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 7](#_Toc137294554)

[Contextualização do documento 7](#_Toc137294555)

[Descrição da empresa 7](#_Toc137294556)

[Funções e responsabilidades 8](#_Toc137294557)

[Processos de Negócio 15](#_Toc137294558)

[PN01 – Parcerias comerciais com os fornecedores 15](#_Toc137294559)

[PN02 – Parcerias comerciais com os clientes 15](#_Toc137294560)

[PN03-Gestão de Stock 16](#_Toc137294561)

[PN04 – Venda 17](#_Toc137294562)

[Método de Avaliação de Risco 18](#_Toc137294563)

[Octave 18](#_Toc137294564)

[Arquitetura dos Sistemas 19](#_Toc137294565)

[Sistema de Administração da Empresa 19](#_Toc137294566)

[Sistema de Comunicação Interna 20](#_Toc137294567)

[Rede Telefónica 20](#_Toc137294568)

[Sistema de Email Interno 20](#_Toc137294569)

[Sistema de Armazenamento de Dados 20](#_Toc137294570)

[Sistema de Produção 21](#_Toc137294571)

[Sistema de Aplicações 21](#_Toc137294572)

[Aplicações de suporte ao funcionário (Computador) 22](#_Toc137294573)

[Aplicação de auxílio de entregas e consulta de stock (Smartphone) 22](#_Toc137294574)

[Recursos 23](#_Toc137294575)

[Físicos 23](#_Toc137294576)

[Humanos 24](#_Toc137294577)

[Dados 26](#_Toc137294578)

[Suporte de Dados 27](#_Toc137294579)

[Aplicações 28](#_Toc137294580)

[Análise e Gestão de Riscos 30](#_Toc137294581)

[Recursos críticos 31](#_Toc137294582)

[Ameaças e vulnerabilidades 35](#_Toc137294583)

[Análise e Avaliação do Risco 40](#_Toc137294584)

[Plano de Mitigação 47](#_Toc137294585)

[Atividades de Mitigação: Base de dados de finanças 47](#_Toc137294586)

[Atividades de Mitigação: Base de dados de clientes 48](#_Toc137294587)

[Atividades de Mitigação: Base de dados de funcionários 48](#_Toc137294588)

[Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos (Transferir) 49](#_Toc137294589)

[Atividades de Mitigação: Aplicação do Sistema de Gestão Financeira 49](#_Toc137294590)

[Atividades de Mitigação: Servidores de bases de dados 49](#_Toc137294591)

[Atividades de Mitigação: Aplicação do Sistema de Apoio ao Cliente 50](#_Toc137294592)

[Atividades de Mitigação: Máquinas e ferramentas de fabricação 51](#_Toc137294593)

[Atividades de Mitigação: Base de dados de entregas 52](#_Toc137294594)

[Atividades de Mitigação: Servidores de deployment de aplicações 52](#_Toc137294595)

[Atividades de Mitigação: Aplicações do Sistema de Gestão dos Recursos Humanos 53](#_Toc137294596)

[Atividades de Mitigação: Base de dados de produtos 53](#_Toc137294597)

[Riscos aceites 54](#_Toc137294598)

[Plano de Recuperação 55](#_Toc137294599)

[Backup 55](#_Toc137294600)

[Guia de Reposição dos Dados 57](#_Toc137294601)

[Plano de Contigência 61](#_Toc137294602)

[Auditoria 63](#_Toc137294603)

[Auditoria Externa 63](#_Toc137294604)

[Simulacros 64](#_Toc137294605)

[Biografia 66](#_Toc137294606)

**Lista de Tabelas**

[Tabela 1 - Departamentos da Dev4Sell 8](#_Toc137294747)

[Tabela 2 - Cargos de cada departamento da Dev4Sell 10](#_Toc137294748)

[Tabela 3 - Recursos Físicos da Dev4Sell 23](#_Toc137294749)

[Tabela 4 - Recursos Humanos da Dev4Sell 24](#_Toc137294750)

[Tabela 5 - Recursos de Dados da Dev4Sell 26](#_Toc137294751)

[Tabela 6 - Recursos de Suporte de Dados da Dev4Sell 27](#_Toc137294752)

[Tabela 7 - Recursos de Aplicações da Dev4Sell 28](#_Toc137294753)

[Tabela 8 - Descrição das classificações dos três pilares da segurança 31](#_Toc137294754)

[Tabela 9 - Análise do nível de impactos nos recursos da Dev4Sell 32](#_Toc137294755)

[Tabela 10 - Descrição das ameaças nos recursos da Dev4Sell 35](#_Toc137294756)

[Tabela 11 - Classificação dos riscos nos recursos da Dev4Sell 40](#_Toc137294757)

[Tabela 12 - Backups da Dev4Sell 55](#_Toc137294758)

[Tabela 13 - Guia de Recuperação de Dados 57](#_Toc137294759)

[Tabela 14 - Plano de Reposição 61](#_Toc137294760)

# Introdução

## Contextualização do documento

O projeto visa apresentar um plano de segurança detalhado para a empresa, levando em consideração as suas metodologias, processos de negócio e recursos. Esse plano engloba uma estratégia completa de gestão de riscos, bem como planos de segurança, recuperação, reposição e contingência.

O plano pretende proteger os ativos, informações e infraestrutura da empresa, identificando e mitigando riscos, implementando medidas preventivas e estabelecendo procedimentos para lidar com incidentes de segurança. Serão adotadas políticas de segurança, controlos de acesso, monitorização, treino de funcionários e auditoria. O plano será revisto regularmente para garantir a sua eficácia contínua.

## Descrição da empresa

A empresa a que será proposto este plano denomina-se de Dev4Sell. O termo "Dev" representa desenvolvimento e "Sell" representa venda, que compõem o nome da empresa e descrevem as suas principais funções.

A Dev4Sell é uma empresa especializada no desenvolvimento e fornecimento de equipamentos eletrónicos para empresas de grande e médio porte, que por sua vez comercializam esses produtos para o público em geral. Além disso, a empresa recebe suporte material de patrocinadores para a fabricação dos seus produtos.

### Funções e responsabilidades

Com base na estrutura da empresa Dev4Sell, segue-se abaixo a tabela com a identificação dos departamentos e as suas descrições:

Tabela - Departamentos da Dev4Sell

|  |  |
| --- | --- |
| Departamentos | Descrição |
| CEO | Lidera a Dev4Sell, atuando como intermediário entre os diferentes diretores e departamentos da empresa. Tem acesso a toda a informação que circula na empresa. |
| Diretor(a) | Responsável por uma área específica da empresa, como finanças, operações, marketing, recursos humanos, etc. Supervisiona e coordena as equipas nessa área e fornece suporte ao CEO a definir decisões estratégicas para a empresa. |
| Departamento de Recursos Humanos | Responsável pela seleção e recrutamento de novos funcionários, além de gerir o desempenho e as relações no ambiente de trabalho. Garantem a conformidade com as normas da empresa. |
| Departamento de Gestão de Sistemas de Informação | Composto por membros da empresa responsáveis pela supervisão da segurança dos dados utilizados nos sistemas e as práticas de segurança da Dev4Sell. |
| Departamento de Vendas | Composto por profissionais de marketing, analistas de mercado que preveem o sucesso de produtos, e gestores de vendas que criam estratégias e planos de negociação com os clientes. |
| Departamento de Finanças | Responsável por todas as atividades financeiras da empresa, tendo de otimizar a utilização dos recursos financeiros disponíveis e fornecer informações precisas e relevantes para a tomada de decisões estratégicas. |
| Departamento de Logística | Encarregado de gerir a movimentação e armazenamento de materiais e produtos, bem como a distribuição e entrega dos mesmos. |
| Departamento de Desenvolvimento e Produção | Responsável pelo design e construção dos equipamentos eletrónicos da empresa. |
| Departamento de Apoio ao cliente | Responsáveis por dar assistência ao cliente via website, móvel ou correio eletrónico, quer seja para esclarecimento de dúvidas ou possíveis negócios. |

A tabela a seguir apresenta os diferentes cargos de cada departamento, acompanhado da quantidade de funcionários que ocupam cada cargo e uma breve descrição das suas responsabilidades. Isso fornecerá uma visão mais detalhada da estrutura organizacional da empresa.

