

Relatório do trabalho da disciplina de Cibersegurança

# Sistema de Segurança da empresa Dev4Sell

---

Pedro Simões - 21140

Gonçalo Cunha - 21145

João Apresentação - 21152

Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)

Junho de 2023

Afirmo por minha honra que não recebi qualquer apoio não autorizado na realização deste trabalho prático. Afirmo igualmente que não copiei qualquer material de livro, artigo, documento web ou de qualquer outra fonte exceto onde a origem estiver expressamente citada.

Pedro Simões - 21140

Gonçalo Cunha - 21145

João Apresentação - 21152

## Índice

INTRODUÇÃO	5
Contextualização do documento	5
Descrição da empresa	5
Funções e responsabilidades	6
PROCESSOS DE NEGÓCIO	7
PN01 – Parcerias comerciais com os fornecedores	7
PN02 – Parcerias comerciais com os clientes	7
PN03-Gestão de Stock	8
PN04 – Venda	9
MÉTODO DE AVALIAÇÃO DE RISCO	10
Octave 10	
ARQUITETURA DOS SISTEMAS	10
Sistema de Administração da Empresa	11
Sistema de Comunicação Interna	11
Rede Telefónica	12
Sistema de Email Interno	12
Sistema de Armazenamento de Dados	12
Sistema de Produção	13
Sistema de Aplicações	13
Aplicação de gestão de stock (Computador)	13
Aplicação de auxílio de entregas e consulta de stock (Smartphone)	14
RECURSOS	15
Físicos 15	
Humanos	16
Dados 17	
Suporte de Dados	18

Aplicações	19
ANÁLISE E GESTÃO DE RISCOS	20
Recursos críticos	21
Ameaças e vulnerabilidades	25
Análise e Avaliação do Risco	29
PLANO DE MITIGAÇÃO	35
Atividades de Mitigação: Base de dados de clientes	35
Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos	36
Atividades de Mitigação: Aplicação do Sistema de Gestão Financeira	36
Atividades de Mitigação: Servidores de bases de dados	37
Atividades de Mitigação: Aplicação do Sistema de Apoio ao Cliente	37
Atividades de Mitigação: Máquinas e ferramentas de fabricação	38
Atividades de Mitigação: Base de dados de entregas	38
Atividades de Mitigação: Servidor de deployment de aplicações	39
Atividades de Mitigação: Aplicações do Sistema de Gestão dos Recursos Humanos	39
Atividades de Mitigação: Base de dados de produtos	40
Riscos aceites	40
PLANO DE RECUPERAÇÃO	41
Backup	41
Guia de recuperação de Dados	42
PLANO DE REPOSIÇÃO	46
PLANO DE CONTINGÊNCIA	47
AUDITORIA	47
Auditoria Externa	47
Simulacros	48
BIOGRAFIA	50

## Lista de Tabelas

Tabela 1 — <descrição da tabela>

**Erro! Marcador não definido.**

## Lista de Figuras

Figura 1 — <descrição da figura>

**Erro! Marcador não definido.**

## Introduo

### Contextualizao do documento

O projeto tem como objetivo apresentar um detalhado plano de segurana para a empresa, levando em considerao suas metodologias, processos de negcio e recursos. Esse plano engloba uma estratgia completa de gesto de riscos, bem como planos de segurana, recuperao, reposio e contingncia.

O plano visa proteger os ativos, informaes e infraestrutura da empresa, identificando e mitigando riscos, implementando medidas preventivas e estabelecendo procedimentos para lidar com incidentes de segurana. Sero adotadas polticas de segurana, controlos de acesso, monitorizao, treinamento de funcionrios e auditoria. O plano ser revisto regularmente para garantir a sua eficcia contnua.

### Descrio da empresa

A empresa a que ser proposto este plano chama-se Dev4Sell. O termo "Dev" representa desenvolvimento e "Sell" representa venda, que compem o nome da empresa e descrevem as suas principais funes.

A Dev4Sell  uma empresa especializada no desenvolvimento e fornecimento de equipamentos eletrnicos para grandes e mdias empresas que comercializam esses produtos para o pblico em geral.

Para a fabricao, a empresa recebe suporte material de patrocinadores que se beneficiam desse fornecimento.

## Funes e responsabilidades

Esta empresa demonstra uma estrutura de cargos, segue-se abaixo as tabelas com a identificao dos departamentos da Dev4Sell com a devida descrio de cada departamento e a anlise a cada um, distinguindo os diferentes elementos que compem cada equipa.

Cargo	Descrio
<b>CEO</b>	Lidera a Dev4Sell, atuando como intermedirio entre os diferentes diretores e departamentos da empresa. Tem acesso a toda a informao que circula na empresa.
<b>Diretor(a)</b>	Responsvel por uma rea especfica da empresa, como finanas, operaes, marketing, recursos humanos, etc. Supervisiona e coordena as equipas nessa rea e fornece suporte ao CEO a definir decises estratgicas para a empresa.
<b>Departamento de Recursos Humanos</b>	Responsvel pela seleo e recrutamento de novos funcionrios, alm de gerir o desempenho e as relaes no ambiente de trabalho. Garantem a conformidade com as normas da empresa.
<b>Departamento de Gesto de Sistemas de Informao</b>	Composto por membros da empresa responsveis pela superviso da segurana dos dados utilizados nos sistemas e as prticas de segurana da Dev4Sell.
<b>Departamento de Vendas</b>	Composto por profissionais de marketing, analistas de mercado que preveem o sucesso de produtos, e gestores de vendas que criam estratgias e planos de negociao com os clientes.
<b>Departamento de Finanas</b>	Responsvel por todas as atividades financeiras da empresa, tendo que otimizar a utilizao dos recursos financeiros disponfveis e fornecer informaes precisas e relevantes para a tomada de decises estratgicas.
<b>Departamento de Logfstica</b>	Encarregado de gerir a movimentao e armazenamento de materiais e produtos, bem como a distribuio e entrega dos mesmos.
<b>Departamento de Desenvolvimento e Produo</b>	Responsvel pelo design e construo dos equipamentos eletrnicos da empresa.
<b>Departamento de Apoio ao cliente</b>	Responsveis por dar assistncia ao cliente via website, mvel ou correio eletrnico, quer seja para esclarecimento de dvidas ou possfveis negcios.

## Processos de Negcio

Processos de negcio garantem o funcionamento eficiente dos padres de trabalho da Dev4Sell. Neste captulo, encontram-se descritos os principais processos que fornecendo uma estrutura slida para a realizao de atividades-chave.

### PN01 – Parcerias comerciais com os fornecedores

Para que a Dev4Sell possa iniciar todos os seus processos de negcio,  necessrio contar com os fornecedores de stock para desenvolvimento dos produtos a serem vendidos. Esses materiais so adquiridos por meio de parcerias com empresas de matria-prima. Abaixo seguem os subprocessos envolvidos nas parcerias realizadas:

**Identificao de stock necessrio:** Este processo inicia-se com a identificao do tipo de artigos que sero necessrios, e depois empresas que podero oferecer esse tipo de servios.

**Dev4Sell entra em contacto com os possveis fornecedores:** Aps a identificao de possveis fornecedores,  realizado um contacto, com o objetivo de marcar uma reunio a fim de negociar.

**Reunio:** durante a reunio  estabelecido os termos e condies desta parceria, envolvendo o tipo de servios esperados, prazos, oramentos, requisitos e clausulas contratuais. Aps a negociao  chegado a um acordo e possivelmente fechado um contrato ou no.

### PN02 – Parcerias comerciais com os clientes

Antes de iniciar o processo de venda, o cliente deve estabelecer uma parceria ou fazer um pedido  Dev4Sell. Neste ponto, ser explicado o desenvolvimento desse processo.

**Cliente entra em contacto com a empresa:** O processo inicia-se quando o cliente entra em contacto com a empresa utilizando o apoio ao cliente ou o correio eletrnico, que ser recebido pelo departamento de atendimento ao cliente.

Se a proposta abordada for do interesse da empresa  retornada uma resposta com o objetivo de agendar uma reunio presencial ou virtual.

**Reunio:** Durante a reunio, so discutidos os interesses do cliente, como servios prestados, oramentos, datas e contratos. A reunio pode resultar em diferentes desfechos, como a reprovo ou possvel interesse. Numa situao de interesse, a proposta ser submetida a um processo de aprovao, com a anlise de vrios departamentos da Dev4Sell para avaliar os benefcios da parceria. Opcionalmente, o cliente poder esperar uma contraproposta da empresa.



**Análise da proposta:** Após receber a proposta, o departamento de vendas realiza uma análise detalhada, avaliando o potencial sucesso dessa parceria. Durante essa análise, eles podem desenvolver estratégias e contrapropostas que beneficiem ambas as partes, visando maximizar os resultados e o valor da parceria.

No caso de ser enviada uma contraproposta ao cliente, este tem a possibilidade solicitar a renegociação até se chegar a uma conclusão satisfatória para ambas as partes. Após chegarem a um acordo, será agendada uma nova reunião para finalizar o contrato ou o pedido sem fidelização.

