P.PORTO
ISCAP

# GESTÃO DE RISCOS DE SISTEMAS DE INFORMAÇÃO

## SAFE INSIDE – ESTUDO DE CASO

PÓS GRADUAÇÃO DOS SISTEMAS DE INFORMAÇÃO EMPRESARIAIS

SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Maio 2020

BRUNA TOMÉ · 12190209 JOÃO PEREIRA · 12190211 RUI RIBEIRO · 6940007

# ÍNDICE DA APRESENTAÇÃO


*«Risco é a possibilidade de sofrer perdas, reduzindo o valor do negócio»*

(Blakley, McDermott, & Geer, 2001; Williams, Ambrose, Bentrem, & Merendino, 2004)

# Introdução

As organizações não podem eliminar totalmente os riscos a que os seus SI/TIC estão sujeitos, pelo que um dos principais desafios dos seus gestores é **reduzir os riscos da segurança da informação** para um **nível aceitável** e de acordo com a **cultura de risco da organização**.

Este trabalho apresenta a da **gestão do risco da segurança informação**, de uma pequena e média empresa (PME) fictícia, criada no âmbito das disciplinas de Gestão Comercial e de Gestão Financeira do curso de Pós Graduação em Sistemas de Informação.

O objetivo principal desta apresentação é **demonstrar os conhecimentos adquiridos no ciclo de vida da gestão do risco de uma organização**, nomeadamente o conceito de risco dos sistemas de informação, a gestão desses riscos e as diferentes abordagens à gestão do risco.

# SAFE INSIDE

## Apresentação da Empresa

Uma ideia de negócio inovadora aplicada ao ensino da condução, assistido por inteligência artificial.

# SAFE INSIDE

A SAFE INSIDE é a única empresa nacional a oferecer uma **experiência de condução controlada** e personalizada aos mais variados fins, tendo por base a utilização de tecnologias de ponta como a **telemetria** e a **inteligência artificial**.

Tanto as **viaturas** como os **utilizadores** estão munidos de **sensores** que recolhem informação em tempo real, e que em conjunto com um sistema de **CCTV** de ponta e outros meios de **recolha de imagem** processam toda a atividade e sugerem, quando necessário, **correções e melhorias** com vista a uma experiência de condução defensiva inesquecível.

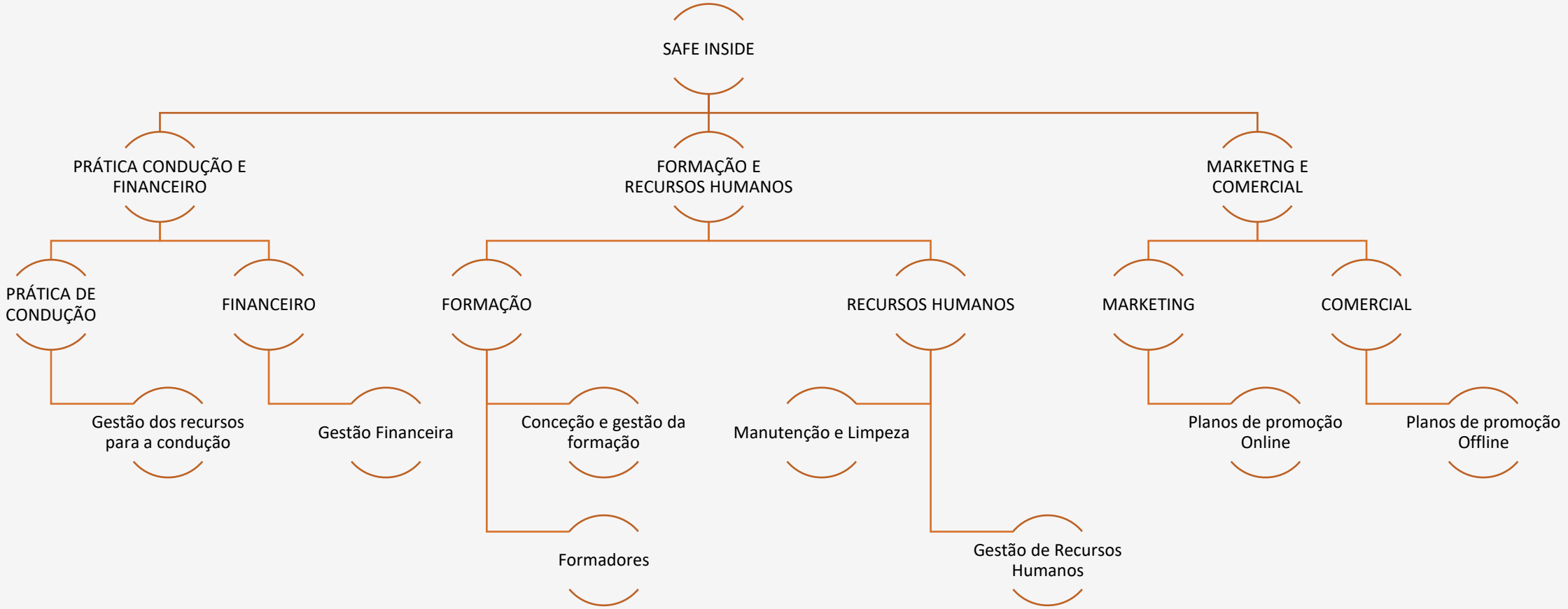
# MISSÃO:

Contribuir ativamente para a redução dos acidentes rodoviários, através da formação de condutores mais conscientes e com uma atitude defensiva. Educar para o civismo e segurança na estrada, dos 8 aos 80, através de uma abordagem lúdica e amiga do ambiente, em prol de um futuro mais seguro e sustentável.

