

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	15
PN01 – Parcerias comerciais com os fornecedores	15
PN02 – Parcerias comerciais com os clientes	15
PN03-Gestão de Stock	16
PN04 – Venda	17
MÉTODO DE AVALIAÇÃO DE RISCO	18
Octave 18	
ARQUITETURA DOS SISTEMAS	19
Sistema de Administração da Empresa	19
Sistema de Comunicação Interna	20
Rede Telefónica	20
Sistema de Email Interno	20
Sistema de Armazenamento de Dados	20
Sistema de Produção	21
Sistema de Aplicações	21
Aplicações de suporte ao funcionário (Computador)	22
Aplicação de auxílio de entregas e consulta de stock (Smartphone)	22
RECURSOS	23
Físicos 23	
Humanos	24
Dados 26	
Suporte de Dados	27

Aplicações	28
ANÁLISE E GESTÃO DE RISCOS	29
Recursos críticos	30
Ameaças e vulnerabilidades	35
Análise e Avaliação do Risco	40
PLANO DE MITIGAÇÃO	46
Atividades de Mitigação: Base de dados de finanças	46
Atividades de Mitigação: Base de dados de clientes	47
Atividades de Mitigação: Base de dados de funcionários	47
Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos (Transferir)	48
Atividades de Mitigação: Aplicação de Gestão Financeira	48
Atividades de Mitigação: Servidores de bases de dados	48
Atividades de Mitigação: Aplicação de Apoio ao Cliente	49
Atividades de Mitigação: Aplicação de Gestão de Vendas e Entregas	49
Atividades de Mitigação: Máquinas e ferramentas de fabricação	50
Atividades de Mitigação: Base de dados de entregas	51
Atividades de Mitigação: Servidores de deployment de aplicações	51
Atividades de Mitigação: Aplicações de Gestão dos Recursos Humanos	51
Atividades de Mitigação: Base de dados de produtos	52
Riscos aceites	53
PLANO DE RECUPERAÇÃO	54
Backup	54
Guia de Reposição dos Dados	56
PLANO DE CONTIGÊNCIA	60
AUDITORIA	62
Auditoria Externa	62
Simulacros	63

CONCLUSÃO	64
BIOGRAFIA	65

Lista de Tabelas

Tabela 1 - Departamentos da Dev4Sell	8
Tabela 2 - Cargos de cada departamento da Dev4Sell	10
Tabela 3 - Recursos Físicos da Dev4Sell	23
Tabela 4 - Recursos Humanos da Dev4Sell	24
Tabela 5 - Recursos de Dados da Dev4Sell	26
Tabela 6 - Recursos de Suporte de Dados da Dev4Sell	27
Tabela 7 - Recursos de Aplicações da Dev4Sell	28
Tabela 8 - Descrição das classificações dos três pilares da segurança	30
Tabela 9 - Análise do nível de impactos nos recursos da Dev4Sell	31
Tabela 10 - Descrição das ameaças nos recursos da Dev4Sell	35
Tabela 11 - Classificação dos riscos nos recursos da Dev4Sell	40
Tabela 12 - Backups da Dev4Sell	54
Tabela 13 - Guia de Recuperação de Dados	56
Tabela 14 - Plano de Reposição	60

Introdução

Contextualização do documento

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

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

Descrição da empresa

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

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

Funes e responsabilidades

Com base na estrutura da empresa Dev4Sell, segue-se abaixo a tabela com a identificao dos departamentos e as suas descries:

Tabela 1 - Departamentos da Dev4Sell

Departamentos	Descrio
CEO	Lidera a Dev4Sell, atuando como intermedirio entre os diferentes diretores e departamentos da empresa. Tem acesso a toda a informao que circula na empresa.
Diretor(a)	Responsvel por uma rea especfica da empresa, como finanas, operaes, marketing, recursos humanos, etc. Supervisiona e coordena as equipas nessa rea e fornece suporte ao CEO a definir decises estratgicas para a empresa.
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	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 de otimizar a

	utilização dos recursos financeiros disponíveis e fornecer informações precisas e relevantes para a tomada de decisões estratégicas.
Departamento de Logística	Encarregado de gerir a movimentação e armazenamento de materiais e produtos, bem como a distribuição e entrega dos mesmos.
Departamento de Desenvolvimento e Produção	Responsável pelo design e construção dos equipamentos eletrónicos da empresa.
Departamento de Apoio ao cliente	Responsáveis por dar assistência ao cliente via website, móvel ou correio eletrónico, quer seja para esclarecimento de dúvidas ou possíveis negócios.

A tabela a seguir apresenta os diferentes cargos de cada departamento, acompanhado da quantidade de funcionrios que ocupam cada cargo e uma breve descrio das suas responsabilidades. Isso fornecer uma viso mais detalhada da estrutura organizacional da empresa.

Tabela 2 - Cargos de cada departamento da Dev4Sell

Departamento	Cargo	Quantidade	Descrio
Departamento de Recursos Humanos	Gerente do Departamento de Recursos Humanos	1	Gere e desenvolve as polticas e prticas relacionadas aos recursos humanos. Supervisiona e garante o correto funcionamento do seu departamento.
	Tcnico de Recursos Humanos	2	Recruta e seleciona novos funcionrios. Coordena e processa toda a documentao empresarial. Realiza treinos de sensibilizao em diversas reas dos recursos humanos.
	Assistente de Recursos Humanos	2	Fornecer suporte administrativo, auxiliando assim os tcnicos e gerente do departamento.
Departamento de Sistemas de Informao	Gerente do Departamento de Sistemas de Informao	1	Supervisiona e coordena todas as atividades relacionadas com a rea dos Sistemas de Informao, garantindo o correto funcionamento do seu departamento. Tem um papel crucial na eficincia e segurana dos SI na empresa.
	Administrador da Bases de Dados	1	Administra as bases de dados da empresa. Conhece o funcionamento de todos os departamentos a nvel de acesso e manipulao da informao.
	Especialista de Segurana da Informao	2	Garante a segurana dos sistemas e dos dados da empresa.