**Contrato:** Durante a fase de contrato, são revistas novamente todas as normas estabelecidas até o momento, como os termos e condições, serviços acordados, preços, responsabilidades e datas. Após a revisão e acordo mútuo, o contrato é assinado pelas entidades envolvidas, formalizando o acordo estabelecido.

**Pedido sem fidelização:** Em situações de exclusão de contrato formal, é firmado apenas um pedido contendo a quantidade específica de artigos solicitados.

## PN03-Gestão de Stock

Para garantir um processo de venda eficiente, é essencial ter uma gestão adequada de stock, permitindo o desenvolvimento contínuo dos produtos sem interrupções. Essa gestão pode ser dividida nos seguintes subprocessos:

**Planeamento:** Inicialmente, são projetados os produtos que serão desenvolvidos em determinado período, e é entregue uma lista de todos os artigos e um plano de construção. Isso pode ser estipulado pela equipa de design e arquitetura do departamento de desenvolvimento.

**Verificação do stock:** Verifica-se o stock existente pelo departamento de logística, e caso haja falta de algum artigo, é feito um pedido a uma empresa parceira especializada. Isso é realizado para garantir o abastecimento adequado.

**Análise:** Antes do pedido, o departamento financeiro realiza uma análise do estado económico atual da empresa. Com base nessa análise é previsto o que deve ser encomendado, e se necessário, é estipulado qual o inventário prioritário. Em seguida, é realizado o pedido de reposição de estoque.

**Pedido de artigos:** Dependendo dos termos do contrato assinalado com os parceiros, é estabelecido um contato para iniciar o processo de reabastecimento, informando sobre a necessidade de determinados artigos.

**Receção e reposição:** O departamento de logística é responsável por receber o material e atualizar o inventário. Caso seja identificado pelo departamento de Controlo de Qualidade algum defeito no produto recebido, será iniciado um processo de negociação para resolver o problema.

**Defeitos/Devoluções:** Em caso de problemas com os materiais recebidos, a Dev4Sell chegará a um acordo com a parceira, mas por norma será realizado substituição dos artigos defeituosos.

## PN04 – Venda

O processo de venda não funcionaria sem os processos de negócio anteriores e destina-se à entrega dos pedidos feitos pelo cliente e encontra-se dividido nos seguintes subprocessos

**Desenvolvimento do produto:** As equipas de design e arquitetura dos produtos enviam os planos para as equipas de desenvolvimento.

Os desenvolvedores analisam esse plano e tratam de produzir os equipamentos com recurso ao stock e software de produção.

**Análise dos produtos desenvolvidos:** O departamento de Controlo de Qualidade submete os equipamentos desenvolvidos a testes de funcionalidade, desempenho e qualidade e consoante o resultado, ocorre a aprovação ou reprovação.

**Faturação:** Após cada pagamento, é emitida uma fatura com os detalhes da transação, servindo como comprovativo de compra. A fatura contém informações como data, número, dados do cliente e vendedor, descrição dos produtos ou serviços, quantidade, preço unitário e total a pagar.

**Encomenda:** Após a confirmação do pedido, o departamento de logística processa a encomenda, prepara os produtos e os envia para as empresas. O envio é feito por meio de serviços de entrega ou o cliente pode optar por levantar os produtos pessoalmente.

**Defeitos/Devoluções:** No caso de o cliente receber produtos defeituosos vendidos pela Dev4Sell, é realizada uma análise do processo de venda para verificar a ocorrência de algum problema. Após a confirmação e apresentação do comprovativo de fatura, por norma são enviados novos artigos para substituir os danificados, mas poderá ocorrer uma negociação.

## Método de Avaliação de Risco

Entre as diversas frameworks de avaliação e gestão de riscos, a que pareceu ser a melhor opção para este plano de segurança foi o OCTAVE, neste caso na versão OCTAVE-S.

### Octave

O OCTAVE é uma metodologia abrangente e flexível para a identificação de riscos através da autoavaliação organizacional, esta ajuda as organizações a aplicar a informação de gestão de risco de segurança para assegurar a sua infraestrutura da informação existente e para proteger seus recursos críticos.

Este apresenta três versões diferentes, das quais nenhuma foi desenvolvida com o objetivo de substituir ou melhorar outra, mas sim com o objetivo de fazer uma melhor adaptação a diferentes tipos de organizações:

- OCTAVE Method
- OCTAVE-S
- OCTAVE Allegro (framework selecionada para este projeto)

A versão do OCTAVE escolhida foi o OCTAVE Allegro tendo em conta que é uma versão projetada organizações de porte médio, que é o caso da Dev4Sell, e também é focada em fazer uma abordagem mais rápida e simplificada da análise e avaliação dos riscos, não exigindo um investimento muito grande de recursos e tempo para fazê-la.

Desta forma também é possível desenvolver uma análise e gestão de riscos mais perceptível, sem exigir conhecimentos extensivos nesta área.

## Arquitetura dos Sistemas

As arquiteturas de sistemas da Dev4Sell desempenham um papel importante na estruturação e no funcionamento eficiente de todos os recursos da empresa, esta é dividida em 4 sistemas que são cruciais para o bom funcionamento da empresa.

Numa fase inicial será referido o funcionamento do sistema de administração empresarial da Dev4Sell, que tem como objetivo fazer a análise e gestão dos vários recursos ou mesmo processos de negócios da empresa, como por exemplo fazer o acompanhamento de uma entrega, fazer a verificação de stock de componentes elétricos produzidos ou mesmo a análise financeira da empresa

De seguida sero abordados os sistemas relativos  comunicacoo interna da empresa e o sistema de armazenamento de dados e como  que estes funcionaro de forma que seja possvel manter uma comunicacoo fluda e eficaz entre diferentes cargos e setores da empresa, algo que tem um peso enorme num bom funcionamento de uma empresa e no sucesso nos procedimentos dos processos de negcio e tambm apresenta um papel muito importante no que toca  seguranca e preservacoo dos dados relacionados com a empresa, produtos e clientes.

Por fim, ser analisado neste captulo os sistemas mais aplicacionais e que contm a lgica de armazenamento correto dos dados e a interacoo com os mesmos que serviro de suporte  anlise de estados de certos processos como entregas ou desenvolvimento de produtos eletrnicos, estes sistemas tm como principal objetivo fazer o apoio direto ao trabalhador de forma que este consiga finalizar com sucesso o seu papel num processo de negcio.

## Sistema de Administrao da Empresa

Este sistema da Dev4Sell tem como principal objetivo efetuar a anlise e gesto de recursos e processos de negcio em curso,  onde os recursos humanos realizam tarefas como:

- Tracking de uma entrega
- Anlise de pedidos feitos pelos clientes
- Anlise financeira da empresa
- Anlise de faturas pendentes
- Reviso perdica de veculos de entrega
- Etc.

De forma a aceder a este sistema, o utilizador ir necessitar de fazer login com a sua conta empresarial que  registada no incio de contrato e as credenciais so atribudas ao recurso contratado.

## Sistema de Comunicao Interna

O sistema de comunicao interna tem como objetivo estabelecer uma ligaoo segura e eficiente entre todas as mquinas localizadas dentro da infraestrutura da Dev4Sell, incluindo maquinaria de produoo, computadores e bases de dados. Includo neste sistema encontra-se tambm uma rede telefnica para a comunicacoo rpida entre funcionrios da empresa e um sistema de email interno para a troca de informacoo mais sensvel.

## Rede Telefónica

Apesar dos funcionários possuírem todos um smartphone empresarial, este não tem a funcionalidade de comunicação entre funcionários a nível interno. Para isso foi criada esta rede telefónica que pode ser utilizada para estabelecer comunicação entre diferentes departamentos e hierarquias de cargos de uma forma mais segura e rápida, quando a ocasião assim o requer, todavia esta deve ser utilizada apenas para comunicar informação com baixa/média sensibilidade ou fazer pedidos de assistência entre funcionários.

## Sistema de Email Interno

O sistema de email interno, como referido anteriormente, é utilizado para a troca de informações mais sensíveis e de maior importância. Este permitirá a criação de um email com o domínio “@dev4sell.pt”, que identificará esse email como uma conta associada à empresa.

Este será um serviço pago à Google a partir de uma subscrição.

## Sistema de Armazenamento de Dados

O sistema de armazenamento de dados terá o papel de realizar os procedimentos estipulados pela empresa para fazer o devido armazenamento, manipulação e acesso a dados relacionados com todo o tipo de informação que passa na empresa, tal como:

- Faturas
- Documentos contratuais
- Pedidos de entrega
- Agenda e estado de entregas
- Stock de produtos
- Dados de clientes e o seu histórico de ações com a Dev4Sell
- Registo de recursos
- Etc.

