo, P., Zacarias, M., & Tribolet, J. (2005). Técnicas e métodos de investigação em Engenharia Organizacional: Projecto de Investigação em Modelação de Processos de Produção. 6a Conferência da Associação Portuguesa de Sistemas de Informação. Portugal

Mamede, H.S. (2006). Segurança Informática nas Organizações. 1ª Edição. Lisboa: FCA – Editora Informática, S.A

Mazzotti, A. (2006). Usos e Abusos dos Estudos de Caso. Cadernos de pesquisa, 129: 637-651

P

Pereira, M. J. L. de Bretãs; Fonseca, J. G.M. (1997). Faces da Decisão: As mudanças de paradigmas e o poder da decisão. São Paulo: Makron Books

Pfleeger, C.P & Pfleeger S.L. (2003). Security in Computing. 3rd edition. Prentice Hall

Pocinho, M. (2012). Metodologias de Investigação e Comunucação do Conhecimento Científico. Lisboa: Lidel - Edições Técnicas, Lda

Q

Quivy, R., & Campenhoudt, L. V. (2017). Manual de Investigação em Ciências Sociais. 7ª Edição. Lisboa: Gradiva

R

Rodrigues, L. S. (2002). Arquiteturas dos Sistemas de Informação. FCA

Rodrigues, M.A.P. (2013). Sistemas de Informação para a logística: Análise e seleção. Dissertação para obtenção do grau de Mestre em Sistemas de Informação de Gestão, Instituto Politécnico de Coimbra

S

Segovia, A. J. (2016, fevereiro, 9). Implementado restrições em instalações de software usando o controle A.12.6.2 da ISO 27001. Retirado de https://advisera.com/27001academy/pt-br/blog/2016/02/09/implementando-restricoes-em-instalacoes-de-software-usando-o-controle-a-12-6-2-da-iso-27001/

Sequesseque, M.T.M. (2017). O impacto da implementação de segurança da informação na usabilidade dos sistemas de informação. Tese de Mestrado em Sistemas de Informação Organizacionais, Instituto Politécnico de Setúbal

Stake, R. E. (1994). Handbook of Qualitative Research. SAGE Publications

Stake, R. E. (1999). Investigación con estudio de casos. Madrid: Morata

Stallings, W. (2000). Network Security Essentials: Applications and Standards. Prentice Hall, USA

T

Thayer-Hart, N., Dykema, J., Elver, K., Schaeffer, N. C., & Stevenson, J. (2010). Survey Fundamentals. A guide to designing and implementing surveys. University of Wisconsin-Madison

TMS – Transportes e Logística, S.A. (2019). Sobre Nós. Retirado de http://www.tms-pt.com/pt/content/34-sobre-nos

Toccato Tecnologia. (2020, fevereiro, 27). Como avaliar a maturidade da empresa? Aprenda!. Retirado de https://blog.toccato.com.br/maturidade-digital/

Toffler, A. (1984). A Terceira Vaga, Edições livros do brasil

W

Waltz, E. (1998). Information Warfare: Principles and Operations. Artech House, USA

Whitman, M.E & Mattord, H.J. (2005). Principles of Information, 2ª Edition, Thomson Course Technology

Y

Yin, Robert K. (1989) - Case Study Research - Design and Methods. Sage Publications Inc, USA

Z

Zúquete, A. (2006). Segurança em Redes Informáticas, FCA

Anexos

Anexo I – Questionário

IPS Instituto Politécnico de Setúbal

Questionário

O objetivo do presente questionário é estudar os processos e procedimentos de cada departamento funcional da TMS relativamente à **segurança da informação**. Este enquadra-se numa investigação no âmbito do Mestrado em Gestão de Sistemas de Informação, realizada no Instituto Politécnico de Setúbal.

Os resultados obtidos serão utilizados apenas para fins académicos (tese de mestrado), sendo pertinente realçar que as respostas dos inquiridos representam apenas a sua opinião individual.

O questionário é anónimo, não devendo por isso colocar a sua identificação em nenhuma das folhas.

Obrigada pela colaboração.

I - Caracterização do Público Alvo

1. Em que departamento se insere a sua função? (assinale apenas uma das opções)

Comercial ☐ Financeiro ☐ Operacional ☐

2. Há quantos anos desempenha funções na TMS?

Menos de 2 ☐ Entre 2 e 5 ☐ Entre 5 e 10 ☐ 10 ou mais ☐

II - Questões Gerais sobre Processos e Procedimentos Internos

Segurança da informação:

É um processo organizado e estruturado que permite preservar a **confidencialidade** (assegurar que a informação apenas é acedida por quem está autorizado a fazê-lo), **integridade** (garantir a exatidão e a credibilidade da informação) e **disponibilidade** (assegurar que as pessoas autorizadas têm acesso à informação e aos ativos associados sempre que necessário) da informação.

3. Tem atribuído algum computador para utilização individual?

Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 5

4. Partilha o seu computador do trabalho com algum/alguns colega/s

Sim ☐ Não ☐

Se respondeu **sim**, com quantas pessoas?

1 ☐ 2 ou 3 ☐ Mais de 3 ☐

Em que circunstâncias partilha? _____

5. Possui acesso ao sistema informático da empresa (sistema de informação e rede informática)?

Sim ☐ Não ☐

6. O sistema de informação tem pré-definida uma sessão individual para o seu utilizador (ID de Utilizador)?

Sim ☐ Não ☐

Se respondeu **não**, essa sessão é partilhada?

Sim ☐ Não ☐

Se **sim**, qual o motivo? _____

7. Possui endereço de correio eletrónico associado ao sistema informático da empresa?

Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 10

8. Utiliza este mesmo endereço para assuntos pessoais?

Sim ☐ Não ☐

9. Apenas tem este endereço de correio eletrónico?

Sim ☐ Não ☐

Se respondeu **não**, quantos endereços de correio eletrónico possui?

1 ☐ 2 ou mais ☐

10. Quando se ausenta da sua área de trabalho, sem ser no final do horário de trabalho, encerra a sessão?

Sim ☐ Não ☐

Se respondeu **não**, como deixa a sessão?

_____

III - Procedimentos relativamente à utilização das Passwords

11. Possui password para acesso ao seu computador de trabalho e/ou ao sistema de informação da empresa?

Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 18

12. A(s) password(s) permitem que tipo de acesso?

Apenas ao computador ☐
Apenas ao sistema de informação ☐
A ambos ☐

Se respondeu **a ambos**, a password é a mesma para as duas situações?

Sim ☐ Não ☐

13. A(s) password(s) foram atribuídas pela empresa ou escolhida(s) por si?

Escolhida(s) por mim ☐ Atribuída(s) pela empresa ☐

14. A(s) password(s) é(são) partilhada(s) com algum colega de trabalho?

Sim ☐ Não ☐

Se respondeu **sim**, com quantas pessoas?

1 ☐ 2 ou 3 ☐ Mais de 3 ☐

Qual o motivo dessa partilha? _____

15. Já alterou a(s) password(s) de acesso?

Sim ☐ Não ☐

Se respondeu **sim**, com que frequência altera a(s) sua(s) password(s)?