	Tcnico de Suporte dos Sistemas de Informao	2	<p>Fornece suporte tcnico no uso de tecnologias de informao.</p> <p>Deve estar pronto a agir assim que uma falha ou avaria relacionada com os sistemas de informao ocorra.</p>
Departamento de Negcios	Gerente do Departamento de Negcios	1	<p>Gere e supervisiona todas as atividades relacionadas s vendas e compras da empresa.</p> <p>Encarregue do correto funcionamento do seu departamento.</p>
	Coordenador de Compras	1	<p>Lidera as atividades de compra, incluindo pesquisa de fornecedores, negociao de contratos e acompanhamento de prazos de entrega.</p> <p>Fornece suporte aos executivos de compras quando necessrio.</p>
	Coordenador de Vendas	1	<p>Lidera as atividades de venda, desenvolvendo estratgias, identificando oportunidades no mercado e garantindo a satisfao do cliente.</p> <p>Fornece suporte aos executivos de vendas quando necessrio.</p>
	Executivo de Compras	2	<p>Realiza o processo de compra, pesquisa por fornecedores, avalia propostas e toma decises de compra.</p>
	Executivo de Vendas	2	<p>Realiza o processo de venda, procura por clientes, fornece informaes sobre os produtos e negocia contratos.</p>
	Analista de Mercado	1	<p>Recolhe informao sobre os consumidores, empresas concorrentes, tendncias, oportunidades de negcio entre outras informaes relevantes do mercado.</p>

Departamento de Marketing	Gerente do Departamento de Marketing	1	Gere e desenvolve as pol�ticas e pr�ticas relacionadas com o marketing da empresa. Supervisiona e garante o correto funcionamento do seu departamento.
	Especialista em Marketing	5	Desenvolve e implementa estrat�gias de marketing para promover os produtos e a empresa.
	Designer Gr�fico	1	Cria materiais gr�ficos e visuais para campanhas de promoo.
Departamento de Finanas	Gerente do Departamento de Finanas	1	Gere as atividades financeiras da empresa, incluindo o controlo de custos e oramentos, e planeamento financeiro. Este supervisiona e garante o correto funcionamento do seu departamento.
	Especialista de An�lise Financeira	1	Analisa e interpreta os dados financeiros da empresa, incluindo elaborao de relat�rios e suporte na tomada de decis�es financeiras.
	Tesoureiro	1	Gere o controle de fluxo de transa�es financeiras e contas banc�rias. Garante a disponibilidade adequada de fundos para investimentos e opera�es da empresa.
Departamento de Log�stica	Gerente do Departamento de Log�stica	1	Supervisiona e gere todas as atividades relacionadas com as atividades log�sticas, tendo assim um papel crucial na organizao de recursos e produtos da empresa. Supervisiona e garante o correto funcionamento do seu departamento.
	T�cnico de Log�stica e Abastecimento	1	Gere o fluxo de materiais e recursos da empresa, al�m da rela�o com fornecedores e planeia a aquisi�o de materiais.

	Analista de Stock de Recursos e Produtos	2	Monitoriza, analisa e gere o stock de produtos e recursos.
	Equipa de Transporte	10	Realizam e asseguram a entrega dos produtos nos perodos estipulados.
Departamento de Desenvolvimento e Produo	Gerente do Departamento de Desenvolvimento e Produo	1	Gere e desenvolve as polticas e prticas relacionadas com o desenvolvimento e produo de componentes eletrnicos da empresa. Supervisiona e garante o correto funcionamento do seu departamento.
	Gestor de Projetos	4	Coordena e executa os projetos relacionados ao desenvolvimento e produo de equipamentos eletrnicos.  um pilar crucial para a comunicao e gesto de recursos necessrios em cada projeto.
	Designer Industrial	3	Cria conceitos de design, desenvolve desenhos tcnicos e modelos 3D dos produtos a serem produzidos.
	Engenheiro de Desenvolvimento de Hardware	15	Responsvel pela produo de componentes eletrnicos a nvel fsico.
	Engenheiro de Desenvolvimento de Software	30	Responsvel pela produo de componentes eletrnicos a nvel lgico. Produz o software necessrio para o funcionamento dos equipamentos e elabora as aplicaes para o consumo de dados, para uso da empresa.
	Especialista em Quality Assurance	5	Garante a fiabilidade e durabilidade dos componentes eletrnicos comprados e produzidos.
Departamento de Apoio ao Cliente	Gerente do Departamento de Apoio ao Cliente	1	Gere e desenvolve as polticas e prticas relacionadas com o atendimento ao cliente da empresa.

			Supervisiona e garante o correto funcionamento do seu departamento.
	Especialistas de Atendimento ao Cliente	10	Fornece suporte e assistência aos clientes.
	Especialistas em Retenção de Clientes	2	Garante a satisfação e minimização ativa da base de clientes.

Processos de Negócio

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

PN01 – Parcerias comerciais com os fornecedores

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

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

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

Reunião: durante a reunião é estabelecido os termos e condições desta parceria, envolvendo o tipo de serviços esperados, prazos, orçamentos, requisitos e cláusulas 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.

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

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

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

Octave

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

Ajuda as organizações a aplicar a informação de gestão de risco de segurança para assegurar a sua infraestrutura da informação existente e proteger os seus recursos críticos.

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

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

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

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

Arquitetura dos Sistemas

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

Numa fase inicial ser referido o funcionamento do sistema de administrao empresarial, que tem como objetivo fazer a anlise e gesto dos vrios recursos ou mesmo processos de negcio da empresa, como por exemplo fazer o acompanhamento de uma entrega, fazer a verificao de stock de componentes eltricos produzidos ou mesmo a anlise financeira da empresa.

De seguida sero abordados os sistemas relativos  comunicao interna da empresa, sistema de armazenamento de dados e sistema de produo. Ser analisada a metodologia de comunicao fluda e eficaz entre as diferentes entidades envolvidas, algo considerativo no sucesso dos processos de negcio e na segurana e preservao dos dados relacionados com a empresa, produtos e clientes.

