

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 copieei 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
Contextualização do documento	7
Descrição da empresa	7
Funções e responsabilidades	8
PROCESSOS DE NEGÓCIO	10
PN01 – Parcerias comerciais com os fornecedores	10
PN02 – Parcerias comerciais com os clientes	10
PN03-Gestão de Stock	11
PN04 – Venda	12
MÉTODO DE AVALIAÇÃO DE RISCO	13
Octave 13	
ARQUITETURA DOS SISTEMAS	13
Sistema de Administração da Empresa	14
Sistema de Comunicação Interna	14
Rede Telefónica	14
Sistema de Email Interno	15
Sistema de Armazenamento de Dados	15
Sistema de Produção	15
Sistema de Aplicações	16
Aplicação de gestão de stock (Computador)	16
Aplicação de auxílio de entregas e consulta de stock (Smartphone)	17
RECURSOS	18
Físicos 18	
Humanos	19
Dados 20	
Suporte de Dados	21

Aplicações	22
ANÁLISE E GESTÃO DE RISCOS	23
Recursos críticos	24
Ameaças e vulnerabilidades	28
Análise e Avaliação do Risco	32
PLANO DE MITIGAÇÃO	38
Atividades de Mitigação: Base de dados de clientes	38
Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos	39
Atividades de Mitigação: Aplicação do Sistema de Gestão Financeira	39
Atividades de Mitigação: Servidores de bases de dados	40
Atividades de Mitigação: Aplicação do Sistema de Apoio ao Cliente	40
Atividades de Mitigação: Máquinas e ferramentas de fabricação	41
Atividades de Mitigação: Base de dados de entregas	41
Atividades de Mitigação: Servidor de deployment de aplicações	42
Atividades de Mitigação: Aplicações do Sistema de Gestão dos Recursos Humanos	42
Riscos aceites	43
PLANO DE SEGURANÇA	44
Entidades envolvidas	44
Políticas de Segurança	44
Controlos de acesso	44
Monitorização e Detecção de Incidentes	44
Resposta a Incidentes	44
Treino e Consciencialização	44
Auditoria	44
Revisão e Melhoria Contínua do Plano de Segurança	44
PLANO DE RECUPERAÇÃO	45
Backup	45
Guia de recuperação de Dados	46

PLANO DE REPOSIÇÃO	50
PLANO DE CONTINGÊNCIA	51
BIOGRAFIA	52

Lista de Tabelas

Tabela 1 — <descrição da tabela>

Erro! Marcador não definido.

Lista de Figuras

Figura 1 — <descrição da figura>

Erro! Marcador não definido.

Introdução

Contextualização do documento

O projeto tem como objetivo apresentar um detalhado plano de segurança para a empresa, levando em consideração 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 visa 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, treinamento 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 chama-se 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 grandes e médias empresas que comercializam esses produtos para o público em geral.

Para a fabricação, a empresa recebe suporte material de patrocinadores que se beneficiam desse fornecimento.

Funes e responsabilidades

Esta empresa demonstra uma estrutura hierrquica de cargos.

Cargo	Descrio
CEO	Lidera a Dev4Sell, atuando como intermedirio entre os diferentes diretores e departamentos da empresa. Tem acesso a todos os dados armazenados no servidor.
Diretor(a)	Responsvel por uma rea especfica da empresa, como finanas, operaes, marketing, recursos humanos, etc. Supervisiona e coordena as equipas nessa rea.
Gestores de Projetos	Encarregados de gerir cada desenvolvimento de projeto e a equipa envolvida. Coordenam o trabalho, definem metas, prazos e recursos necessrios para o sucesso do projeto.
Departamento de Recursos Humanos	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.
Departamento de Gesto de Sistemas de Informao (Analista de Segurana e Diretor)	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.
Departamento de Vendas	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.
Departamento de Finanas	Responsvel por todas as atividades financeiras da empresa, tendo que otimizar a utilizao dos recursos financeiros disponveis e fornecer informaes precisas e relevantes para a tomada de decises estratgicas.
Departamento de Logstica	Encarregado de gerir a movimentao e armazenamento de materiais e produtos, bem como a distribuio e entrega dos mesmos.
Equipa de Desenvolvimento	Responsvel pelo design e construo dos equipamentos eletrnicos da empresa.
Equipa de Apoio ao cliente	Responsveis por dar assistncia ao cliente via website, mvel ou correio eletrnico, quer seja para esclarecimento de dvidas ou possveis 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.