# VISÃO:

Ser a referência em experiências de condução em ambiente controlado, contribuindo para o sucesso e segurança dos nossos clientes através de uma metodologia inovadora, promotora de destreza e autoconfiança. Trabalhar com e em prol da comunidade, defendendo e transmitindo uma atitude cívica, defensiva e amiga do ambiente em tudo quanto esteja relacionado com a condução de veículos motorizados.

# SAFE INSIDE


SAFE INSIDE
PRÁTICA CONDUÇÃO E FINANCEIRO
FORMAÇÃO E RECURSOS HUMANOS
MARKETNG E COMERCIAL
PRÁTICA DE CONDUÇÃO
FINANCEIRO
FORMAÇÃO
RECURSOS HUMANOS
MARKETING
COMERCIAL
Gestão dos recursos para a condução
Gestão Financeira
Conceção e gestão da formação
Formadores
Manutenção e Limpeza
Gestão de Recursos Humanos
Planos de promoção Online
Planos de promoção Offline

# SAFE INSIDE

A SAFE INSIDE **não tem Departamento de Gestão de Sistemas de Informação**, sendo que todas as tarefas inerentes ao desenvolvimento de aplicações, administração de sistemas, comunicações e *helpdesk* são efetuadas em ***outsourcing*** por diversos fornecedores.

A gestão dos contratos de TI e de assuntos relacionados com a presença online e de redes socias da organização, é efetuada pelo **CISO** que acumula funções de gestão comercial e *marketing*.

