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

ESCOLA SUPERIOR DE TECNOLOGIA IPCA

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

Lista de Tabelas

Lista de Figuras

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.

Funções e responsabilidades

Esta empresa demonstra uma estrutura hierárquica de cargos.

Cargo	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 que 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.

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 económico atual da empresa. Com base nessa análise é previsto o que deve ser encomendado, e se necessário, é estipulado qual o inventário prioritário. Em seguida, é realizado o pedido de reposição de estoque.

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

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

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

Octave

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

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

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

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

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

Arquitetura dos Sistemas

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

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

De seguida 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 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 aplicacionais 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 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 eletrônicos que serão colocados para venda ou mesmo para a reposição e preparação de stock para futuras vendas.

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

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

Sistema de Aplicações

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

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

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

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

Aplicação de gestão de stock (Computador)

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

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

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

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

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

Recursos

De forma que a empresa tenha o bom funcionamento dos sistemas, será necessário que esta contenha recursos, que tratam-se de meios que podem ser utilizados para um determinado fim, estes possuem um valor e são quem sofrem os 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

Nome	Descrição	Sistemas em que é utilizado
Infraestrutura	Estrutura física da empresa que serve de suporte para o funcionamento dos sistemas e equipamentos da Dev4Sell.	• Sistema de Administração da Empresa • Sistema de Comunicação Interna • Sistema de Armazenamento de Dados • Sistema de Produção • Sistema de Aplicações
Computadores	Equipamento de auxílio que tem serve de interação com o sistema de gestão de produtos da empresa e tratar de outros assuntos administrativos e financeiros.	• 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 reproduzidos na Dev4Sell.	• Sistema de Armazenamento de Dados • Sistema de Produção • Sistema de Aplicações
Máquinas e ferramentas de fabricação	Equipamentos de utilizados no processo de produção e um produto eletrônico da empresa.	• 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 na Dev4Sell. Utilizados para transportar os produtos.	• Sistema de Administração da Empresa

Humanos

Nome	Descrição	Responsabilidades
Equipa de desenvolvimento de software	Equipa que tem o papel de desenvolver o funcionamento lógico dos produtos	• Sistema de Administração da Empresa • Sistema de Comunicação Interna • Sistema de Armazenamento de Dados • Sistema de Produção • Sistema de Aplicações

Equipa de produção de hardware	Equipa que tem o papel de desenvolver fisicamente os produtos com auxílio de maquinarias.	• 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.	• 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.	• 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 contêm 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 contêm 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 serviços da Google, pagando uma subscrição, que terão como objetivo fazer o armazenamento de documentos como relatórios, contratos, faturas, etc.
Servidor de backup de base de dados	Recurso que serve de salvaguarda 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 pelo funcionários

Aplicações

Nome	Descrição
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).
Aplicação do Sistema de Gestão de Stock	Aplicação de controlo e gestão de stock presente nos armazéns da empresa.
Aplicação do Sistema de Gestão de Vendas e Entregas	Aplicação que auxilia a Dev4Shell no processo de gestão de vendas, desde o registo do pedido até à entrega do produto ao cliente.
Aplicação do Sistema de Gestão de Recursos Humanos	Aplicação que facilita a administração e a gestão das atividades relacionadas aos funcionários da empresa.
Aplicação do Sistema de Gestão Financeira	Aplicação que ajuda a empresa a controlar e gerir as suas atividades financeiras, esta rastreará qualquer tipo de transação e gastos feitos pela mesma e também analisará pagamentos pendentes relacionados com o negócio da empresa ou não.
Aplicação de Sistema de Apoio ao Cliente	Aplicação que permite a Dev4Sell gerir, analisar e atender a pedidos feitos pelos clientes, exibindo na sua interface solicitações de produtos, queixas ou pedidos de ajuda dos mesmos que não tenham sido feitos via chamada telefónica.
Rede de Comunicação Interna da Empresa	Infraestrutura de comunicação interna da empresa, esta estabelecerá a ligação entre os diferentes departamentos e níveis hierárquicos 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 a vir 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 críticos

Recursos que tenham um nível de impacto acima de médio em qualquer um dos três principais pilares da segurança quando sofre um ataque, será considerado como "crítico", estes são recursos que necessitarão de especial atenção, pois um ataque feito aos mesmo, mesmo sem nenhum tipo de preparo ou com preparo para o receber, poderá ter um prejuízo enorme para a empresa.