Raramente ☐ Uma única vez ☐ Mensalmente ☐ Anualmente ☐

16. Qual o processo que utiliza para guardar a(s) sua(s) password(s)?

Memorização ☐ Post-it ☐ Outro ☐. Qual? _____

17. Que opções efetua na escolha da(s) sua(s) password(s)? (assinale todos os itens aplicáveis)

Escolha aleatória de caracteres ☐
Números e letras ☐
Só números ☐
Só letras ☐
Nome de animais de estimação ☐
Nome de familiares ☐

18. Tem acesso ás contas bancárias da empresa, através de password?

Sim ☐ Não ☐

19. A(s) password(s) de acesso às contas bancárias são partilhadas com algum colega de trabalho?

Sim ☐ Não ☐

Se respondeu **sim**, com quantas pessoas partilha?

1 ☐ 2 ou 3 ☐ Mais de 3 ☐

Qual o motivo dessa partilha? _____

20. A(s) password(s), de acesso às contas bancárias, que utiliza são de:

Acesso total às contas ☐ Acesso restrito ☐ Apenas consulta ☐

21. Qual o processo que utiliza para guardar a(s) password(s) de acesso às contas bancárias?

Memorização ☐ Post-it ☐ Outro ☐. Qual? _____

IV - Segurança da Informação Confidencial da Empresa

22. Para desempenho da sua função trabalha diretamente com informação necessária para a atividade da empresa?

Sim ☐ Não ☐

Se respondeu **sim**, de que tipo é essa informação? (selecionar todas as opções aplicáveis)

Operacional ☐
Financeira ☐
Técnica ☐
Manutenção ☐
Stock ☐
Outra ☐
Qual? _____

23. A informação selecionada na pergunta 22. é registada posteriormente no sistema de informação da empresa?

Sim ☐ Não ☐

Se respondeu **sim**, quem regista? (indique a função da pessoa responsável por esta ação se não for o inquirido)

_____

24. Para desempenho da sua função, trabalha com informação confidencial e/ou sensível (passwords bancárias, documentação financeira, dados dos colaboradores etc.)?

Sim ☐ Não ☐

Se respondeu **sim**, que tipo de informação? (selecionar todas as opções aplicáveis)

Contratos de Trabalho ☐
Informação sobre vencimentos ☐
Informação Financeira ☐
Informações e dados pessoais dos colaboradores ☐
Documentação relativa a contencioso ☐
Documentação confidencial da empresa ☐
Outra ☐
Qual? _____

25. A informação selecionada na questão 24. Está em que formato?

	Papel	Digital	Ambos
Contratos de Trabalho	☐	☐	☐
Informação sobre vencimentos	☐	☐	☐
Informação Financeira	☐	☐	☐
Informações e dados pessoais dos colaboradores	☐	☐	☐
Documentação relativa a contencioso	☐	☐	☐
Documentação confidencial da empresa	☐	☐	☐
Outra	☐	☐	☐

26. Classifique a facilidade de acesso à informação em formato papel, pelos colaboradores não autorizados. (**6** para **muito fácil** e **1** para **muito difícil**)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

27. Se está em formato digital, qual o processo que realiza para aceder à informação?

Apenas acedo, o meu utilizador tem permissão para tal ☐
Através de Password ☐
Outra ☐
Qual? _____

V - Impressão de Documentos através do Sistema Informático

28. Possui acesso à impressão de documentos através do sistema informático da empresa?

Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 34

29. Essa impressão é efetuada em modo privado?

Sim ☐ Não ☐ Nem Sempre ☐

Se respondeu **sim**, avançar para a questão 33

30. Depois de imprimir um documento saí do local de trabalho e vai buscar a impressão?

Sim ☐ Não ☐

Se respondeu **não**, como imprime?

_____

31. Que atitude toma quando não encontra os documentos que mandou imprimir na impressora? (selecionar todas as opções aplicáveis)

Pergunta aos colegas se alguém encontrou o documento em questão ☐
Tenta encontrar o documento ☐
Imprime novamente ☐
Verifica se ainda aguarda impressão ☐
~~Documentação relativa a contencioso~~ ☐
Nunca aconteceu ☐
Outra ☐
Qual? _____

32. Quando não consegue imprimir documentos através da impressora qual a sua atitude? (assinale apenas uma das opções)

Tenta imprimir mais tarde ☐
Verifica se a impressora tem algum problema ☐
Tenta imprimir novamente ☐
Verifica se ainda aguarda impressão ☐
Cancela a impressão ☐
Outra ☐
Qual? _____

33. Já alguma vez encontrou documentos que não os seus na impressora partilhada da empresa?

Sim ☐ Não ☐

Se respondeu **sim**, que atitude tomou? (selecionar todas as opções aplicáveis)

Deixa junto à impressora ☐
Guarda ☐
Deita fora ou destrói o documento ☐
Tenta entregar ao proprietário ☐
Lê o documento ☐
Outra ☐
Qual? _____

VI - Questões Gerais sobre a Segurança do Sistema Informático

34. Já presenciou alguma violação da segurança do sistema informático da empresa (Por exemplo, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?

Sim ☐ Não ☐

Se respondeu **sim**, que atitude tomou quando presenciou essa violação?

Propôs medidas para a resolução do problema ☐
Informou a administração ☐
Advertiu o/(a) infrator(a) ☐
Outra ☐
Qual? _____

35. Na sua opinião, classifique o grau de segurança do sistema informático da empresa. (**6** para **elevado** e **1** para **baixo**)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

36. Classifique em que medida considera que a segurança do sistema informático é importante para o desempenho das suas funções diárias? (**6** para **muito importante** e **1** para **pouco importante**)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

Fim do questionário.
Obrigada pela colaboração!

Anexo II – Tratamento Estatístico do Questionário

IPS Instituto Politécnico de Setúbal

Questionário

O objetivo do presente questionário é estudar os processos e procedimentos de cada departamento funcional da TMS relativamente à **segurança da informação**. Este enquadra-se numa investigação no âmbito do Mestrado em Gestão de Sistemas de Informação, realizada no Instituto Politécnico de Setúbal.

Os resultados obtidos serão utilizados apenas para fins académicos (tese de mestrado), sendo pertinente realçar que as respostas dos inquiridos representam apenas a sua opinião individual.

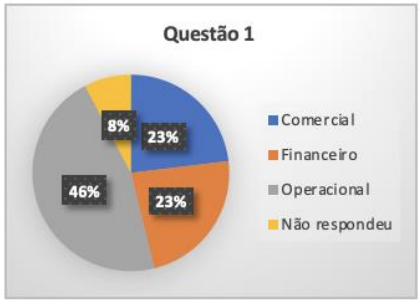
O questionário é anónimo, não devendo por isso colocar a sua identificação em nenhuma das folhas.

Obrigada pela colaboração.

I - Caracterização do Público Alvo

1. Em que departamento se insere a sua função? (assinale apenas uma das opções)

Comercial ☐ Financeiro ☐ Operacional ☐



2. Há quantos anos desempenha funções na TMS?

Menos de 2 ☐ Entre 2 e 5 ☐ Entre 5 e 10 ☐ 10 ou mais ☐

II - Questões Gerais sobre Processos e Procedimentos Internos

Segurança da informação:

É um processo organizado e estruturado que permite preservar a **confidencialidade** (assegurar que a informação apenas é acedida por quem está autorizado a fazê-lo), **integridade** (garantir a exatidão e a credibilidade da informação) e **disponibilidade** (assegurar que as pessoas autorizadas têm acesso à informação e aos ativos associados sempre que necessário) da informação.

3. Tem atribuído algum computador para utilização individual?

Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 5

	Respostas
Sim	13
Não	0

4. Partilha o seu computador do trabalho com algum/alguns colega/s

Sim ☐ Não ☐

Se respondeu **sim**, com quantas pessoas?