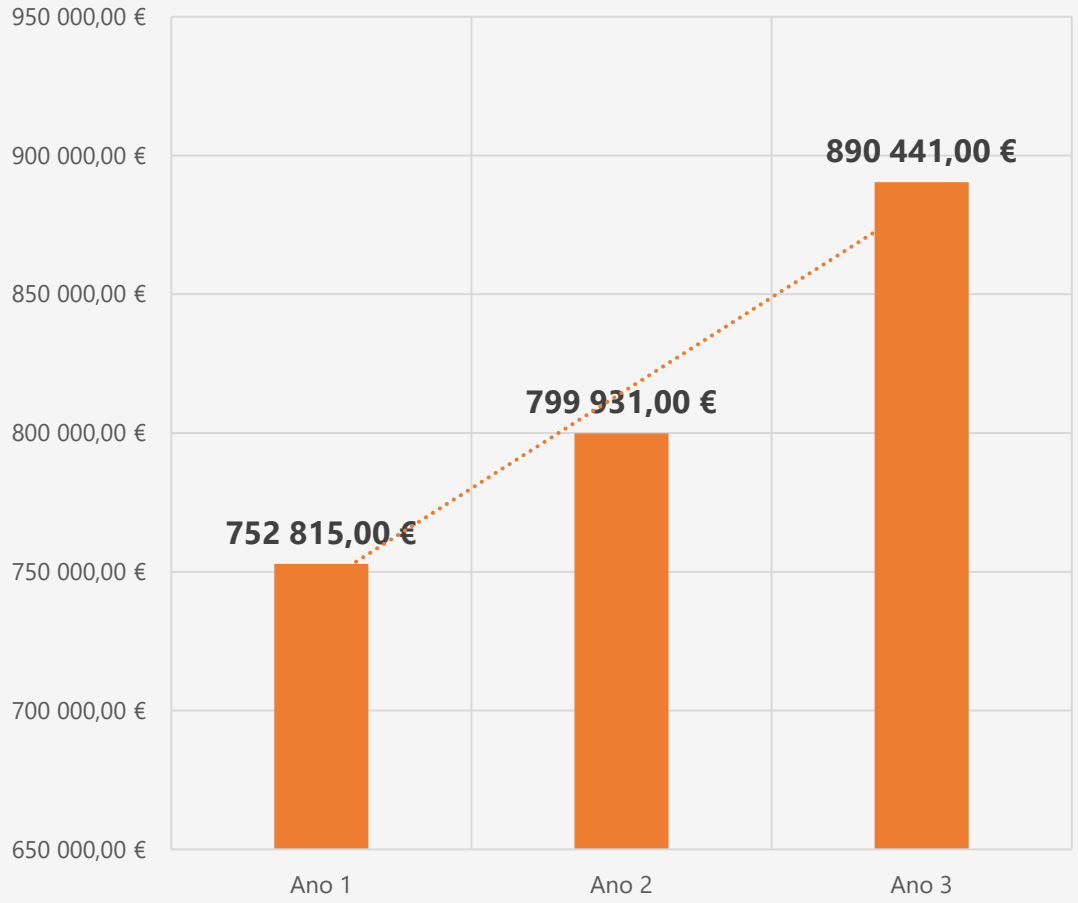
# SAFE INSIDE


SAFE INSIDE

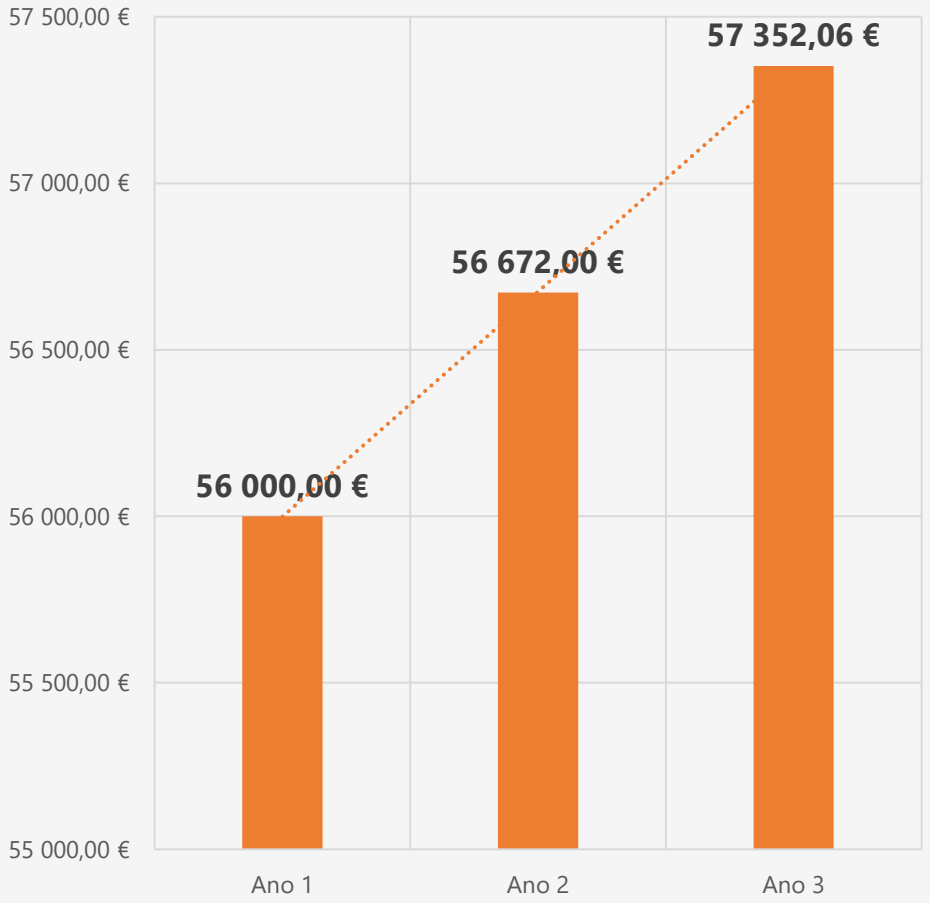
- Sediada no Porto
- 30.000m$^2$
- Excelentes acessibilidades
- 5 automóveis híbridos
- 3 motociclos
- 2 quadriciclos
- 4 salas
- Bar