Por fim, ser analisado neste captulo os sistemas aplicacionais que contm a lgica de armazenamento dos dados e a interao com os mesmos que serviro de suporte  anlise de estados de certos processos como entregas ou desenvolvimento de produtos eletrnicos. Estes sistemas tm como principal objetivo apoiar diretamente os funcionrios de forma a contribuir beneficamente para o seu papel num processo de negcio.

Sistema de Administrao da Empresa

Sistema de anlise e gesto de recursos e processos de negcio em curso. Os recursos humanos realizam tarefas como:

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

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

Sistema de Comunicação Interna

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

Rede Telefónica

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

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

Sistema de Email Interno

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

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

Sistema de Armazenamento de Dados

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

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

Devido a este também estar responsável pelo tratamento e segurança dos dados altamente valiosos, torna-se num dos sistemas mais importantes e que possivelmente mais impactantes na empresa em caso de uma ameaça se tornar numa agressão.

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

Sistema de Produção

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

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

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

Sistema de Aplicações

Sistema de suporte a todos os sistemas anteriormente referidos, fornecendo uma interface interativa para haver a comunicação entre os funcionários e os dados registados em base.

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

Tendo em conta o tipo de funcionário registado em base de dados, este terá acesso direto após o login à respetiva página associada à função dele. Por exemplo, após um funcionário do departamento de finanças efetuar o login na aplicação, será redirecionado para a interface de análise de histórico de faturas, vendas feitas recentemente, etc.

Foram criados dois tipos de aplicação distintas, aplicação para desktop que terá acesso a diversas interfaces respetivas a cada recurso humano e aplicação para smartphone que terá funcionalidades rápidas como visualização de stock instantâneo, visualização de pedidos de entrega e a monitorização de uma entrega.

Aplicações de suporte ao funcionário (Computador)

Aplicação principal para auxiliar o trabalho de cada membro da empresa no qual, dependendo do login, cada funcionário será redirecionado para a sua respetiva interface:

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

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

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

A aplicação mobile apresentará funcionalidades mais simples e de rápida consulta para os elementos da equipa de entregas, estando assim incluídas as funcionalidades de:

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

Recursos

Para o sucesso na performance dos sistemas ser necessrio que esta contenha recursos, que se trata de meios que podem ser utilizados para um determinado fim. Estes possuem um valor e sofrem ataques, sejam estes 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

Ativos tangveis, como instalaes e equipamentos, que suportam as operaes da empresa.

Tabela 3 - Recursos Fsicos da Dev4Sell

Nome	Descrio	Sistemas em que  utilizado
Infraestrutura	Estrutura fsica da empresa que serve de suporte para o funcionamento dos sistemas e equipamentos.	<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 e Telemveis	Equipamento de auxlio para interao com os sistemas.	<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 produzidos.	<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 utilizados no processo de produo.	<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o 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. Utilizados para transportar os produtos.	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa

Humanos

Todos os departamentos que integram os funcionrios que contribuem para o correto funcionamento da empresa. Encontra-se uma descrio mais detalhada de cada departamento no subcaptulo da descrio da empresa.

Tabela 4 - Recursos Humanos da Dev4Sell

Nome	Sistemas em que atuam
Departamento de Recursos Humanos	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa

	<ul style="list-style-type: none"> • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Aplicaes
Departamento de Sistemas de Informao	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados
Departamento de Negcios	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Aplicaes
Departamento de Marketing	<ul style="list-style-type: none"> • Sistema de Comunicao Interna
Departamento de Finanas	<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
Departamento de Logstica	<ul style="list-style-type: none"> • Sistema de Administrao da Empresa • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados

	<ul style="list-style-type: none"> • Sistema de Aplicaes
Departamento de Desenvolvimento e Produo	<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 • Sistema de Produo
Departamento de Apoio ao Cliente	<ul style="list-style-type: none"> • Sistema de Comunicao Interna • Sistema de Armazenamento de Dados • Sistema de Aplicaes

Dados

Toda a informao armazenada em sistemas de bases de dados.

Tabela 5 - Recursos de Dados da Dev4Sell

Nome	Descrio	Fonte dos dados	Nvel de Acesso	Responsvel pelos dados
Base de dados de produtos	Base de dados que contm a informao acerca do armazm de stock de produtos desenvolvidos e recursos comprados.	Produtos desenvolvidos e comprados.	Mdio	Gerente do Departamento de Logstica
Base de dados de clientes	Base de dados que contm as informaes dos clientes da empresa.	Entidades que entrem em contacto com a empresa e que estejam interessadas na compra de um produto ou interaes com a empresa.	Alto	Gerente do Departamento de Apoio ao Cliente

Base de dados de funcionrios	Base de dados que contm as informaes dos funcionrios da empresa e registos de performance.	Recursos humanos contratados, histrico de vendas e anlise de KPIs.	Alto	Gerente do Departamento dos Recursos Humanos
Base de dados de entregas	Regista o progresso de cada entrega que foi feita pela empresa, registando datas, locais e estados.	Pedidos feitos pelos clientes, relatrios de equipas de entrega e atualizaes na aplicao do sistema de entregas.	Alto	Gerente do Departamento de Logstica
Base de dados de finanas	Regista informaes relacionadas s transaes e faturao, incluindo detalhes de vendas, pagamentos e outras informaes financeiras relevantes.	Transaes realizadas pela empresa ou pelos clientes.	Alto	Gerente do Departamento de Finanas
Base de dados de testes de verses	Regista resultados testes executados aps a submisso de verses novas de cada aplicao.	Verso testada, quantidade de utilizadores, quantidade de requests executados, quantidade de requests com resposta OK, tempo de execuo.	Mdio	Gerente do Departamento de Desenvolvimento e Produo

Suporte de Dados

Infraestrutura e tecnologias que armazenam e protegem os dados.

Tabela 6 - Recursos de Suporte de Dados da Dev4Sell

Nome	Descrio
Servidores de deployment de aplicaes	Recurso de alto desempenho e confiabilidade responsvel por disponibilizar e executar as aplicaes em um ambiente operacional.
Impressoras	Recurso responsvel pela impresso de documentos como relatrios, 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 de armazenar documentos como relatrios, contratos, faturas, etc.
Servidor de backup de base de dados	Recurso que serve de reserva 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 pelos funcionrios.