1 ☐ 2 ou 3 ☐ Mais de 3 ☐

Em que circunstâncias partilha? _____

Respostas
Quando estou de férias ou de baixa
Férias
Férias/Ausências
No caso de férias
Quando estou de férias

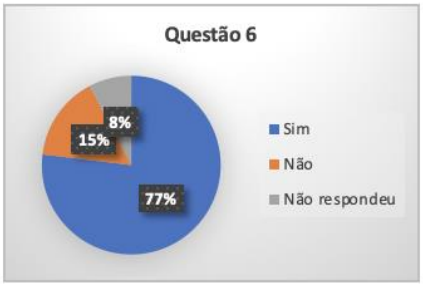
5. Possui acesso ao sistema informático da empresa (sistema de informação e rede informática)?

Sim ☐ Não ☐

	Respostas
Sim	13
Não	0

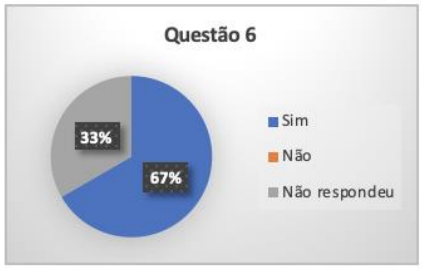
6. O sistema de informação tem pré-definida uma sessão individual para o seu utilizador (ID de Utilizador)?

Sim ☐ Não ☐



Se respondeu **não**, essa sessão é partilhada?

Sim ☐ Não ☐



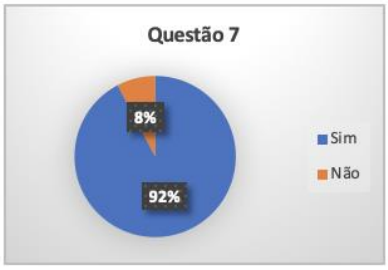
Se **sim**, qual o motivo? _____

Respostas
O utilizador é partilhado (departamento)
Falta de licenças

7. Possui endereço de correio eletrónico associado ao sistema informático da empresa?

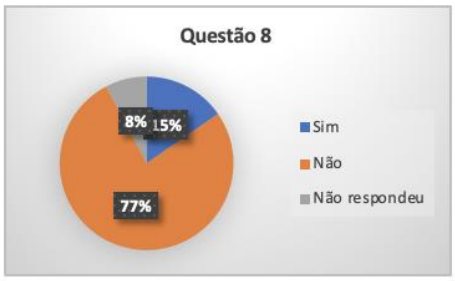
Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 10



8. Utiliza este mesmo endereço para assuntos pessoais?

Sim ☐ Não ☐



9. Apenas tem este endereço de correio eletrónico?

Sim ☐ Não ☐

Se respondeu **não**, quantos endereços de correio eletrónico possui?

1 ☐ 2 ou mais ☐

	Respostas
1	1
2 ou mais	8

10. Quando se ausenta da sua área de trabalho, sem ser no final do horário de trabalho, encerra a sessão?

Sim ☐ Não ☐

Se respondeu **não**, como deixa a sessão?

Se respondeu não, como deixa a sessão?
Sessão ativa
Suspensa
Suspensa
Não respondeu
Encerra automaticamente ao fim de alguns segundos

III - Procedimentos relativamente à utilização das Passwords

11. Possui password para acesso ao seu computador de trabalho e/ou ao sistema de informação da empresa?

Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 18

	Respostas
Sim	13
Não	0

12. A(s) password(s) permitem que tipo de acesso?

Apenas ao computador ☐
Apenas ao sistema de informação ☐
A ambos ☐

Se respondeu **a ambos**, a password é a mesma para as duas situações?

Sim ☐ Não ☐

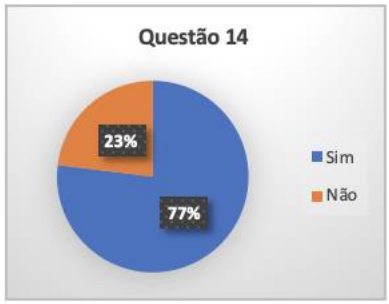
5

13. A(s) password(s) foram atribuídas pela empresa ou escolhida(s) por si?

Escolhida(s) por mim ☐ Atribuída(s) pela empresa ☐

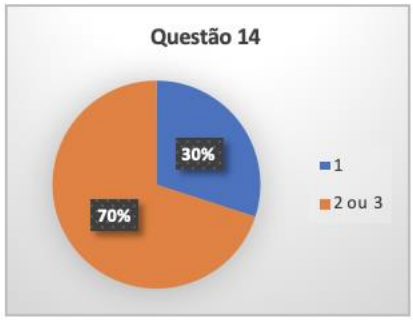
14. A(s) password(s) é(são) partilhada(s) com algum colega de trabalho?

Sim ☐ Não ☐



Se respondeu **sim**, com quantas pessoas?

1 ☐ 2 ou 3 ☐ Mais de 3 ☐



Qual o motivo dessa partilha? _____

Respostas	
Quando estou de férias	1
Quando estou de férias ou doente	1
É password de departamento	1
licenças	1
Férias	1
O mesmo departamento	1
Não respondeu	3

15. Já alterou a(s) password(s) de acesso?

Sim ☐ Não ☐

Se respondeu **sim**, com que frequência altera a(s) sua(s) password(s)?

Raramente ☐ Uma única vez ☐ Mensalmente ☐ Anualmente ☐

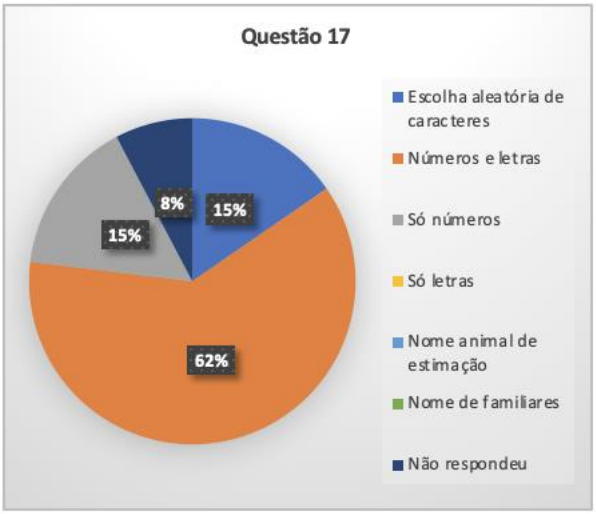
	Respostas
Raramente	2
Uma única vez	
Mensalmente	1
Anualmente	1
Não Respondeu	1

16. Qual o processo que utiliza para guardar a(s) sua(s) password(s)?

Memorização ☐ Post-it ☐ Outro ☐. Qual? _____

17. Que opções efetua na escolha da(s) sua(s) password(s)? (assinale todos os itens aplicáveis)

Escolha aleatória de caracteres ☐
Números e letras ☐
Só números ☐
Só letras ☐
Nome de animais de estimação ☐
Nome de familiares ☐



18. Tem acesso ás contas bancárias da empresa, através de password?

Sim ☐ Não ☐

	Respostas Questão 18
Sim	3
Não	10

19. A(s) password(s) de acesso às contas bancárias são partilhadas com algum colega de trabalho?

Sim ☐ Não ☐

	Respostas
Sim	3
Não	0

Se respondeu **sim**, com quantas pessoas partilha?