Por causa do mesmo estar responsável pelo tratamento e segurança de dados bastante valiosos, torna-se num dos sistemas mais importantes e que possivelmente provocariam maior impacto na empresa em caso de uma ameaça se tornar numa agressão.

A base de dados utilizará a linguagem SQL Server e como IDE o SSMS (SQL Server Management Studio).

## Sistema de Produção

O sistema de produção é responsável pelo planeamento, desenvolvimento e montagem de componentes eletrónicos que serão colocados para venda ou mesmo para a reposição e preparação de stock para futuras vendas.

Este é composto pela equipa de desenvolvimento que ficará encarregue de fazer o design do componente em causa, bem como o funcionamento lógico e físico do mesmo. Para que isto seja alcançado com sucesso, a equipa terá o auxílio das máquinas, ferramentas de produção e máquinas de testes de componentes.

Como ferramentas de auxílio, os designers de hardware e desenvolvedores de software para os componentes utilizarão uma grande diversidade de linguagens e ambientes de desenvolvimento integrado, tendo em conta a gama de produtos a ser produzida.

## Sistema de Aplicações

O sistema de aplicações da Dev4Sell tem como objetivo auxiliar todos os sistemas anteriormente referidos, fornecendo uma interface interativa para haver a comunicação entre os funcionários da empresa e os dados registados em base.

Tal como foi mencionado no sistema de email interno, cada utilizador terá um email com o domínio da empresa, fazendo assim a identificação de cada funcionário.

Tendo em conta o tipo de funcionário, que é informação que está registada em base de dados, este terá acesso direto após o login à respetiva página associada à função dele, por exemplo após um funcionário do departamento de finanças efetuar o login, na aplicação, será redirecionado para a interface que tratará de fazer a análise de histórico de faturas dependentes, vendas feitas recentemente, etc.

Foram criadas dois tipos de aplicação distintas, aplicação para desktop que terá acesso a diversas interfaces respetivas a cada recurso humano e aplicação para smartphone que terá funcionalidades rápidas como visualização de stock instantâneo, visualização de pedidos de entrega e a funcionalidade de realizar o auxílio de uma entrega, registando assim o processo da entrega.

### Aplicação de gestão de stock (Computador)

Esta aplicação, tal como já foi referido, é a aplicação principal para auxiliar o trabalho de cada membro da empresa Dev4Sell, no qual dependendo do login, cada funcionário será redirecionado para a sua respetiva interface:

- Interface de análise financeira da empresa
- Interface de análise de estatística de vendas, análise e gestão de clientes
- Interface de análise detalhada de materiais, componentes desenvolvidos e maquinaria usada para a produção de produtos eletrónicos
- Interface de workflow de projetos de equipas de desenvolvimento
- Interface para gestão de recursos humanos da empresa

### **Aplicação de auxílio de entregas e consulta de stock (Smartphone)**

A aplicação mobile apresentará funcionalidades mais simples e de rápida consulta para os elementos da equipa de suporte técnico, que está encarregue de fazer a entrega de produtos, estando assim incluídas as funcionalidades de:

- Consultar e responder a pedidos de entrega de produtos feitos pelo cliente
- Verificação de stock de produtos
- Realizar a entrega, alterando o estado da mesma sempre que necessário, esta informação é importante e cada alteração será registada na base de dados, para futuramente analisar pontos a melhorar nas entregas

## Recursos

De forma que a empresa tenha o bom funcionamento dos sistemas, ser necessrio que esta contenha recursos, que tratam-se de meios que podem ser utilizados para um determinado fim, estes possuem um valor e so quem sofrem os ataques, sejam estes fsicos, cibernticos, etc.

Os recursos podem ser divididos em 5 tipos, nos quais sero analisados:

- Fsicos
- Humanos
- Dados
- Suporte de Dados
- Aplicaes

### Fsicos

Nome	Descrio	Sistemas em que  utilizado
<b>Infraestrutura</b>	Estrutura fsica da empresa que serve de suporte para o funcionamento dos sistemas e equipamentos da Dev4Sell.	<ul style="list-style-type: none"> <li>• Sistema de Administrao da Empresa</li> <li>• Sistema de Comunicao Interna</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produo</li> <li>• Sistema de Aplicaes</li> </ul>
<b>Computadores</b>	Equipamento de auxlio que tem serve de interao com o sistema de gesto de produtos da empresa e tratar de outros assuntos administrativos e financeiros.	<ul style="list-style-type: none"> <li>• Sistema de Administrao da Empresa</li> <li>• Sistema de Comunicao Interna</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produo</li> <li>• Sistema de Aplicaes</li> </ul>
<b>Mquinas de teste de componentes</b>	Conjunto de equipamentos utilizados para realizar a <i>quality assurance</i> dos equipamentos reproduzidos na Dev4Sell.	<ul style="list-style-type: none"> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produo</li> <li>• Sistema de Aplicaes</li> </ul>
<b>Mquinas e ferramentas de fabricao</b>	Equipamentos de utilizados no processo de produo e um produto eletrnico da empresa.	<ul style="list-style-type: none"> <li>• Sistema de Produo</li> </ul>



<b>Router Gateway</b>	Dispositivo que irá estabelecer a ligação entre a rede local com a internet, todos os dispositivos estarão ligados a este equipamento para ter acesso à internet.	<ul style="list-style-type: none"> <li>• Sistema de Administração da Empresa</li> <li>• Sistema de Comunicação Interna</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Aplicações</li> </ul>
<b>Switches</b>	Equipamentos necessários para estabelecer a ligação entre equipamentos na rede local.	<ul style="list-style-type: none"> <li>• Sistema de Administração da Empresa</li> <li>• Sistema de Comunicação Interna</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produção</li> <li>• Sistema de Aplicações</li> </ul>
<b>Armazém de produtos</b>	Local de armazenamento de equipamentos eletrônicos desenvolvidos pela empresa.	<ul style="list-style-type: none"> <li>• Sistema de Administração da Empresa</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produção</li> </ul>
<b>Camiões de entrega</b>	Equipamento de auxílio às entregas e recolhas de produtos na Dev4Sell. Utilizados para transportar os produtos.	<ul style="list-style-type: none"> <li>• Sistema de Administração da Empresa</li> </ul>

## Humanos

Nome	Descrição	Responsabilidades
<b>Equipa de desenvolvimento de software</b>	Equipa que tem o papel de desenvolver o funcionamento lógico dos produtos	<ul style="list-style-type: none"> <li>• Sistema de Administração da Empresa</li> <li>• Sistema de Comunicação Interna</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produção</li> <li>• Sistema de Aplicações</li> </ul>

<b>Equipa de produção de hardware</b>	Equipa que tem o papel de desenvolver fisicamente os produtos com auxílio de maquinarias.	<ul style="list-style-type: none"> <li>• Sistema de Administração da Empresa</li> <li>• Sistema de Comunicação Interna</li> <li>• Sistema de Armazenamento de Dados</li> <li>• Sistema de Produção</li> <li>• Sistema de Aplicações Assegurar a qualidade dos produtos desenvolvidos</li> </ul>
<b>Equipa de suporte técnico</b>	Equipa de apoio e entrega de produtos ao cliente. Esta também tem o papel de auxiliar outros recursos em caso de algum problema.	<ul style="list-style-type: none"> <li>• Assegurar que algum problema ou queixa que um cliente tenha, seja resolvido</li> <li>• Realizar de forma sucessiva as entregas de produtos aos clientes</li> <li>• Estar disponível e ter a capacidade de resolução de problemas relacionados a recursos da empresa, principalmente físicos.</li> </ul>
<b>Equipa de vendas</b>	Equipa que entra em contacto com os clientes e trata de negociar cada venda.	<ul style="list-style-type: none"> <li>• Negociar e manter uma boa relação entre os clientes e a Dev4Sell</li> </ul>

## Dados

Nome	Descrição	Fonte dos dados	Nível de Acesso	Responsável pelos dados
<b>Base de dados de produtos</b>	Base de dados que contém a informação acerca do armazém de produtos desenvolvidos, bem	Produtos desenvolvidos pela Dev4Sell, armazéns de armazenamento	Médio	...

	como o stock disponvel.	de equipamentos.		
<b>Base de dados de clientes</b>	Base de dados que contm as informaes dos clientes da empresa.	Entidades que entrem em contacto com a empresa que estejam interessadas na compra de um produto, interaes com a empresa.	Alto	...
<b>Base de dados de entregas</b>	Regista o progresso de cada entrega que foi feita pela empresa, registando datas, locais e estados.	Transaes monetrias, relatrios de equipas de suporte tcnico e atualizaes na aplicao do sistema de entregas.	Alto	...
<b>Base de dados de testes de verses</b>	Regista resultados testes executados aps a submisso de verses novas de cada aplicao.	Verso testada, quantidade de utilizadores, quantidade de requests executados, quantidade de requests com resposta OK, tempo de execuo.	Mdio	...