Pilar de Segurança	Baixo	Médio	Alto
Privacidade	Quando a informação foi divulgada sem autorização necessária e possa provocar um impacto baixo nas operações e recursos organizacionais ou indivíduos e de fácil resolução.	Quando a informação foi divulgada sem autorização necessária e possa provocar um impacto médio nas operações e recursos organizacionais ou indivíduos e ter uma resolução com poucos prejuízos e de grau de dificuldade média.	Quando a informação foi divulgada sem autorização necessária e possa provocar um impacto alto nas operações e recursos organizacionais ou indivíduos e de difícil resolução.
Integridade	Quando a informação é alterada ou destruída sem autorização necessária e possa provocar um impacto baixo nas operações e recursos organizacionais ou indivíduos e de fácil resolução.	Quando a informação é alterada ou destruída sem autorização necessária e possa provocar um impacto médio nas operações e recursos organizacionais ou indivíduos e ter uma resolução com poucos prejuízos e de grau de dificuldade média.	Quando a informação é alterada ou destruída sem autorização necessária e possa provocar um impacto alto nas operações e recursos organizacionais ou indivíduos e de difícil resolução.

Disponibilidade	Quando o acesso ou uso de informações de um sistema pode vir a ter um impacto baixo nas operações organizacionais, recursos e de fácil resolução organizacionais, ou indivíduos.	Quando o acesso ou uso de informações de um sistema pode vir a ter um impacto médio nas operações organizacionais, recursos organizacionais, ou indivíduos e ter uma resolução com poucos prejuízos e de grau de dificuldade média.	Quando o acesso ou uso de informações de um sistema pode vir a ter um impacto alto nas operações organizacionais, recursos organizacionais, ou indivíduos e de difícil resolução.

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

Recurso	Impacto		
	Privacidade	Integridade	Disponibilidade
Infraestrutura	Baixo	Médio	Médio
Computadores	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
Equipa de desenvolvimento de software	Baixa	Baixa	Média
Equipa de produção de hardware	Baixa	Baixa	Média
Equipa de suporte técnico	Baixa	Baixa	Média
Equipa de vendas	Baixa	Baixa	Média
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 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 do Sistema de Gestão de Stock	Baixo	Médio	Médio
Aplicação do Sistema de Gestão de Vendas e Entregas	Alto	Médio	Alto
Aplicação do Sistema de Gestão de Recursos Humanos	Alto	Médio	Médio
Aplicação do Sistema de Gestão Financeira	Alto	Médio	Médio
Aplicação de Sistema de Apoio ao Cliente	Alto	Médio	Alto
Rede de Comunicação Interna da Empresa	Alto	Médio	Médio

Acima conseguimos verificar quais os recursos críticos dos que foram mencionados no capítulo 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 informação tiveram o seu especial destaque, obviamente tendo em conta com o tipo de dados que se está a ter em conta, por exemplo é 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 à lista de recursos críticos, sendo que a divulgação, perda ou até mesmo alteração de dados, bem como a interrupção de serviços de informação possuem um impacto pelo menos preocupante (médio/alto).

As aplicações possuem informações das bases de dados, mesmo que cada aplicação está a receber informação de uma base de dados em específico, não deixa de ser possível informação sensível a ser roubada ou alterada no sistema. Há aplicações que o seu grau de preocupação, nestas situações, é menor, como por exemplo a Aplicação de Gestão de Stock. Os servidores de deployment de aplicações também foi destacada, pois, caso este deixe de funcionar, todas as

aplicações irão parar de rodar 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, tendo em conta que sem este, o sistema não consegue estabelecer ligação entre a rede privada e a rede pública (externa), o que incapacita as comunicações entre cliente-empresa.

A rede interna do sistema 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, sem estas, a produção poderá atrasar-se bastante, fazendo com que os clientes esperem muito tempo e, consequentemente, baixe a reputação da empresa.

Ameaças e vulnerabilidades

As ameaças são potenciais agressões que ainda não se manifestaram, portanto, fazer a identificação de cada uma 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 ela:

<table>
<tr><th>Recurso</th><th>Acesso</th><th>Ator</th><th>Motivo</th><th>Resultado</th><th>Impacto</th></tr>
<tr><td rowspan="4">Máquinas e ferramentas de fabricação</td><td rowspan="4">Físico</td><td rowspan="4">Interno</td><td rowspan="2">Intencional</td><td>Perda/Destruição</td><td>Alto</td></tr>
<tr><td>Interrupção</td><td>Médio</td></tr>
<tr><td rowspan="2">Acidental</td><td>Perda/Destruição</td><td>Alto</td></tr>
<tr><td>Interrupção</td><td>Médio</td></tr>
<tr><td rowspan="2">Router Gateway</td><td>Físico</td><td>Interno</td><td>Intencional</td><td>Interrupção</td><td>Alto</td></tr>
<tr><td>Rede/Sistema</td><td>Externo</td><td>Intencional</td><td>Interrupção</td><td>Alto</td></tr>
<tr><td></td><td>Rede/Sistema</td><td>Externo</td><td>Intencional</td><td>Divulgação</td><td>Médio</td></tr>
</table>