1 ☐ 2 ou 3 ☐ Mais de 3 ☐

	Respostas
1	
2 ou 3	3
Mais de 3	

Qual o motivo dessa partilha? _____

Respostas
O utilizador do site do banco é partilhado (No departamento)
Método incutido pela empresa
Não respondeu

20. A(s) password(s), de acesso às contas bancárias, que utiliza são de:

Acesso total às contas ☐ Acesso restrito ☐ Apenas consulta ☐

	Resposta
Acesso total ás contas	
Acesso restrito	3
Apenas consulta	

21. Qual o processo que utiliza para guardar a(s) password(s) de acesso às contas bancárias?

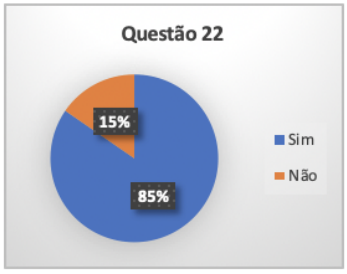
Memorização ☐ Post-it ☐ Outro ☐. Qual? _____

Respostas
Papel
Caderno
Não respondeu

IV - Segurança da Informação Confidencial da Empresa

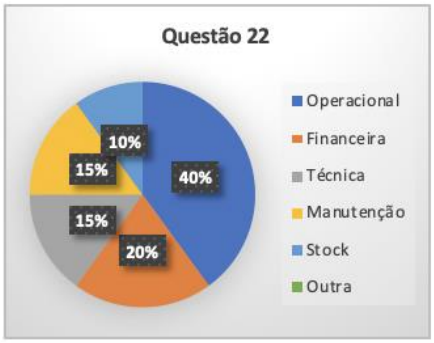
22. Para desempenho da sua função trabalha diretamente com informação necessária para a atividade da empresa?

Sim ☐ Não ☐



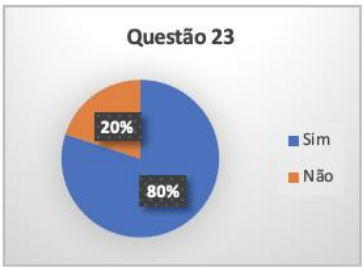
Se respondeu **sim**, de que tipo é essa informação? (selecionar todas as opções aplicáveis)

Operacional ☐
Financeira ☐
Técnica ☐
Manutenção ☐
Stock ☐
Outra ☐
Qual? _____



23. A informação selecionada na pergunta 22. é registada posteriormente no sistema de informação da empresa?

Sim ☐ Não ☐



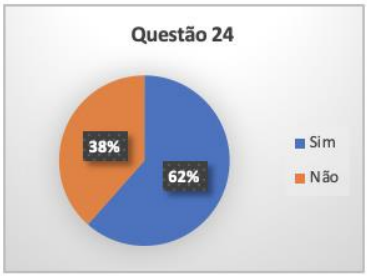
Se respondeu **sim**, quem regista? (indique a função da pessoa responsável por esta ação se não for o inquirido)

_____

Respostas
Gestor de Tráfego
Não respondeu
Administração

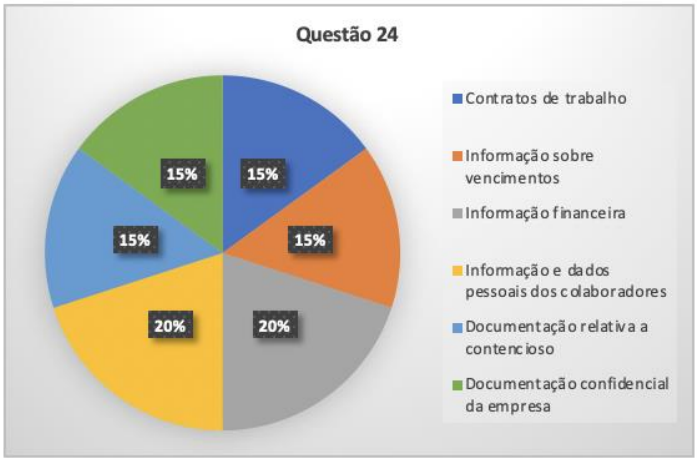
24. Para desempenho da sua função, trabalha com informação confidencial e/ou sensível (passwords bancárias, documentação financeira, dados dos colaboradores etc.)?

Sim ☐ Não ☐



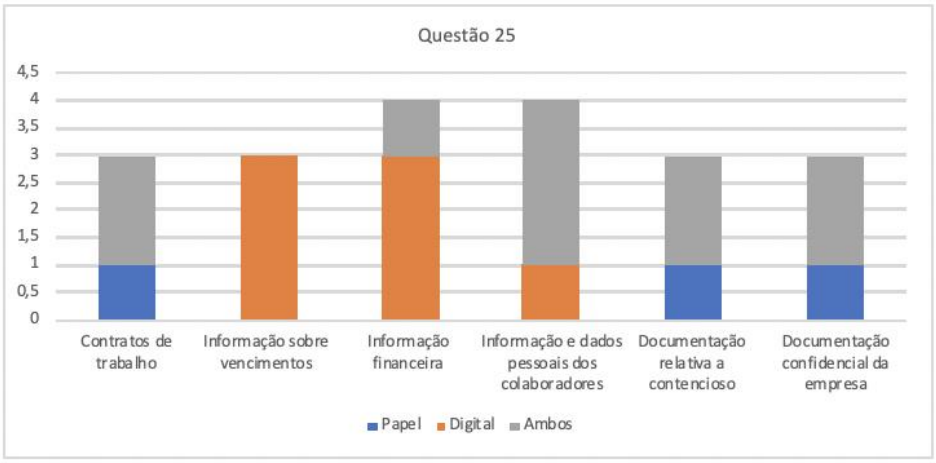
Se respondeu **sim**, que tipo de informação? (selecionar todas as opções aplicáveis)

Contratos de Trabalho ☐
Informação sobre vencimentos ☐
Informação Financeira ☐
Informações e dados pessoais dos colaboradores ☐
Documentação relativa a contencioso ☐
Documentação confidencial da empresa ☐
Outra ☐
Qual? _____



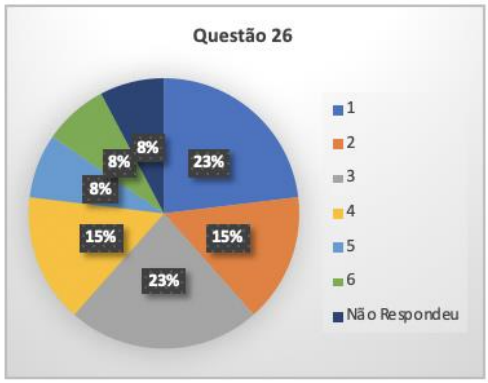
25. A informação selecionada na questão 24. Está em que formato?