Anlise da proposta: Aps receber a proposta, o departamento de vendas realiza uma anlise detalhada, avaliando o potencial sucesso dessa parceria. Durante essa anlise, eles podem desenvolver estratgias 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 renegociao at se chegar a uma concluso satisfatria para ambas as partes. Aps chegarem a um acordo, ser agendada uma nova reunio para finalizar o contrato ou o pedido sem fidelizao.

Contrato: Durante a fase de contrato, so revistas novamente todas as normas estabelecidas at o momento, como os termos e condies, servios acordados, preos, responsabilidades e datas. Aps a reviso e acordo mtuo, o contrato  assinado pelas entidades envolvidas, formalizando o acordo estabelecido.

Pedido sem fidelizao: Em situaes de excluso de contrato formal,  firmado apenas um pedido contendo a quantidade especfica de artigos solicitados.

PN03-Gesto de Stock

Para garantir um processo de venda eficiente,  essencial ter uma gesto adequada de stock, permitindo o desenvolvimento contnuo dos produtos sem interrupes. Essa gesto pode ser dividida nos seguintes subprocessos:

Planeamento: Inicialmente, so projetados os produtos que sero desenvolvidos em determinado perodo, e  entregue uma lista de todos os artigos e um plano de construo. Isso pode ser estipulado pela equipa de design e arquitetura do departamento de desenvolvimento.

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

Anlise: Antes do pedido, o departamento financeiro realiza uma anlise do estado econmico atual da empresa. Com base nessa anlise  previsto o que deve ser encomendado, e se necessrio,  estipulado qual o inventrio prioritrio. Em seguida,  realizado o pedido de reposio de estoque.

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

Receo e reposio: O departamento de logstica  responsvel por receber o material e atualizar o inventrio. Caso seja identificado pelo departamento de Controlo de Qualidade algum defeito no produto recebido, ser iniciado um processo de negociao para resolver o problema.

Defeitos/Devolues: Em caso de problemas com os materiais recebidos, a Dev4Sell chegar a um acordo com a parceira, mas por norma ser realizado substituio dos artigos defeituosos.

PN04 – Venda

O processo de venda no funcionaria sem os processos de negcio anteriores e destina-se  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 produo.

Anlise 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 aprovao ou reprovao.

Faturao: Aps cada pagamento,  emitida uma fatura com os detalhes da transao, servindo como comprovativo de compra. A fatura contm informaes como data, nmero, dados do cliente e vendedor, descrio dos produtos ou servios, quantidade, preo unitrio e total a pagar.

Encomenda: Aps a confirmao do pedido, o departamento de logstica processa a encomenda, prepara os produtos e os envia para as empresas. O envio  feito por meio de servios de entrega ou o cliente pode optar por levantar os produtos pessoalmente.

Defeitos/Devolues: No caso de o cliente receber produtos defeituosos vendidos pela Dev4Sell,  realizada uma anlise do processo de venda para verificar a ocorrncia de algum problema. Aps a confirmao e apresentao do comprovativo de fatura, por norma so enviados novos artigos para substituir os danificados, mas poder ocorrer uma negociao.

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)

Falar de motivos por ter sido utilizado o OCTAVE Allegro

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 serão abordados os sistemas relativos à comunicação interna da empresa e o sistema de armazenamento de dados e como é que estes funcionarão de forma que seja possível manter uma comunicação fluída e eficaz entre diferentes cargos e setores da empresa, algo que Sistema de Segurança da empresa Dev4Sell

tem um peso enorme num bom funcionamento de uma empresa e no sucesso nos procedimentos dos processos de negócio e também apresenta um papel muito importante no que toca à segurança e preservação dos dados relacionados com a empresa, produtos e clientes.

Por fim, será analisado neste capítulo os sistemas mais aplicativos e que contêm a lógica de armazenamento correto 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 fazer o apoio direto ao trabalhador de forma que este consiga finalizar com sucesso o seu papel num processo de negócio.