Base de dados de produtos				Modificação	Alto
				Interrupção	Alto
Base de dados de clientes	Rede/Sistema	Externo	Intencional	Divulgação	Alto
				Modificação	
				Interrupção	
Base de dados de entregas	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 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	Divulgação	Alto
				Modificação	Alto
				Perda/Destruição	Alto
Aplicação de Sistema 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
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 da Dev4Sell, quaisquer que sejam as propriedades das ameaças, são de calibre médio/alto, sendo assim, terá de ser feita a avaliação de cada risco possível, de forma a perceber quais os riscos que necessitarão de maior prioridade.

As ameaças apresentam várias propriedades com diferentes valores:

- Recurso crítico: recurso que pode sofrer a ameaça 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: Razão 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 acidental, 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
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 entregas	Impacto	N/A	8
	Gravidade	N/A	7
	Probabilidade	N/A	1
	Média	N/A	5,3
	Média Final	5.3	
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 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

	Média	5.7	6.3
	Média Final	6	
Aplicação de Sistema de Apoio ao Cliente	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 as variáveis fornecidas:

- 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: medida atribuída à chance de um evento ocorrer

De forma a fazer um sistema de pontuação justo, foi preciso ter em causa tanto ameaças 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 não possuí o ator num desses valores e é assumido totalmente o valor do risco do ator que causão a agressão, por exemplo, as máquinas sendo que não têm nenhum tipo de ameaça externa, vai-se assumir totalmente o valor de risco interno.

Para cada valor de risco (interno e externo) é calculada a média entre as três variáveis fornecidas.

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

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

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

Plano de Mitigação

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

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

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

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

Atividades de Mitigação: Base de dados de clientes

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

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

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

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

Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos

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

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

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

Atividades de Mitigação: Aplicação do Sistema de Gestão Financeira

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

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

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

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

Atividades de 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 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 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 detetarão lacunas no sistema de segurança da app. Os testes serão implementados com auxílio da ferramenta Selenium em junção com um software de VPN para fazer várias simulações de diferentes tipos de acesso a contas e mesmo ataques à aplicação de diferentes localizações.

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

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

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 eletrônicos não são desenvolvidos e, consequentemente, 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 eletrônicos, 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 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 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

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

Atividades de Mitigação: Base de dados de produtos

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

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

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

Riscos aceites

<FAZER TEXTO>

Plano de 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 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 recuperação de Dados

Um guia de recuperação de dados é um conjunto de instruções/procedimentos que detalha de forma especifica e clara sobre como recuperar dados perdidos, danificados, corrompidos ou inacessíveis de dispositivos de armazenamento para normal funcionamento do sistema.

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

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	- Tentar 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 Reposição

<Falar sobre este plano>

Plano de Contingência

<Falar sobre este plano>

Auditoria

A auditoria pretende controlar a observância das medidas de segurança informática aprovadas, consiste em operações periódicas de controlo das medidas de segurança, esta 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.

A auditoria na Dev4Sell será efetuada 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 ter de contratar auditores internos, esta decisão evita gastos adicionais com salários e despesas desnecessárias 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 as regulamentações e padrões de segurança impostas pela mesma, identificar falhas e vulnerabilidades de segurança nos sistemas de informação, avaliar a eficácia das políticas impostas 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 o planeamento juntamente com a empresa em causa dos procedimentos e objetivos a serem atingidos.

A auditoria deve ter como procedimentos os seguintes passos:

- Verificar a integridade física da infraestrutura da Dev4Sell
- Verificar a integridade física das máquinas de produção de componentes eletrônicos
- 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 para serem executados como por exemplo efetuar testes de penetração de sistemas, revisão de políticas e procedimentos da empresa, entre outros.

Finalmente, deve ser realizado um relatório com os resultados obtidos na auditoria realizada, juntamente com a identificação de vulnerabilidades encontradas.

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

Simulacros

<Explicar a importância dos simulacros e como estes serão feitos>

<Simulacro surpresa para avaliação e revisão>

<Simulacros treino onde todos são avisados>

Biografia

<Biografia>