	Papel	Digital	Ambos
Contratos de Trabalho	☐	☐	☐
Informação sobre vencimentos	☐	☐	☐
Informação Financeira	☐	☐	☐
Informações e dados pessoais dos colaboradores	☐	☐	☐
Documentação relativa a contencioso	☐	☐	☐
Documentação confidencial da empresa	☐	☐	☐
Outra	☐	☐	☐



26. Classifique a facilidade de acesso à informação em formato papel, pelos colaboradores não autorizados. (**6** para **muito fácil** e **1** para **muito difícil**)

1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐



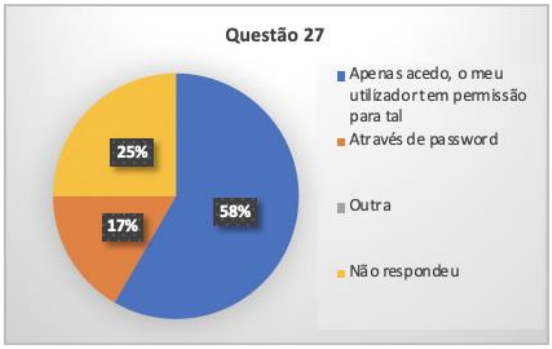
27. Se está em formato digital, qual o processo que realiza para aceder à informação?

Apenas acedo, o meu utilizador tem permissão para tal ☐

Através de Password ☐

Outra ☐

Qual? _____



12

V - Impressão de Documentos através do Sistema Informático

28. Possui acesso à impressão de documentos através do sistema informático da empresa?

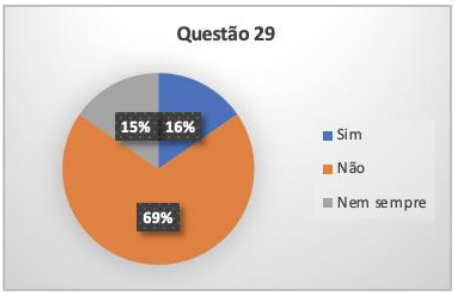
Sim ☐ Não ☐

Se respondeu **não**, avançar para a questão 34

	Respostas
Sim	13
Não	0

29. Essa impressão é efetuada em modo privado?

Sim ☐ Não ☐ Nem Sempre ☐



Se respondeu **sim**, avançar para a questão 33

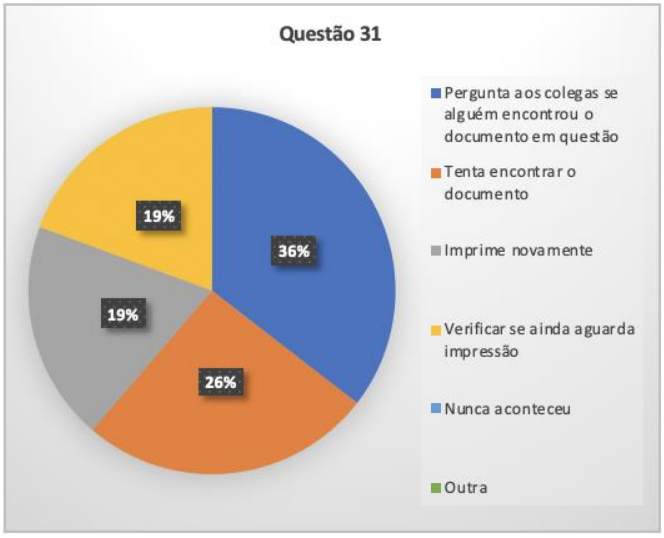
30. Depois de imprimir um documento saí do local de trabalho e vai buscar a impressão?

Sim ☐ Não ☐

Se respondeu **não**, como imprime?

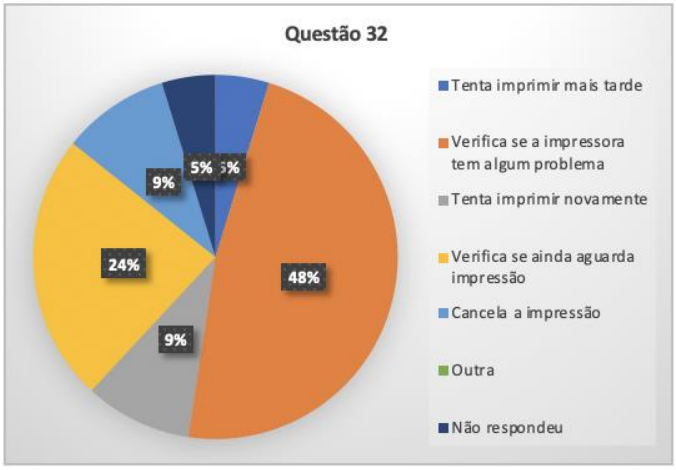
31. Que atitude toma quando não encontra os documentos que mandou imprimir na impressora? (selecionar todas as opções aplicáveis)

Pergunta aos colegas se alguém encontrou o documento em questão ☐
Tenta encontrar o documento ☐
Imprime novamente ☐
Verifica se ainda aguarda impressão ☐
Documentação relativa a contencioso ☐
Nunca aconteceu ☐
Outra ☐
Qual? _____



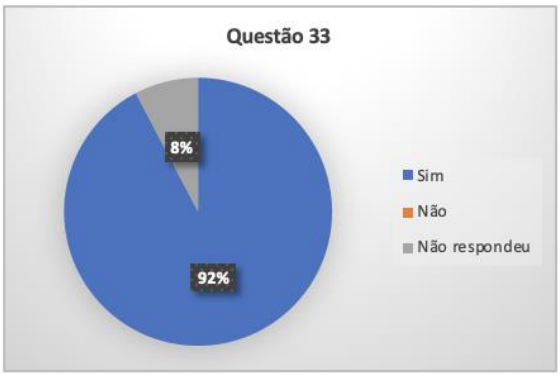
32. Quando não consegue imprimir documentos através da impressora qual a sua atitude? (assinale apenas uma das opções)

Tenta imprimir mais tarde ☐
Verifica se a impressora tem algum problema ☐
Tenta imprimir novamente ☐
Verifica se ainda aguarda impressão ☐
Cancela a impressão ☐
Outra ☐
Qual? _____



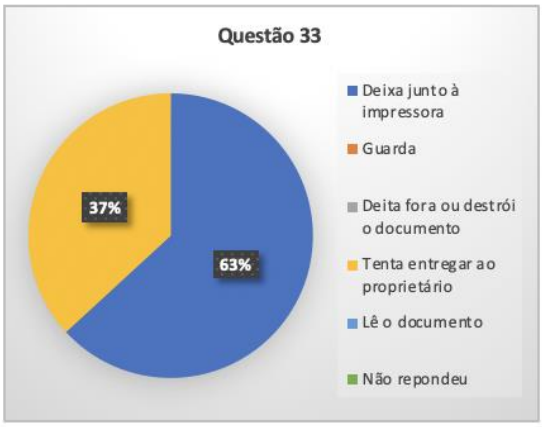
33. Já alguma vez encontrou documentos que não os seus na impressora partilhada da empresa?

Sim ☐ Não ☐



Se respondeu **sim**, que atitude tomou? (selecionar todas as opções aplicáveis)

Deixa junto à impressora ☐
Guarda ☐
Deita fora ou destrói o documento ☐
Tenta entregar ao proprietário ☐
Lê o documento ☐
Outra ☐
Qual? _____



VI - Questões Gerais sobre a Segurança do Sistema Informático

34. Já presenciou alguma violação da segurança do sistema informático da empresa (Por exemplo, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?

Sim ☐ Não ☐

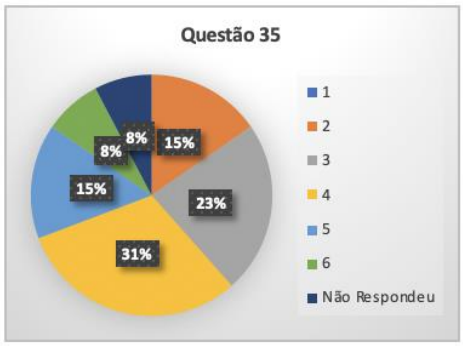
	Respostas
Sim	0
Não	13

Se respondeu **sim**, que atitude tomou quando presenciou essa violação?