Aplicaes

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

Tabela 7 - Recursos de Aplicaes da Dev4Sell

Nome	Descrio
Ambientes de desenvolvimento (IDE)	Recurso que fornece um conjunto de ferramentas para facilitar o desenvolvimento de software.
Aplicao de Gesto de Stock	Aplicao de controlo e gesto de stock presente nos armazns da empresa.
Aplicao de Gesto de Vendas e Entregas	Aplicao que auxilia no processo de gesto de vendas, desde o registo do pedido at  entrega do produto ao cliente.
Aplicao 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 de Gesto Financeira	Aplicao que ajuda a empresa a controlar e gerir as suas atividades financeiras. Esta rastrear qualquer tipo de transaes e tambm analisar pagamentos pendentes relacionados com o negcio da empresa ou no.
Aplicao de Apoio ao Cliente	Aplicao que permite gerir, analisar e atender a pedidos feitos pelos clientes, exibindo na sua interface solicitaes de produtos, queixas ou pedidos de ajuda que no tenham sido feitos via chamada telefnica.
Rede de Comunicao Interna da Empresa	Infraestrutura de comunicao interna da empresa, que estabelecer a ligao entre os diferentes departamentos da Dev4Sell.

Anlise e Gesto de Riscos

Tendo em conta o elevado nmero de recursos da Dev4Sell, assume-se a possibilidade de uma vasta diversidade de riscos. Estes sero analisados, tendo em causa o seu impacto e prejuzo.

Em geral,  possvel analisar que os riscos, dependendo de cada um, iro afetar os seguintes fatores:

- Sade dos recursos humanos;
- Produtividade de desenvolvedores e equipa de produo de produtos;
- Reputao da Dev4Sell;
- Eficincia e cuidado na entrega de produtos.

Inicialmente, sero identificados os recursos crticos, que so os recursos que no caso de um dos trs pilares da segurana associados for afetado, o seu impacto para empresa  de nvel alto/catastrfico.

De seguida sero identificadas as ameaas aos recursos para a empresa estar ciente dos ataques que esta possa vir a sofrer e fazer uma preparao para evit-los ou mesmo reduzir impactos.

Por fim, ser feita a anlise e avaliao dos riscos onde ser atribuda uma classificao, em diferentes fatores:

- Impacto
- Gravidade
- Probabilidade

Isto far com que seja possvel tomar decises em relao a quais riscos compensa mitigar, resolver ou simplesmente ignorar.

Recursos crticos

Recursos que tenham um nvel de impacto alto em qualquer um dos trs principais pilares da segurana quando sofre um ataque.

Estes recursos necessitaro de especial ateno, pois quando sofrem um ataque podero causar um enorme prejuzo para a empresa.

Tabela 8 - Descrio das classificaes dos trs pilares da segurana

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, recursos e entidades. 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, recursos e entidades. Resoluo com poucos prejuzos e de grau de dificuldade mdio.	Quando a informao foi divulgada sem autorizao necessria e possa provocar um impacto alto nas operaes, recursos e entidades. Difcil resoluo.
Integridade	Quando o recurso  alterado ou destruido sem autorizao necessria e possa provocar um impacto baixo nas operaes, recursos e entidades. Fcil resoluo.	Quando o recurso  alterado ou destruido sem autorizao necessria e possa provocar um impacto mdio nas operaes, recursos e entidades. Resoluo com poucos prejuzos e de grau de dificuldade mdio.	Quando o recurso  alterado ou destruido sem autorizao necessria e possa provocar um impacto alto nas operaes, recursos e entidades. Difcil resoluo.
Disponibilidade	Quando o acesso ou uso de recursos de um sistema pode vir a	Quando o acesso ou uso de recursos de um sistema pode vir a	Quando o acesso ou uso de recursos de um sistema pode vir a

	ter um impacto baixo nas operaes, recursos e entidades. Fcil resoluo	ter um impacto mdio nas operaes, recursos e entidades. Resoluo com poucos prejuzos e de grau de dificuldade mdia.	ter um impacto alto nas operaes, recursos e entidades Difcil resoluo.
--	--	---	---

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

Tabela 9 - Anlise do nvel de impactos nos recursos da Dev4Sell

Recurso	Impacto		
	Privacidade	Integridade	Disponibilidade
Infraestrutura	Baixo	Mdio	Mdio
Computadores e Telemveis	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

Departamento de Recursos Humanos	Baixa	Baixa	Mdia
Departamento de Sistemas de Informao	Baixa	Baixa	Mdia
Departamento de Negcios	Baixa	Baixa	Mdia
Departamento de Marketing	Baixa	Baixa	Mdia
Departamento de Finanas	Baixa	Baixa	Mdia
Departamento de Logstica	Baixa	Baixa	Mdia
Departamento de Desenvolvimento e Produo	Baixa	Baixa	Mdia
Departamento de Apoio ao Cliente	Baixa	Baixa	Mdia
Base de dados de produtos	Alta	Alta	Alta
Base de dados de clientes	Alta	Alta	Alta
Base de dados de funcionrios	Alta	Alta	Alta
Base de dados de entregas	Alta	Alta	Alta
Base de dados de finanas	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 de Gesto de Stock	Baixo	Mdio	Mdio
Aplicao de Gesto de Vendas e Entregas	Alto	Mdio	Alto
Aplicao de Gesto de Recursos Humanos	Alto	Mdio	Mdio
Aplicao de Gesto Financeira	Alto	Mdio	Mdio
Aplicao de Apoio ao Cliente	Alto	Mdio	Alto

Rede de Comunicao Interna da Empresa	Alto	Mdio	Mdio
---	------	-------	-------

Todos os recursos de dados tiveram destaque, sendo assim, todas as bases de dados e os seus servidores foram adicionados  lista de recursos crticos, sendo que a divulgao, perda ou alterao dos dados, bem como a interrupo de servios de informao provocam um impacto no mnimo preocupante (mdio/alto).