Tabela 2 - Cargos de cada departamento da Dev4Sell

|  |  |  |  |
| --- | --- | --- | --- |
| Departamento | Cargo | Quantidade | Descrição |
| Departamento de Recursos Humanos | Gerente do Departamento de Recursos Humanos | 1 | Gere e desenvolve as políticas e práticas relacionadas aos recursos humanos.  Supervisiona e garante o correto funcionamento do seu departamento. |
| Técnico de Recursos Humanos | 2 | Recruta e seleciona novos funcionários.  Coordena e processa toda a documentação empresarial.  Realiza treinos de sensibilização em diversas áreas dos recursos humanos. |
| Assistente de Recursos Humanos | 2 | Fornece suporte administrativo, auxiliando assim os técnicos e gerente do departamento. |
| Departamento de Sistemas de Informação | Gerente do Departamento de Sistemas de Informação | 1 | Supervisiona e coordena todas as atividades relacionadas com a área dos Sistemas de Informação, garantindo o correto funcionamento do seu departamento.  Tem um papel crucial no eficiência e segurança dos SI na empresa. |
| Administrador da Bases de Dados | 1 | Administra as bases de dados da empresa.  Conhece o funcionamento de todos os departamentos a nível de acesso e manipulação da informação. |
| Especialista de Segurança da Informação | 2 | Garante a segurança dos sistemas e dos dados da empresa. |
| Técnico de Suporte dos Sistemas de Informação | 2 | Fornece suporte técnico no uso de tecnologias de informação.  Deve estar pronto a agir assim que uma falha ou avaria relacionada com os sistemas de informação ocorra. |
| Departamento de Negócios | Gerente do Departamento de Negócios | 1 | Gere e supervisiona todas as atividades relacionadas às vendas e compras da empresa.  Encarregue do correto funcionamento do seu departamento. |
| Coordenador de Compras | 1 | Lidera as atividades de compra, incluindo pesquisa de fornecedores, negociação de contratos e acompanhamento de prazos de entrega.  Fornece suporte aos executivos de compras quando necessário. |
| Coordenador de Vendas | 1 | Lidera as atividades de venda, desenvolvendo estratégias, identificando oportunidades no mercado e garantindo a satisfação do cliente.  Fornece suporte aos executivos de vendas quando necessário. |
| Executivo de Compras | 2 | Realiza o processo de compra, pesquisa por fornecedores, avalia propostas e toma decisões de compra. |
| Executivo de Vendas | 2 | Realiza o processo de venda, procura por clientes, fornece informações sobre os produtos e negoceia contratos. |
| Analista de Mercado | 1 | Recolhe informação sobre os consumidores, empresas concorrentes, tendências, oportunidades de negócio entre outras informações relevantes do mercado. |
| Departamento de Marketing | Gerente do Departamento de Marketing | 1 | Gere e desenvolve as políticas e práticas relacionadas com o marketing da empresa.  Supervisiona e garante o correto funcionamento do seu departamento. |
| Especialista em Marketing | 5 | Desenvolve e implementa estratégias de marketing para promover os produtos e a empresa. |
| Designer Gráfico | 1 | Cria materiais gráficos e visuais para campanhas de promoção. |
| Departamento de Finanças | Gerente do Departamento de Finanças | 1 | Gere as atividades financeiras da empresa, incluindo o controlo de custos e orçamentos, e planeamento financeiro.  Este supervisiona e garante o correto funcionamento do seu departamento. |
| Especialista de Análise Financeira | 1 | Analisa e interpreta os dados financeiros da empresa, incluindo elaboração de relatórios e suporte na tomada de decisões financeiras. |
| Tesoureiro | 1 | Gere o controle de fluxo de transações financeiras e contas bancárias.  Garante a disponibilidade adequada de fundos para investimentos e operações da empresa. |
| Departamento de Logística | Gerente do Departamento de Logística | 1 | Supervisiona e gere todas as atividades relacionadas com as atividades logísticas, tendo assim um papel crucial na organização de recursos e produtos da empresa.  Supervisiona e garante o correto funcionamento do seu departamento. |
| Técnico de Logística e Abastecimento | 1 | Gere o fluxo de materiais e recursos da empresa, além da relação com fornecedores e planeia a aquisição de materiais. |
| Analista de Stock de Recursos e Produtos | 2 | Monitoriza, analisa e gere o stock de produtos e recursos. |
| Equipa de Transporte | 10 | Realizam e asseguram a entrega dos produtos nos períodos estipulados. |
| Departamento de Desenvolvimento e Produção | Gerente do Departamento de Desenvolvimento e Produção | 1 | Gere e desenvolve as políticas e práticas relacionadas com o desenvolvimento e produção de componentes eletrônicos da empresa.  Supervisiona e garante o correto funcionamento do seu departamento. |
| Gestor de Projetos | 4 | Coordena e executa os projetos relacionados ao desenvolvimento e produção de equipamentos eletrônicos.  É um pilar crucial para a comunicação e gestão de recursos necessários em cada projeto. |
| Designer Industrial | 3 | Cria conceitos de design, desenvolve desenhos técnicos e modelos 3D dos produtos a serem produzidos. |
| Engenheiro de Desenvolvimento de Hardware | 15 | Responsável pela produção de componentes eletrônicos a nível físico. |
| Engenheiro de Desenvolvimento de Software | 30 | Responsável pela produção de componentes eletrônicos a nível lógico.  Produz o software necessário para o funcionamento dos equipamentos e elabora as aplicações para o consumo de dados, para uso da empresa. |
| Especialista em Quality Assurance | 5 | Garante a fiabilidade e durabilidade dos componentes eletrônicos comprados e produzidos. |
| Departamento de Apoio ao Cliente | Gerente do Departamento de Apoio ao Cliente | 1 | Gere e desenvolve as políticas e práticas relacionadas com o atendimento ao cliente da empresa.  Supervisiona e garante o correto funcionamento do seu departamento. |
| Especialistas de Atendimento ao Cliente | 10 | Fornece suporte e assistência aos clientes. |
| Especialistas em Retenção de Clientes | 2 | Garante a satisfação e minimização ativa da base de clientes. |

# Processos de Negócio

Processos de negócio garantem o funcionamento eficiente dos padrões de trabalho da Dev4Sell. Neste capítulo, encontram-se descritos os principais processos que fornecendo uma estrutura sólida para a realização de atividades-chave.

## PN01 – Parcerias comerciais com os fornecedores

Para que a Dev4Sell possa iniciar todos os seus processos de negócio, é necessário contar com os fornecedores de stock para desenvolvimento dos produtos a serem vendidos. Esses materiais são adquiridos por meio de parcerias com empresas de matéria-prima. Abaixo seguem os subprocessos envolvidos nas parcerias realizadas:

**Identificação de stock necessário:** Este processo inicia-se com a identificação do tipo de artigos que serão necessários, e depois empresas que poderão oferecer esse tipo de serviços.

**Dev4Sell entra em contacto com os possíveis fornecedores:** Após a identificação de possíveis fornecedores, é realizado um contacto, com o objetivo de marcar uma reunião a fim de negociar.

**Reunião:** durante a reunião é estabelecido os termos e condições desta parceria, envolvendo o tipo de serviços esperados, prazos, orçamentos, requisitos e clausulas contratuais. Após a negociação é chegado a um acordo e possivelmente fechado um contrato ou não.

## PN02 – Parcerias comerciais com os clientes

Antes de iniciar o processo de venda, o cliente deve estabelecer uma parceria ou fazer um pedido à Dev4Sell. Neste ponto, será 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 eletrónico, que será recebido pelo departamento de atendimento ao cliente.

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

**Reunião:** Durante a reunião, são discutidos os interesses do cliente, como serviços prestados, orçamentos, datas e contratos. A reunião pode resultar em diferentes desfechos, como a reprovação ou possível interesse. Numa situação de interesse, a proposta será submetida a um processo de aprovação, com a análise de vários departamentos da Dev4Sell para avaliar os benefícios da parceria. Opcionalmente, o cliente poderá 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 econômico 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 a 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

O método de avaliação de risco é utilizado para fazer a identificação, análise e avaliação dos riscos presentes nos sistemas, portanto fazer a seleção correta da framework a utilizar é crucial.

Entre as diversas ferramentas de avaliação e gestão de riscos, a que pareceu ser a melhor opção para este plano de segurança foi o OCTAVE, versão Allegro.

## Octave

O OCTAVE é uma metodologia abrangente e flexível para a identificação de riscos através da autoavaliação organizacional.

Ajuda as organizações a aplicar a informação de gestão de risco de segurança para assegurar a sua infraestrutura da informação existente e proteger os 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 Allegro tendo em conta que é uma versão projetada para 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 percetível, sem exigir conhecimentos extensivos nesta área.

# Arquitetura dos Sistemas

A arquitetura da Dev4Sell encontra-se dividida em 5 sistemas que desempenham um papel importante na estruturação e no funcionamento eficiente de todos os recursos da empresa.

