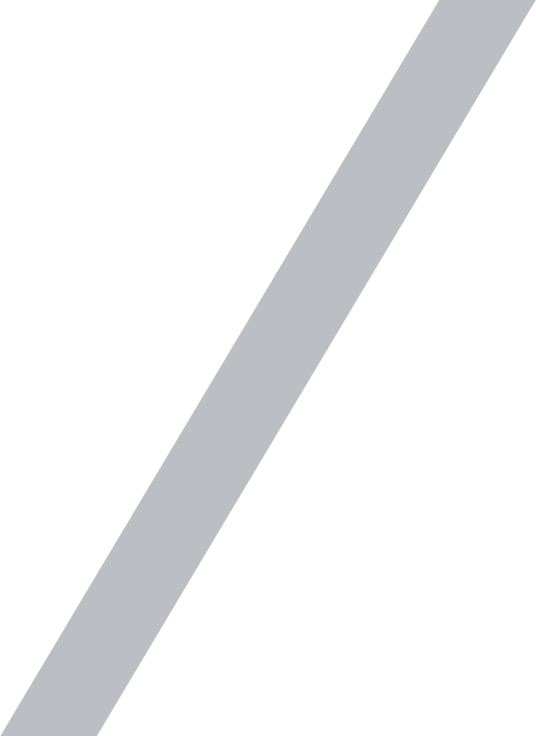
|  |
| --- |
| BUSINESS  CONTINUITY PLAN |

|  |
| --- |
| ASIST 2018/2019  30 de Novembro 2018,  Grupo X41. |

|  |  |
| --- | --- |
|  |  |



Norberto Sousa, 1120608

Marco Carneiro, 1160777

Hugo Fernandes, 1161155

Hugo Carvalho, 1161569

Índice

Introdução2

Empresa3

Apresentação da empresa3

Estrutura de negócio3

O programa da empresa4

Infraestrutura física da empresa5

Infraestrutura informática da empresa6

Soluções9

Solução Para a Estrutura Informática da Empresa9

Solução Com Orçamento9

Solução Sem Orçamento15

*Business Continuity Plan*18

*Threat and Risk Analysis*18

*Business Impact Analysis*19

*Disaster Recovery Plan*20

Prevenção de Falhas21

*Recovery Point Objective*22

*Recovery Time Objective*22

*Recovery Time Objective* de Contigência23

Conclusão23

Bibliografia24

|  |
| --- |
| INTRODUÇÃO |

INTRODUÇÃO

Este relatório tem como objetivo dar a conhecer o *Business Continuity Plan* (BCP) desenhado para responder às necessidades da empresa, que para todos os efeitos, permanecerá anônima neste relatório.

Numa primeira parte é dado a conhecer o ramo industrial onde esta entidade opera, bem como a sua infraestrutura atual.

Posteriormente é apresentado duas possíveis soluções para responder às necessidades da empresa ao nível de infraestrutura informática em que uma delas representa a solução ideal e a outra tem os custos que a empresa poderia suportar em conta. Neste momento também é apresentado o investimento que seria necessário para concretizar estas duas infraestruturas e por que razão se escolheu determinados equipamentos e porque se desenvolveu a infraestrutura dessa maneira.

Por fim e com base na nova infraestrutura, que tem em conta os custos da empresa, é apresentado o novo Plano de Continuidade de Negócio que visa oficializar diversas normas, estratégias e planos de ação que a empresa deve seguir para preservar o seu bom funcionamento e evitar possíveis prejuízos face a situações adversas.

|  |
| --- |
| EMPRESA |

APRESENTAÇÃO DA EMPRESA

A empresa opera na área da *corseterie*, focando-se na confeção e comercialização de *lingerie*, pijamas e roupa interior feminina e masculina. Na fase de prosperidade da empresa, esta contava com 400 funcionários e colaboradores. Com a chegada da crise financeira a Portugal, foi necessário um corte nas despesas, causando a redução do pessoal de 400 para 100. Atualmente a empresa recuperou da crise e exporta produtos para lojas locais, grandes superfícies como o *El Corte Inglés* e para o estrangeiro como Inglaterra e Estados Unidos da América.

