

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	5
Contextualização do documento	5
Descrição da empresa	5
Funções e responsabilidades	6
PROCESSOS DE NEGÓCIO	13
PN01 – Parcerias comerciais com os fornecedores	13
PN02 – Parcerias comerciais com os clientes	13
PN03-Gestão de Stock	14
PN04 – Venda	15
MÉTODO DE AVALIAÇÃO DE RISCO	16
Octave 16	
ARQUITETURA DOS SISTEMAS	17
Sistema de Administração da Empresa	17
Sistema de Comunicação Interna	18
Rede Telefónica	18
Sistema de Email Interno	18
Sistema de Armazenamento de Dados	18
Sistema de Produção	19
Sistema de Aplicações	19
Aplicação de gestão de stock (Computador)	20
Aplicação de auxílio de entregas e consulta de stock (Smartphone)	20
RECURSOS	21
Físicos 21	
Humanos	22
Dados 24	
Suporte de Dados	25

Aplicações	25
ANÁLISE E GESTÃO DE RISCOS	27
Recursos críticos	28
Ameaças e vulnerabilidades	32
Análise e Avaliação do Risco	36
PLANO DE MITIGAÇÃO	43
Atividades de Mitigação: Base de dados de clientes	43
Atividades de Mitigação: Servidor de armazenamento em nuvem de documentos	44
Atividades de Mitigação: Aplicação do Sistema de Gestão Financeira	44
Atividades de Mitigação: Servidores de bases de dados	45
Atividades de Mitigação: Aplicação do Sistema de Apoio ao Cliente	45
Atividades de Mitigação: Máquinas e ferramentas de fabricação	46
Atividades de Mitigação: Base de dados de entregas	46
Atividades de Mitigação: Servidor de deployment de aplicações	47
Atividades de Mitigação: Aplicações do Sistema de Gestão dos Recursos Humanos	47
Atividades de Mitigação: Base de dados de produtos	48
Riscos aceites	48
PLANO DE RECUPERAÇÃO	49
Backup	49
Guia de recuperação de Dados	50
PLANO DE CONTIGÊNCIA	55
AUDITORIA	57
Auditoria Externa	57
Simulacros	58
BIOGRAFIA	60

Lista de Tabelas

Tabela 1 - Departamentos da Dev4Sell	6
Tabela 2 - Cargos de cada departamento da Dev4Sell	8
Tabela 3 - Recursos Físicos da Dev4Sell	21
Tabela 4 - Recursos Humanos da Dev4Sell	22
Tabela 5 - Recursos de Dados da Dev4Sell	24
Tabela 6 - Recursos de Suporte de Dados da Dev4Sell	25
Tabela 7 - Recursos de Aplicações da Dev4Sell	25
Tabela 8 - Descrição das classificações dos três pilares da segurança	28
Tabela 9 - Análise do nível de impactos nos recursos da Dev4Sell	29
Tabela 10 - Descrição das ameaças nos recursos da Dev4Sell	32
Tabela 11 - Classificação dos riscos nos recursos da Dev4Sell	37
Tabela 12 - Backups da Dev4Sell	49
Tabela 13 - Guia de Recuperação de Dados	51
Tabela 14 - Plano de reposição	55

Lista de Figuras

Figura 1 — <descrição da figura>

Erro! Marcador não definido.

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.

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 bom funcionamento do seu departamento.
	Tcnicos de Recursos Humanos	2	Responsvel por fazer o recrutamento e seleo de novos funcionrios, coordenar e processar toda a documentao relativa aos mesmos, realizar treinos de sensibilizao aos recursos humanos em diferentes reas.
	Assistentes de Recursos Humanos	2	Fornecer suporte administrativo ao departamento dos recursos humanos, auxiliando assim os tcnicos e gerente.
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 bom funcionamento do seu departamento. Tem um papel crucial na eficincia e segurana dos SI na empresa.
	Administrador da Bases de Dados	1	Responsvel pela administrao e manuteno das bases de dados da empresa. Deve ter o conhecimento do funcionamento de todos os departamentos a nvel de acesso e manipulao da informao.
	Especialista de Segurana da Informao	2	Garantem a segurana dos sistemas e dos dados da empresa.
	Tcnico de Suporte dos Sistemas de Informao	2	Fornecem suporte tcnico aos funcionrios em relao ao uso de tecnologias de informao. Estes devem estar prontos a agir assim que uma falha ou avaria relacionada com os sistemas de informao ocorra.