Numa fase inicial será referido o funcionamento do sistema de administração empresarial, que tem como objetivo fazer a análise e gestão dos vários recursos ou mesmo processos de negócio 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 serão abordados os sistemas relativos à comunicação interna da empresa, sistema de armazenamento de dados e sistema de produção. Será analisada a metodologia de comunicação fluída e eficaz entre as diferentes entidades envolvidas, algo considerativo no sucesso dos processos de negócio e na segurança e preservação dos dados relacionados com a empresa, produtos e clientes.

Por fim, será analisado neste capítulo os sistemas aplicacionais que contêm a lógica de armazenamento dos dados e a interação com os mesmos que servirão de suporte à análise de estados de certos processos como entregas ou desenvolvimento de produtos eletrônicos. Estes sistemas têm como principal objetivo apoiar diretamente os funcionários de forma a contribuir beneficamente para o seu papel num processo de negócio.

## Sistema de Administração da Empresa

Sistema de análise e gestão de recursos e processos de negócio em curso. Os recursos humanos realizam tarefas como:

* Monitorização de uma entrega;
* Análise de pedidos feitos pelos clientes;
* Análise financeira da empresa;
* Análise de faturas pendentes;
* Revisão periódica de veículos de entrega;
* Etc.

Para aceder a este sistema, o utilizador necessitará de fazer login com as suas credenciais empresariais que são registadas durante o primeiro contrato.

## Sistema de Comunicação Interna

Sistema que estabelece uma ligação segura e eficiente entre todos os equipamentos localizados na infraestrutura, incluindo a maquinaria de produção, computadores e bases de dados. É incluída uma rede telefónica para a comunicação rápida entre funcionários e um sistema de email interno para a troca de informação mais sensível.

### Rede Telefónica

Apesar dos funcionários deterem de um smartphone empresarial, este não possui funcionalidade de comunicação interna. Para isso foi criada esta rede telefónica utilizada para estabelecer comunicação entre diferentes departamentos de uma forma mais segura e rápida.

É de notar que esta deve ser utilizada apenas para comunicar informação de baixa ou média sensibilidade.

### Sistema de Email Interno

O sistema de email interno é utilizado para trocar informações mais sensíveis e de maior importância. Este permitirá a criação de um email com o domínio “@dev4sell.pt”, que o identificará como uma conta associada à empresa.  
 Este será um serviço pago à Google a partir de uma subscrição.

## Sistema de Armazenamento de Dados

Sistema que segue os procedimentos estipulados pela empresa, para fazer o devido armazenamento, manipulação e acesso a dados relacionados com todo o tipo de informação que circula pela empresa, tal como:

* Faturas;
* Documentos contratuais;
* Pedidos de entrega;
* Agenda e estado dos pedidos;
* Stock de produtos;
* Dados de clientes e o seu histórico de ações;
* Registo de recursos;
* Etc.

Devido a este também estar responsável pelo tratamento e segurança dos dados altamente valiosos, torna-se num dos sistemas mais importantes e que possivelmente mais impactantes 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

Sistema responsável pelo planeamento, desenvolvimento e montagem de componentes eletrônicos que serão colocados para venda ou para a reposição e preparação de futuras vendas.

É composto pela equipa de desenvolvimento que ficará encarregue de desenhar a 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.

Como ferramentas de auxílio no desenvolvimento dos componentes, será utilizado uma grande diversidade de linguagens e ambientes de desenvolvimento integrado, tendo em conta a gama de produtos a ser produzida.

## Sistema de Aplicações

Sistema de suporte a todos os sistemas anteriormente referidos, fornecendo uma interface interativa para haver a comunicação entre os funcionários 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, identificando cada funcionário.

Tendo em conta o tipo de funcionário registado 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 de análise de histórico de faturas, vendas feitas recentemente, etc.

Foram criados 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 monitorização de uma entrega.

### Aplicações de suporte ao funcionário (Computador)

Aplicação principal para auxiliar o trabalho de cada membro da empresa 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 eletrônicos
* Interface de workflow de projetos de equipas de desenvolvimento
* Interface para gestão de recursos humanos da empresa

Para a maior parte dos funcionários, esta é a única forma de eles terem uma interação e visualização da informação armazenada em base, portanto, o bom funcionamento deste sistema é crucial.

### 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 entregas, estando assim incluídas as funcionalidades de:

* Consultar e responder a pedidos de entrega feitos pelo cliente;
* Verificação de stock;
* Alterar o estado da entrega 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

Para o sucesso na performance dos sistemas será necessário que esta contenha recursos, que se trata de meios que podem ser utilizados para um determinado fim. Estes possuem um valor e sofrem ataques, sejam estes físicos, cibernéticos, etc.  
 Os recursos podem ser divididos em 5 tipos, nos quais serão analisados:

* Físicos;
* Humanos;
* Dados;
* Suporte de Dados;
* Aplicações.

## Físicos

Ativos tangíveis, como instalações e equipamentos, que suportam as operações da empresa.

Tabela 3 - Recursos Físicos da Dev4Sell

|  |  |  |
| --- | --- | --- |
| Nome | Descrição | Sistemas em que é utilizado |
| Infraestrutura | Estrutura física da empresa que serve de suporte para o funcionamento dos sistemas e equipamentos. | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Produção * Sistema de Aplicações |
| Computadores e Telemóveis | Equipamento de auxílio para interação com os sistemas. | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Produção * Sistema de Aplicações |
| Máquinas de teste de componentes | Conjunto de equipamentos utilizados para realizar a *quality assurance* dos equipamentos produzidos. | * Sistema de Armazenamento de Dados * Sistema de Produção * Sistema de Aplicações |
| Máquinas e ferramentas de fabricação | Equipamentos utilizados no processo de produção. | * Sistema de Produção |
| Router Gateway | 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. | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Aplicações |
| Switches | Equipamentos necessários para estabelecer a ligação entre equipamentos na rede local. | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Produção * Sistema de Aplicações |
| Armazém de produtos | Local de armazenamento de equipamentos eletrônicos desenvolvidos pela empresa. | * Sistema de Administração da Empresa * Sistema de Armazenamento de Dados * Sistema de Produção |
| Camiões de entrega | Equipamento de auxílio às entregas e recolhas de produtos. Utilizados para transportar os produtos. | * Sistema de Administração da Empresa |

## Humanos

Todos os departamentos que integram os funcionários que contribuem para o correto funcionamento da empresa. Encontra-se uma descrição mais detalhada de cada departamento no subcapítulo da descrição da empresa.

Tabela 4 - Recursos Humanos da Dev4Sell

|  |  |
| --- | --- |
| Nome | Sistemas em que atuam |
| Departamento de Recursos Humanos | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Aplicações |
| Departamento de Sistemas de Informação | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados |
| Departamento de Negócios | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Aplicações |
| Departamento de Marketing | * Sistema de Comunicação Interna |
| Departamento de Finanças | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Aplicações |
| Departamento de Logística | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Aplicações |
| Departamento de Desenvolvimento e Produção | * Sistema de Administração da Empresa * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Aplicações * Sistema de Produção |
| Departamento de Apoio ao Cliente | * Sistema de Comunicação Interna * Sistema de Armazenamento de Dados * Sistema de Aplicações |

## Dados

Toda a informação armazenada em sistemas de bases de dados.

Tabela 5 - Recursos de Dados da Dev4Sell

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nome | Descrição | Fonte dos dados | Nível de Acesso | Responsável pelos dados |
| Base de dados de produtos | Base de dados que contêm a informação acerca do armazém de stock de produtos desenvolvidos e recursos comprados. | Produtos desenvolvidos e comprados. | Médio | Gerente do Departamento de Logística |
| Base de dados de clientes | Base de dados que contêm as informações dos clientes da empresa. | Entidades que entrem em contacto com a empresa e que estejam interessadas na compra de um produto ou interações com a empresa. | Alto | Gerente do Departamento de Apoio ao Cliente |
| Base de dados de funcionários | Base de dados que contêm as informações dos funcionários da empresa e registos de performance. | Recursos humanos contratados, histórico de vendas e análise de KPIs. | Alto | Gerente do Departamento dos Recursos Humanos |
| Base de dados de entregas | Regista o progresso de cada entrega que foi feita pela empresa, registando datas, locais e estados. | Pedidos feitos pelos clientes, relatórios de equipas de entrega e atualizações na aplicação do sistema de entregas. | Alto | Gerente do Departamento de Logística |
| Base de dados de finanças | Regista informações relacionadas às transações e faturação, incluindo detalhes de vendas, pagamentos e outras informações financeiras relevantes. | Transações realizadas pela empresa ou pelos clientes. | Alto | Gerente do Departamento de Finanças |
| Base de dados de testes de versões | Regista resultados testes executados após a submissão de versões novas de cada aplicação. | Versão testada, quantidade de utilizadores, quantidade de requests executados, quantidade de requests com resposta OK, tempo de execução. | Médio | Gerente do Departamento de Desenvolvimento e Produção |

## Suporte de Dados

Infraestrutura e tecnologias que armazenam e protegem os dados.