# SAFE INSIDE

## Volume de Negócios




## Outros Rendimentos



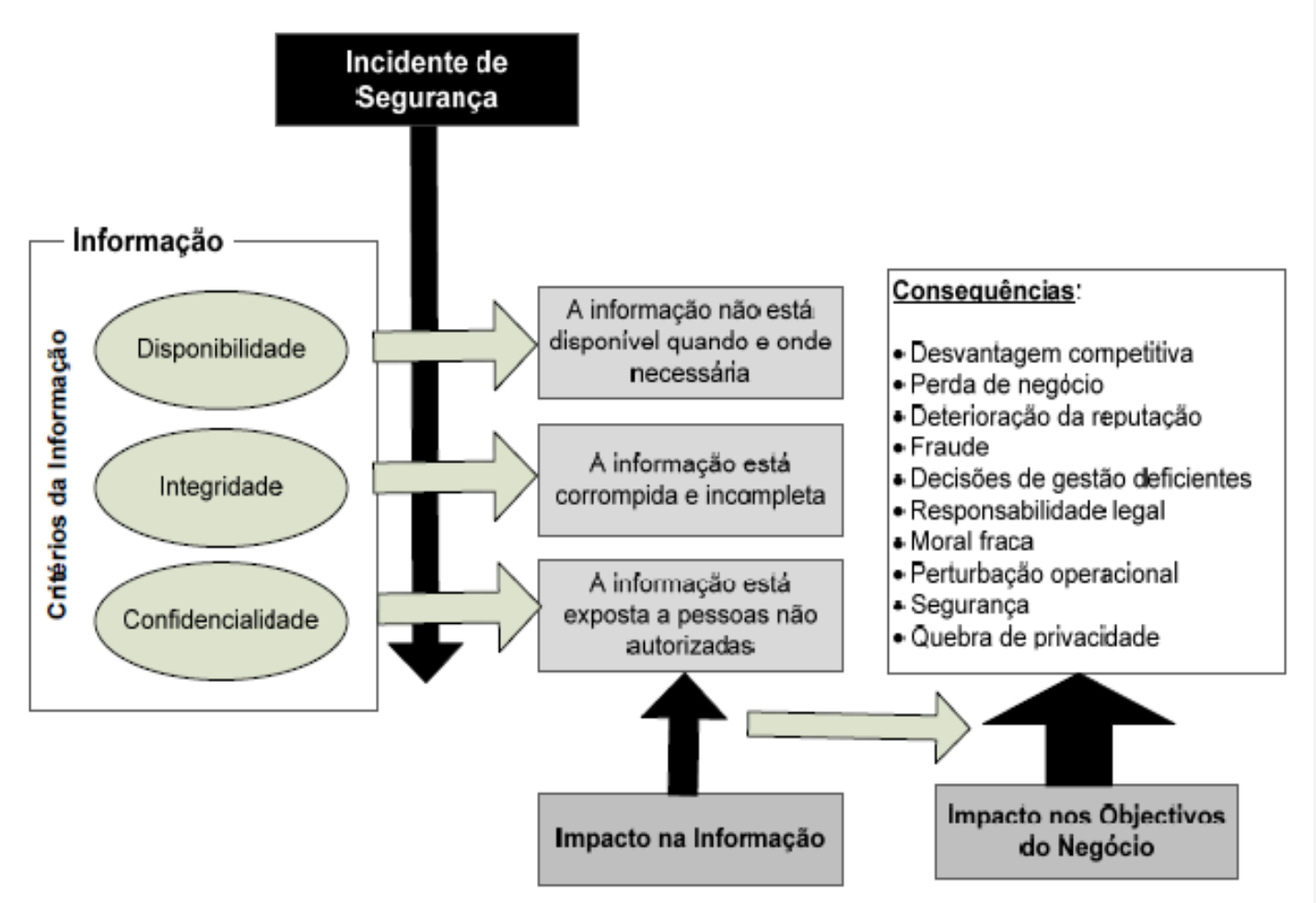
# GESTÃO DE RISCO

A informação é um dos ativos fundamentais das pequenas e médias empresas (PMEs). A proteção da informação pelos gestores destas empresas assume-se como um desafio primordial para assegurar a sua competitividade numa economia globalizada e bastante competitiva.

# Introdução

Os incidentes de segurança da informação são eventos imprevistos que têm uma elevada probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação, os quais têm origem, nas vulnerabilidades dos sistemas operativos, abuso das contas ou permissões válidas de utilizadores e erros não intencionais.

**Ao comprometer a disponibilidade, integridade e confidencialidade da informação, os incidentes de segurança, podem ter consequências desastrosas nos objetivos do negócio.**

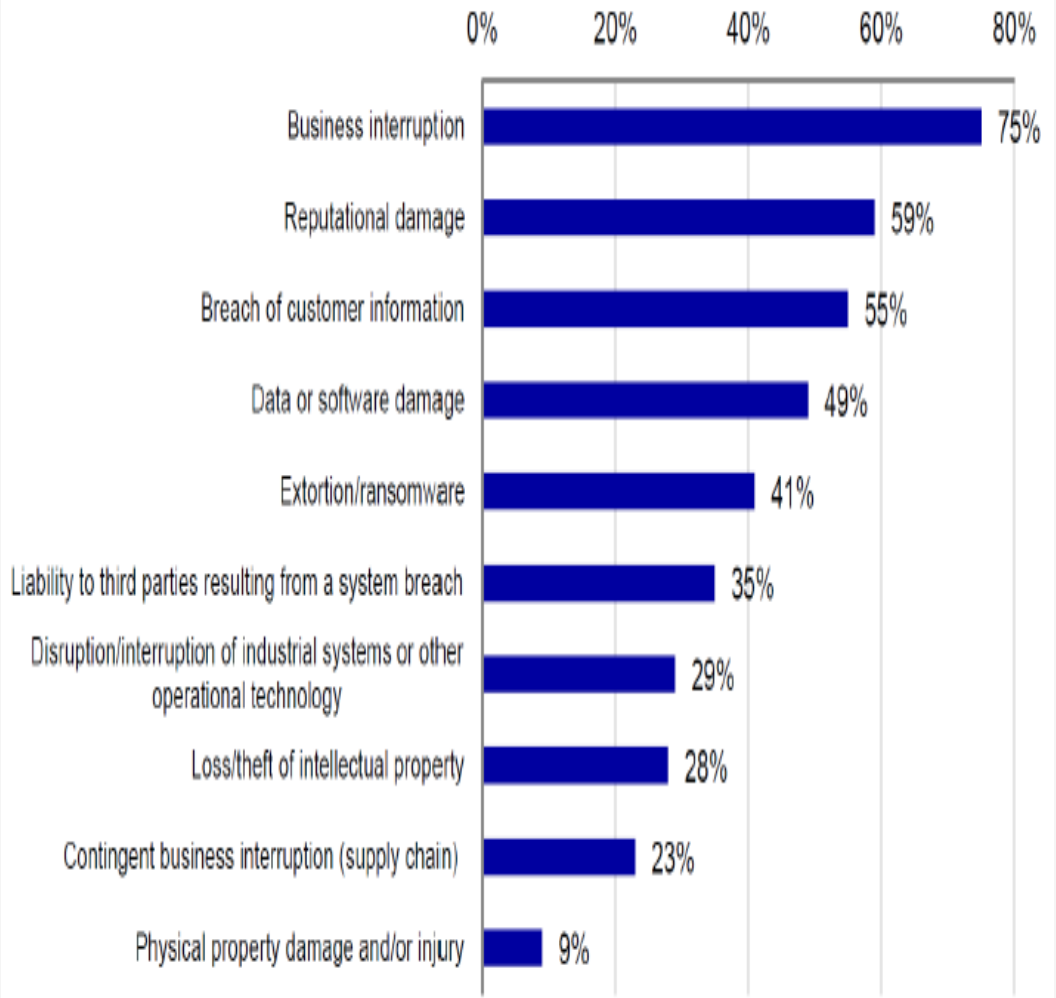


# GESTÃO DE RISCO

Um dos **maiores ativos** de uma organização são os **dados dos clientes,** pois através destes **as políticas e objetivos da empresa são planeados e alargados**.