Sistema de Administração da Empresa

Este sistema da Dev4Sell tem como principal objetivo efetuar a análise e gestão de recursos e processos de negócio em curso, é onde os recursos humanos realizam tarefas como:

- Tracking de uma entrega
- Análise de pedidos feitos pelos clientes
- Análise financeira da empresa
- Análise de faturas pendentes
- Revisão periódica de veículos de entrega
- Etc.

De forma a aceder a este sistema, o utilizador irá necessitar de fazer login com a sua conta empresarial que é registada no início de contrato e as credenciais são atribuídas ao recurso contratado.

Sistema de Comunicação Interna

O sistema de comunicação interna tem como objetivo estabelecer uma ligação segura e eficiente entre todas as máquinas localizadas dentro da infraestrutura da Dev4Sell, incluindo maquinaria de produção, computadores e bases de dados. Incluído neste sistema encontra-se também uma rede telefónica para a comunicação rápida entre funcionários da empresa e um sistema de email interno para a troca de informação mais sensível.

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 Sistema de Segurança da empresa Dev4Sell

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  composto pela equipa de desenvolvimento que ficar encarregue de fazer o design do componente em causa, bem como o funcionamento lgico e fsico do mesmo. Para que isto seja alcanado com sucesso, a equipa ter o auxlio das mquinas, ferramentas de produo e mquinas de testes de componentes.

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

Sistema de Aplicaes

O sistema de aplicaes da Dev4Sell tem como objetivo auxiliar todos os sistemas anteriormente referidos, fornecendo uma interface interativa para haver a comunicao entre os funcionrios da empresa e os dados registados em base.

Tal como foi mencionado no sistema de email interno, cada utilizador ter um email com o domnio da empresa, fazendo assim a identificao de cada funcionrio.

Tendo em conta o tipo de funcionrio, que  informao que est registada em base de dados, este ter acesso direto aps o login  respetiva pgina associada  funo dele, por exemplo aps um funcionrio do departamento de finanas efetuar o login, na aplicao, ser redirecionado para a interface que tratar de fazer a anlise de histrico de faturas dependentes, vendas feitas recentemente, etc.

Foram criadas dois tipos de aplicao distintas, aplicao para desktop que ter acesso a diversas interfaces respetivas a cada recurso humano e aplicao para smartphone que ter funcionalidades rpidas como visualizao de stock instantneo, visualizao de pedidos de entrega e a funcionalidade de realizar o auxlio de uma entrega, registando assim o processo da entrega.

Aplicao de gesto de stock (Computador)

Esta aplicao, tal como j foi referido,  a aplicao principal para auxiliar o trabalho de cada membro da empresa Dev4Sell, no qual dependendo do login, cada funcionrio ser redirecionado para a sua respetiva interface:

- Interface de anlise financeira da empresa
- Interface de anlise de estatstica de vendas, anlise e gesto de clientes
- Interface de anlise detalhada de materiais, componentes desenvolvidos e maquinaria usada para a produo de produtos eletrnicos
- Interface de workflow de projetos de equipas de desenvolvimento
- Interface para gesto 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
Infraestrutura	Estrutura fsica da empresa que serve de suporte para o funcionamento dos sistemas e equipamentos da Dev4Sell.	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Produo • Sistema de Aplicaes
Computadores	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"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Produo • Sistema de Aplicaes
Mquinas de teste de componentes	Conjunto de equipamentos utilizados para realizar a <i>quality assurance</i> dos equipamentos reproduzidos na Dev4Sell.	<ul style="list-style-type: none"> • Sistema de Armazenamento de Dados • Sistema de Produo • Sistema de Aplicaes
Mquinas e ferramentas de fabricao	Equipamentos de utilizados no processo de produo e um produto eletrnico da empresa.	<ul style="list-style-type: none"> • Sistema de Produo

Router Gateway	Dispositivo que ir estabelecer a ligao entre a rede local com a internet, todos os dispositivos estar ligados a este equipamento para ter acesso  internet.	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Aplicaes
Switches	Equipamentos necessrios para estabelecer a ligao entre equipamentos na rede local.	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Produo • Sistema de Aplicaes
Armazm de produtos	Local de armazenamento de equipamentos eletrnicos desenvolvidos pela empresa.	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Armazenamento de Dados • Sistema de Produo
Camies de entrega	Equipamento de auxlio s entregas e recolhas de produtos na Dev4Sell. Utilizados para transportar os produtos.	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa

Humanos

Nome	Descrio	Responsabilidades
Equipa de desenvolvimento de software	Equipa que tem o papel de desenvolver o funcionamento lgico dos produtos	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Produo • Sistema de Aplicaes

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

Dados

Nome	Descrição	Fonte dos dados	Nível de Acesso	Responsável pelos dados
Base de dados de produtos	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 disponível.	de equipamentos.		
Base de dados de clientes	Base de dados que contém as informações dos clientes da empresa.	Entidades que entrem em contacto com a empresa que estejam interessadas na compra de um produto, interações com a empresa.	Alto	...
Base de dados de entregas	Regista o progresso de cada entrega que foi feita pela empresa, registando datas, locais e estados.	Transações monetárias, relatórios de equipas de suporte técnico e atualizações na aplicação do sistema de entregas.	Alto	...
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	...

Suporte de Dados

Nome	Descrição
Servidores de deployment de aplicações	Recursos de capacidade de armazenamento de alto desempenho e confiabilidade responsáveis por fornecer um local centralizado para armazenar e gerir os dados da empresa.
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 servios da Google, pagando uma subscrio, que tero como objetivo fazer o armazenamento de documentos como relatrios, contratos, faturas, etc.
Servidor de backup de base de dados	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.
Armazenamento de backup em disco	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
Ambientes de desenvolvimento (IDE)	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).
Aplicao do Sistema de Gesto de Stock	Aplicao de controlo e gesto de stock presente nos armazns da empresa.
Aplicao do Sistema de Gesto de Vendas e Entregas	Aplicao que auxilia a Dev4Shell no processo de gesto de vendas, desde o registo do pedido at  entrega do produto ao cliente.
Aplicao do Sistema de Gesto de Recursos Humanos	Aplicao que facilita a administrao e a gesto das atividades relacionadas aos funcionrios da empresa.
Aplicao do Sistema de Gesto Financeira	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.
Aplicao de Sistema de Apoio ao Cliente	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.
Rede de Comunicao Interna da Empresa	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
Privacidade	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.
Integridade	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.

Disponibilidade	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
Mquinas e ferramentas de fabricao	Fsico	Interno	Intencional	Perda/Destruio	Alto
				Interrupo	Mdio
			Acidental	Perda/Destruio	Alto
				Interrupo	Mdio
Router Gateway	Fsico	Interno	Intencional	Interrupo	Alto
	Rede/Sistema	Externo	Intencional	Interrupo	Alto
	Rede/Sistema	Externo	Intencional	Divulgao	Mdio

Base de dados de produtos				Modificao	Alto
				Interrupo	Alto
Base de dados de clientes	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	
				Interrupo	
Base de dados de entregas	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	
				Interrupo	
Servidor de armazenamento em nuvem para documentos	Rede/Sistema	Interno	Intencional	Divulgao	Alto
				Modificao	Alto
		Externo	Intencional	Divulgao	Alto
				Modificao	Alto
Servidores de deployment de aplicaes	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
Servidores de bases de dados	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
Aplicao de Sistema de Apoio ao Cliente	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
Rede de Comunicao Interna da Empresa	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 várias 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
Mquinas e ferramentas de fabricao	Impacto	6	N/A
	Gravidade	3	N/A
	Probabilidade	5	N/A
	Mdia	4,7	N/A
	Mdia Final	5.3	
Router Gateway	Impacto	7	7
	Gravidade	3	4
	Probabilidade	3	2
	Mdia	4,3	4,3
	Mdia Final	4.3	
Base de dados de produtos	Impacto	N/A	7
	Gravidade	N/A	5
	Probabilidade	N/A	1
	Mdia	N/A	4,3
	Mdia Final	4.3	
Base de dados de clientes	Impacto	N/A	9
	Gravidade	N/A	9
	Probabilidade	N/A	2