Tabela 6 - Recursos de Suporte de Dados da Dev4Sell

|  |  |
| --- | --- |
| Nome | Descrição |
| Servidores de deployment de aplicações | Recurso de alto desempenho e confiabilidade responsável por disponibilizar e executar as aplicações em um ambiente operacional. |
| Impressoras | Recurso responsável pela impressão de documentos como relatórios, faturas, contratos, etc. |
| Servidores de bases de dados | Recurso que tem o objetivo de armazenar e gerir todos os dados relacionados com a Dev4Shell. |
| Servidor de armazenamento em nuvem para documentos | A Dev4Sell utiliza serviços da Google, pagando uma subscrição, que terão como objetivo de armazenar documentos como relatórios, contratos, faturas, etc. |
| Servidor de backup de base de dados | Recurso que serve de reserva do servidor de base de dados. Este é utilizado para realizar cópias de segurança dos dados críticos da empresa. |
| Armazenamento de backup em disco | Servidor responsável por armazenar o backup de todos os discos utilizados pelas máquinas da empresa, de modo a manter em registo as ações realizadas pelos funcionários. |

## Aplicações

Softwares e ferramentas utilizadas para analisar, processar e manipular os dados.

Tabela 7 - Recursos de Aplicações da Dev4Sell

|  |  |
| --- | --- |
| Nome | Descrição |
| Ambientes de desenvolvimento (IDE) | Recurso que fornece um conjunto de ferramentas para facilitar o desenvolvimento de software. |
| Aplicação de Gestão de Stock | Aplicação de controlo e gestão de stock presente nos armazéns da empresa. |
| Aplicação de Gestão de Vendas e Entregas | Aplicação que auxilia no processo de gestão de vendas, desde o registo do pedido até à entrega do produto ao cliente. |
| Aplicação de Gestão de Recursos Humanos | Aplicação que facilita a administração e a gestão das atividades relacionadas aos funcionários da empresa. |
| Aplicação de Gestão Financeira | Aplicação que ajuda a empresa a controlar e gerir as suas atividades financeiras. Esta rastreará qualquer tipo de transações e também analisará pagamentos pendentes relacionados com o negócio da empresa ou não. |
| Aplicação de Apoio ao Cliente | Aplicação que permite gerir, analisar e atender a pedidos feitos pelos clientes, exibindo na sua interface solicitações de produtos, queixas ou pedidos de ajuda que não tenham sido feitos via chamada telefónica. |
| Rede de Comunicação Interna da Empresa | Infraestrutura de comunicação interna da empresa, que estabelecerá a ligação entre os diferentes departamentos da Dev4Sell. |

# Análise e Gestão de Riscos

Tendo em conta o elevado número de recursos da Dev4Sell, assume-se a possibilidade de uma vasta diversidade de riscos. Estes serão analisados, tendo em causa o seu impacto e prejuízo.

Em geral, é possível analisar que os riscos, dependendo de cada um, irão afetar os seguintes fatores:

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

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

De seguida serão 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.

Por fim, será feita a análise e avaliação dos riscos onde será atribuída uma classificação, em diferentes fatores:

* Impacto
* Gravidade
* Probabilidade

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

## Recursos críticos

Recursos que tenham um nível de impacto alto em qualquer um dos três principais pilares da segurança quando sofre um ataque.

Estes recursos necessitarão de especial atenção, pois quando sofrem um ataque poderão causar um enorme prejuízo para a empresa.

Tabela 8 - Descrição das classificações dos três pilares da segurança

|  |  |  |  |
| --- | --- | --- | --- |
| Pilar de Segurança | Baixo | Médio | Alto |
| **Privacidade** | Quando a informação foi divulgada sem autorização necessária e possa provocar um impacto baixo nas operações, recursos e entidades.  Fácil resolução. | Quando a informação foi divulgada sem autorização necessária e possa provocar um impacto médio nas operações, recursos e entidades.  Resolução com poucos prejuízos e de grau de dificuldade médio. | Quando a informação foi divulgada sem autorização necessária e possa provocar um impacto alto nas operações, recursos e entidades.  Difícil resolução. |
| **Integridade** | Quando o recurso é alterado ou destruído sem autorização necessária e possa provocar um impacto baixo nas operações, recursos e entidades.  Fácil resolução. | Quando o recurso é alterado ou destruído sem autorização necessária e possa provocar um impacto médio nas operações, recursos e entidades.  Resolução com poucos prejuízos e de grau de dificuldade médio. | Quando o recurso é alterado ou destruído sem autorização necessária e possa provocar um impacto alto nas operações, recursos e entidades.  Difícil resolução. |
| **Disponibilidade** | Quando o acesso ou uso de recursos de um sistema pode vir a ter um impacto baixo nas operações, recursos e entidades.  Fácil resolução | Quando o acesso ou uso de recursos de um sistema pode vir a ter um impacto médio nas operações, recursos e entidades.  Resolução com poucos prejuízos e de grau de dificuldade média. | Quando o acesso ou uso de recursos de um sistema pode vir a ter um impacto alto nas operações, recursos e entidades  Difícil resolução. |

Segue-se abaixo a lista de recursos anteriormente mencionada, com a devida análise de nível de impacto:

Tabela 9 - Análise do nível de impactos nos recursos da Dev4Sell

|  |  |  |  |
| --- | --- | --- | --- |
| Recurso |  | Impacto |  |
| Privacidade | Integridade | Disponibilidade |
| Infraestrutura | Baixo | Médio | Médio |
| Computadores e Telemóveis | Baixo | Baixo | Baixo |
| Impressoras | Baixo | Baixo | Baixo |
| Máquinas de teste de componentes | Baixo | Baixo | Médio |
| Ferramentas de fabricação | Baixo | Baixo | Alto |
| Router Gateway | Alto | Baixo | Alto |
| Switches | Baixo | Médio | Médio |
| Armazém de produtos | Baixo | Médio | Médio |
| Camiões de entrega | Baixa | Média | Média |
| Departamento de Recursos Humanos | Baixa | Baixa | Média |
| Departamento de Sistemas de Informação | Baixa | Baixa | Média |
| Departamento de Negócios | Baixa | Baixa | Média |
| Departamento de Marketing | Baixa | Baixa | Média |
| Departamento de Finanças | Baixa | Baixa | Média |
| Departamento de Logística | Baixa | Baixa | Média |
| Departamento de Desenvolvimento e Produção | Baixa | Baixa | Média |
| Departamento de Apoio ao Cliente | Baixa | Baixa | Média |
| Base de dados de produtos | Alta | Alta | Alta |
| Base de dados de clientes | Alta | Alta | Alta |
| Base de dados de funcionários | Alta | Alta | Alta |
| Base de dados de entregas | Alta | Alta | Alta |
| Base de dados de finanças | Alta | Alta | Alta |
| Base de dados de testes de versões | Baixa | Média | Média |
| Servidor de armazenamento em nuvem para documentos | Alta | Alta | Média |
| Servidores de deployment de aplicações | Médio | Médio | Alto |
| Servidores de bases de dados | Alto | Alto | Alto |
| Servidor de backup de base de dados | Médio | Alto | Médio |
| Armazenamento de backup em disco | Médio | Alto | Baixo |
| Ambientes de Desenvolvimento Integrado (IDE) | Baixo | Baixo | Baixo |
| Aplicação de Gestão de Stock | Baixo | Médio | Médio |
| Aplicação de Gestão de Vendas e Entregas | Alto | Médio | Alto |
| Aplicação de Gestão de Recursos Humanos | Alto | Médio | Médio |
| Aplicação de Gestão Financeira | Alto | Médio | Médio |
| Aplicação de Apoio ao Cliente | Alto | Médio | Alto |
| Rede de Comunicação Interna da Empresa | Alto | Médio | Médio |

Todos os recursos de dados tiveram destaque, sendo assim, todas as bases de dados e os seus servidores foram adicionados à lista de recursos críticos, sendo que a divulgação, perda ou alteração dos dados, bem como a interrupção de serviços de informação provocam um impacto no mínimo preocupante (médio/alto).