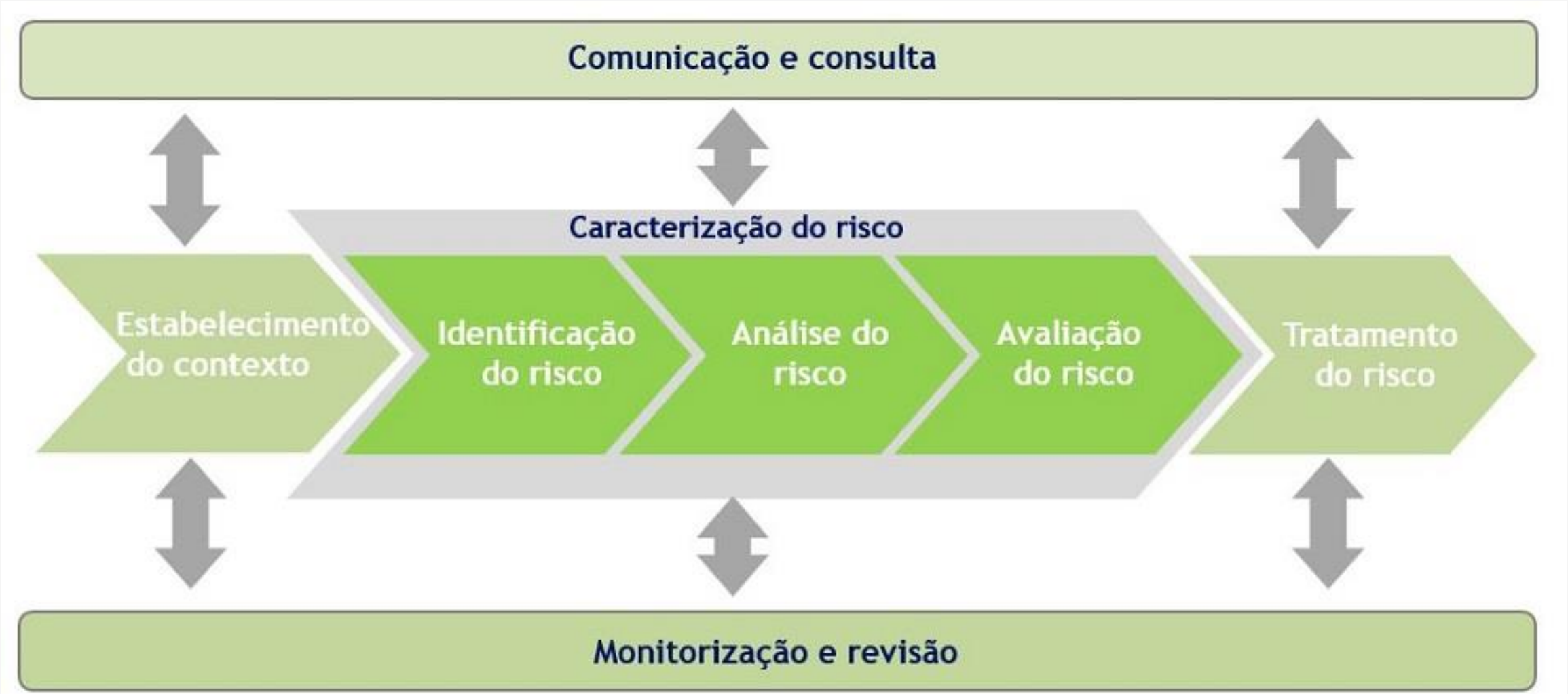
A **fuga de informação** representa **graves perdas** de uma instituição, cujos danos vão desde **perda de reputação ao afastamento de clientes, parceiros e até mesmo colaboradores, processos jurídicos e danos financeiros**.

Assim, **a utilização de palavras-passe fortes**, com **regras rígidas para a sua gestão**, do conhecimento de toda a empresa é importante para manter a Segurança da Informação.




**Fonte:** Marsh and Microsoft Cyber perception survey – Cybersecurity - Nordea (2018)

# GESTÃO DE RISCO | Metodologia



# GESTÃO DE RISCO | Identificação

**No processo de gestão de risco foi identificada a seguinte situação:**

**Existe uma possibilidade de roubo das palavras-passe dos utilizadores da plataforma de Enterprise Resource Planning (ERP)**, alojada num serviço de computação em ***cloud*** (nos servidores do fornecedor do aplicativo), que é utilizada pela organização para **gestão** e **disponibilização** de toda a documentação gerada no âmbito da **execução da sua atividade**, nomeadamente no que diz respeito aos processos Comercial, Financeiro, Documental e Estratégico.

# GESTÃO DE RISCO | Identificação

**O risco identificado, teve por base:**

- A experiência na utilização da plataforma é indicativa de que o seu fornecedor não tem uma política de palavras-passe alinhada com as práticas internas da organização;
- O conhecimento de que outro cliente da plataforma foi alvo de um ataque malicioso.

Durante este processo, identificou-se que a ameaça poderia ter efetivamente **origem num ataque malicioso externo**, levado a cabo tirando partido da **vulnerabilidade de uma política deficiente de palavras-passe**, e constatou-se que este **vetor de ataque poderia colocar em causa a confidencialidade, integridade e disponibilidade** da informação que se encontrava alojada neste ativo.