Propôs medidas para a resolução do problema ☐
Informou a administração ☐
Advertiu o/(a) infrator(a) ☐
Outra ☐
Qual? _____

35. Na sua opinião, classifique o grau de segurança do sistema informático da empresa. (**6** para **elevado** e **1** para **baixo**)

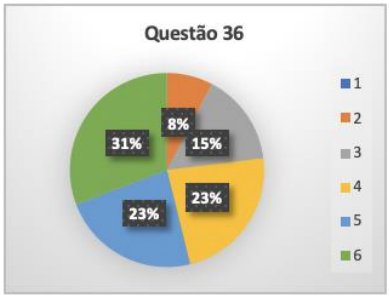
1	2	3	4	5	6
☐	☐	☐	☐	☐	☐



36. Classifique em que medida considera que a segurança do sistema informático é importante para o desempenho das suas funções diárias? (**6** para **muito importante** e **1** para **pouco importante**)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

Fim do questionário.
Obrigada pela colaboração!



Anexo III – Entrevista ao Diretor Geral

IPS Instituto Politécnico de Setúbal
Escola Superior de Ciências Empresariais

Entrevista ao Diretor Geral da TMS – Transportes & Logística, S.A

I – Apreciação Geral sobre a Postura da Empresa Relativamente à Segurança da Informação

1. Considera a informação um dos ativos da empresa?

Sim ☒ Não ☐

Se não, avançar para a questão 3

2. Se sim, qual o grau de importância? (6 para muito importante e 1 para pouco importante)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☒

3. Considera necessária a implementação de medidas para proteger a informação da empresa?

Sim ☒ Não ☐

Se respondeu não, avançar para questão 11

4. Se sim, porquê?

Porque a informação é importante! Alguma é confidencial e outra crítica à atividade da empresa. Pelo que deverá ser protegida.

5. A TMS dispõe de algum tipo de políticas (normas/regulamentos/regras/procedimentos) para garantir a segurança da informação?

Sim ☒ Não ☒ ← Não de forma estruturada

Se respondeu não, avançar para a questão 11

6. Se sim, quais?

Política de Backup da informação. Hierarquia de acessos à informação (rede dentro do ERP).

7. Há quanto tempo são implementadas as políticas (normas/regulamentos/regras/procedimentos) na empresa?

Desde 2004

8.Todos os colaboradores têm conhecimento das políticas?

Sim ☐ Não ☒

9. Se sim, de que forma? _____

10. Quem é o responsável pelo cumprimentos de todas as políticas (normas/regulamentos/regras/procedimentos) implementados? Que função exerce na empresa?

O responsável é externo. Outsourcing. Techouse – Assistência Técnica e Serviços, LDA

II- Acesso ao Sistema de Informação

Um **sistema de Informação (SI)** é um sistema constituído por pessoas, procedimentos e equipamentos que recolhe , processa, armazena e distribuí informação com objetivos específicos.

11. Quantos trabalhadores têm acesso ao Sistema de Informação da empresa?

18 no escritório, 4 na Portaria, 1 na Oficina e 1 no armazém do norte. Ou seja, ao todo 24 trabalhadores.

12. Classifique a facilidade de acesso físico ao sistema de informação da empresa (6 para muito difícil e 1 para muito fácil)

	1	2	3	4	5	6
Área circundante à empresa	☐	☐	☐	☐	☒	☐
Acesso ao edifício do escritório	☐	☒	☐	☐	☐	☐
Acesso ao armazém	☐	☐	☒	☐	☐	☐
Corredores e hall de entrada	☐	☒	☐	☐	☐	☐
Sala de servidor e arquivo	☐	☐	☐	☐	☒	☐
Salas de reunião	☐	☐	☐	☐	☐	☒
Salas da administração	☐	☐	☐	☐	☐	☒
Open Space onde acontecem as atividades operacionais	☐	☒	☐	☐	☐	☐

13. Nos locais onde tem acesso ao sistema informação da empresa, especifique que atividades estão proibidas?

Fumar ☒ | Efetuar download de ficheiros ☐ | Todas as anteriores ☐
Comer/Beber ☐ | Realizar cópias dos programas ☐ | Nenhuma das anteriores ☐
Realizar cópias dos documentos ☐ | Instalar/desinstalar software ☒

14. De que forma estão proibidas as atividades enunciadas na questão 13?

Senso Comum ☒ Políticas (normas/regulamentos/regras/procedimentos) ☐

III – Ligações – Rede da Empresa e acesso à Internet

15. Que tipo de conexão utiliza a empresa para aceder à Internet?

Fibra ótica ☒ ADSL ☐ Satélite ☐

16. Como é que a empresa faz a distribuição da internet?

Por cabo ☒ Wireless ☐ Ambos ☐

17. Relativamente ao tipo de servidor, qual ou quais são os tipos de servidores utilizados?

Impressão ☐
Web ☐
Bases de Dados ☒
Correio Eletrónico ☒
Programas ou Ficheiros ☒
Outro. Qual? ☐

_____

18. Que mecanismos (ferramentas e/ou software) utiliza para proteção dos computadores da empresa?

Firewall ☒
Antivírus ☒
Antispyware ☒
Bitlocker ☐
Outro. Qual? ☐

_____

19. Com que frequência atualiza esses mecanismos?

Sempre que existe uma atualização ☒
Sempre que possível ☐
Anualmente ☐
Nunca ☐

20. Existe correio eletrónico na empresa?

Sim ☒ Não ☐

Se não avançar para a questão 22

21. Se sim, existe implementado algum sistema de filtragem de mensagens de correio eletrónico?

Sim existe

Se sim, qual? Sei que existe mas não sei qual é.

IV – Acesso, Proteção, Manutenção e Assistência do Servidor

22. Existe alguém responsável pelo servidor (para além da administração da empresa)?

Sim ☒ Não ☐

Se não, avançar para a questão 31

23. Se sim, esse responsável é:

Interno ☐ Externo ☒ Ambos ☐

Se for externo, avançar para a questão 27

Se for Interno ou Ambos, avançar para a questão seguinte (24)

24. Se é Interno, que é e de quem depende (indique a função)?

_____

25. Qual o nível de responsabilidade?

Total ☐ Parcial ☐ % ___

26. Que tarefas lhe estão atribuídas?

_____

27. Se é Externo, quem é e de quem depende?

Techouse – Assistência Técnica e Serviços, LDA

28. Existe algum contrato celebrado com o responsável pelo servidor?

Sim ☒ Não ☐

Se não, avançar para a questão 31

29. Se sim, o que está acordado?

Proteção ☒
Assistência ☒
Manutenção ☒
Manutenção Preventiva ☒
Outro. Qual? ☐

_____

30. Qual a validade do contrato? Renova automaticamente?

Renova automaticamente

31. Como fica assegurada a proteção, manutenção e assistência do servidor?

Procedimentos definidos pelo fornecedor

V – Cópias de Segurança

32. São realizadas cópias de segurança do sistema?

Sim ☒ Não ☐

Se respondeu não, avançar para a questão 46

33. Se sim, qual a sua periodicidade?

Diariamente (incrementais) e Semanalmente (Totais)

34. Existe algum responsável pela gestão das cópias de segurança?

Sim ☒ Não ☐

Se não avançar para a questão 46

35. Se sim, esse responsável é:

Interno ☐ Externo ☒

36. Se é interno, quem é e de quem depende?

_____

37. Como é realizado todo o processo de gestão das cópias de segurança pelo responsável interno?

_____

_____

38. Se é externo, quem é e de quem depende?

Techouse – Assistência Técnica e Serviços, LDA

39. Existe algum contrato relacionado com a gestão das cópias de segurança?

Sim ☒ Não ☐

Se não, avançar para a questão 42

40. Se sim, o que está acordado?

Armazenamento das cópias de segurança ☒ **Onde?** Sítiu remoto (Servidor NAS)

Periodicidade das cópias de segurança ☒ **Com que frequência?** Diariamente (incrementais) e semanalmente (totais)

Manutenção de todo o equipamento ☒ **Que equipamento?** Todo

Outra ☐ Qual?_____

41. Qual a validade do contrato? Renova automaticamente?

Renova automaticamente

42. Existiu algum incidente provocado pela falta de manutenção e/ou assistência do responsável pela gestão das cópias de segurança?