Departamento de Negcios	Gerente do Departamento de Negcios	1	Gere e supervisiona todas as atividades relacionadas s vendas e compras da empresa na empresa. Est encarregue do bom funcionamento do seu departamento.
	Coordenador de Compras	1	Responsvel por conduzir as atividades de compra, como a pesquisa e o relacionamento de fornecedores, a negociao de contratos e o acompanhamento de prazos de entrega. Estes tambm fornecem suporte quando necessrios aos executivos de compras.
	Coordenador de Vendas	1	Lidera a equipa de vendas desenvolvendo estratgias de venda, identificando oportunidades no mercado e garantindo a satisfao do cliente. Estes tambm fornecem suporte quando necessrios aos executivos de vendas.
	Executivos de Compras	2	Realizam o processo de compra, pesquisam por fornecedores, avaliam propostas e tomam decises de compra.
	Executivos de Vendas	2	Realizam atividades de venda, procurar por clientes fornecendo informaes sobre os produtos da Dev4Sell e negociar contratos.
	Analista de Mercado	1	Faz a recolha de informao sobre os consumidores, empresas concorrentes, tendncia, oportunidades de negcio entre outras informaes relevantes do mercado.
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 bom funcionamento do seu departamento.

	Especialistas em Marketing	5	Responsveis por desenvolver e implementar estratgias de marketing para promover os produtos e a empresa.
	Designer Grfico	1	Cria materiais grficos e visuais para campanhas de marketing de forma a promover a Dev4Sell e os seus produtos.
Departamento de Finanas	Gerente do Departamento de Finanas	1	Gere as atividades financeiras da empresa, incluindo fazer o controlo de custos e oramentos, realizar o planeamento financeiro e fazer a gesto de contas a pagar e a receber. Este supervisiona e garante o bom funcionamento do seu departamento.
	Especialistas de Anlise Financeira	1	Responsvel pela anlise e interpretao de dados financeiros da empresa, elaborao de relatrios e suporte na tomada de decises financeiras.
	Tesoureiro	1	Responsvel por gerir as atividades de tesouraria, incluindo o controlo de fluxo de transaes financeiras.
Departamento de Logstica	Gerente do Departamento de Logstica	1	Supervisiona e gere todas as atividades relacionadas com as atividades logsticas da Dev4Sell, tendo assim um papel crucial na organizao de recursos e produtos da empresa.
	Tcnico de Logstica e Abastecimento	1	Desempenha o papel de gerir de forma eficiente o fluxo de materiais e recursos da empresa, fazendo o devido planeamento de aquisio de materiais e a gesto de fornecedores da Dev4Sell.
	Analista de Stock de Recursos e Produtos	2	Responsveis por realizar a monitorizao, anlise, gesto de todo o stock de produtos existentes na empresa, bem como todo o stock de recursos a serem utilizados como os recursos de backup.

	Equipa de Transporte	10	Responsveis por assegurar 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 bom funcionamento do seu departamento.
	Gestores de Projetos	4	So responsveis pela coordenao e execuo dos projetos relacionados ao desenvolvimento e produo de equipamentos eletrnicos. So pilares cruciais para a comunicao e gesto de recursos necessrios em cada projeto.
	Designers Industriais	3	Criam conceitos de design, desenvolver desenhos tcnicos e modelos 3D dos produtos a serem desenvolvidos e produzidos.
	Engenheiros de Desenvolvimento de Hardware	15	Responsveis pela produo de componentes eletrnicos a nvel fsico.
	Engenheiros de Desenvolvimento de Software	30	Responsveis pela produo de componentes eletrnicos a nvel lgico. Estes produzem o software necessrio para o funcionamento dos equipamentos e produzem as aplicaes para o consumo de dados presentes nas bases de dados por parte dos funcionrios da Dev4Sell.
	Especialistas em Quality Assurance	5	Garantir a fiabilidade e durabilidade dos componentes eletrnicos produzidos na Dev4Sell.
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 bom funcionamento do seu departamento.
	Especialistas de Atendimento ao Cliente	10	Responsvel por fornecer suporte e assistncia aos clientes da empresa.