## Suporte de Dados

Nome	Descrio
<b>Servidores de deployment de aplicaes</b>	Recursos de capacidade de armazenamento de alto desempenho e confiabilidade responsveis por fornecer um local centralizado para armazenar e gerir os dados da empresa.
<b>Impressoras</b>	Recurso responsvel pela impresso de documentos como relatrios, faturas, contratos, etc.
<b>Servidores de bases de dados</b>	Recurso que tem o objetivo de armazenar e gerir todos os dados relacionados com a Dev4Shell.

<b>Servidor de armazenamento em nuvem para documentos</b>	A Dev4Sell utiliza servios da Google, pagando uma subscrio, que tero como objetivo fazer o armazenamento de documentos como relatrios, contratos, faturas, etc.
<b>Servidor de backup de base de dados</b>	Recurso que serve de salvaguarda do servidor de base de dados. Este  utilizado para realizar cpias de segurana dos dados crticos da empresa.
<b>Armazenamento de backup em disco</b>	Servidor responsvel por armazenar o backup de todos os discos utilizados pelas mquinas da empresa, de modo a manter em registo as aes realizadas pelo funcionrios

## Aplicaes

Nome	Descrio
<b>Ambientes de desenvolvimento (IDE)</b>	Recurso de suporte a desenvolvedores e outros trabalhadores da empresa que fornece um conjunto de ferramentas para facilitar o desenvolvimento de software e hardware (produtos).
<b>Aplicao do Sistema de Gesto de Stock</b>	Aplicao de controlo e gesto de stock presente nos armazns da empresa.
<b>Aplicao do Sistema de Gesto de Vendas e Entregas</b>	Aplicao que auxilia a Dev4Shell no processo de gesto de vendas, desde o registo do pedido at  entrega do produto ao cliente.
<b>Aplicao do Sistema de Gesto de Recursos Humanos</b>	Aplicao que facilita a administrao e a gesto das atividades relacionadas aos funcionrios da empresa.
<b>Aplicao do Sistema de Gesto Financeira</b>	Aplicao que ajuda a empresa a controlar e gerir as suas atividades financeiras, esta rastrear qualquer tipo de transao e gastos feitos pela mesma e tambm analisar pagamentos pendentes relacionados com o negcio da empresa ou no.
<b>Aplicao de Sistema de Apoio ao Cliente</b>	Aplicao que permite a Dev4Sell gerir, analisar e atender a pedidos feitos pelos clientes, exibindo na sua interface solicitaes de produtos, queixas ou pedidos de ajuda dos mesmos que no tenham sido feitos via chamada telefnica.
<b>Rede de Comunicao Interna da Empresa</b>	Infraestrutura de comunicao interna da empresa, esta estabelecer a ligao entre os diferentes departamentos e nveis hierrquicos da Dev4Sell.

## Análise e Gestão de Riscos

Tendo em conta o elevado número de recursos da Dev4Sell, estaremos também presentes a uma grande diversidade de riscos, mesmo sendo preocupantes ou não, algo que será analisado a seguir, teremos de ter todos em causa pois todos terão o seu impacto e prejuízo.

Em geral, é possível analisar que os riscos, dependendo de cada um, irão afetar a empresa em:

- Saúde dos recursos humanos
- Produtividade de desenvolvedores e equipa de produção de produtos
- Reputação da Dev4Sell
- Eficiência e cuidado na entrega de produtos

Tratam-se de pontos de extrema importância para a empresa e os seus trabalhadores, portanto, fazer uma boa análise e gestão de riscos é de grande importância.

De forma inicial, serão identificados os recursos críticos, que são os recursos que no caso de um dos três pilares da segurança associados a eles for afetado, o seu impacto para empresa é de nível alto/catastrófico.

De seguida irão ser identificadas as ameaças aos recursos para a empresa estar ciente dos ataques que esta possa vir a sofrer e fazer uma preparação para evitá-los ou mesmo reduzir impactos ao máximo.

Por fim, será feita a análise e avaliação riscos onde será atribuída uma classificação em cada risco, em diferentes níveis:

- Impacto
- Gravidade
- Probabilidade

Isto fará com que seja possível tomar decisões em relação a quais riscos compensa mitigar, resolver ou simplesmente ignorar.

## Recursos crticos

Recursos que tenham um nvel de impacto acima de mdio em qualquer um dos trs principais pilares da segurana quando sofre um ataque, ser considerado como “crtico”, estes so recursos que necessitaro de especial ateno, pois um ataque feito aos mesmo, mesmo sem nenhum tipo de preparo ou com preparo para o receber, poder ter um prejuzo enorme para a empresa.

Pilar de Segurana	Baixo	Mdio	Alto
<b>Privacidade</b>	Quando a informao foi divulgada sem autorizao necessria e possa provocar um impacto baixo nas operaes e recursos organizacionais ou indivduos e de fcil resoluo.	Quando a informao foi divulgada sem autorizao necessria e possa provocar um impacto mdio nas operaes e recursos organizacionais ou indivduos e ter uma resoluo com poucos prejuzos e de grau de dificuldade mdia.	Quando a informao foi divulgada sem autorizao necessria e possa provocar um impacto alto nas operaes e recursos organizacionais ou indivduos e de difcil resoluo.
<b>Integridade</b>	Quando a informao  alterada ou destruda sem autorizao necessria e possa provocar um impacto baixo nas operaes e recursos organizacionais ou indivduos e de fcil resoluo.	Quando a informao  alterada ou destruda sem autorizao necessria e possa provocar um impacto mdio nas operaes e recursos organizacionais ou indivduos e ter uma resoluo com poucos prejuzos e de grau de dificuldade mdia.	Quando a informao  alterada ou destruda sem autorizao necessria e possa provocar um impacto alto nas operaes e recursos organizacionais ou indivduos e de difcil resoluo.

<b>Disponibilidade</b>	Quando o acesso ou uso de informaes de um sistema pode vir a ter um impacto baixo nas operaes organizacionais, recursos e de fcil resoluo organizacionais, ou indivduos.	Quando o acesso ou uso de informaes de um sistema pode vir a ter um impacto mdio nas operaes organizacionais, recursos organizacionais, ou indivduos e ter uma resoluo com poucos prejuzos e de grau de dificuldade mdia.	Quando o acesso ou uso de informaes de um sistema pode vir a ter um impacto alto nas operaes organizacionais, recursos organizacionais, ou indivduos e de difcil resoluo.
------------------------	--	---	---

Segue-se abaixo a lista de recursos anteriormente mencionada, com a devida anlise de nvel de impacto:

Recurso	Impacto		
	Privacidade	Integridade	Disponibilidade
Infraestrutura	Baixo	Mdio	Mdio
Computadores	Baixo	Baixo	Baixo
Impressoras	Baixo	Baixo	Baixo
Mquinas de teste de componentes	Baixo	Baixo	Mdio
Ferramentas de fabricao	Baixo	Baixo	Alto
Router Gateway	Alto	Baixo	Alto
Switches	Baixo	Mdio	Mdio
Armazm de produtos	Baixo	Mdio	Mdio

Camies de entrega	Baixa	Mdia	Mdia
Equipa de desenvolvimento de software	Baixa	Baixa	Mdia
Equipa de produo de hardware	Baixa	Baixa	Mdia
Equipa de suporte tcnico	Baixa	Baixa	Mdia
Equipa de vendas	Baixa	Baixa	Mdia
Base de dados de produtos	Alta	Alta	Alta
Base de dados de clientes	Alta	Alta	Alta
Base de dados de entregas	Alta	Alta	Alta
Base de dados de testes de verses	Baixa	Mdia	Mdia
Servidor de armazenamento em nuvem para documentos	Alta	Alta	Mdia
Servidores de deployment de aplicaes	Mdio	Mdio	Alto
Servidores de bases de dados	Alto	Alto	Alto
Servidor de backup de base de dados	Mdio	Alto	Mdio
Armazenamento de backup em disco	Mdio	Alto	Baixo



Ambientes de Desenvolvimento Integrado (IDE)	Baixo	Baixo	Baixo
Aplicao do Sistema de Gesto de Stock	Baixo	Mdio	Mdio
Aplicao do Sistema de Gesto de Vendas e Entregas	Alto	Mdio	Alto
Aplicao do Sistema de Gesto de Recursos Humanos	Alto	Mdio	Mdio
Aplicao do Sistema de Gesto Financeira	Alto	Mdio	Mdio
Aplicao de Sistema de Apoio ao Cliente	Alto	Mdio	Alto
Rede de Comunicao Interna da Empresa	Alto	Mdio	Mdio

Acima conseguimos verificar quais os recursos crticos dos que foram mencionados no captulo dos Recursos, tendo estes sido sublinhados de forma a criar destaque nos mesmos.

Todos os recursos que estejam relacionados com bases de dados ou outros tipos de armazenamento de informao tiveram o seu especial destaque, obviamente tendo em conta com o tipo de dados que se est a ter em conta, por exemplo  muito mais preocupante que os dados de um cliente sejam divulgados do que os dados de um certo produto que se encontra em stock de venda. Sendo assim, todas as bases de dados e seus servidores foram adicionados  lista de recursos crticos, sendo que a divulgao, perda ou at mesmo alterao de dados, bem como a interrupo de servios de informao possuem um impacto pelo menos preocupante (mdio/alto).