Cada aplicao consome informao de uma base de dados em especfico. Em caso de agresso existem aplicaes de grau de preocupao menor, como por exemplo a Aplicao de Gesto de Stock. Os servidores de deployment de aplicaes tambm foram destacados, pois caso sejam interrompidos, todas as aplicaes terminam 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, pois na sua ausncia, o sistema no consegue estabelecer ligao entre a rede privada e a rede pblica (externa), incapacitando as comunicaes para fora da empresa via Internet.

A rede interna 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. Durante a sua ausncia, ocorrer atrasos na produo, resultando no incumprimento de prazos estipulados. Isso pode afetar negativamente a reputao e os lucros da empresa.

Ameaas e vulnerabilidades

As ameaas so potenciais agresses que ainda no se manifestaram. A identificao destas  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:

Tabela 10 - Descrio das ameaas nos recursos da Dev4Sell

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
Base de dados de produtos	Rede/Sistema	Externo	Intencional	Divulgao	Mdio
				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 funcionrios	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	
Base de dados de finanas	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	Fsico	Interno	Intencional	Interrupo	Mdio
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruio	Alto
				Interrupo	Mdio
Servidores de bases de dados	Fsico	Interno	Intencional	Interrupo	Mdio
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruio	Alto

				Interrupo	Mdio
Servidor de backup de base de dados	Fsico	Interno	Intencional	Interrupo	Baixo
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruio	Alto
				Interrupo	Mdio
Armazenamento de backup em discos	Fsico	Interno	Intencional	Divulgao	Baixo
				Modificao	Alto
				Perda/Destruio	Mdio
			Acidental	Perda/Destruio	Mdio
Aplicao de Gesto de Recursos Humanos	Fsico	Interno	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Mdio
	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Mdio
Aplicao de Gesto Financeira	Fsico	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
Aplicao de Apoio ao Cliente	Fsico	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
Aplicao de Gesto de Vendas e Entregas	Fsico	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	Fsico	Interno	Intencional	Interrupo	Mdio
			Acidental	Interrupo	Mdio
	Rede/Sistema	Externo	Intencional	Interrupo	Mdio

Acima  possvel verificar que sendo estes recursos crticos, os impactos causados nos sistemas de informao so de calibre mdio/alto, sendo assim, ser feita a avaliao de cada risco possvel, de forma a perceber quais os prioritrios.

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

- Recurso crtico: recurso que pode sofrer a ameaa;
- Acesso: forma como o atacante acede ao recurso. Pode ser classificado como:
 - Fsico;
 - Rede/Sistema.
- Ator: entidade que efetua o ataque. Pode ser classificado como:
 - Interno;
 - Externo.
- Motivo: motivo do ataque. Pode ser classificado como:
 - Acidental;
 - Intencional.
- Resultado: ao executada pelo atacante. Pode ser classificado como:
 - Divulgao - divulgao ou visualizao de informaes sensveis;
 - Modificao - modificao de informaes importantes ou confidenciais;
 - Destruio - Destruio ou perda de informaes importantes, hardware ou software;
 - Interrupo - Interrupo de acesso a informaes importantes, software, aplicativos ou servios.
- Impacto: nvel de danos ou consequncias causadas. Pode ser classificado como:
 - Baixo;
 - Mdio;
 - Alto.

Ser feita agora a anlise de alguns casos em particular da tabela acima.

Ameaas que possuem um ator interno com motivo acidental,  assumido que tanto um recurso humano como uma causa natural possa ter sido a fonte da agresso.

Como  possvel observar, os recursos que foram classificados como alto no impacto esto relacionados a informaes altamente sensveis, como dados de clientes, financeiros, entre outros. Alm disso, esses recursos esto associados a bases de dados que armazenam toda a informao que circula entre os sistemas da empresa, tornando-se extremamente valiosos para a organizao.

Deve-se considerar tambm os restantes recursos crticos que apresentam valores mais baixos no impacto, como  o caso da Aplicao do Sistema de Gesto de Recursos Humanos, pois este tem acesso direto a dados e documentos sensveis como contratos. Apesar de no ser possvel manipul-los, consegue divulg-los.

Anlise e Avaliao do Risco

Para finalizar a anlise do risco, ser implementada uma tabela que ir conter cada recurso e a classificao de cada fator referido na introduo deste captulo: impacto, gravidade e probabilidade.

Tendo em conta que cada um destes valores no tem uma forma de ser atribudo detalhadamente, ser feita uma atribuio de pontos (0-10), para que seja possvel criar um sistema hierrquico das ameaas analisadas.

Segue-se ento abaixo a tabela referente  anlise de risco:

Tabela 11 - Classificao dos riscos nos recursos da Dev4Sell

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	
	Impacto	N/A	7

Base de dados de produtos	Gravidade	N/A	6
	Probabilidade	N/A	2
	Mdia	N/A	5
	Mdia Final	5	
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 funcionrios	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	
	Impacto	N/A	9

Base de dados de finanas	Gravidade	N/A	9
	Probabilidade	N/A	2
	Mdia	N/A	6,7
	Mdia Final	6.7	
Base de dados de testes de verses	Impacto	N/A	5
	Gravidade	N/A	6
	Probabilidade	N/A	1
	Mdia	N/A	4
	Mdia Final	4	
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	
	Impacto	9	9

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

Aplicao de Gesto Financeira	Gravidade	4	6
	Probabilidade	4	4
	Mdia	5.7	6.3
	Mdia Final	6	
Aplicao de Apoio ao Cliente	Impacto	9	9
	Gravidade	4	6
	Probabilidade	3	3
	Mdia	5.3	6
	Mdia Final	5.7	
Aplicao de Gesto de Vendas e Entregas	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 os fatores fornecidos:

- 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: expectativa de um evento ocorrer.

Para estabelecer um sistema de pontuao justo, levamos em conta as ameaas causadas tanto internamente quanto externamente. Quando no ocorre nenhum incidente, atribumos o valor "N/A" para indicar a ausncia de risco. Estes no so associados ao clculo da mdia.

 calculada a mdia entre as trs variveis fornecidas de cada coluna (interna e externa) separadamente.