Cada aplicação consome informação de uma base de dados em específico. Em caso de agressão existem aplicações de grau de preocupação menor, como por exemplo a Aplicação de Gestão de Stock. Os servidores de deployment de aplicações também foram destacados, pois caso sejam interrompidos, todas as aplicações terminam e os funcionários perdem temporariamente o seu suporte de trabalho e acesso aos dados da empresa.

O router gateway também tem o seu grau de importância, pois na sua ausência, o sistema não consegue estabelecer ligação entre a rede privada e a rede pública (externa), incapacitando as comunicações para fora da empresa via Internet.

A rede interna também deve estar sempre disponível e protegida, tendo em conta que se uma entidade externa maligna entrar no sistema tem a possibilidade de roubar informação.

Por fim, as máquinas de produção são cruciais tendo em conta que são os principais recursos para desenvolver o produto para venda. Durante a sua ausência, ocorrerá atrasos na produção, resultando no incumprimento de prazos estipulados. Isso pode afetar negativamente a reputação e os lucros da empresa.

## Ameaças e vulnerabilidades

As ameaças são potenciais agressões que ainda não se manifestaram. A identificação destas é crucial para o desenvolvimento de um plano de segurança.

Segue-se abaixo uma tabela que apresentará todos os recursos críticos mencionados anteriormente com a identificação das ameaças e diferentes atributos relacionados com elas:

Tabela 10 - Descrição das ameaças nos recursos da Dev4Sell

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Recurso | Acesso | Ator | Motivo | Resultado | Impacto |
| **Máquinas e ferramentas de fabricação** | Físico | Interno | Intencional | Perda/Destruição | Alto |
| Interrupção | Médio |
| Acidental | Perda/Destruição | Alto |
| Interrupção | Médio |
| **Router Gateway** | Físico | Interno | Intencional | Interrupção | Alto |
| Rede/Sistema | Externo | Intencional | Interrupção | Alto |
| **Base de dados de produtos** | Rede/Sistema | Externo | Intencional | Divulgação | Médio |
| Modificação | Alto |
| Interrupção | Alto |
| **Base de dados de clientes** | Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação |
| Interrupção |
| **Base de dados de funcionários** | Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação |
| Interrupção |
| **Base de dados de entregas** | Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação |
| Interrupção |
| **Base de dados de finanças** | Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação |
| Interrupção |
| **Servidor de armazenamento em nuvem para documentos** | Rede/Sistema | Interno | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Externo | Intencional | Divulgação | Alto |
| Modificação | Alto |
| **Servidores de deployment de aplicações** | Físico | Interno | Intencional | Interrupção | Médio |
| Perda/Destruição | Alto |
| Acidental | Perda/Destruição | Alto |
| Rede/Sistema | Externo | Intencional | Perda/Destruição | Alto |
| Interrupção | Médio |
| **Servidores de bases de dados** | Físico | Interno | Intencional | Interrupção | Médio |
| Perda/Destruição | Alto |
| Acidental | Perda/Destruição | 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 | Baixo |
| Modificação | Alto |
| Perda/Destruição | Médio |
| Acidental | Perda/Destruição | Médio |
| **Aplicação 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 de Gestão Financeira** | Físico | Interno | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Perda/Destruição | Alto |
| Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Perda/Destruição | Alto |
| **Aplicação de Apoio ao Cliente** | Físico | Interno | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Perda/Destruição | Alto |
| Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Perda/Destruição | Alto |
| **Aplicação de Gestão de Vendas e Entregas** | Físico | Interno | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Perda/Destruição | Alto |
| Rede/Sistema | Externo | Intencional | Divulgação | Alto |
| Modificação | Alto |
| Perda/Destruição | Alto |
| **Rede de Comunicação Interna da Empresa** | Físico | Interno | Intencional | Interrupção | Médio |
| Acidental | Interrupção | Médio |
| Rede/Sistema | Externo | Intencional | Interrupção | Médio |

Acima é possível verificar que sendo estes recursos críticos, os impactos causados nos sistemas de informação são de calibre médio/alto, sendo assim, será feita a avaliação de cada risco possível, de forma a perceber quais os riscos prioritários.

As ameaças apresentam várias propriedades com diferentes valores:

* Recurso crítico: recurso que pode sofrer a ameaça;
* Acesso: forma como o atacante acede ao recurso. Pode ser classificado como:
  + Físico;
  + Rede/Sistema.
* Ator: entidade que efetua o ataque. Pode ser classificado como:
  + Interno;
  + Externo.
* Motivo: motivo do ataque. Pode ser classificado como:
  + Acidental;
  + Intencional.
* Resultado: ação executada pelo atacante. Pode ser classificado como:
  + 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. Pode ser classificado como:
  + Baixo;
  + Médio;
  + Alto.

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

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

Como é possível observar, os recursos que foram classificados como alto no impacto estão relacionados a informações altamente sensíveis, como dados de clientes, financeiros, entre outros. Além disso, esses recursos estão associados a bases de dados que armazenam toda a informação que circula entre os sistemas da empresa, tornando-se extremamente valiosos para a organização, se não os mais valiosos.

Deve-se considerar também os restantes recursos críticos que apresentam valores mais baixos no impacto, como é o caso da Aplicação do Sistema de Gestão de Recursos Humanos, pois este tem acesso direto a dados e documentos sensíveis como contratos. Apesar de não conseguir manipulação, 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 de cada fator referido na introdução deste capítulo: impacto, gravidade e probabilidade.

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

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

Tabela 11 - Classificação dos riscos nos recursos da Dev4Sell

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Recurso | Atributos | Valor do Risco | | |
| Interno | Externo | |
| **Máquinas e ferramentas de fabricação** | Impacto | 6 | N/A | |
| Gravidade | 3 | N/A | |
| Probabilidade | 5 | N/A | |
| Média | 4,7 | N/A | |
| **Média Final** | 5.3 | | |
| **Router Gateway** | Impacto | 7 | 7 | |
| Gravidade | 3 | 4 | |
| Probabilidade | 3 | 2 | |
| Média | 4,3 | 4,3 | |
| **Média Final** | 4.3 | | |
| **Base de dados de produtos** | Impacto | N/A | 7 | |
| Gravidade | N/A | 6 | |
| Probabilidade | N/A | 2 | |
| Média | N/A | 5 | |
| **Média Final** | 5 | | |
| **Base de dados de clientes** | Impacto | N/A | 9 | |
| Gravidade | N/A | 9 | |
| Probabilidade | N/A | 2 | |
| Média | N/A | 6,7 | |
| **Média Final** | 6.7 | | |
| **Base de dados de funcionários** | Impacto | N/A | | 9 |
| Gravidade | N/A | | 9 |
| Probabilidade | N/A | | 2 |
| Média | N/A | | 6,7 |
| **Média Final** | 6.7 | | |
| **Base de dados de entregas** | Impacto | N/A | 8 | |
| Gravidade | N/A | 7 | |
| Probabilidade | N/A | 1 | |
| Média | N/A | 5,3 | |
| **Média Final** | 5.3 | | |
| **Base de dados de finanças** | Impacto | N/A | | 9 |
| Gravidade | N/A | | 9 |
| Probabilidade | N/A | | 2 |
| Média | N/A | | 6,7 |
| **Média Final** | 6.7 | | |
| **Base de dados de testes de versões** | Impacto | N/A | | 5 |
| Gravidade | N/A | | 6 |
| Probabilidade | N/A | | 1 |
| Média | N/A | | 4 |
| **Média Final** | 4 | | |
| **Servidor de armazenamento em nuvem para documentos** | Impacto | 9 | 9 | |
| Gravidade | 6 | 8 | |
| Probabilidade | 2 | 2 | |
| Média | 5.7 | 6.3 | |
| **Média total** | 6 | | |
| **Servidores de deployment de aplicações** | Impacto | 7 | 7 | |
| Gravidade | 5 | 8 | |
| Probabilidade | 2 | 2 | |
| Média | 4.7 | 5.7 | |
| **Média Final** | 5.2 | | |
| **Servidores de bases de dados** | Impacto | 9 | 9 | |
| Gravidade | 5 | 8 | |
| Probabilidade | 2 | 2 | |
| Média | 5.3 | 6.3 | |
| **Média Final** | 5.8 | | |
| **Servidor de backup de base de dados** | Impacto | 6 | 6 | |
| Gravidade | 4 | 5 | |
| Probabilidade | 2 | 2 | |
| Média | 4 | 4,3 | |
| **Média Final** | 4.2 | | |
| **Armazenamento de backup em discos** | Impacto | 3 | N/A | |
| Gravidade | 7 | N/A | |
| Probabilidade | 2 | N/A | |
| Média | 4 | N/A | |
| **Média Final** | 4 | | |
| **Aplicação de Gestão de Recursos Humanos** | Impacto | 7 | 8 | |
| Gravidade | 5 | 6 | |
| Probabilidade | 2 | 2 | |
| Média | 4.7 | 5.3 | |
| **Média Final** | 5 | | |
| **Aplicação de Gestão Financeira** | Impacto | 9 | 9 | |
| Gravidade | 4 | 6 | |
| Probabilidade | 4 | 4 | |
| Média | 5.7 | 6.3 | |
| **Média Final** | 6 | | |
| **Aplicação de Apoio ao Cliente** | Impacto | 9 | 9 | |
| Gravidade | 4 | 6 | |
| Probabilidade | 3 | 3 | |
| Média | 5.3 | 6 | |
| **Média Final** | 5.7 | | |
| **Aplicação de Gestão de Vendas e Entregas** | Impacto | 9 | | 9 |
| Gravidade | 4 | | 6 |
| Probabilidade | 3 | | 3 |
| Média | 5.3 | | 6 |
| **Média Final** | 5.7 | | |
| **Rede de Comunicação Interna da Empresa** | Impacto | 5 | 7 | |
| Gravidade | 3 | 4 | |
| Probabilidade | 2 | 2 | |
| Média | 3.3 | 4.3 | |
| **Média Final** | 3.8 | | |