As aplicaes possuem informaes das bases de dados, mesmo que cada aplicao est a receber informao de uma base de dados em especfico, no deixa de ser possvel informao sensvel a ser roubada ou alterada no sistema. H aplicaes que o seu grau de preocupao, nestas situaes,  menor, como por exemplo a Aplicao de Gesto de Stock. Os servidores de deployment de aplicaes tambm foi destacada, pois, caso este deixe de funcionar, todas as Sistema de Segurana da empresa Dev4Sell

aplicaes iro parar de rodar e os funcionrios perdem temporariamente o seu suporte de trabalho e acesso aos dados da empresa.

O router gateway tambm tem o seu grau de importncia, tendo em conta que sem este, o sistema no consegue estabelecer ligao entre a rede privada e a rede pblica (externa), o que incapacita as comunicaes entre cliente-empresa.

A rede interna do sistema tambm deve estar sempre disponvel e protegida, tendo em conta que se uma entidade externa maligna entrar no sistema tem a possibilidade de roubar informao.

Por fim, as mquinas de produo so cruciais tendo em conta que so os principais recursos para desenvolver o produto para venda, sem estas, a produo poder atrasar-se bastante, fazendo com que os clientes esperem muito tempo e, conseqentemente, baixe a reputao da empresa.

## Ameaas e vulnerabilidades

As ameaas so potenciais agresses que ainda no se manifestaram, portanto, fazer a identificao de cada uma  crucial para o desenvolvimento de um plano de segurana.

Segue-se abaixo uma tabela que apresentar todos os recursos crticos mencionados anteriormente com a identificao das ameaas e diferentes atributos relacionados com ela:

Recurso	Acesso	Ator	Motivo	Resultado	Impacto
<b>Mquinas e ferramentas de fabricao</b>	Fsico	Interno	Intencional	Perda/Destruio	Alto
				Interrupo	Mdio
			Acidental	Perda/Destruio	Alto
				Interrupo	Mdio
<b>Router Gateway</b>	Fsico	Interno	Intencional	Interrupo	Alto
	Rede/Sistema	Externo	Intencional	Interrupo	Alto
	Rede/Sistema	Externo	Intencional	Divulgao	Mdio

<b>Base de dados de produtos</b>				Modificao	Alto
				Interrupo	Alto
<b>Base de dados de clientes</b>	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	
				Interrupo	
<b>Base de dados de entregas</b>	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	
				Interrupo	
<b>Servidor de armazenamento em nuvem para documentos</b>	Rede/Sistema	Interno	Intencional	Divulgao	Alto
				Modificao	Alto
		Externo	Intencional	Divulgao	Alto
				Modificao	Alto
<b>Servidores de deployment de aplicaes</b>	Físico	Interno	Intencional	Interrupo	Médio
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruio	Alto
				Interrupo	Médio
<b>Servidores de bases de dados</b>	Físico	Interno	Intencional	Interrupo	Médio
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto

	Rede/Sistema	Externo	Intencional	Perda/Destruição	Alto
				Interrupção	Médio
Servidor de backup de base de dados	Físico	Interno	Intencional	Interrupção	Baixo
				Perda/Destruição	Alto
			Acidental	Perda/Destruição	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruição	Alto
				Interrupção	Médio
	Armazenamento de backup em discos	Físico	Interno	Intencional	Divulgação
Modificação					Alto
Perda/Destruição					Médio
Acidental				Perda/Destruição	Médio
Aplicação do Sistema de Gestão de Recursos Humanos	Físico	Interno	Intencional	Divulgação	Alto
				Modificação	Alto
				Perda/Destruição	Médio
	Rede/Sistema	Externo	Intencional	Divulgação	Alto
				Modificação	Alto
				Perda/Destruição	Médio
Aplicação do Sistema de Gestão Financeira	Físico	Interno	Intencional	Divulgação	Alto
				Modificação	Alto
				Perda/Destruição	Alto

	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Alto
<b>Aplicao de Sistema de Apoio ao Cliente</b>	Físico	Interno	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Alto
<b>Rede de Comunicao Interna da Empresa</b>	Físico	Interno	Intencional	Interrupo	Médio
			Acidental	Interrupo	Médio
	Rede/Sistema	Externo	Intencional	Interrupo	Médio

Acima  possível verificar que sendo estes recursos críticos, os impactos causados nos sistemas de informao da Dev4Sell, quaisquer que sejam as propriedades das ameaas, so de calibre médio/alto, sendo assim, terá de ser feita a avaliao de cada risco possível, de forma a perceber quais os riscos que necessitaro de maior prioridade.

As ameaas apresentam vrias propriedades com diferentes valores:

- Recurso crítico: recurso que pode sofrer a ameaa em causa
- Acesso: forma como o atacante acede ao recurso, este pode ter como valores:
  - Físico
  - Rede/Sistema
- Ator: entidade que efetua o ataque, este pode ter como valores:
  - Interno
  - Externo
- Motivo: Razo para o ataque ter sido feito, este pode ter como valores:
  - Acidental
  - Intencional

- Resultado: ação executada nos sistemas de informação por parte do atacante, este pode ter como valores:
  - Divulgação - divulgação ou visualização de informações sensíveis
  - Modificação - modificação de informações importantes ou confidenciais
  - Destruição - Destruição ou perda de informações importantes, hardware ou software
  - Interrupção - Interrupção de acesso a informações importantes, software, aplicativos ou serviços
- Impacto: Nível de danos ou consequências causadas aos sistemas de informação da organização, este pode ter como valores:
  - Baixo
  - Médio
  - Alto

Será feita agora a análise de alguns casos em particular da tabela acima.

Ameaças que possuem um ator interno com motivo accidental, é assumido que tanto um recurso humano como uma causa natural possa ter sido a fonte da agressão em causa.

Como é possível verificar, os recursos que receberam mais valores “Alto” na coluna do impacto ou estão relacionadas com informações bastante sensíveis como dados de clientes, dados financeiros da empresa, etc. ou estão relacionadas com bases de dados, sendo estas onde toda a informação circulada entre os sistemas está armazenada, tornando-se um dos recursos mais valiosos da organização, senão a mais valiosa.

Há que ter em atenção também os restantes recursos críticos que apresentaram valores mais baixos no impacto, como é o caso da Aplicação do Sistema de Gestão de Recursos Humanos, tendo em conta que este tem acesso direto a dados e documentos sensíveis como contratos feitos entre cada funcionário, apesar de não conseguir fazer a modificação dos mesmos, consegue divulgá-los.

## Análise e Avaliação do Risco

Para finalizar a análise do risco, será implementada uma tabela que irá conter cada recurso e a classificação em cada aspeto que foi referido na introdução a este capítulo: impacto, gravidade e probabilidade.

Tendo em conta que cada um destes valores não tem uma forma de ser detalhadamente atribuído um valor numericamente correto, será feita uma atribuição de pontos (0-10), para que seja possível fazer um sistema hierárquico das ameaças analisadas em cada recurso.

Segue-se então abaixo tabela referente à análise de risco:

Recurso	Atributos	Valor do Risco	
		Interno	Externo
<b>Mquinas e ferramentas de fabricao</b>	Impacto	6	N/A
	Gravidade	3	N/A
	Probabilidade	5	N/A
	Mdia	4,7	N/A
	<b>Mdia Final</b>	5.3	
<b>Router Gateway</b>	Impacto	7	7
	Gravidade	3	4
	Probabilidade	3	2
	Mdia	4,3	4,3
	<b>Mdia Final</b>	4.3	
<b>Base de dados de produtos</b>	Impacto	N/A	7
	Gravidade	N/A	6
	Probabilidade	N/A	2
	Mdia	N/A	5
	<b>Mdia Final</b>	5	
<b>Base de dados de clientes</b>	Impacto	N/A	9
	Gravidade	N/A	9
	Probabilidade	N/A	2

	Mdia	N/A	6,7
	<b>Mdia Final</b>	6.7	
<b>Base de dados de entregas</b>	Impacto	N/A	8
	Gravidade	N/A	7
	Probabilidade	N/A	1
	Mdia	N/A	5,3
	<b>Mdia Final</b>	5.3	
<b>Servidor de armazenamento em nuvem para documentos</b>	Impacto	9	9
	Gravidade	6	8
	Probabilidade	2	2
	Mdia	5.7	6.3
	<b>Mdia total</b>	6	
<b>Servidores de deployment de aplicaes</b>	Impacto	7	7
	Gravidade	5	8
	Probabilidade	2	2
	Mdia	4.7	5.7
	<b>Mdia Final</b>	5.2	
<b>Servidores de bases de dados</b>	Impacto	9	9
	Gravidade	5	8
	Probabilidade	2	2