Por fim  calculada a mdia total entre as duas colunas, constando que valores "N/A" no entram no clculo.

Com os valores obtidos j  possvel ver hierarquicamente quais os riscos mais preocupantes para o plano de mitigao, tendo sido esta a ordem obtida:

- Base de dados de finanas: 6.7
- Base de dados de clientes: 6.7
- Base de dados de funcionrios: 6.7
- Servidor de armazenamento em nuvem para documentos: 6
- Aplicao de Gesto Financeira: 6
- Servidores de bases de dados: 5.8
- Aplicao de Apoio ao Cliente: 5.7
- Aplicao de Vendas e Entregas: 5.7
- Mquinas e ferramentas de fabricao: 5.3
- Base de dados de entregas: 5.3
- Servidores de deployment de aplicaes: 5.2
- Aplicao de Gesto de Recursos Humanos: 5
- Base de dados de produtos: 5
- Router Gateway: 4.3
- Servidor de backup de base de dados: 4.2
- Base de dados de testes de verses: 4
- Armazenamento de backup em discos: 4
- Rede de Comunicao Interna da Empresa: 3.8

Plano de Mitigao

Calculados os valores dos riscos associados aos recursos, tem de ser implementando um plano de mitigao, que define as atividades necessrias para eliminar ou reduzir o risco inaceitvel.

A partir deste plano, ser selecionado os riscos a mitigar, bem como a descrio das atividades/políticas a aplicar em cada recurso selecionado. Isto ir permitir que a probabilidade do risco reduza, ou anule.

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

- Base de dados de finanas;
- Base de dados de clientes;
- Base de dados de funcionrios;
- Servidor de armazenamento em nuvem para documentos;
- Aplicao de Gesto Financeira;
- Servidores de bases de dados;
- Aplicao de Apoio ao Cliente;
- Mquinas e ferramentas de fabricao;
- Base de dados de entregas;
- Servidores de deployment de aplicaes;
- Aplicao de Gesto de Recursos Humanos;
- Base de Dados de Produtos.

Atividades de Mitigao: Base de dados de finanas

O acesso  base de dados de finanas da empresa deve ser restrito a todos os funcionrios exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informao e ao Gerente do Departamento de Finanas, excluindo possveis atores envolvidos em ataques futuros.

Deve estar disponvel 24 horas por dia, tentando apresentar o mximo de disponibilizao s aplicaes de suporte aos funcionrios, pois consomem constantemente os dados armazenados.

Devem ser registados todos os acessos efetuados, bem como as operaes (queries) que foram executadas. Isto permitir que em caso de uma agresso, 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 base de dados periodicamente, explicado no Plano de Recuperao.

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

O acesso  base de dados de clientes deve ser restrito a todos os funcionrios exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informao, aos Engenheiros de Software que iro trabalhar na Aplicao de Apoio ao Cliente e Entregas e ao Gerente do Departamento de Atendimento ao Cliente, excluindo possveis atores envolvidos em ataques futuros.

Deve estar disponvel 24 horas por dia, tentando apresentar o mximo de disponibilizao s aplicaes de suporte aos funcionrios, pois consomem constantemente os dados armazenados.

Devem ser registados todos os acessos efetuados, bem como as operaes (queries) que foram executadas. Isto permitir que em caso de uma agresso, 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 base de dados periodicamente, explicado no Plano de Recuperao.

Atividades de Mitigao: Base de dados de funcionrios

O acesso  base de dados de funcionrios da empresa deve ser restrito a todos os funcionrios exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informao e ao Gerente do Departamento de Recursos Humanos, excluindo possveis atores envolvidos em ataques futuros.

Deve estar disponvel 24 horas por dia, tentando apresentar o mximo de disponibilizao s aplicaes de suporte aos funcionrios, pois consomem constantemente os dados armazenados.

Devem ser registados todos os acessos efetuados, bem como as operaes (queries) que foram executadas. Isto permitir que em caso de uma agresso, 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 base de dados periodicamente, explicado no Plano de Recuperao.

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

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

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

Atividades de Mitigação: Aplicação de Gestão Financeira

Deve ser feito um controlo de acessos à aplicação de gestão financeira, controlando assim acessos indevidos, por exemplo um login feito com sucesso fora da rede empresarial.

As realizações de testes de segurança têm um papel crucial neste aspeto, pois detetarão lacunas no sistema de segurança da app. Os testes serão implementados com auxílio da ferramenta Selenium em junção a um software de VPN para fazer várias simulações de diferentes tipos de acesso a contas e mesmo ataques à aplicação de diferentes localizações.

De forma a manter o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

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

Atividades de Mitigação: Servidores de bases de dados

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

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

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

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

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

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

Atividades de Mitigação: Aplicação de Apoio ao Cliente

Deve ser feito um controlo de acessos à aplicação de apoio ao cliente, controlando os acessos indevidos, por exemplo um login feito com sucesso fora da rede empresarial.

As realizações de testes de segurança têm um papel crucial neste aspeto, pois estes detetarão lacunas no sistema de segurança da app. Os testes serão implementados com auxílio da ferramenta Selenium em junção a um software de VPN para fazer várias simulações de diferentes tipos de acesso a contas e mesmo ataques à aplicação de diferentes localizações.

De forma a manter o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

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

Atividades de Mitigação: Aplicação de Gestão de Vendas e Entregas

Deve ser feito um controlo de acessos à aplicação de gestão de vendas e entregas, controlando assim acessos indevidos, por exemplo um login feito com sucesso fora da rede empresarial.

As realizações de testes de segurança têm um papel crucial neste aspeto, pois estes detetarão lacunas no sistema de segurança da app. Os testes serão implementados com auxílio da ferramenta Selenium em junção a um software de VPN para fazer várias simulações de diferentes tipos de acesso a contas e mesmo ataques à aplicação de diferentes localizações.

De forma a manter o controlo de tudo o que está a ser efetuado na aplicação, ficarão registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificação da entidade e operações malignas.