	Especialistas em Retenção de Clientes	2	Têm a responsabilidade de garantir a satisfação contínua dos clientes e minimizar a perda dos clientes existentes.
--	---------------------------------------	---	--

Processos de Negcio

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

PN01 – Parcerias comerciais com os fornecedores

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

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

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

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

PN02 – Parcerias comerciais com os clientes

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

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

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

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

Anlise da proposta: Aps receber a proposta, o departamento de vendas realiza uma anlise detalhada, avaliando o potencial sucesso dessa parceria. Durante essa anlise, eles podem desenvolver estratgias e contrapropostas que beneficiem ambas as partes, visando maximizar os resultados e o valor da parceria.

No caso de ser enviada uma contraproposta ao cliente, este tem a possibilidade solicitar a renegociao at se chegar a uma concluso satisfatria para ambas as partes. Aps chegarem a um acordo, ser agendada uma nova reunio para finalizar o contrato ou o pedido sem fidelizao.

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

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

PN03-Gesto de Stock

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

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

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

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

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

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

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

PN04 – Venda

O processo de venda no funcionaria sem os processos de negcio anteriores e destina-se  entrega dos pedidos feitos pelo cliente e encontra-se dividido nos seguintes subprocessos

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

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

Anlise dos produtos desenvolvidos: O departamento de Controlo de Qualidade submete os equipamentos desenvolvidos a testes de funcionalidade, desempenho e qualidade e consoante o resultado, ocorre a aprovao ou reprovao.

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

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

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

Método de Avaliação de Risco

O método de avaliação de risco é utilizado para fazer a identificação, análise e avaliação dos riscos presentes nos seus 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, neste caso na versão OCTAVE Allegro.

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 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 OCTAVE 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

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

Numa fase inicial ser referido o funcionamento do sistema de administrao empresarial da Dev4Sell, que tem como objetivo fazer a anlise e gesto dos vrios recursos ou mesmo processos de negcios 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 e o sistema de armazenamento de dados e como  que estes funcionaro de forma que seja possvel manter uma comunicao fluda e eficaz entre diferentes cargos e setores da empresa, algo que tem um peso enorme no correto funcionamento de uma empresa e no sucesso dos procedimentos dos processos de negcio e tambm apresenta um papel muito importante no que toca  segurana e preservao dos dados relacionados com a empresa, produtos e clientes.

Por fim, ser analisado neste captulo os sistemas mais aplicacionais e que contm a lgica de armazenamento correto dos dados e a 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 fazer o apoio direto ao trabalhador de forma que este consiga finalizar com sucesso o seu papel num processo de negcio.

Sistema de Administrao da Empresa

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

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

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

Sistema de 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 eletrónicos que serão colocados para venda ou mesmo para a reposição e preparação de stock para futuras vendas.

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

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

Sistema de Aplicações

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

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

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

Foram 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 funcionalidade de realizar o auxílio de uma entrega, registando assim o processo da entrega.

Aplicações de suporte ao funcionário (Computador)

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

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

Para a maior parte dos funcionários, esta é a única forma de eles terem uma interação e visualização com a 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 suporte técnico, que está encarregue de fazer a entrega de produtos, estando assim incluídas as funcionalidades de:

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

Recursos

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

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

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

Fsicos

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

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

Humanos

Tabela 4 - Recursos Humanos da Dev4Sell

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

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

Dados

Tabela 5 - Recursos de Dados da Dev4Sell

Nome	Descrição	Fonte dos dados	Nível de Acesso	Responsável pelos dados
Base de dados de produtos	Base de dados que contém a informação acerca do armazém de produtos desenvolvidos, bem como o stock disponível.	Produtos desenvolvidos pela Dev4Sell, armazéns de armazenamento de equipamentos.	Médio	Gerente do Departamento de Logística
Base de dados de clientes	Base de dados que contém as informações dos clientes da empresa.	Entidades que entrem em contacto com a empresa que estejam interessadas na compra de um produto, interações com a empresa.	Alto	Gerente do Departamento de Apoio ao Cliente
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	Gerente do Departamento de Vendas
Base de dados de testes de versões	Regista resultados testes executados após a submissão de versões novas de cada aplicação.	Versão testada, quantidade de utilizadores, quantidade de requests executados, quantidade de requests com resposta OK, tempo de execução.	Médio	Gerente do Departamento de Desenvolvimento e Produção

Suporte de Dados

Tabela 6 - Recursos de Suporte de Dados da Dev4Sell

Nome	Descrio
Servidores de deployment de aplicaes	Recursos de capacidade de armazenamento de alto desempenho e confiabilidade responsveis por fornecer um local centralizado para armazenar e gerir os dados da empresa.
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 fazer o armazenamento de documentos como relatrios, contratos, faturas, etc.
Servidor de backup de base de dados	Recurso que serve de salvaguarda do servidor de base de dados. Este  utilizado para realizar cpias de segurana dos dados crticos da empresa.
Armazenamento de backup em disco	Servidor responsvel por armazenar o backup de todos os discos utilizados pelas mquinas da empresa, de modo a manter em registo as aes realizadas pelos funcionrios

Aplicaes

Tabela 7 - Recursos de Aplicaes da Dev4Sell

Nome	Descrio
Ambientes de desenvolvimento (IDE)	Recurso de suporte a desenvolvedores e outros trabalhadores da empresa que fornece um conjunto de ferramentas para facilitar o desenvolvimento de software e hardware (produtos).
Aplicao do Sistema de Gesto de Stock	Aplicao de controlo e gesto de stock presente nos armazns da empresa.
Aplicao do Sistema de Gesto de Vendas e Entregas	Aplicao que auxilia a Dev4Shell no processo de gesto de vendas, desde o registo do pedido at  entrega do produto ao cliente.

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

Trata-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 crticos

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

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

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

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

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

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

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

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

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

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

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

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

Ameaas e vulnerabilidades

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

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

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

Servidores de bases de dados	Físico	Interno	Intencional	Interrupo	Médio
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruio	Alto
				Interrupo	Médio
Servidor de backup de base de dados	Físico	Interno	Intencional	Interrupo	Baixo
				Perda/Destruio	Alto
			Acidental	Perda/Destruio	Alto
	Rede/Sistema	Externo	Intencional	Perda/Destruio	Alto
				Interrupo	Médio
Armazenamento de backup em discos	Físico	Interno	Intencional	Divulgao	Baixo
				Modificao	Alto
				Perda/Destruio	Médio
			Acidental	Perda/Destruio	Médio
Aplicao do Sistema de Gesto de Recursos Humanos	Físico	Interno	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Médio
	Rede/Sistema	Externo	Intencional	Divulgao	Alto
				Modificao	Alto
				Perda/Destruio	Médio

Aplicao do Sistema 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 Sistema 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
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 da Dev4Sell, quaisquer que sejam as propriedades das ameaas, so de calibre mdio/alto, sendo assim, ter de ser feita a avaliao de cada risco possvel, de forma a perceber quais os riscos que necessitaro de maior prioridade.

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

- Recurso crtico: recurso que pode sofrer a ameaa em causa
- Acesso: forma como o atacante acede ao recurso, este pode ter como valores:
 - Fsico

- 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 no tem uma forma de ser detalhadamente atribuído um valor numericamente correto, ser feita uma atribuio de pontos (0-10), para que seja possível fazer um sistema hierrquico das ameaas analisadas em cada recurso.