Observando a tabela acima conseguimos obter o valor de risco final associado a cada recurso crítico da empresa, tendo em conta os fatores fornecidos:

* Impacto: consequências e danos causados na empresa assim que uma agressão ocorre;
* Gravidade: efeitos secundários e danos a longo prazo causados na empresa após uma agressão;
* Probabilidade: expectativa de um evento ocorrer.

Para estabelecer um sistema de pontuação justo, levamos em conta as ameaças causadas tanto internamente quanto externamente. Quando não ocorre nenhum incidente, atribuímos o valor "N/A" para indicar a ausência de risco. Estes não serão associados ao cálculo da média.

É calculada a média entre as três variáveis fornecidas de cada coluna (interna e externa) separadamente.

Por fim é calculada a média total entre as duas colunas, constando que valores “N/A” não entram no cálculo.

Com os valores obtidos já é possível ver hierarquicamente quais os riscos mais preocupantes para o plano de mitigação, tendo sido esta a ordem obtida:

* Base de dados de finanças: 6.7
* Base de dados de clientes: 6.7
* Base de dados de funcionários: 6.7
* Servidor de armazenamento em nuvem para documentos: 6
* Aplicação de Gestão Financeira: 6
* Servidores de bases de dados: 5.8
* Aplicação de Apoio ao Cliente: 5.7
* Aplicação de Vendas e Entregas: 5.7
* Máquinas e ferramentas de fabricação: 5.3
* Base de dados de entregas: 5.3
* Servidores de deployment de aplicações: 5.2
* Aplicação 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
* Base de dados de testes de versões: 4
* Armazenamento de backup em discos: 4
* Rede de Comunicação Interna da Empresa: 3.8

# Plano de Mitigação

Calculados os valores dos riscos associados aos recursos, tem de ser implementando um plano de mitigação, que define as atividades necessárias para eliminar ou reduzir o risco inaceitável.

A partir deste plano, será selecionado os riscos a mitigar, bem como a descrição das atividades/políticas a aplicar em cada recurso selecionado. Isto irá permitir que a probabilidade do risco reduza, ou anule.

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

* Base de dados de finanças;
* Base de dados de clientes;
* Base de dados de funcionários;
* Servidor de armazenamento em nuvem para documentos;
* Aplicação de Gestão Financeira;
* Servidores de bases de dados;
* Aplicação de Apoio ao Cliente;
* Máquinas e ferramentas de fabricação;
* Base de dados de entregas;
* Servidores de deployment de aplicações;
* Aplicação de Gestão de Recursos Humanos;
* Base de Dados de Produtos.

### Atividades de Mitigação: Base de dados de finanças

O acesso à base de dados de finanças da empresa deve ser restrito a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação e ao Gerente do Departamento de Finanças, excluindo possíveis atores envolvidos em ataques futuros.

Deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização às aplicações de suporte aos funcionários, pois 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, bem como as operações (queries) que foram executadas. Isto permitirá que em caso de uma agressão, 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 base de dados periodicamente, explicado no Plano de Recuperação.

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

O acesso à base de dados de clientes deve ser restrito a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação, aos Engenheiros de Software que irão trabalhar na Aplicação de Apoio ao Cliente e Entregas e ao Gerente do Departamento de Atendimento ao Cliente, excluindo possíveis atores envolvidos em ataques futuros.

Deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização às aplicações de suporte aos funcionários, pois 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, bem como as operações (queries) que foram executadas, isto permitirá que em caso de uma agressão, 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 base de dados periodicamente, explicado no Plano de Recuperação.

### Atividades de Mitigação: Base de dados de funcionários

O acesso à base de dados de funcionários da empresa deve ser restrito a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação e ao Gerente do Departamento de Recursos Humanos, excluindo possíveis atores envolvidos em ataques futuros.

Deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização às aplicações de suporte aos funcionários, pois 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, bem como as operações (queries) que foram executadas, isto permitirá que em caso de uma agressão, 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 base de dados periodicamente, explicado no Plano de Recuperação.

### Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos (Transferir)

Para o servidor de armazenamento em nuvem de documentos fique mais seguro, deve-se encriptar todo o tipo de documentos que são armazenados nesta cloud. Caso a cloud seja atacada, o atacante enfrentará dificuldades e pode até mesmo ser incapaz de desencriptar as informações.

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 de Gestão Financeira

Deve ser feito um controlo de acessos à aplicação de gestão financeira, controlando assim acessos indevidos, 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 a 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 o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

Devem ser feitos periodicamente workshops de sensibilização às práticas de segurança no desenvolvimento e utilização do software. Isto alertará os funcionários a implementar práticas mais seguras no desenvolvimento e utilização da aplicação, evitando riscos de segurança.

### Atividades de Mitigação: Servidores de bases de dados

Os servidores de base de dados deverão ter acesso restrito a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação, CEO e Diretor da Dev4Sell.

Deverá estar funcional 24 horas por dia, tendo em conta que sem os servidores, nenhuma base de dados estará funcional para ser consumida pelas aplicações utilizadas na empresa.

De forma a limitar o acesso aos servidores, estes deverão estar localizados de forma segura dentro da infraestrutura empresarial, numa sala restrita com controlo de acesso através de cartões para fazer a sua autenticação.

Estas salas deverão conter um sistema de monitoramento de segurança, utilizando equipamentos como câmaras de segurança e sensores, de forma a conseguir detetar e tentar intercetar algum tipo de acesso ou atividade suspeita.

Toda a atividade que envolva o acesso à sala de servidores e aos servidores em si, ficará registada em logs, a identificação do cartão e hora de acesso. Isto permitirá que, em caso de ataque, seja feita uma análise dos acessos aos servidores.

Algo que será mencionado nas atividades de mitigação relacionadas a todas as bases de dados é a informação que deve ser criptografada, o que é algo que não evita qualquer tipo de agressão feita, mas consegue evitar ou, pelo menos, ganhar tempo até o atacante decifrar a informação roubada.

(trocaria por isto)

Um aspeto a ser mencionado nas atividades de mitigação relacionadas a todas as bases de dados é a sua criptografia. Embora não seja uma medida infalível para evitar uma agressão, proporcionará uma camada adicional de proteção, aumentando a complexidade de decifração para o atacante e ganhando tempo valioso.

### Atividades de Mitigação: Aplicação de Apoio ao Cliente

Deve ser feito um controlo de acessos à aplicação de apoio ao cliente, controlando os acessos indevidos, 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 a 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 o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

Devem ser feitos periodicamente workshops de sensibilização às práticas de segurança no desenvolvimento e utilização do software. Isto alertará os funcionários a implementar práticas mais seguras no desenvolvimento e utilização da aplicação, evitando riscos de segurança.

### Atividades de Mitigação: Aplicação de Gestão de Vendas e Entregas

Deve ser feito um controlo de acessos à aplicação de gestão de vendas e entregas, controlando assim acessos indevidos, 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 a 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 o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

Devem ser feitos periodicamente workshops de sensibilização às práticas de segurança no desenvolvimento e utilização do software. Isto alertará os funcionários a implementar práticas mais seguras no desenvolvimento e utilização da aplicação, evitando riscos de segurança.