ESTRUTURA DE NEGÓCIO

A estrutura de negócio da companhia está dividida pelos seguintes setores de operação:

* *Design*, onde acontece todo o processo criativo para a elaboração das coleções a serem comercializadas pela empresa.
* Corte, onde é efetuado o corte automatizado do tecido, usando como molde os modelos das peças a confecionar.
* Armazém de Matérias Primas, onde se armazena e contabiliza todos os recursos ao dispor da empresa para confecionar produtos.
* Confeção, em que se faz a ligação dos diferentes componentes produzidos pelo corte para criar as peças, ou seja, o produto final.
* Armazém de Produto Acabado, onde se armazenam todos os produtos com recurso a um software, para que mais tarde este seja transferido ou para a loja da fábrica ou para os seus diversos clientes
* Comercial, em que se decide como divulgar a marca e estabelece a ponte entre a empresa e os atuais ou potenciais clientes.
* Contabilidade, onde é feita todo o controlo financeiro da empresa seja de lucros de vendas a gastos com materiais, salários e equipamentos.
* Loja, onde é feita a venda das peças produzidas pela empresa.

O PROGRAMA DA EMPRESA

Para o bom funcionamento da empresa esta depende de um programa escrito em Clipper que é um compilador de 16 bits da linguagem xBase inicialmente desenvolvido para o ambiente DOS e que, de forma rápida, foi abandonado devido ao crescente uso de redes computacionais e aparecimento de discos partilhados com recurso a SGBD (Sistema de Gerenciamento de Banco de Dados), uma vez que

|  |
| --- |
| EMPRESA |

o Clipper foi desenhado para uma época em que cada sistema era isolado do outro e em que as bases de dados eram conjuntos de arquivos em disco acessíveis por apenas um utilizador.

O programa contempla as seguintes funcionalidades:

* Criação da ficha técnica de uma peça, contemplando informações como o material usado, o tamanho da peça, custo e tempo necessário para confecionar a mesma.
* Criação de ordens de produção que especificam o que deve ser confecionado pelos operários do setor do corte e confeção da empresa.
* Registo de produto no *stock*, onde se dá por terminada a ordem de produção e regista-se os produtos no inventário do armazém de produto acabado como pertencentes a uma encomenda.
* Etiquetagem dos produtos e verificação de encomendas em que após etiquetar um produto este é atribuído a uma divisória numerada de uma estante, como por exemplo a estante B gaveta 38, e é feita uma verificação do conteúdo da encomenda estar de acordo com os produtos registados nessa gaveta.
* Criação de rotinas de contabilidade para serem analisadas e posteriormente registadas no software SAGE.
* Registo de marcação de ponto para depois determinar eventuais faltas dos funcionários.

|  |
| --- |
| EMPRESA |

INFRAESTRUTURA FÍSICA DA EMPRESA

A empresa está dividida em dois pisos como representam as seguintes plantas, que também ilustram onde se situam cada um dos setores chave da empresa:

A screenshot of a cell phone

Description automatically generated

Figura 1 - Planta 1º Piso

A screenshot of a cell phone

Description automatically generated

Figura 2 - Planta 2º Piso

|  |
| --- |
| EMPRESA |

INFRAESTRUTURA INFORMÁTICA DA EMPRESA

A empresa atualmente encontra-se com um sistema muito desatualizado e heterogéneo comtemplando o seguinte inventário:

* 14 computadores com sistema operativo Windows 98 para permitir o uso do programa da empresa
* 9 computadores com o sistema operativo Windows XP para uso de software não compatível com o Windows 98 como o Lectra, programa de modelagem usado pelo setor do design e corte.
* 2 computadores com o sistema operativo Windows 7, em que um é o computador responsável pelo uso do software SAGE e o outro é o computador pessoal do diretor geral da empresa
* 2 computadores com o sistema operativo Windows 10, em que é o computador pessoal da responsável pela contabilidade e o outro o computador pessoal do chefe da empresa
* 5 s*witches*
* 2 *routers* em que um deles é o do ISP (*Internet Service Provider*)
* 1 *firewall* destinada á proteção do tráfego telefónico da empresa
* 1 sistema de segurança instalado e mantido por terceiros.
* 2 APs (*Access* *Points*)
* 1 dispositivo de redireccionamento de chamadas telefónicas instalado e mantido por terceiros.
* 3 computadores com que funcionam como servidores da empresa. Um servidor que delega pedidos ao modulo de produção e de contabilidade (designados respetivamente servidores F e G). Estes servidores para além de conterem toda a informação gerada pelo programa da empresa também é onde se situa o servidor de emails da empresa.
* 1 dispositivo que funciona como NAS, permitindo á empresa cópias diárias do sistema de ficheiros para serem guardados como *backups*.
* 12 telefones espalhados por toda a fábrica.
* 1 impressora

|  |
| --- |
| EMPRESA |

As figuras seguintes apresentam a disposição destes equipamentos na empresa de uma perspetiva física e lógica.