Segue-se ento abaixo 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	
Base de dados de produtos	Impacto	N/A	7
	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 entregas	Impacto	N/A	8
	Gravidade	N/A	7
	Probabilidade	N/A	1
	Mdia	N/A	5,3
	Mdia Final	5.3	
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	
Servidores de bases de dados	Impacto	9	9
	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

	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

	Mdia Final	3.8
--	--------------------	------------

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

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

De forma a estabelecer um sistema de pontuao justa, consideramos tanto as ameaas provenientes de elementos internos quanto externos. Em casos em que apenas um dos tipos de ameaas est presente, atribumos o valor "N/A" ao risco que no envolve o ator ausente, e assumimos integralmente o valor do risco relacionado ao ator que causa a agresso. Por exemplo, no caso das mquinas, em que no h ameaa externa, assumimos completamente o valor do risco interno.

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

Para os casos em que apresentam agresses com ambos os atores,  feita a mdia das mdias obtidas por ambos os valores risco (interno e externo).

Com os valores obtidos j  possvel ver hierarquicamente quais os riscos que  preciso ter mais em ateno para o plano de mitigao tendo sido esta a ordem obtida:

- Base de dados de clientes: 6.7
- Servidor de armazenamento em nuvem para documentos: 6
- Aplicao do Sistema de Gesto Financeira: 6
- Servidores de bases de dados: 5.8
- Aplicao de Sistema de Apoio ao Cliente: 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 do Sistema 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 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 subcapítulo 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 a todos os funcionários exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informação, aos Engenheiros de Software que irão trabalhar na Aplicação de Apoio ao Cliente e Entregas e ao Gerente do Departamento de Atendimento ao Cliente, excluindo assim uma grande quantidade de possíveis atores a ataques à mesma, bem como esta deve estar disponível 24 horas por dia, tentando apresentar o máximo de disponibilização às aplicações de suporte aos funcionários da Dev4Sell, pois consomem constantemente os dados armazenados.

De forma a poder manter registo de ações efetuada à base de dados, devem ser mantidos registos de todos os acessos efetuados 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 estar explicado no Plano de Recuperao.

Atividades de Mitigao: Servidor de armazenamento em nuvem de documentos (Transferir)

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

De forma que o servidor de armazenamento em nuvem de documentos fique mais seguro, deve-se encriptar todo o tipo de documento que  armazenado nesta cloud. Com isto, mesmo que a cloud seja atacado, o atacante perder muito tempo ou poder at mesmo no conseguir descriptar a informao roubada.

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

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

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

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

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

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

Os servidores de base de dados devero ter acesso restrito a todos os funcionrios exceto aos recursos humanos pertencentes ao Departamento de Sistemas de Informao, CEO e Diretor da Dev4Sell e dever estar funcional 24 horas por dia, tendo em conta que sem os servidores, nenhuma base de dados estar funcional para ser consumida pelas aplicaes utilizadas na empresa.

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

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

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

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

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

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

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

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

Atividades de 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, conseqüentemente, a empresa não consegue gerar vendas.

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

Assim que um desenvolvedor de hardware for contratado, deve ser agendado um treino de sensibilização à segurança na utilização das máquinas de fabricação de componentes 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 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 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 às aplicações de suporte aos funcionários da Dev4Sell, pois consomem constantemente os dados armazenados.

De forma a poder manter registo de aes efetuada  base de dados, devem ser mantidos registos de todos os acessos efetuados  mesma, bem como as operaes (queries) que foram executadas, isto permitir que em caso de uma agresso tenha sido efetuada, estes logs mostraro quem teve acesso  base de dados, quando, onde e como.

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

Atividades de Mitigao: Servidores de deployment de aplicaes

Os servidores de deployment de aplicaes devero ter acesso restrito a todos os funcionrios exceto ao Gerente do Departamento dos Sistemas de Informao, Tcnicos de Suporte de TI e ao Gerente do Departamento de Desenvolvimento e Produo e dever estar funcional 24 horas por dia, tendo em conta que estes so a base para o funcionamento de todas as aplicaes nos computadores e telemveis de cada funcionrio.