### Atividades de Mitigação: Máquinas e ferramentas de fabricação

As máquinas e ferramentas de fabricação são recursos físicos essenciais no processo de desenvolvimento dos componentes eletrônicos vendidos. Sem esses recursos, o negócio não seria possível.

É importante que sejam feitas inspeções periodicamente à maquinaria de produção para garantir que se encontram em boas condições. Deve ser sempre verificado se há algum tipo de desgaste extremo ou qualquer outro problema que possa afetar a qualidade de produção, a segurança do recurso ou de quem está a utilizá-lo.

Assim que um desenvolvedor de hardware for contratado, deve ser agendado um treino de utilização, de forma a evitar problemas que possam afetar a sua segurança e a avaria das máquinas.

Devem ser realizados workshops de sensibilização às medidas de segurança a todos os desenvolvedores de hardware periodicamente, tendo em conta a atualização destas. De forma a prevenir em caso de acidentes a lesão de um funcionário, devem ser fornecidos os devidos equipamentos de proteção que serão de uso obrigatório enquanto estiverem em regime de trabalho.

Em caso de acidente que envolva a maquinaria de produção, qualquer que seja o nível de gravidade, este deve ser reportado e registado. Isto permitirá que seja identificado o problema e atenuará futuros riscos à zona de maquinaria.

No caso de algum funcionário que faça parte da equipa de desenvolvimento de hardware necessitar de aceder às máquinas, deverá utilizar o equipamento de proteção adequado e ser acompanhado por um desenvolvedor de hardware.

?(Não quererias dizer antes alguém que não seja da equipa de hardware)?

### Atividades de Mitigação: Base de dados de entregas

O acesso à base de dados de entregas deve ser restrito a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação, aos Engenheiros de Software que irão trabalhar na Aplicação de Gestão de Vendas e Entregas e ao Gerente do Departamento de Logística, excluindo possíveis atores envolvidos em ataques futuros.

Deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização às aplicações de suporte aos funcionários, pois 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, bem como as operações (queries) que foram executadas, isto permitirá que em caso de uma agressão, 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 base de dados periodicamente, explicado no Plano de Recuperação.

### Atividades de Mitigação: Servidores de deployment de aplicações

Os servidores de deployment de aplicações deverão ter acesso restrito a todos os funcionários exceto ao Gerente do Departamento dos Sistemas de Informação, Técnicos de Suporte de TI e ao Gerente do Departamento de Desenvolvimento e Produção e deverá estar funcional 24 horas por dia, tendo em conta que são a base para o funcionamento de todas as aplicações nos computadores e telemóveis de cada funcionário.

De forma a limitar o acesso aos servidores, estes deverão estar localizados numa localização segura dentro da infraestrutura empresarial, ou seja, numa sala restrita com controlo de acesso adequado, utilizando cartões de identificação da empresa para fazer a sua autenticação.

Estas salas deverão conter um sistema de monitoramento de segurança, utilizando equipamentos como câmaras de segurança e sensores, de forma a conseguir detetar e tentar intercetar algum tipo de acesso ou atividade suspeita.

Toda a atividade que envolva o acesso à sala de servidores e aos servidores em si, ficará registada em logs, anotando a identificação do cartão acedido e hora de acesso ao mesmo, isto permitirá que em caso de ataque seja feita uma análise ao histórico de quem teve o acesso aos servidores.

### Atividades de Mitigação: Aplicações de Gestão dos Recursos Humanos

Deve ser feito um controlo de acessos à aplicação de gestão dos recursos humanos, controlando assim acessos indevidos, 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 a 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 o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

Devem ser feitos periodicamente workshops de sensibilização às práticas de segurança no desenvolvimento e utilização do software. Isto alertará os funcionários a implementar práticas mais seguras no desenvolvimento e utilização da aplicação, evitando riscos de segurança.

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

O acesso à base de dados de produtos deve ser restrito a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação, aos Engenheiros de Software que irão trabalhar na Aplicação de Gestão de Stock e ao Gerente do Departamento de Logística, excluindo possíveis atores envolvidos em ataques futuros.

Deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização aos sistemas de informação, pois 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, bem como as operações (queries) que foram executadas, isto permitirá que em caso de uma agressão, 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 base de dados periodicamente, explicado no Plano de Recuperação.

### Riscos aceites

Tal como já foi mencionado, os riscos que apresentaram uma avaliação inferior á metade serão aceites pela empresa, não entrando no plano de mitigação.

Segue-se abaixo a lista de recursos que não se qualificaram:

* Router Gateway;
* Servidor de backup de base de dados;
* Base de dados de testes de versões;
* Armazenamento de backup em discos;
* Rede de Comunicação Interna da Empresa.

Mesmo que os riscos associados a estes recursos sejam aceites, não devem ser descartados em futuras avaliações, tendo em conta que podem apresentar vulnerabilidades desconhecidas e obter uma pontuação mais elevada.

# Plano de Recuperação

O plano de recuperação é um conjunto de estratégias e ações desenvolvidas para proteger os dados no caso de ocorrer uma agressão nos recursos críticos. Os principais objetivos deste plano são fornecer detalhes sobre o sistema de backups implementado e permitir a recuperação de informações. Na tabela apresentada abaixo está elaborado o sistema de backups implementado, acompanhado de parâmetros que o descrevem.

## Backup

Um backup é uma cópia de segurança de dado e permite a recuperação da informação em caso de perda ou corrupção.

Tabela - Backups da Dev4Sell

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Recurso | Informação | Local de armazenamento | Periodicidade | Notas |
| Base de dados de produtos | - Contém o armazenamento de dados relativos aos produtos em armazém | - Servidor de backup  - Disco Rígido | Diariamente | - São feitas snapshots da base de dados de 2 em 2 horas |
| Base de dados de clientes | - Contém o armazenamento de dados relativos aos clientes da empresa | - Servidor de backup  - Disco Rígido | Diariamente | - São feitas snapshots da base de dados de 2 em 2 horas |
| Base de dados de funcionários | - Contém o armazenamento de dados relativos aos funcionários da empresa | - Servidor de backup  - Disco Rígido | Diariamente | - São feitas snapshots da base de dados de 2 em 2 horas |
| Base de dados de entregas | - Contém o armazenamento de dados relativos às entregas da empresa | - Servidor de backup  - Disco Rígido | Diariamente | - São feitas snapshots da base de dados de 2 em 2 horas |
| Base de dados de finanças | - Contém o armazenamento de dados relativos às finanças da empresa | - Servidor de backup  - Disco Rígido | Diariamente | - São feitas snapshots da base de dados de 2 em 2 horas |
| Servidores de deployment de aplicações | ­- Aplicações a decorrer | - Data center | 1 vez | - Este servidor atua quando o servidor principal é interrompido ou destruído |
| 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 é interrompido ou destruído |
| Aplicação do Sistema de Gestão de Recursos Humanos | - Consome Base de dados  - Aplicação para a secção de recursos humanos trabalhar | - Base de dados de teste de versões | Sempre que houver uma nova versão da aplicação desenvolvida | - Quando necessário aplicar um backup é necessário detalhar a versão restaurada |
| Aplicação do Sistema de Gestão Financeira | - Consome Base de dados  - Aplicação para a secção de Gestão Financeira trabalhar | - Base de dados de teste de versões | Sempre que houver uma nova versão da aplicação desenvolvida | - Quando necessário aplicar um backup é necessário detalhar a versão restaurada |
| Aplicação de Sistema de Apoio ao Cliente | - Consome Base de dados  - Aplicação para atendimento ao cliente | - Base de dados de teste de versões | Sempre que houver uma nova versão da aplicação desenvolvida | - Quando necessário aplicar um backup é necessário detalhar a versão restaurada |

## Guia de Reposição dos Dados

O guia de recuperação de dados é um conjunto de instruções/procedimentos que detalha de forma especifica e clara a forma de recuperar dados perdidos, danificados, corrompidos ou inacessíveis de dispositivos de armazenamento.

Nas tabelas abaixo iremos demonstrar as etapas de recuperação de dados de cada recurso critico.