# GESTÃO DE RISCO | Análise

**Nos critérios de aferição do impacto do risco, foram observadas as seguintes dimensões:**

**Reputação** – A ocorrência do risco identificado pode colocar em causa a reputação da organização (por exemplo: perda de confiança de partes interessadas);

**Legal** – A ocorrência do risco identificado poderá colocar em causa responsabilidades legais e/ou regulatórias da organização (por exemplo: responsabilidades regulatórias sectoriais, regulamento de proteção de dados);

**Serviço a clientes** – A ocorrência do risco identificado poderá colocar em causa o serviço prestado aos clientes da organização (por exemplo: SLA, incumprimento de um nível de serviço, indisponibilidade do sistema);

**Financeiro** – A ocorrência do risco identificado pode levar a que a organização possa incorrer em custos financeiros não previstos (por exemplo: coimas, recursos adicionais para resolução do problema).

# GESTÃO DE RISCO | Análise

Relativamente aos critérios de aferição da **probabilidade de ocorrência do risco**, foram observadas as seguintes dimensões:

- Experiência e estatísticas aplicáveis para a probabilidade de ameaça;
- A motivação e as capacidades que mudam com o tempo e os recursos disponíveis para um possível atacante, bem como a perceção de atratividade e da vulnerabilidade dos ativos para um possível atacante;

**Com base nesta análise, determinou-se que a probabilidade do risco ocorrer é Alta.**

# GESTÃO DE RISCO | Avaliação

A **avaliação de impacto** foi efetuada com base na matriz sistematizada na metodologia do risco da organização:

1 – Pequeno, 2 – Moderado, 3 – Elevado, 4 – Catastrófico

Um impacto

**"4 – Catastrófico"**

no risco em causa

# GESTÃO DE RISCO | Avaliação

De seguida, efetuou-se o exercício de avaliação da **probabilidade** de o risco ocorrer. Consultada a metodologia e face às possibilidades apresentadas:

1 – Improvável, 2 – Provável, 3 – Muito Provável, 4 – Quase certa

A probabilidade seria

**"4 – Quase certa"**

# GESTÃO DE RISCO | Avaliação

Calculou-se com base no produto do **impacto pela probabilidade**, o nível do risco

**(A = I * P)**

Tendo por base os critérios de identificação do nível do risco da tabela de níveis:

- **[1 a 2] – Nível baixo**
- **[3 a 6] – Nível Médio**
- **[8 a 12] – Alto**
- **[16] – Muito Alto**

Concluiu-se que o nível de risco é

**16**

Sendo este

**Muito Alto**

Face ao nível identificado, a organização **não o pode aceitar**, uma vez que todos os riscos de nível "**Muito Alto**" devem **ser obrigatoriamente tratados**, exceto se tiverem sido formalmente aceites pela Gestão de Topo.

# GESTÃO DE RISCO | Tratamento

No âmbito do processo de tratamento do risco, procedemos á seleção da opção mais adequada e à identificação dos controlos que possam ser implementados para **mitigar**, **evitar**, ou **transferir** o risco.

No caso em concreto do risco identificado, a opção mais adequada foi a de **mitigar o risco**, ou seja, reduzir a probabilidade e/ou impacto de um evento adverso para limites aceitáveis, através de implementação de controlos ou medidas.

# GESTÃO DE RISCO | Tratamento

A organização, na sua sessão de gestão do risco, pode tomar a decisão estratégica de o **mitigar** e de executar as seguintes atividades:

**1. Garantir que o fornecedor da plataforma altera a sua política de gestão de palavras-passe em conformidade com boas práticas, no espaço de 1 trimestre, com os seguintes requisitos:**

- **1.1.** As palavras passe deverão ter um mínimo de 10 caracteres, incluindo letras em maiúsculas e minúsculas e caracteres não alfanuméricos.
- **1.2.** Deverá existir uma politica de alteração obrigatória da palavra passe de 90 em 90 dias.
- **1.3.** O sistema deverá bloquear automaticamente ao fim da 3ª tentativa falhada.
- **1.4.** Autenticação em dois fatores, misturando o par de utilizador/password, com envio de pin por SMS ou email.

**2. Avaliar outras plataformas que prestem o mesmo serviço, com as condições consideradas como adequadas pela organização, no espaço de um semestre.**

# GESTÃO DE RISCO | Tratamento

Foi identificado o **CISO** da organização como responsável pela execução e controlo das atividades.