	Mdia	5.3	6.3
	<b>Mdia Final</b>	5.8	
<b>Servidor de backup de base de dados</b>	Impacto	6	6
	Gravidade	4	5
	Probabilidade	2	2
	Mdia	4	4,3
	<b>Mdia Final</b>	4.2	
<b>Armazenamento de backup em discos</b>	Impacto	3	N/A
	Gravidade	7	N/A
	Probabilidade	2	N/A
	Mdia	4	N/A
	<b>Mdia Final</b>	4	
<b>Aplicao do Sistema de Gesto de Recursos Humanos</b>	Impacto	7	8
	Gravidade	5	6
	Probabilidade	2	2
	Mdia	4.7	5.3
	<b>Mdia Final</b>	5	
<b>Aplicao do Sistema de Gesto Financeira</b>	Impacto	9	9
	Gravidade	4	6
	Probabilidade	4	4

	Mdia	5.7	6.3
	<b>Mdia Final</b>	6	
<b>Aplicao de Sistema de Apoio ao Cliente</b>	Impacto	9	9
	Gravidade	4	6
	Probabilidade	3	3
	Mdia	5.3	6
	<b>Mdia Final</b>	5.7	
<b>Rede de Comunicao Interna da Empresa</b>	Impacto	5	7
	Gravidade	3	4
	Probabilidade	2	2
	Mdia	3.3	4.3
	<b>Mdia Final</b>	3.8	

Observando a tabela acima conseguimos obter o valor de risco final associado a cada recurso crtico da empresa, tendo em conta as variveis fornecidas:

- Impacto: consequncias e danos causados na empresa assim que uma agresso ocorre
- Gravidade: efeitos secundrios e danos a longo prazo causados na empresa aps uma agresso
- Probabilidade: medida atribuda  chance de um evento ocorrer

De forma a fazer um sistema de pontuao justo, foi preciso ter em causa tanto ameaas com atores internos ou externos, sendo que houve casos que houve apenas um destes atores, foi atribudo o valor de N/A ao valor do risco que no possui o ator num desses valores e  assumido totalmente o valor do risco do ator que causo a agresso, por exemplo, as mquinas sendo que no tm nenhum tipo de ameaa externa, vai-se assumir totalmente o valor de risco interno.

Para cada valor de risco (interno e externo)  calculada a mdia entre as trs variveis fornecidas.

Para os casos em que apresentam agressões com ambos os atores, é feita a média das médias obtidas por ambos os valores risco (interno e externo).

Com os valores obtidos já é possível ver hierarquicamente quais os riscos que é preciso ter mais em atenção para o plano de mitigação tendo sido esta a ordem obtida:

- Base de dados de clientes: 6.7
- Servidor de armazenamento em nuvem para documentos: 6
- Aplicação do Sistema de Gestão Financeira: 6
- Servidores de bases de dados: 5.8
- Aplicação de Sistema de Apoio ao Cliente: 5.7
- Máquinas e ferramentas de fabricação: 5.3
- Base de dados de entregas: 5.3
- Servidores de deployment de aplicações: 5.2
- Aplicação do Sistema de Gestão de Recursos Humanos: 5
- Base de dados de produtos: 5
- Router Gateway: 4.3
- Servidor de backup de base de dados: 4.2
- Armazenamento de backup em discos: 4
- Rede de Comunicação Interna da Empresa: 3.8

## Plano de Mitigação

Agora que foram calculados os valores dos riscos associados aos recursos críticos da Dev4Sell, tem de ser implementando um plano de mitigação, que define as atividades necessárias para eliminar ou reduzir o risco inaceitável para um recurso crítico.

A partir deste plano, irá ser feita a seleção de riscos a mitigar, bem como a descrição das atividades/políticas a aplicar em cada recurso selecionado, isto irá permitir que a probabilidade do risco seja menor, ou até mesmo nula.

Tendo em conta que os valores atribuídos aos riscos no sub-capítulo da análise de riscos foram dentro do intervalo de valores 0-10, ficou definido que todos os riscos que tivessem uma classificação média acima de metade do valor máximo do intervalo sejam mitigados/transferidos, sendo assim, serão mitigados/transferidos os riscos associados aos seguintes recursos:

- Base de dados de clientes
- Servidor de armazenamento em nuvem para documentos
- Aplicação do Sistema de Gestão Financeira
- Servidores de bases de dados
- Aplicação de Sistema de Apoio ao Cliente
- Máquinas e ferramentas de fabricação
- Base de dados de entregas
- Servidores de deployment de aplicações
- Aplicação do Sistema de Gestão de Recursos Humanos
- Base de Dados de Produtos

### Atividades de Mitigação: Base de dados de clientes

O acesso à base de dados de clientes deve ser restrito ao **Quem deve ter acesso**, excluindo assim uma grande quantidade de possíveis atores a ataques à mesma, bem como deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização aos sistemas de informação, pois estes consomem constantemente os dados armazenados.

De forma a poder manter registo de ações efetuada à base de dados, devem ser mantidos registos de todos os acessos efetuados à mesma, bem como as operações (queries) que foram executadas, isto permitirá que em caso de uma agressão tenha sido efetuada, estes logs mostrarão quem teve acesso à base de dados, quando, onde e como.

Deverá também ser feito um backup da base de dados diariamente, de forma a repor os dados em caso de ataque. Dentro deste intervalo diário, serão feitos registos em ficheiros de

texto dos snapshots da database periodicamente, algo que estará explicado no Plano de Recuperação.

### **Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos**

- ➔ Sendo que este recurso utiliza serviços de terceiros, estes ficarão responsabilizados pelo risco ocorrido, no caso do acesso indevido ao recurso for feito a partir de uma conta fora da empresa (melhorar o texto)
- ➔ Meter mais alguma coisa?

De forma que o servidor de armazenamento em nuvem de documentos fique mais seguro, deve-se encriptar todo o tipo de documento que é armazenado nesta cloud. Com isto, mesmo que a cloud seja atacado, o atacante perderá muito tempo ou poderá até mesmo não conseguir descriptar a informação roubada.

Tendo em conta que este é um serviço prestado pela Google, qualquer tipo de agressão que tenha sido feita a este servidor será transferida para a entidade prestadora do serviço.

### **Atividades de Mitigação: Aplicação do Sistema de Gestão Financeira**

Deve ser feito um controlo de acessos à aplicação do sistema de gestão financeira, controlando assim acessos indevidos à mesma, por exemplo um login feito com sucesso fora da rede empresarial. As realizações de testes de segurança têm um papel crucial neste aspeto, pois estes detetarão lacunas no sistema de segurança da app. Os testes serão implementados com auxílio da ferramenta Selenium em junção com um software de VPN para fazer várias simulações de diferentes tipos de acesso a contas e mesmo ataques à aplicação de diferentes localizações.

De forma a manter controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs da mesma, de forma que caso haja algum ataque ou atividade duvidosa no software, seja mais fácil de identificar a entidade e operações malignas.

Devem ser feitas também workshops de sensibilização às práticas de segurança no desenvolvimento e utilização do software periodicamente, isto irá alertar os funcionários a implementar práticas mais seguras no desenvolvimento e utilização da aplicação, fazendo com que estes evitem correr riscos de segurança.

- ➔ Efetuar workshops de sensibilização às práticas de segurança no desenvolvimento de software (isto se forem os nossos programadores a criar as aplicações, caso seja um serviço de terceiros, apenas transfere-se o risco)

## Atividades de Mitigao: Servidores de bases de dados

Os servidores de base de dados devero ter acesso restrito, sendo permitido que apenas o/os **Quem deve ter acesso** terem este acesso e devero estar funcional 24 horas por dia, tendo em conta que sem os servidores, nenhuma base de dados estar funcional para ser consumida pelas aplicaes utilizadas na empresa.

De forma a limitar o acesso aos servidores, estes devero estar localizados numa localizao segura dentro da infraestrutura empresarial, ou seja, numa sala restrita com controlo de acesso adequado, utilizando cartes de identificao da empresa para fazer a sua autenticao.

Estas salas devero conter um sistema de monitoramento de segurana, utilizando equipamentos como cmaras de segurana e sensores, de forma a conseguir detetar e tentar interceptar algum tipo de acesso ou atividade suspeita.

Toda a atividade que envolva o acesso  sala de servidores e aos servidores em si, ficar registado em logs, anotando a identificao do carto acedido e hora de acesso ao mesmo, isto permitir que em caso de ataque seja feita uma anlise ao histrico de quem teve o acesso aos servidores.

Algo que ser mencionado nas atividades de mitigao relacionadas a todas as bases de dados  a informao que deve ser criptografada, o que  algo que no evita qualquer tipo de agresso feita, mas consegue evitar ou, pelo menos, ganhar tempo at o atacante decifrar a informao roubada.