Tabela 13 - Guia de Recuperação de Dados

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Recurso | Ordem | Verificações | Subordem | Ação Corretiva |
| Bases de dados\* | 1 | - Identificar a causa da perca de dados | 1.1 | - Determinar o motivo da perca de dados na BD. |
| 1.2 | - Verificar a extensão 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 restauração, criando uma base de dados |
| 3.2 | - Efetuar o backup para a nova base de dados |
| 4 | - Fazer verificação dos dados inseridos na nova base de dados | 4.1 | - Verificar se os dados estão corretos |
| 4.2 | - Executar testes de consulta dos registos e relações diretamente no IDE da base de dados ou a partir de uma API para testes |
| 5 | - Atualizar as configurações nas aplicações para a nova base dados | 5.1 | - Configurar as conexões às bases de dados, alterando as connection strings de cada aplicação |
| 5.2 | - Atualizar identificadores, chaves e relações entre objetos |
| 6 | Efetuar um novo backup | 6.1 | - Realizar novo backup dos dados atuais para possível futuro ataque próximo |
| Servidores de deployment de aplicações | 1 | - Avaliar a causa da interrupção do servidor | 1.1 | - Identificar a causa da interrupção do servidor e das aplicações |
| 1.2 | - Obter informações 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 produção para evitar danos adicionais |
| 2.2 | - Restaurar o servidor usando o backup mais recente do sistema |
| 3 | - Testar as aplicações restauradas | 3.1 | - Após a restauração efetuar testes nas aplicações (funcionalidades) |
| 3.2 | - Monitorizar os “logs” das aplicações para verificar se há erros posteriores ao backup |
| 4 | - Implementar medidas preventivas (após efetuado o restauro) | 4.1 | - Assim que o servidor for restaurado, rever as medidas de segurança |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 Contigência

O plano de reposição irá assegurar que os recursos necessários estejam disponíveis em caso de agressão, de modo a manter os sistemas técnicos em funcionamento.

Tabela 14 - Plano de Reposição

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Situação | Nível de gravidade | Descrição | Tipo de Ação | Ação | Notas |
| Danos na infraestrutura | Grave | Infraestrutura completamente destruída | Manual | Aluguer temporário de um local de trabalho e recuperação de bens e recursos | Poderá levar a danificação de material interno |
| Ligeiro | Leves danos na estrutura ou danos irreparáveis em móveis | Manual | Reparação/Substituição |
| Avaria de equipamentos físicos (computadores, máquinas de teste, máquinas de fabricação, router, switches, impressoras, servidores, discos rígidos) | Grave | Danos irreparáveis | Manual | Substituição | Deverá ser mantido em stock recursos físicos novos e peças para garantir uma substituição, se necessário |
| Ligeiro | Danos leves | Manual | Reparação |
| Avaria da fonte elétrica | Grave | Descarga total | Automática | Ativação de geradores de fonte elétrica | Será verificado o estado dos dados e recursos físicos  Manutenção e testes regulares |
| Danos nos produtos do armazém | Grave | Danos irreparáveis | Manual | Descartar e nova construção | Manter em stock as peças necessárias para fazer a reparação de um equipamento  Manter o plano de construção do produto até à devida venda |
| Ligeiro | Danos leves | Manual | Reparação |
| Avaria nos camiões de entrega | Grave | Imobilizado ou irreparável | Manual | Substituição ou outsourcing | Deverá existir veículos de emergência  Deverá ser contactado um reboque em caso de avaria |
| Ligeiro | Ligeira avaria que não afeta na totalidade o desempenho, mas necessita de uma revisão | Manual | Contactar terceiros para reparação e substituição temporária |
| Ausência de empregados | Grave | Ausência temporal bastante prolongada | Manual | Novos contratos para substituição | É considerado bastante prolongado quando ultrapassa 1 mês. |
| Ligeiro | Ausência temporal pouco prolongada | Manual | Outsourcing |
| Falha nos sistemas de base de dados | Grave | Decesso à informação bastante prolongada | Automático | Uso dos backups | Analisar Plano de Recuperação |
| Ligeiro | Decesso à informação pouco prolongada | Automático |
| Falha nas apps da empresa | Grave | Decesso às aplicações bastante prolongada | Automático | Utilizar o sistema de backup de versões da aplicação | Analisar Plano de Recuperação |
| Ligeiro | Decesso às aplicações pouco prolongada | Automático |

# Auditoria

A auditoria pretende controlar a observância das medidas de segurança informática aprovadas. Consiste em operações periódicas de controlo das medidas de segurança e pode ser assumida por auditores internos ou externos.

Desempenha um papel fundamental para garantir a privacidade, integridade e disponibilidade dos dados e informações em uma empresa. Ao avaliar os processos relacionados aos sistemas de informação, a auditoria contribui para a proteção dos recursos da empresa, para a mitigação de riscos e para a eficiência e a transparência dos processos de negócio.

Será realizada por auditores externos, levando em consideração que se trata de uma empresa de pequena/média dimensão e que aparenta estar em crescimento, portanto não justifica o contrato de auditores internos. Esta decisão evita gastos adicionais com salários e despesas a longo prazo.

### Auditoria Externa

A auditoria externa é um processo em que uma empresa especializada e independente é contratada para avaliar os sistemas de informação de uma organização.

Tem como objetivos garantir que a empresa se encontre em conformidade com os regulamentos e padrões de segurança, identificar falhas e vulnerabilidades de proteção dos sistemas de informação, avaliar a eficácia das políticas impostas, certificar que as instalações e outros recursos físicos se encontram em condições e oferecer recomendações para melhoria.

O auditor deve inicialmente fazer a recolha de informação relevante sobre os sistemas de informação da Dev4Sell e, com esses dados, fazer um plano 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 física da infraestrutura;
* Verificar a integridade física das máquinas de produção;
* Verificar a integridade física dos camiões de entrega de produtos;
* Verificar a segurança de acesso à 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:

* Efetuar testes de penetração de sistemas;
* Revisão de políticas e procedimentos da empresa;
* Interrogatório a funcionários escolhidos aleatoriamente, em relação a medidas de segurança atuais;
* Etc.

Finalmente, deve ser registado num relatório os resultados obtidos durante a auditoria, 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 podem ser agendadas mais avaliações, por exemplo em caso de serem 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. 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 realizados workshops, palestras e formações de sensibilização à segurança no trabalho, porém também ocorrerá simulações de simulacros como forma de treino, nos quais todos os funcionários serão alertados com 1 dia de antecedência. Estes simulacros de treino serão acompanhados pelos recursos humanos pertencentes ao Departamento de Recursos Humanos e ao Departamento de Sistemas de Informação, que irão orientar as etapas 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.

Ocorrerá simulacros surpresa (não anunciados previamente) uma vez por semestre e devidamente planeados tendo em conta os riscos mais prováveis de acontecer à empresa. Apenas o CEO, Diretor e Gerentes dos Departamentos de Recursos Humanos e Sistemas de Informação serão notificados desta simulação e os restantes funcionários não serão instruídos como acontece nos exercícios previamente alertados, como forma de os testar numa situação real.

Será feita uma avaliação no final de cada simulacro surpresa, sendo registado num relatório todos os eventos ocorridos na simulação da agressão. Ficam 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 os agendamentos destes eventos devem ser devidamente planeados entre o CEO, Diretor e Gerentes dos Departamentos de Recursos Humanos e Sistemas de Informação de forma a não prejudicar o negócio da empresa.

# Conclusão

Embora este cenário seja fictício e a simplificação dos processos da framework OCTAVE alegro tenha sido aplicada, acreditamos firmemente que este trabalho desempenhou um papel crucial na aprendizagem dos procedimentos básicos para realizar uma auditoria de risco e, por consequência, desenvolver um plano de segurança. Ao longo deste projeto, adquirimos conhecimentos valiosos sobre a identificação e avaliação de riscos, bem como sobre a implementação de medidas de segurança adequadas para proteger os ativos de uma empresa. Compreendemos a importância de uma abordagem estruturada e sistemática para gerir os riscos de segurança tendo sempre em consideração as ameaças, vulnerabilidades e impactos potenciais em todas as áreas operacionais. Além disso, ao praticarmos a execução de uma auditoria de risco, ganhamos uma visão mais clara sobre como os diferentes componentes de um plano de segurança se interconectam. Aprendemos a mapear os objetivos de segurança da empresa, definir controlos adequados e implementar políticas eficazes que abordem as lacunas identificadas. Também reconhecemos a importância de envolver todas as partes interessadas, desde a alta administração até os colaboradores de todos os níveis, para garantir a conformidade e o comprometimento com as práticas de segurança. Em suma, mesmo considerando a natureza simplificada deste cenário fictício, este trabalho proporcionou uma base sólida para entender e gerir a segurança em uma empresa. Estamos confiantes de que estas habilidades e conhecimentos adquiridos prepararam-nos para enfrentar desafios reais relacionados à segurança empresarial do futuro, possibilitando a proteção efetiva dos ativos e a mitigação dos riscos associados.

Biografia

<Biografia>