	Mdia	N/A	6,7
	Mdia Final	6.7	
Base de dados de entregas	Impacto	N/A	8
	Gravidade	N/A	7
	Probabilidade	N/A	1
	Mdia	N/A	5,3
	Mdia Final	5.3	
Servidor de armazenamento em nuvem para documentos	Impacto	9	9
	Gravidade	6	8
	Probabilidade	2	2
	Mdia	5.7	6.3
	Mdia total	6	
Servidores de deployment de aplicaes	Impacto	7	7
	Gravidade	5	8
	Probabilidade	2	2
	Mdia	4.7	5.7
	Mdia 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 do Sistema de Gestão de Recursos Humanos	Impacto	7	8
	Gravidade	5	6
	Probabilidade	2	2
	Média	4.7	5.3
	Média Final	5	
Aplicação do Sistema de Gestão Financeira	Impacto	9	9
	Gravidade	4	6
	Probabilidade	4	4

	Mdia	5.7	6.3
	Mdia Final	6	
Aplicao de Sistema de Apoio ao Cliente	Impacto	9	9
	Gravidade	4	6
	Probabilidade	3	3
	Mdia	5.3	6
	Mdia Final	5.7	
Rede de Comunicao Interna da Empresa	Impacto	5	7
	Gravidade	3	4
	Probabilidade	2	2
	Mdia	3.3	4.3
	Mdia Final	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 atribuída  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 atribuído 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
- Router Gateway: 4.3
- Base de dados de produtos: 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 Mitigao

Agora que foram calculados os valores dos riscos associados aos recursos crticos da Dev4Sell, tem que ser implementando um plano de mitigao, que define as atividades necessrias para eliminar ou reduzir o risco inaceitvel para um recurso crtico.

A partir deste plano, ir ser feita a seleo de riscos a mitigar, bem como a descrio das atividades/polticas a aplicar em cada recurso selecionado, isto ir permitir que a probabilidade do risco seja menor, ou at mesmo nula.

Tendo em conta que os valores atribudos aos riscos no sub-captulo da anlise de riscos foram dentro do intervalo de valores 0-10, ficou definido que todos os riscos que tivessem uma classificao mdia acima de metade do valor mximo do intervalo sejam mitigados/transferidos, sendo assim, sero mitigados/transferidos os riscos associados aos seguintes recursos:

- Base de dados de clientes
- Servidor de armazenamento em nuvem para documentos
- Aplicao do Sistema de Gesto Financeira
- Servidores de bases de dados
- Aplicao de Sistema de Apoio ao Cliente
- Mquinas e ferramentas de fabricao
- Base de dados de entregas
- Servidores de deployment de aplicaes
- Aplicao do Sistema de Gesto de Recursos Humanos

Atividades de Mitigao: Base de dados de clientes

O acesso  base de dados de clientes 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 tamb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 armazenamento em nuvem de documentos

- ➔ Sendo que este recurso utiliza servios de terceiros, estes ficaro 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  armazenado nesta cloud. Com isto, mesmo que a cloud seja atacado, o atacante perder muito tempo ou poder at mesmo no conseguir descriptar a informao roubada.

Tendo em conta que este  um servio prestado pela Google, qualquer tipo de agresso que tenha sido feita a este servidor ser transferida para a entidade prestadora do servio.

Atividades de Mitigao: Aplicao do Sistema de Gesto Financeira

Deve ser feito um controlo de acessos  aplicao do sistema de gesto financeira, 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mb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.

- ➔ Efetuar workshops de sensibilizao s prticas de segurana no desenvolvimento de software (isto se forem os nossos programadores a criar as aplicaes, caso seja um servio de terceiros, apenas transfere-se o risco)

Atividades de Mitigação: Servidores de bases de dados

Os servidores de base de dados deverão ter acesso restrito, sendo permitido que apenas o/os **Quem deve ter acesso** terem este acesso e 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 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 interceder algum tipo de acesso ou atividade suspeita.

Toda a atividade que envolva o acesso à sala de servidores e aos servidores em si, ficará registado 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.

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.

Atividades de Mitigação: Aplicação do Sistema de Apoio ao Cliente

Deve ser feito um controlo de acessos à aplicação do sistema de apoio ao cliente, 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 detetam 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.