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

Atividades de Mitigação: Máquinas e ferramentas de fabricação

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

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

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

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

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

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

Atividades de Mitigação: Base de dados de entregas

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

Deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização às aplicações de suporte aos funcionários, pois consomem constantemente os dados armazenados.

Devem ser registados todos os acessos efetuados, bem como as operações (queries) que foram executadas. Isto permitirá que em caso de uma agressão, estes logs mostrarão quem teve acesso à base de dados, quando, onde e como.

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

Atividades de Mitigação: Servidores de deployment de aplicações

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

De forma a limitar os acessos aos servidores, estes devem estar localizados de forma segura, dentro da infraestrutura empresarial numa sala restrita controlada por um sensor de RFID.

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

Atividades de Mitigação: Aplicações de Gestão dos Recursos Humanos

Deve ser feito um controlo de acessos à aplicação de gestão dos recursos humanos, controlando assim acessos indevidos, por exemplo um login feito com sucesso fora da rede empresarial.

As 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 a 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 o controlo de tudo o que est a ser efetuado na aplicao, ficaro registados todos os logs, para que no caso de algum ataque ou atividade suspeita no software, seja simples a identificao da entidade e operaes malignas.

Devem ser feitos periodicamente workshops de sensibilizao s prticas de segurana no desenvolvimento e utilizao do software. Isto alertar os funcionrios a implementar prticas mais seguras no desenvolvimento e utilizao da aplicao, evitando riscos de segurana.

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

O acesso  base de dados de produtos deve ser restrito a todos os funcionrios exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informao, aos Engenheiros de Software que iro trabalhar na Aplicao de Gesto de Stock e ao Gerente do Departamento de Logstica, excluindo possveis atores envolvidos em ataques futuros.

Deve estar disponvel 24 horas por dia, tentando apresentar o mximo de disponibilizao aos sistemas de informao, pois consomem constantemente os dados armazenados.

Devem ser registados todos os acessos efetuados, bem como as operaes (queries) que foram executadas. Isto permitir que em caso de uma agresso, 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 base de dados periodicamente, explicado no Plano de Recuperao.

Riscos aceites

Tal como j foi mencionado, os riscos que apresentaram uma avaliao inferior  metade so aceites pela empresa, no entrando no plano de mitigao.

Segue-se abaixo a lista de recursos que no se qualificaram:

- Router Gateway;
- Servidor de backup de base de dados;
- Base de dados de testes de verses;
- Armazenamento de backup em discos;
- Rede de Comunicao Interna da Empresa.

Mesmo que os riscos associados a estes recursos sejam aceites, no devem ser descartados em futuras avaliaes, tendo em conta que podem apresentar vulnerabilidades desconhecidas e obter uma pontuao mais elevada.

Plano de Recuperao

O plano de recuperao  um conjunto de estratgias e aes desenvolvidas para proteger os dados no caso de ocorrer uma agresso nos recursos crticos. Os principais objetivos deste plano so fornecer detalhes sobre o sistema de backups implementado e permitir a recuperao de informaes. Na tabela apresentada abaixo est elaborado o sistema de backups implementado, acompanhado de parmetros que o descrevem.

Backup

Um backup  uma cpia de segurana de dado e permite a recuperao da informao em caso de perda ou corrupo.

Tabela 12 - Backups da Dev4Sell

Recurso	Informao	Local de armazenamento	Periodicidade	Notas
Base de dados de produtos	- Contm o armazenamento de dados relativos aos produtos em armazm	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas
Base de dados de clientes	- Contm o armazenamento de dados relativos aos clientes da empresa	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas
Base de dados de funcionrios	- Contm o armazenamento de dados relativos aos funcionrios da empresa	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas

Base de dados de entregas	- Cont�m o armazenamento de dados relativos �s entregas da empresa	- Servidor de backup - Disco R�gido	Diariamente	- S�o feitas snapshots da base de dados de 2 em 2 horas
Base de dados de finanas	- Cont�m o armazenamento de dados relativos �s finanas da empresa	- Servidor de backup - Disco R�gido	Diariamente	- S�o feitas snapshots da base de dados de 2 em 2 horas
Servidores de deployment de aplica�es	- Aplica�es a decorrer	- Data center	1 vez	- Este servidor atua quando o servidor principal � interrompido ou destr�ido
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 destr�ido
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 Reposio dos Dados

O guia de reposio de dados  um conjunto de instrues/procedimentos que detalha de forma especfica e clara a forma de recuperar dados perdidos, danificados, corrompidos ou inacessveis de dispositivos de armazenamento.

Nas tabelas abaixo iremos demonstrar as etapas de recuperao de dados de cada recurso crtico.

Tabela 13 - Guia de Recuperao de Dados

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	- 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
Aplicaes dos sistemas**	1	- Diagnosticar a causa da falha da aplicao	1.1	- Analisar as mensagens de erro
			1.2	- Identificar a causa da falha da aplicao
	2	- Isolar e restaurar a aplicao	2.1	- Isolar a aplicao afetada do ambiente de produo para evitar que a falha se propague
			2.2	- Restaurar a aplicao recorrendo  verso mais recente e que apresente os melhores resultados obtidos em testes
	3	- Verificar a conexo e recursos necessrios	3.1	- Verificar a conexo com a rede para garantir que a aplicao est conectada com o servidor
	4	- Testes e monitorizao do restauro	4.1	- Realizar testes abrangentes a toda a aplicao restaurada para verificar as funcionalidades
			4.2	Implementar mecanismos de monitorizao 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 Contingncia

O plano de contingncia ir assegurar que os recursos necessrios estejam disponveis em caso de agresso, de modo a manter os sistemas tcnicos em funcionamento.