## Atividades de Mitigao: Aplicao do Sistema de Apoio ao Cliente

Deve ser feito um controlo de acessos  aplicao do sistema de apoio ao cliente, controlando assim acessos indevidos  mesma, por exemplo um login feito com sucesso fora da rede empresarial. As realizaes de testes de segurana tm um papel crucial neste aspeto, pois estes detetaro lacunas no sistema de segurana da app. Os testes sero implementados com auxlio da ferramenta Selenium em juno com um software de VPN para fazer vrias simulaes de diferentes tipos de acesso a contas e mesmo ataques  aplicao de diferentes localizaes.

De forma a manter controlo de tudo o que est a ser efetuado na aplicao, ficaro registados todos os logs da mesma, de forma que caso haja algum ataque ou atividade duvidosa no software, seja mais fcil de identificar a entidade e operaes malignas.

Devem ser feitas tambm workshops de sensibilizao s prticas de segurana no desenvolvimento e utilizao do software periodicamente, isto ir alertar os funcionrios a implementar prticas mais seguras no desenvolvimento e utilizao da aplicao, fazendo com que estes evitem correr riscos de segurana.

## Atividades de Mitigao: Mquinas e ferramentas de fabricao

As mquinas e ferramentas de fabricao de produtos para venda so os recursos mais lucrativos para a empresa, tendo em conta que sem estas, os componentes eletrnicos no so desenvolvidos e, conseqentemente, a empresa no consegue gerar vendas.

Com isto,  importantssimo que sejam feitas inspees periodicamente  maquinaria de produo para garantir que estas se encontram em boas condies de funcionamento. Deve ser sempre verificado se h algum tipo de desgaste excessivo ou qualquer outro problema que possa afetar a qualidade de produo de produtos ou a segurana do recurso em si ou de quem est a utiliz-lo.

Assim que um desenvolvedor de hardware for contratado, deve ser agendado um treino de sensibilizao  segurana na utilizao das mquinas de fabricao de componentes eletrnicos, de forma que o trabalhador evite cometer erros que possam afetar a sua segurana e a avaria de uma mquina.

Devem ser feitos tambm workshops de sensibilizao  segurana a todos os desenvolvedores de hardware periodicamente, tendo em conta que as medidas de segurana esto sempre a ser atualizadas. Tendo em conta que o mau funcionamento ou desgaste de uma mquina pode levar  falta de segurana de um trabalhador, as boas prticas de segurana no sero o suficiente para evitar que certos incidentes aconteam, por isso deve ser fornecido os devidos equipamentos de segurana aos trabalhadores, estes so de uso obrigatrio quando os mesmos se encontram perto de uma mquina.

Em caso de acidente que envolva a maquinaria de produo, por mais mnimo que seja, este deve ser reportado e registado, isto permitir que seja feita uma melhor identificao de problemas que o recurso possa apresentar e evitar ou, pelo menos, atenuar ainda mais futuros riscos  zona de maquinaria, este dever utilizar o equipamento de proteo adequado e ser acompanhado por um desenvolvedor de hardware.

## Atividades de Mitigao: Base de dados de entregas

O acesso  base de dados de entregas deve ser restrito ao **Quem deve ter acesso**, excluindo assim uma grande quantidade de possveis atores a ataques  mesma, bem como deve estar disponvel 24 horas por dia, tentando apresentar o mximo de disponibilizao aos sistemas de informao, pois estes consomem constantemente os dados armazenados.

De forma a poder manter registo de aes efetuada  base de dados, devem ser mantidos registos de todos os acessos efetuados  mesma, bem como as operaes (queries) que foram

executadas, isto permitir que em caso de uma agresso tenha sido efetuada, estes logs mostraro quem teve acesso  base de dados, quando, onde e como.

Dever tm ser feito um backup da base de dados diariamente, de forma a repor os dados em caso de ataque. Dentro deste intervalo dirio, sero feitos registos em ficheiros de texto dos snapshots da database periodicamente, algo que estar explicado no Plano de Recuperao.

### **Atividades de Mitigao: Servidor de deployment de aplicaes**

Os servidores de deployment de aplicaes devero ter acesso restrito, sendo permitido que apenas o/os **Quem deve ter acesso** terem este acesso e dever estar funcional 24 horas por dia, tendo em conta que sem este  a base para o funcionamento de todas as aplicaes a funcionarem nos computadores e telemveis de cada funcionrio.

De forma a limitar o acesso aos servidores, estes devero estar localizados numa localizao segura dentro da infraestrutura empresarial, ou seja, numa sala restrita com controlo de acesso adequado, utilizando cartes de identificao da empresa para fazer a sua autenticao.

Estas salas devero conter um sistema de monitoramento de segurana, utilizando equipamentos como cmaras de segurana e sensores, de forma a conseguir detetar e tentar intercepar algum tipo de acesso ou atividade suspeita.

Toda a atividade que envolva o acesso  sala de servidores e aos servidores em si, ficar registado em logs, anotando a identificao do carto acedido e hora de acesso ao mesmo, isto permitir que em caso de ataque seja feita uma anlise ao histrico de quem teve o acesso aos servidores.

### **Atividades de Mitigao: Aplicaes do Sistema de Gesto dos Recursos Humanos**

Deve ser feito um controlo de acessos  aplicao do sistema de gesto dos recursos humanos, controlando assim acessos indevidos  mesma, por exemplo um login feito com sucesso fora da rede empresarial. As realizaes de testes de segurana tm um papel crucial neste aspeto, pois estes detetaro lacunas no sistema de segurana da app. Os testes sero implementados com auxlio da ferramenta Selenium em juno com um software de VPN para fazer vrias simulaes de diferentes tipos de acesso a contas e mesmo ataques  aplicao de diferentes localizaes.

De forma a manter controlo de tudo o que est a ser efetuado na aplicao, ficaro registados todos os logs da mesma, de forma que caso haja algum ataque ou atividade duvidosa no software, seja mais fcil de identificar a entidade e operaes malignas.

Devem ser feitas tm workshops de sensibilizao s prticas de segurana no desenvolvimento e utilizao do software periodicamente, isto ir alertar os funcionrios a Sistema de Segurana da empresa Dev4Sell



implementar práticas mais seguras no desenvolvimento e utilização da aplicação, fazendo com que estes evitem correr riscos de segurança.

### Atividades de Mitigação: Base de dados de produtos

O acesso à base de dados de produtos deve ser restrito ao **Quem deve ter acesso**, excluindo assim uma grande quantidade de possíveis atores a ataques à mesma, bem como deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização aos sistemas de informação, pois estes consomem constantemente os dados armazenados.

De forma a poder manter registo de ações efetuada à base de dados, devem ser mantidos registos de todos os acessos efetuados à mesma, bem como as operações (queries) que foram executadas, isto permitirá que em caso de uma agressão tenha sido efetuada, estes logs mostrarão quem teve acesso à base de dados, quando, onde e como.

Deverá também ser feito um backup da base de dados diariamente, de forma a repor os dados em caso de ataque. Dentro deste intervalo diário, serão feitos registos em ficheiros de texto dos snapshots da database periodicamente, algo que estará explicado no Plano de Recuperação.

### Riscos aceites

<FAZER TEXTO>

## Plano de Recuperao

O plano de recuperao  um conjunto de estratgias e aes desenvolvidas para salvaguardar informao no caso de haver uma agresso nos recursos crticos. Tem como objetivos principais delinear os detalhes do sistema de backups implementado permitindo a recuperao de informao em caso de falha, corrupo, alterao ou destruio de um recurso da Dev4Sell.

Na tabela apresentada a baixo est elaborado o sistema de backups implementado.

### Backup

Recurso	Informao	Local de armazenamento	Periodicidade	Notas
Base de dados de produtos	- Contm o armazenamento de dados relativos aos produtos em armazm	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas
Base de dados de clientes	- Contm o armazenamento de dados relativos aos clientes da empresa	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas
Base de dados de entregas	- Contm o armazenamento de dados relativos s entregas da empresa	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas
Servidores de deployment de aplicaes	- Aplicaes a decorrer	- Data center	1 vez	- Este servidor atua quando o servidor

				principal  interrompido ou destruido
Servidores de bases de dados	- Infraestrutura centralizada que suporta as bases de dados consumidas	- Data center	1 vez	- Este servidor atua quando o servidor principal  interrompido ou destruido
Aplicao do Sistema de Gesto de Recursos Humanos	- Consome Base de dados - Aplicao para a seco de recursos humanos trabalhar	- Base de dados de teste de verses	Sempre que houver uma nova verso da aplicao desenvolvida	- Quando necessrio aplicar um backup  necessrio detalhar a verso restaurada
Aplicao do Sistema de Gesto Financeira	- Consome Base de dados - Aplicao para a seco de Gesto Financeira trabalhar	- Base de dados de teste de verses	Sempre que houver uma nova verso da aplicao desenvolvida	- Quando necessrio aplicar um backup  necessrio detalhar a verso restaurada
Aplicao de Sistema de Apoio ao Cliente	- Consome Base de dados - Aplicao para atendimento ao cliente	- Base de dados de teste de verses	Sempre que houver uma nova verso da aplicao desenvolvida	- Quando necessrio aplicar um backup  necessrio detalhar a verso restaurada

## Guia de recuperao de Dados

Um guia de recuperao de dados  um conjunto de instrues/procedimentos que detalha de forma especifca e clara sobre como recuperar dados perdidos, danificados, corrompidos ou inacessiveis de dispositivos de armazenamento para normal funcionamento do sistema.