Atividades de Mitigação: Máquinas e ferramentas de fabricação

As máquinas e ferramentas de fabricação de produtos para venda são os recursos mais lucrativos para a empresa, tendo em conta que sem estas, os componentes eletrónicos não são desenvolvidos e, conseqüentemente, a empresa não consegue gerar vendas.

Com isto, é importantíssimo que sejam feitas inspeções periodicamente à maquinaria de produção para garantir que estas se encontram em boas condições de funcionamento. Deve ser sempre verificado se há algum tipo de desgaste excessivo ou qualquer outro problema que possa afetar a qualidade de produção de produtos ou a segurança do recurso em si ou de quem está a utilizá-lo.

Assim que um desenvolvedor de hardware for contratado, deve ser agendado um treino de sensibilização à segurança na utilização das máquinas de fabricação de componentes eletrónicos, de forma que o trabalhador evite cometer erros que possam afetar a sua segurança e a avaria de uma máquina.

Devem ser feitos também workshops de sensibilização à segurança a todos os desenvolvedores de hardware periodicamente, tendo em conta que as medidas de segurança estão sempre a ser atualizadas. Tendo em conta que o mau funcionamento ou desgaste de uma máquina pode levar à falta de segurança de um trabalhador, as boas práticas de segurança não serão o suficiente para evitar que certos incidentes aconteçam, por isso deve ser fornecido os devidos equipamentos de segurança aos trabalhadores, estes são de uso obrigatório quando os mesmos se encontram perto de uma máquina.

Em caso de acidente que envolva a maquinaria de produção, por mais mínimo que seja, este deve ser reportado e registado, isto permitirá que seja feita uma melhor identificação de problemas que o recurso possa apresentar e evitará ou, pelo menos, atenuará ainda mais futuros riscos à zona de maquinaria, este deverá utilizar o equipamento de proteção adequado e ser acompanhado por um desenvolvedor de hardware.

Atividades de Mitigação: Base de dados de entregas

O acesso à base de dados de entregas 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 deployment de aplicações

Os servidores de deployment de aplicações deverão ter acesso restrito, sendo permitido que apenas o/os **Quem deve ter acesso** terem este acesso e deverá estar funcional 24 horas por dia, tendo em conta que sem este é a base para o funcionamento de todas as aplicações a funcionarem 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 intercepar algum tipo de acesso ou atividade suspeita.

Toda a atividade que envolva o acesso à sala de servidores e aos servidores em si, ficará registado 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 do Sistema de Gestão dos Recursos Humanos

Deve ser feito um controlo de acessos à aplicação do sistema de gestão dos recursos humanos, 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 Sistema de Segurança da empresa Dev4Sell

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

Riscos aceites

Tal como já foi referido anteriormente, os riscos que apresentaram uma avaliação com valor inferior a 5 foram aceites, não tomando nenhuma ação especial em caso de agressão, todavia, há recursos com riscos mitigados que possuem a mesma estrutura que recursos com riscos aceites, com isto, é possível adicionar algumas medidas a esses recursos, que é o caso da Base de Dados de Produtos, tendo assim as seguintes atividades de mitigação:

- Acesso a esta base de dados deve ser restrita a X pessoa
- Esta deve estar disponível 24 horas por dia
- Manter em registo todos os acessos e alterações efetuadas na base de dados
- Deve ser feito um backup da base de dados diariamente, com registo em ficheiros de snapshots feitos de 2 em 2 horas

Plano de Segurança

<Resumo ou introdução ao plano de segurança e falar dos seguintes pontos>

Entidades envolvidas

Políticas de Segurança

Controlos de acesso

Monitorização e Detecção de Incidentes

Resposta a Incidentes

Treino e Consciencialização

Auditoria

Revisão e Melhoria Contínua do Plano de Segurança

Plano de Recuperação

O plano de recuperação é um conjunto de estratégias e ações desenvolvidas para salvaguardar informação no caso de haver uma agressão nos recursos críticos. Tem como objetivos principais delinear os detalhes do sistema de backups implementado permitindo a recuperação de informação em caso de falha, corrupção, alteração ou destruição de um recurso da Dev4Sell.

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

Backup

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 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
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  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 inacessveis de dispositivos de armazenamento para normal funcionamento do sistema.

Nas tabelas a baixo iremos 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 Contingência

<Falar sobre este plano>

Biografia

<Biografia>