Tabela 14 - Plano de Reposio

Situao	Nvel de gravidade	Descrio	Tipo de Ao	Ao	Notas
Danos na infraestrutura	Grave	Infraestrutura completamente destruda	Manual	Aluguer temporrio de um local de trabalho e recuperao de bens e recursos	Poder levar a danificao de material interno
	Ligeiro	Leves danos na estrutura ou danos irreparveis em mveis	Manual	Reparao/Substituio	
Avaria de equipamentos fsicos (computadores, mquinas de teste, mquinas de fabricao, router, switches, impressoras, servidores, discos rgidos)	Grave	Danos irreparveis	Manual	Substituio	Dever ser mantido em stock recursos fsicos novos e peas para garantir uma substituio, se necessrio
	Ligeiro	Danos leves	Manual	Reparao	
Avaria da fonte eltrica	Grave	Descarga total	Automtica	Ativao de geradores de fonte eltrica	Ser verificado o estado dos dados e recursos fsicos Manuteno e testes regulares
Danos nos produtos do armazm	Grave	Danos irreparveis	Manual	Descartar e nova construo	Manter em stock as peas necessrias para fazer a reparao de um equipamento
	Ligeiro	Danos leves	Manual	Reparao	

					Manter o plano de construo do produto at  devida venda
Avaria nos camies de entrega	Grave	Imobilizado ou irreparvel	Manual	Substituio ou outsourcing	Dever existir veculos de emergncia Dever ser contactado um reboque em caso de avaria
	Ligeiro	Ligeira avaria que no afeta na totalidade o desempenho, mas necessita de uma reviso	Manual	Contactar terceiros para reparao e substituio temporria	
Ausncia de empregados	Grave	Ausncia temporal bastante prolongada	Manual	Novos contratos para substituio	 considerado bastante prolongado quando ultrapassa 1 ms.
	Ligeiro	Ausncia temporal pouco prolongada	Manual	Outsourcing	
Falha nos sistemas de base de dados	Grave	Decesso  informao bastante prolongada	Automtico	Uso dos backups	Analisar Plano de Recuperao
	Ligeiro	Decesso  informao pouco prolongada	Automtico		
Falha nas apps da empresa	Grave	Decesso  aplicaes bastante prolongada	Automtico	Utilizar o sistema de backup de verses da aplicao	Analisar Plano de Recuperao
	Ligeiro	Decesso  aplicaes pouco prolongada	Automtico		

Auditoria

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

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

Ser realizada por auditores externos, levando em considerao que se trata de uma empresa de pequena/mdia dimenso e que aparenta estar em crescimento, portanto no justifica o contrato de auditores internos. Esta deciso evita gastos adicionais com slrios e despesas a longo prazo.

Auditoria Externa

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

Tem como objetivos garantir que a empresa se encontre em conformidade com os regulamentos e padres de segurana, identificar falhas e vulnerabilidades de proteo dos sistemas de informao, certificar que as instalaes e outros recursos fsicos se encontrem em condies e oferecer recomendaes para melhoria.

O auditor deve inicialmente fazer a recolha de informao relevante sobre os sistemas de informao da Dev4Sell e fazer um plano juntamente com a empresa dos procedimentos e objetivos a serem atingidos.

A auditoria deve ter como procedimentos os seguintes passos:

- Verificar a integridade fsica da infraestrutura;
- Verificar a integridade fsica das mquinas de produo;
- Verificar a integridade fsica dos camies de entrega de produtos;
- Verificar a segurana de acesso  sala de servidores de bases de dados, backup e deployment;
- Verificar vulnerabilidades na rede privada;
- Verificar acessos indevidos a aplicaes da empresa;
- Verificar acessos indevidos  bases de dados das empresas;
- Verificar se as polticas de segurana da empresa esto a ser cumpridas;
- Realizar uma anlise e avaliao de riscos para fazer a identificao de possveis ameaas face os resultados da auditoria;
- Identificao de falhas ou vulnerabilidades de segurana nos sistemas de informao;

- Revisão e avaliação do plano de segurança da empresa;
- Recomendações de alterações a serem efetuadas no plano de segurança da empresa.

Estes procedimentos poderão ter diferentes abordagens:

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

Finalmente, deve ser registado num relatório os resultados obtidos durante a auditoria, juntamente com a identificação de vulnerabilidades encontradas e o que a empresa tem por melhorar a nível de segurança.

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

Simulacros

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

Como já foi referido anteriormente no documento, serão realizados workshops, palestras e formações de sensibilização à segurança no trabalho, porém também ocorrerá simulacros de treino, nos quais todos os funcionários serão alertados com 1 dia de antecedência. Estes simulacros de treino serão acompanhados pelos recursos humanos pertencentes ao Departamento de Recursos Humanos e ao Departamento de Sistemas de Informação, que irão orientar as etapas a serem executadas de forma que os procedimentos de segurança sejam eficazes. Isto também poderá revelar certas vulnerabilidades no plano de segurança e devem ser feitos pelo menos três vezes por semestre.

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

Ser feita uma avaliao no final de cada simulacro surpresa, sendo registado num relatrio todos os eventos ocorridos na simulao da agresso. Ficam anotados os riscos que foram simulados, pontos fortes e pontos fracos nos procedimentos de segurana, de forma que sejam tomadas medidas corretivas e sejam atualizados os protocolos de segurana, se necessrio.

Importante tambm anotar que os agendamentos destes eventos devem ser devidamente planeados entre o CEO, Diretor e Gerentes dos Departamentos de Recursos Humanos e Sistemas de Informao de forma a no prejudicar o negcio da empresa.

Concluso

Embora este cenrio seja fictcio e os processos da framework OCTAVE tenham sido abordados de forma mais ampla, acreditamos firmemente que este trabalho desempenhou um papel crucial na aprendizagem dos conceitos bsicos para desenvolver um plano de segurana.

Ao longo deste projeto, adquirimos conhecimentos valiosos sobre a identificao e avaliao de riscos, bem como sobre a implementao de medidas de segurana adequadas para proteger uma empresa.

Compreendemos a importncia de uma abordagem estruturada e sistemtica para gerir os riscos de segurana tendo sempre em considerao as ameaas, vulnerabilidades e impactos potenciais em todas as reas operacionais.

Biografia

Alberts, C., & Dodofee, A. (2003). *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley.

Teixeira, P. (s.d.). Cobit.

Teixeira, P. (s.d.). Organizações + Octave.

Teixeira, P. (s.d.). Segurança nos Sistemas de Informação.

Teixeira, P. (s.d.). Segurança, políticas e práticas.