Nas tabelas a baixo iramos demonstrar os processos a detalhar para os recursos crticos. Como os procedimentos para todas as bases de dados e aplicaes funcionam da mesma forma apresentamos apenas um exemplo de cada tipo de recurso.

Recurso	Ordem	Verificaes	Subordem	Ao Corretiva
Bases de dados*	1	- Identificar a causa da perda de dados	1.1	- Determinar o motivo da perda de dados na BD.
			1.2	- Verificar a extenso da perda de dados
	2	- Verificar a integridade do backup	2.1	- Verificar se existe um backup para a base de dados em causa - Verificar se este backup apresenta dados corrompidos
			2.2	- Verificar o estado
	3	- Fazer restauro dos dados	3.1	- Preparar o ambiente de restaurao, criando uma base de dados
			3.2	- Efetuar o backup para a nova base de dados
	4	- Fazer verificao dos dados inseridos na nova base de dados	4.1	- Verificar se os dados esto corretos
			4.2	- Executar testes de consulta dos registos e relaes diretamente no IDE da base de dados ou a partir de uma API para testes
	5	- Atualizar as configuraes nas aplicaes para a nova base dados	5.1	- Configurar as conexes s bases de dados, alterando as connection strings de cada aplicao

			5.2	- Atualizar identificadores, chaves e relaes entre objetos
	6	Efetuar um novo backup	6.1	- Realizar novo backup dos dados atuais para possvel futuro ataque prximo
Servidores de deployment de aplicaes	1	- Avaliar a causa da interrupo do servidor	1.1	- Identificar a causa da interrupo do servidor e das aplicaes
			1.2	- Tentar obter informaes sobre eventos que ocorreram antes da falha
	2	- Isolar o problema e tentar restaurar o servidor	2.1	- Isolar o servidor afetado do ambiente de produo para evitar danos adicionais
			2.2	- Restaurar o servidor usando o backup mais recente do sistema
	3	- Testar as aplicaes restauradas	3.1	- Aps a restaurao efetuar testes nas aplicaes (funcionalidades)
			3.2	- Monitorizar os “logs” das aplicaes para verificar se h erros posteriores ao backup
	4	- Implementar medidas preventivas (aps efetuado o restauro)	4.1	- Assim que o servidor for restaurado, rever as medidas de segurana

Aplicações dos sistemas**	1	- Diagnosticar a causa da falha da aplicação	1.1	- Analisar as mensagens de erro
			1.2	- Identificar a causa da falha da aplicação
	2	- Isolar e restaurar a aplicação	2.1	- Isolar a aplicação afetada do ambiente de produção para evitar que a falha se propague
			2.2	- Restaurar a aplicação recorrendo à versão mais recente e que apresente os melhores resultados obtidos em testes
	3	- Verificar a conexão e recursos necessários	3.1	- Verificar a conexão com a rede para garantir que a aplicação está conectada com o servidor
	4	- Testes e monitorização do restauro	4.1	- Realizar testes abrangentes a toda a aplicação restaurada para verificar as funcionalidades
			4.2	Implementar mecanismos de monitorização para prevenir problemas semelhantes futuros

*\*Este procedimento é utilizado da mesma forma para todos os recursos que sejam base de dados.*

*\*\*Este procedimento é utilizado da mesma forma para todos os recursos que sejam aplicações.*

## **Plano de Reposição**

<Falar sobre este plano>

## Plano de Contingncia

<Falar sobre este plano>

## Auditoria

A auditoria pretende controlar a observncia das medidas de segurana informtica aprovadas, consiste em operaes peridicas de controlo das medidas de segurana, esta pode ser assumida por auditores internos ou externos.

Desempenha um papel fundamental para garantir a privacidade, integridade e disponibilidade dos dados e informaes em uma empresa. Ao avaliar os processos relacionados aos sistemas de informao, a auditoria contribui para a proteo dos recursos da empresa, para a mitigao de riscos e para a eficincia e a transparncia dos processos de negcio.

A auditoria na Dev4Sell ser efetuada por auditores externos, levando em considerao que se trata de uma empresa de pequena/mdia dimenso e que aparenta estar em crescimento, portanto no justifica ter de contratar auditores internos, esta deciso evita gastos adicionais com slrios e despesas desnecessrias a longo prazo.

### Auditoria Externa

A auditoria externa  um processo em que uma empresa especializada e independente  contratada para avaliar os sistemas de informao de uma organizao.

Tem como objetivos garantir que a empresa se encontre em conformidade com as regulamentaes e padres de segurana impostas pela mesma, identificar falhas e vulnerabilidades de segurana nos sistemas de informao, avaliar a eficcia das polticas impostas, certificar que as instalaes e outros recursos fsicos se encontram nas condies necessrias para a eficcia e segurana do trabalho e oferecer recomendaes para melhoria.

O auditor deve inicialmente fazer a recolha de informao relevante sobre os sistemas de informao da Dev4Sell e, com esses dados, fazer o planeamento juntamente com a empresa em causa dos procedimentos e objetivos a serem atingidos.

A auditoria deve ter como procedimentos os seguintes passos:

- Verificar a integridade fsica da infraestrutura da Dev4Sell
- Verificar a integridade fsica das mquinas de produo de componentes eletrnicos
- Verificar a integridade fsica dos camies de entrega de produtos
- Verificar a segurana de acesso  sala de servidores de bases de dados, backup e deployment
- Verificar vulnerabilidades na rede privada



- Verificar acessos indevidos a aplicações da empresa
- Verificar acessos indevidos às bases de dados das empresas
- Verificar se as políticas de segurança da empresa estão a ser cumpridas pelos trabalhadores
- Realizar uma análise e avaliação de riscos para fazer a identificação de possíveis ameaças face os resultados da auditoria
- Identificação de falhas ou vulnerabilidades de segurança nos sistemas de informação
- Revisão e avaliação do plano de segurança da empresa
- Recomendações de alterações a serem efetuadas no plano de segurança da empresa

Estes procedimentos poderão ter diferentes abordagens para serem executados como por exemplo efetuar testes de penetração de sistemas, revisão de políticas e procedimentos da empresa, fazer um conjunto de questões a funcionários escolhidos de forma aleatória em relação a medidas de segurança na empresa, entre outros.

Finalmente, deve ser realizado um relatório com os resultados obtidos na auditoria realizada, juntamente com a identificação de vulnerabilidades encontradas e o que a empresa tem por melhorar a nível de segurança.

A auditoria deve ser realizada pelo menos 1 vez por ano, sendo que pode ser agendada mais avaliações em caso, por exemplo, de serem feitas e implementadas alterações no plano de segurança da empresa.

## Simulacros

Os simulacros são exercícios de simulação da ocorrência de uma agressão em um recurso da empresa que implique um impacto alto na mesma, são essenciais para testar a eficácia dos procedimentos de segurança, identificar vulnerabilidades nesses procedimentos e capacitar os funcionários a responder de forma adequada aos acidentes.

Como já foi referido anteriormente no documento, serão feitos workshops, palestras e formações de sensibilização à segurança no trabalho para os funcionários da Dev4Sell, porém também serão realizados simulacros de treino, no qual todos os funcionários serão avisados 1 dia antes da ocorrência do mesmo. Estes simulacros de treino serão acompanhados por **Quem tiver de liderar (Gestor/Diretor RH)**, que irá fazer a orientação aos funcionários dos passos a serem executados de forma que os procedimentos de segurança sejam eficazes, isto também poderá revelar certas vulnerabilidades no plano de segurança e devem ser feitos pelo menos três vezes por semestre anual.

Os simulacros surpresa serão realizados uma vez por semestre anual e devidamente planeados tendo em conta os riscos mais prováveis de acontecer à empresa, apenas **Quem**

**tiver deva ser avisado** serão notificados desta simulação, os restantes membros da empresa não saberão das datas agendadas para a realização dos simulacros e não terão o auxílio de outros funcionários da mesma forma que tiveram nos treinos.

Por fim será feita uma avaliação no final de cada simulacro surpresa, ficando registado num relatório todos os eventos ocorridos na simulação da agressão, deverão ficar anotados os riscos que foram simulados, pontos fortes e pontos fracos nos procedimentos de segurança, de forma que sejam tomadas medidas corretivas e sejam atualizados os protocolos de segurança, se necessário.

Importante também anotar que o agendamento destes eventos devem ser devidamente planeados entre **Membros importantes da empresa** e não devem prejudicar o negócio da empresa, focando-se a realizarem-se em épocas de vendas mais baixas e com menos quantidade de produção.

## **Biografia**

<Biografia>