Sim ☒ Não ☐

Se não, avançar para a questão 46

43. Se sim, esses incidentes foram graves?

Sim ☒ Não ☐

Se não, avançar para a questão 45

44. Se sim, numa escala de 1 a 6 classifique a gravidade desse incidente (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☒

45. Mencione os principais danos causados pelo incidente?

Perca total de informação de gestão. Entre junho de N-1 e Abril do ano N

VI – Gestão de Acessos ao Sistema Informático

Sistema Informático é a parte automatizada do sistema de informação. Ou seja, executa e processa todas as tarefas recorrendo às tecnologias da informação e comunicação.

46. Existe algum responsável pela atribuição de acessos ao sistema de informação da empresa?

Sim ☒ Não ☐

Se não, avançar para a questão 50

47. Se sim, quem é e de quem depende?

Quem define é a TMS mas quem executa é a Techouse.

48. Que tipo de acessos são atribuídos aos colaboradores?

Rede da Empresa ☒
Conta de email da empresa ☒
Linha telefónica ☒
Outra. Qual? ☐

_____

49. Como é efetuada a atribuição de acessos?

Perfil de utilizador ☒
Pessoa Individual ☐
Outro. Qual? ☐

_____

50. Existe algum ERP (Enterprise Resource Planning) na empresa?

Sim ☒ Não ☐

Se não, avançar para a questão 57

51. Se sim qual é?

Microsoft Dynamics NAV

52. Alguém está responsável pela atribuição de acessos ao ERP da empresa?

Sim ☒ Não ☐

Se não avançar para a questão 54

53. Se sim, quem é e de quem depende?

Diretor Geral

54. Como é efetuada a atribuição de acessos ao ERP?

5

Perfil de utilizador ☒
Pessoa Individual ☐
Outro. Qual? ☐

---

55. Relativamente à informação confidencial (documentação financeira, dados dos colaboradores etc.) contida no sistema da empresa, existe algum tipo de cuidados especiais na atribuição de acessos?

Sim ☒ Não ☐

Se não, avançar para a questão 57

56. Se sim, quais?

Permissões definidas no perfil de utilizador

VII – Acessos ao Edifício Principal da Empresa[1]

57. As entradas e saídas do edifício são registadas e/ou controladas?

Sim ☒ Não ☐

Se não avançar para a questão 64

58. Se sim, qual o método utilizado para registar e/ou controlar as entradas e saídas do edifício da empresa?

Cartão com ID do colaborador ☒
Impressão digital ☐
Código alfanumérico ☐
Outra. Qual? ☐

---

59. O método identificado é individual ou coletivo?

Individual ☒ Coletivo ☐

60. Existe algum responsável pela atribuição de acessos ao edifício, de acordo com o método de controlo de entradas e saídas da empresa?

Sim ☒ Não ☐

Se não avançar para a questão 62

61. Se sim, como é efetuada a atribuição de acessos?

Perfil de utilizador ☒
Pessoa Individual ☐
Outro. Qual? ☐

---

62. A informação recolhida pelo método utilizado fica registada?

Sim ☒ Não ☐

Se não, avançar para a questão 64

63. Se sim, onde fica armazenada?

No servidor.

64. Existe horário noturno na TMS?

---

[1] Edifício onde acontece toda a atividade administrativa, financeira e operacional da empresa. Contem os escritórios da administração e das restantes chefias bem como o armazém, ponte de ligação com a atividade de armazenagem e distribuição desempenhada pela empresa.

Sim ☒ Não ☐

Se não, avançar para questão 69

65. Se sim, os trabalhadores têm acesso ao escritório durante o horário noturno?

Sim ☐ Não ☒ ← Apenas o responsável do armazém

66. Se sim, acesso total ou parcial?

Total ☒ Parcial ☐

Se total, avançar para a questão 68

67. Se parcial, em que sentido, quais as restrições impostas?

_____

68. Para que finalidade?

Fotocópia de documentação.

VIII – Acessos ao Logipark[2]

69. Existe registo das entradas e saídas do Logipark?

Sim ☒ Não ☐

Se não, avançar para a questão 75

70. Se sim, quem é o responsável pelo registo?

O vigilante da portaria e o sistema eletrónico de controlo de entradas e saídas.

71. Qual o método utilizado para registar e/ou controlar as entradas e saídas do Logipark?

Para além do cartão com o ID da pessoa autorizada a entrar nas instalações contamos também com o controlo presencial do vigilante

72. Essa informação está correta e atual?

Sim ☒ Não ☐ Não sei ☐

73. A informação recolhida pelo método utilizado fica registada na rede da empresa?

Sim ☒ Não ☐

Se sim avançar para a questão 75

74. Se não, onde fica armazenada?

_____

IX – Segurança do perímetro do Logipark[2]

75. Existe algum responsável pela segurança do perímetro do logipark?

Sim ☒ Não ☐

Se não, avançar para a questão 79

76. Se sim, esse responsável é:

Interno ☐ Externo ☒

77. Se for interno, quem é e de quem depende?

_____

Se for externo, quem é e de quem depende?

Augusto Carvalho Unipessoal, LDA, empresa de outsourcing que comtempla os serviços de portaria e vigilância de todo o Logipark

_____

[2] Logipark é a denominação dada ao complexo logístico da TMS. Este é composto por uma oficina, o edifico principal dos escritórios, o armazém, local de lavagem de viaturas, parqueamento e portaria.

78. Que funções executa para garantir a segurança?

Vigilância do perímetro ☒
Controlo de entradas e saídas ☒
Serviço de portaria ☒
Triagem do pessoal autorizado ☒
Outro. Qual? ☐

_____

79. Existe alguma/as empresa/s de outsourcing que frequente o logipark?

Sim ☒ Não ☐

Se não, fim da entrevista.

80. Se sim, para que finalidade?

Limpeza, manutenção e controlo de pragas

81. Se sim, com que periodicidade?

Mensalmente ☐
Semanalmente ☐
Diariamente ☒
Ocasionalmente ☐
Raramente ☐

82. As empresas de outsoucing têm algum acesso privilegiado?

Sim ☐ Não ☐ Apenas algumas ☒

83. Se sim ou apenas algumas, quais?

Limpeza (acesso total a todo o edifício além de ter chave da empresa para limpar aos fins-de-semana) e manutenção (acesso parcial, apenas a algum equipamento informático e sempre ou quase sempre em dias de semana)

84. E de que forma?

Chave ☒
Autorização para ☒
Outra. Qual? ☐

_____

Obrigada pela colaboração!