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

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

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

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

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

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

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

Atividades de Mitigao: 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 assim uma grande quantidade de possveis atores a ataques  mesma, bem como deve estar disponvel 24 horas por dia, tentando apresentar o mximo de disponibilizao aos sistemas de informao, pois estes consomem constantemente os dados armazenados.

De forma a poder manter registo de aes efetuada  base de dados, devem ser mantidos registos de todos os acessos efetuados  mesma, bem como as operaes (queries) que foram executadas, isto permitir que em caso de uma agresso tenha sido efetuada, estes logs mostraro quem teve acesso  base de dados, quando, onde e como.

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

Riscos aceites

Tal como j foi mencionado, os riscos que apresentaram uma avaliao inferior ao valor de 5 sero aceites pela empresa, no entrando assim para o plano de mitigao, segue-se abaixo a lista de recursos que no se qualificaram para o mesmo:

- 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, estes 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 salvaguardar informao no caso de haver uma agresso nos recursos crticos. Tem como objetivos principais delinear os detalhes do sistema de backups implementado permitindo a recuperao de informao em caso de falha, corrupo, alterao ou destruio de um recurso da Dev4Sell.

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

Backup

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 entregas	- Contm o armazenamento de dados relativos s entregas da empresa	- Servidor de backup - Disco Rgido	Diariamente	- So feitas snapshots da base de dados de 2 em 2 horas

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

Guia de Reposio dos Dados

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

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

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	- Tentar obter informaes sobre eventos que ocorreram antes da falha
	2	- Isolar o problema e tentar restaurar o servidor	2.1	- Isolar o servidor afetado do ambiente de produo para evitar danos adicionais
			2.2	- Restaurar o servidor usando o backup mais recente do sistema
	3	- Testar as aplicaes restauradas	3.1	- Aps a restaurao efetuar testes nas aplicaes (funcionalidades)
			3.2	- Monitorizar os “logs” das aplicaes para verificar se h erros posteriores ao backup

	4	- Implementar medidas preventivas (após efetuado o restauro)	4.1	- Assim que o servidor for restaurado, rever as medidas de segurança
--	---	---	-----	--

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  utilizado da mesma forma para todos os recursos que sejam base de dados.*

***Este procedimento  utilizado da mesma forma para todos os recursos que sejam aplicaes.*

Plano de Contigncia

O plano de reposio 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 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, certificar que as instalações e outros recursos físicos se encontram nas condições necessárias para a eficácia e segurança do trabalho 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, fazer um conjunto de questões a funcionários escolhidos de forma aleatória em relação a medidas de segurança na empresa, entre outros.

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

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

Simulacros

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

Como já foi referido anteriormente no documento, serão feitos workshops, palestras e formações de sensibilização à segurança no trabalho para os funcionários da Dev4Sell, porém também serão realizados simulacros de treino, no qual todos os funcionários serão avisados 1 dia antes da ocorrência do mesmo. Estes simulacros de treino serão acompanhados pelos recursos humanos pertencentes ao Departamento de Recursos Humanos e ao Departamento de Sistemas de Informação, que irão fazer a orientação aos funcionários dos passos a serem executados de forma que os procedimentos de segurança sejam eficazes, isto também poderá revelar certas vulnerabilidades no plano de segurança e devem ser feitos pelo menos três vezes por semestre anual.

Os simulacros surpresa serão realizados uma vez por semestre anual e devidamente planeados tendo em conta os riscos mais prováveis de acontecer à empresa, apenas o CEO, Diretor e Gerentes dos Departamentos de Recursos Humanos e Sistemas de Informação serão notificados desta simulação, os restantes membros da empresa não saberão das datas agendadas para a realização dos simulacros e não terão o auxílio de outros funcionários da mesma forma que tiveram nos treinos.

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

Importante também anotar que os agendamentos destes eventos devem ser devidamente planeados entre o CEO, Diretor e Gerentes dos Departamentos de Recursos Humanos e Sistemas de Informação e não devem prejudicar o negócio da empresa, focando-se a realizarem-se em épocas de vendas mais baixas e com menos quantidade de produção.

Biografia

<Biografia>