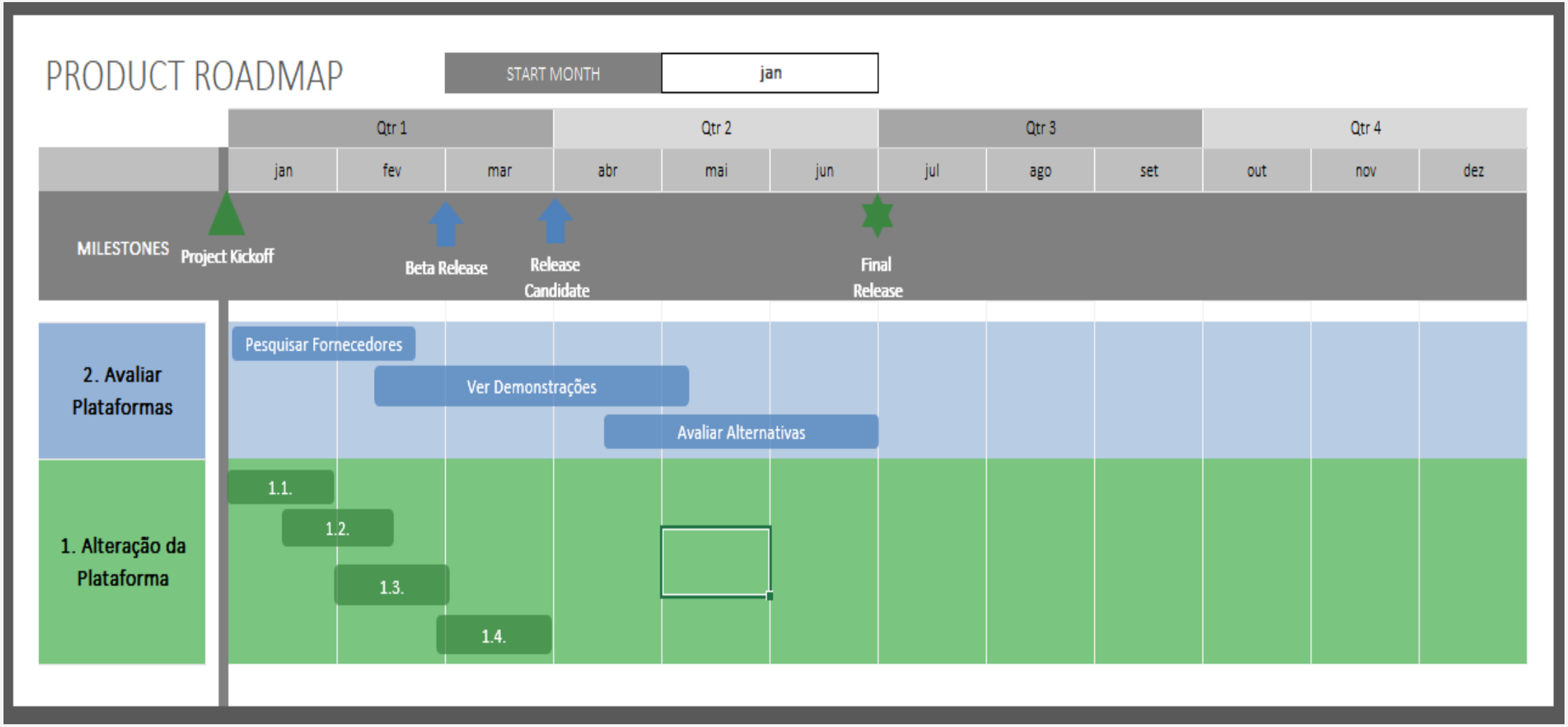
As **datas foram definidas** com base nas prioridades atribuídas aos riscos identificados tendo em conta o **nível de risco** e a **criticidade** dos ativos envolvidos.

# GESTÃO DE RISCO | Quadro Resumo

| | |
|---|---|
| **Descrição do Risco** | Possibilidade de acesso indevido a informação de projetos da organização |
| **Ativo** | Plataforma Online ERP |
| **Responsável do Risco** | CISO - Chief Information Security Officer |
| **Ameaça** | Ataque malicioso de força bruta às palavras-passe |
| **Vulnerabilidade** | Política de palavras-passe deficiente |
| **Confidencialidade** | Sim |
| **Integridade** | Sim |
| **Disponibilidade** | Sim |
| **Impacto** | 4 – Catastrófico |
| **Probabilidade** | 4 – Quase Certa |
| **Nível do Risco** | 16 – Muito Alta |
| **Estratégia** | Mitigar |
| **Ações** | - Garantir que o fornecedor da plataforma altera a sua política de gestão de palavras-passe em conformidade com boas práticas, no espaço de 1 trimestre<br>- Avaliar outras plataformas que prestem o mesmo serviço, com as condições consideradas como adequadas pela organização, no espaço de um semestre |
| **Responsável pelas ações** | CISO - Chief Information Security Officer |

# ROADMAP

# ROADMAP DA IMPLEMENTAÇÃO DOS CONTROLOS



# RELAÇÃO CUSTO BENEFÍCIO

O investimento em segurança da informação deve estar em consonância com o nível de risco que a organização está disposta a suportar, tendo sempre em atenção que o investimento efetuado para evitar um incidente de segurança deve ser inferior aos custos resultantes do incidente que se pretende evitar.

# GESTÃO DE RISCO | Relação Custo Benefício

Dado que a **segurança é um custo pelo facto de se fazer negócio**, esta deve ser uma preocupação dos responsáveis financeiros das organizações, **apesar de ser uma das últimas funções a ser dotada de fundos financeiros para o desenvolvimento das suas atividades** (Quinnild, Fusile, & Smith, 2006).

Os impactos financeiros provocados por um incidente de segurança podem ter assumir três formas potenciais:

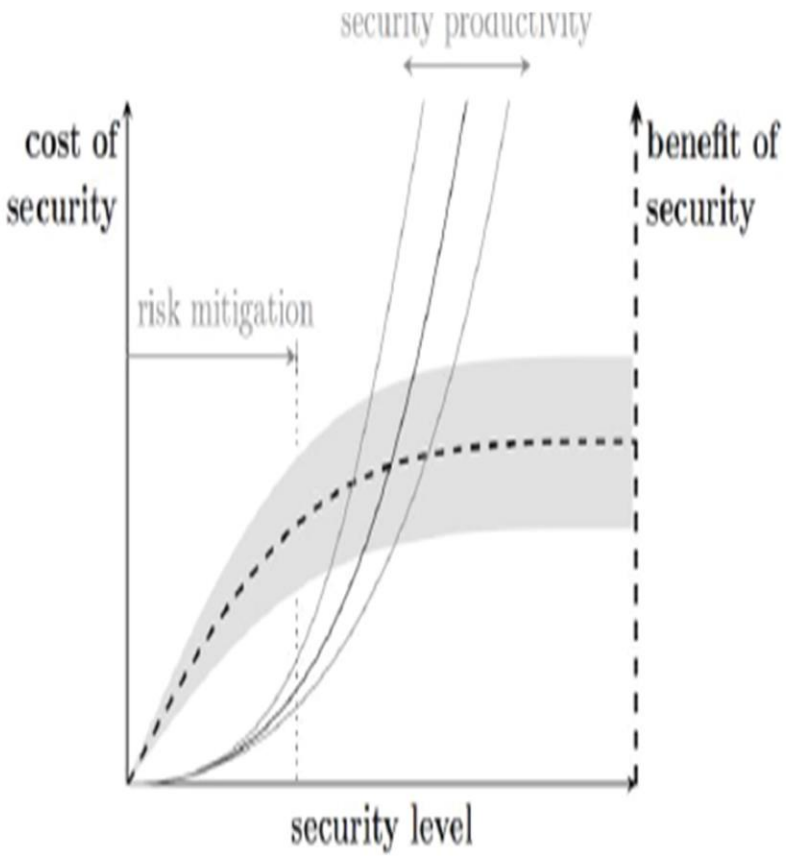
**Impacto económico imediato**
o custo de reparação ou substituição dos sistemas e interrupção das operações do negócio e dos fluxos de caixa;

**Impacto económico de curto prazo**
perda de clientes devido à incapacidade de entregar produtos ou serviços e impacto negativo na reputação da organização;

**Impacto económico de longo prazo**
declínio na avaliação de mercado da organização e do valor das ações no mercado de capitais

# GESTÃO DE RISCO | Relação Custo Benefício

Para tal, é necessário **quantificar os custos e os benefícios** dos softwares de segurança, associando sempre que possível os custos aos respetivos benefícios, procurando definir o nível de segurança.




Fonte: Security Metrics and Security Investment Models (Böhme, 2010)

# GESTÃO DE RISCO | Relação Custo Benefício

**Quantificação dos custos para implementar as soluções?**

| Tarefa | Valor | Duração |
|---|---|---|
| 1 - Encargos com desenvolvimento de funcionalidades | 5 000,00 € | 3 meses |
| 2 - Encargos com nova plataforma | 50 000,00 € | 6 meses |

# GESTÃO DE RISCO | Relação Custo Benefício

## Quantificação dos benefícios de implementar as soluções?

De uma forma simples, o nível de segurança permite prevenir incidentes, podendo traduzir-se num benefício de segurança. Podemos estimar os benefícios de segurança considerando **perdas que teria ocorrido caso não houvesse medidas de segurança**.

Interessará uma estratégia em que os benefícios superem os custos. Uma das métricas habitualmente utilizadas é a rentabilidade do investimento em segurança (***ROSI – Return on Security Investment***)

$$ROSI = \frac{benefit\ of\ security - cost\ of\ security}{cost\ of\ security}$$

# GESTÃO DE RISCO | Relação Custo Benefício

**Quantificação dos benefícios de implementar as soluções?**

Segundo Gordon e Loeb (2002), o investimento **não se deve concentrar nos conjuntos de informação com maior vulnerabilidade** pois podem ser excessivamente caros de proteger.
Os autores defendem ainda que as empresas **devem gastar apenas uma pequena fração (37%) da perda esperada** no caso de uma violação para maximizar o benefício esperado do investimento.

***«Furthermore, for two broad classes of security breach probability functions, the optimal amount to invest in information security should not exceed 37% (≈1/e) of the expected loss due to a security breach.»***
***(Gordon e Loeb, 2002)***

# GESTÃO DE RISCO | Relação Custo Benefício

## Quantificação dos benefícios de implementar as soluções?

Relativamente ao caso de estudo, a perda esperada, caso não se implementassem nenhumas medidas, e com base em estatísticas existentes, foi calculada da seguinte forma:

| | |
|---|---|
| Dias de Atividade | 365 |
| Faturação anual | 900 000,00 € |
| Faturação ao dia | 2 465,75 € |
| Dias médios de interrupção * | 10 |
| Custo médio de Interrupção | 24 657,53 € |
| Resgate médio de ransomware * | 6 000,00 € |
| Custos de recuperação sistemas | 5 000,00 € |
| **Total de Perdas Esperadas = Benefícios** | **35 657,53 €** |



* ***Considerando entre 5 a 6 ataques por ano***

# GESTÃO DE RISCO | Relação Custo Benefício

## Quantificação do Retorno em Investimento de Segurança?

$$ROSI = \frac{benefit\ of\ security - cost\ of\ security}{cost\ of\ security}$$

1 - Encargos com desenvolvimento de funcionalidades

**ROSI** = (35 657,00 € - 5 000,00 €) / 5 000,00 €

**ROSI** = 6,1314 **14,02%**

# GESTÃO DE RISCO | Relação Custo Benefício

## Quantificação do Retorno em Investimento de Segurança?

$$ROSI = \frac{benefit\ of\ security - cost\ of\ security}{cost\ of\ security}$$

2 - Encargos com nova plataforma

**ROSI** = $\frac{35\,657{,}00\ € - 50\,000{,}00\ €}{50\,000{,}00\ €}$

**ROSI** = -0,28686 **140,22%**

# GESTÃO DE RISCO | Relação Custo Benefício

**#1 tem uma relação de custo benefício adequada e deveria ser autorizada**

**#2 é completamente desajustada e não deveria ser validada pelo CEO da empresa**

# OBRIGADO

Bruna, João & Rui