Anexo IV – Política de Passwords

Política de Passwords – TMS – Transportes & Logística, S.A

Objetivo:

O objetivo da presente política é assegurar que todas as passwords da empresa cumpram os requisitos para garantir a confidencialidade, integridade e disponibilidade da informação presente no sistema de informação.

Aplicabilidade:

Esta política destina-se a todos os colaboradores da TMS – Transportes & Logística, S.A que tenham necessidade de usar, criar ou atualizar as suas passwords organizacionais.

Documentos de referência:

ISO/IEC 27000:2014

ISO/IEC 27001:2013

ISO/IEC 27002:2013

Diretrizes:

Passwords gerais:

1. As passwords dos colaboradores são pessoais e intransmissíveis, sendo a garantia de identidade assegurada pela posse de um segredo detido por cada utilizador;
2. As passwords nunca devem ser partilhadas, mesmo entre colegas ou chefias;
3. As passwords não devem ser reveladas ou enviadas eletronicamente;
4. As passwords utilizadas para acesso aos sistemas e software da empresa não devem ser partilhadas entre sistemas ou similares às usadas em contas pessoais;
5. As passwords não devem ser escritas ou guardadas fisicamente no escritório;
6. Está proibido a opção “guardar password” em sites e aplicações;
7. O utilizador, colaborador da empresa, é que escolhe qual será a sua password;

8. As passwords dos utilizadores devem ser alteradas a cada 90 dias, sem possibilidade de utilização das últimas três anteriores;
9. Todas as passwords criadas devem ser fortes: Longas, complexas e incluir letras, números e caracteres especiais;
10. Tamanho mínimo da password para a generalidade dos utilizadores – 8 caracteres;
11. Tamanho máximo da password para a generalidade dos utilizadores – 12 caracteres;
12. Número de tentativas antes de bloqueio – 20;
13. Duração do bloqueio da conta 20 minutos;
14. As passwords são gravadas centralmente de forma cifrada, sendo do conhecimento exclusivo de cada utilizador.

Passwords da administração:

Todos os pontos anteriores são aplicáveis, contudo, relativamente aos critérios de atualização/criação de novas passwords para a administração existem algumas diferenças.

Todas as passwords criadas devem ser fortes: Longas, complexas e incluir letras, números e caracteres especiais;

1. Tamanho mínimo das passwords para a administração – 10 caracteres;
2. Tamanho máximo das passwords para a administração – 18 caracteres;
3. Número de tentativas antes de bloqueio – 10;
4. Duração do bloqueio da conta 40 minutos.

Passwords bancárias:

1. As passwords de acesso ás contas bancárias dos colaboradores são pessoais e intransmissíveis, sendo a garantia de identidade assegurada pela posse de um segredo detido por cada utilizador;
2. As passwords nunca devem ser partilhadas, mesmo entre colegas ou chefias;
3. As passwords não devem ser reveladas ou enviadas eletronicamente;
4. As passwords não devem ser escritas ou guardadas fisicamente no escritório;

5. Está proibido a opção “guardar password” no site da instituições bancárias;
6. O utilizador, colaborador da empresa, terá de escolher a sua password de acordo com as regras de segurança da instituição bancária;
7. As passwords dos utilizadores devem ser alteradas de acordo com as regras de segurança da instituição bancária;

Incumprimento:

O não cumprimento da presente política fará com que existam sanções estipuladas pela administração da empresa.

Anexo V – Política de Impressão

Política de Impressão – TMS – Transportes & Logística, S.A

Objetivo:

O objetivo da presente política é assegurar a confidencialidade e disponibilidade da informação impressa através do sistema de informação da empresa.

Aplicabilidade:

Esta política destina-se a todos os colaboradores da TMS – Transportes & Logística, S.A que efetuem impressões de documentação através do sistema de informação da empresa.

Documentos de referência:

ISO/IEC 27000:2014

ISO/IEC 27001:2013

ISO/IEC 27002:2013

Diretrizes:

Com a função de impressão privada, é possível encriptar e proteger, com uma palavra-passe, documentação da empresa.

Os colaboradores terão de escolher uma palavra-passe, à priori, para proteção da documentação que têm intenção de imprimir, depois terão de memorizar esse código e digitá-lo no painel da impressora, identificando a documentação como sua. Depois de digitado e autentificado o código, a documentação poderá ser desbloqueada para impressão.

1. A impressão de documentação através do sistema de informação da empresa terá de ser efetuada em modo privado;
2. As passwords de desbloqueio de impressão são pessoais e intransmissíveis;
3. Os colaboradores é que escolhem qual será a password de desbloqueio de impressão;

4. Enquanto a impressão da documentação não estiver concluída os colaboradores da empresa não poderão se ausentar de perto da impressora;
5. Assim que a impressão estiver concluída levar a documentação para o local devido;
6. Não deixar a documentação no tabuleiro da impressora;
7. Em caso de se encontrar documentação que não pertença ao colaborador que mandou imprimir devolver ao destinatário;
8. Se a impressora bloquear a impressão devido a um problema técnico da mesma, tentar resolver (falta de papel, folhas encravadas, falta de tinta nos tinteiros, problemas fáceis de resolver sem ser necessários conhecimentos técnicos sobre o equipamento) e aguardar que a impressão finalize;
9. A digitalização de documentação é efetuada presencialmente pelo colaborador que tem acesso à informação contida no documento;
10. A cópia de documentação é efetuada presencialmente pelo colaborador que tem acesso à informação contida no documento.

Incumprimento:

O não cumprimento da presente política e a negligência do tratamento da informação fará com que existam sanções estipuladas pela administração da empresa.

Anexo VI – Política de utilização de hardware e software

Política de Utilização de Hardware e Software

Objetivo:

O objetivo desta política é garantir a segurança do sistema de informação da empresa, nomeadamente, contra as ações dos colaboradores relativamente ao uso do software e hardware para a realização das suas funções diárias.

Aplicabilidade:

Esta política destina-se a todos os colaboradores da TMS – Transportes & Logística, S.A que utilizem o software e o hardware da empresa.

Documentos de referência:

ISO/IEC 27000:2014

ISO/IEC 27001:2013

ISO/IEC 27002:2013

Restrições/Diretrizes:

Utilização do Hardware:

1. Os colaboradores apenas poderão utilizar o hardware que a empresa indicar como sendo necessário para desempenhar a função para a qual foram contratados;
2. Durante o uso deverão preservar os equipamentos;
3. Não podem mudar os equipamentos de lugar sem autorização;
4. Estão proibidas atividades como, fumar, beber e comer perto do hardware de modo a assegurar a preservação do mesmo;
5. Não colocar pens USB ou CD's pessoais no hardware da empresa;
6. Desligar sempre os equipamentos quando terminar a sua tarefa diária.

Utilização do Software:

1. Apenas os colaboradores autorizados deverão instalar ou desinstalar software;
2. Apenas e só se pode instalar software nas máquinas para uso profissional;
3. Os colaboradores não podem baixar software da Internet ou trazer software de casa sem autorização;
4. Os colaboradores não podem efetuar cópia do software instalado sem autorização.

Incumprimento:

O não cumprimento da presente política e a negligência do uso e da preservação do equipamento e software informático fará com que existam sanções estipuladas pela administração da empresa.