A close up of a map

Description automatically generated

Figura 3 - Vista Lógica da Rede

|  |
| --- |
| EMPRESA |
|  |

A screenshot of a cell phone

Description automatically generated

Figura 4 - Distribuição Física 1º Piso

A screenshot of a cell phone

Description automatically generated

Figura 5 - Distribuição Física 2º Piso

|  |
| --- |
| SOLUÇÕES |

SOLUÇÃO PARA A INFRAESTRUTURA INFORMÁTICA DA EMPRESA

Após discussão com a empresa, decidiu-se apresentar duas alternativas para resolver o problema proposto. Uma destas soluções tem em conta a capacidade da empresa em investir numa solução, em que esta não pode superar os 5000 euros, e a outra representa a solução ideal para garantir a continuidade de negócio. Ambas as soluções apresentam o esquema lógico da nova infraestrutura e o orçamento necessário para essa alternativa.

É de salientar que neste momento está a ser desenvolvida uma aplicação web que visa substituir o atual programa da empresa, não sendo necessário a preocupação com a compatibilidade do Clipper.

SOLUÇÃO COM ORÇAMENTO

A close up of a map

Description automatically generated

Figura 6 - Vista Lógica Solução Com Orçamento

|  |
| --- |
| SOLUÇÕES |

A screenshot of a cell phone

Description automatically generated

Figura 7 - Vista Física da Rede º1 Piso 1

A screenshot of a cell phone

Description automatically generated

Figura 8 - Vista Física da Rede º1 Piso 2

|  |
| --- |
| SOLUÇÕES |

A screenshot of a cell phone

Description automatically generated

Figura 9 - Armário de Dispositivos do 1º PisoA screenshot of a cell phone

Description automatically generated

Figura 10 - Vista Física da Rede º2 Piso 1

|  |
| --- |
| SOLUÇÕES |

A screenshot of a cell phone

Description automatically generated

Figura 11 - Vista Física da Rede º2 Piso 2

A close up of a computer

Description automatically generated

Figura 12 - Armário de Dispositivos 2º Piso

Nesta solução definiu-se como prioridade a atualização dos computadores da empresa de todos os equipamentos com sistema operativo Windows 98 para Windows XP já que este permite o uso da nova aplicação.

Uma vez que o Windows XP permite a utilização da mesma licença em múltiplos dispositivos e a empresa já possui uma licença, não existe a necessidade de comprar novas licenças.

A infraestrutura terá apenas um servidor no qual estarão todos os serviços da empresa, sejam estes o servidor de base de dados da aplicação, a própria aplicação e o servidor de *email*. Este servidor terá 4 entradas para colocar os respetivos disco rígidos, de modo a poder operar em *raid* 1 (duplicação total do disco para outro idêntico de maneira a que se um falhar o outro pode manter a funcionalidade do sistema). Este servidor terá uma UPS (*Uninterrupted Power Supply*) ligada que terá como principal objetivo permitir uma janela de aproximadamente 30 minutos para encerrar o dispositivo de forma correta em caso de falta de energia.

Quanto á estrutura de rede foi decidido adquirir equipamentos Cisco *refurbished* (equipamentos usados por outras empresas que foram descartados e delegados a terceiros para reparação e venda dos mesmos), uma vez que têm o preço mais em conta e não existe a necessidade de adquirir as licenças para os mesmos externamente. Para além dos *switchs* e do *router*, é necessária uma Cisco ASA (*Adaptative Security Appliance*) com FirePower (sistema Cisco capaz de filtrar, monitorizar, e prevenir ataques informáticos de forma muito mais complexa).

|  |
| --- |
| SOLUÇÕES |

A razão por se escolher equipamentos Cisco é devido á fácil configuração, segurança e administração do equipamento, com características como uma CLI (*command-line interface*) capaz de auto completar os comandos e apresentar ajuda e descrição de cada comando possível. Ao nível da separação lógica dos diferentes departamentos foi efetuada a divisão da rede com recurso a vlans, usando os 3560 para *intervlan routing* com o protocolo HSRP. Para garantir a segurança dos dispositivos de rede, o servidor terá também um sistema AAA com recurso ao protocolo RADIUS que usa protocolo UDP para comunicação e é pouco exigente em termos de recursos face a outras alternativas.

|  |
| --- |
| SOLUÇÕES |

O inventário e orçamento proposto é o seguinte:

* 3 *switchs* Cisco *catalyst* 2960 de 24 portas (3 \* 150,65€)
* 3 *multilayer* *switchs* Cisco *catalyst* 3560 de 24 portas (3 \* 198,37€)
* 1 *router* Cisco *catalyst* 2911 (1 \* 417,89€)
* 1 *firewall* Cisco ASA 5506-X (1 \* 409,99€)
* 1 servidor HP ProLiant DL360 (2 \* 189,97€)
* 4 disco rígidos Dell 1 *terabyte* (4 \* 270,00€)
* 1 UPS APC Smart-UPS (1 \* 368,53€)
* 2 Access Points Ubiquiti UAP-AC-LR (2 \* 82,85€)
* 2 cabos RJ45 de 305m (2 \* 158,52€)
* 1 chave Windows server 2016 (1 \* 710,99€)

|  |
| --- |
|  |

Como maior parte do processamento da rede vai ocorrer nos 3560 e 2960, optou-se por comprar um equipamento extra de cada para uma eventual avaria de um dos equipamentos ativos. Como o servidor é o dispositivo mais critico para o bom funcionamento da empresa, efetuou-se a compra de um segundo servidor para caso o outro tenha uma avaria.

Com este inventário, o total a pagar pela empresa seria 4 897,14€.

|  |
| --- |
| SOLUÇÕES |

SOLUÇÃO SEM ORÇAMENTO

A close up of a map

Description automatically generated

Figura 13 - Vista Lógica da Solução Sem Orçamento

|  |
| --- |
| SOLUÇÕES |

A screenshot of a video game

Description automatically generated

Figura 14 - Armário de Dispositivos do 1º Piso

A close up of a machine

Description automatically generated

Figura 15 - Armário de Dispositivos do 2º Piso

|  |
| --- |
| SOLUÇÕES |

Uma vez que a solução anterior apresentava uma estrutura operacional adequada às necessidades da empresa, as únicas alterações necessárias seriam a passagem de todos os computadores não para o Windows XP, mas para o Windows 7, a compra de equipamentos ainda não usados, a separação de serviços oferecidos pelo servidor em outros servidores distintos de maneira a reduzir o risco de falha e melhoramentos de segurança

O inventário e orçamento proposto é o seguinte:

* 3 *switchs* Cisco catalyst 2960 de 24 portas (3 \* 673,51€)
* 3 *multilayer* switchs Cisco catalyst 3560 de 24 portas (3 \* 1359,30€)
* 1 *router* Cisco catalyst 2911 (1 \* 1687,67€)
* 1 *firewall* Cisco ASA 5506-X (1 \* 420,72€)
* 5 servidores HP ProLiant DL360 (5 \* 2856,06€)
* 16 disco rígidos Dell 1 *terabyte* (16 \* 270,00€)
* 4 UPS APC Smart-UPS (4 \* 368,53€)
* 2 Access Points Ubiquiti UAP-AC-LR (2 \* 82,85€)
* 2 cabos RJ45 de 305m (2 \* 158,52€)
* 4 chaves Windows server 2016 (4 \* 710,99€)
* 22 chaves Windows 7 (preços variáveis, mas indo pela média de 22 \* 58,00€)

Nesta proposta o custo é muito mais elevado, sendo este 32883,94€. É adquirido um *switch* 2960 e 3560 extra por uma questão de prevenção no caso de uma possível avaria. Pelo mesmo motivo, também é adquirido um servidor extra. A proposta não contempla o custo da nova ligação 4G para providenciar redundância á que já existe, que é uma ligação de fibra ótica, usando a nova ligação para emergências. Para o servidor AAA, em vez do protocolo RADIUS, optou-se pelo protocolo TACACS+ da Cisco, que apesar de ser mais exigente ao nível de recursos, providência certas melhorias em comparação com o RADIUS como a encriptação de toda a informação partilhada entre o servidor AAA e o dispositivo, a separação dos processos AAA e o uso de TCP como protocolo de comunicação.

|  |
| --- |
| BCP |

*Business Continuity Plan* (BCP)

De maneira a assegurar o bom funcionamento da empresa, é necessário estabelecer o BCP da mesma, que é constituído por múltiplos elementos que permitem apurar o que realmente é necessário ter em conta para que este plano seja viável. Deve-se salientar que este plano se aplica á situação da empresa com a nova infraestrutura, sendo necessária revisões deste documento com regularidade, propondo-se aqui uma avaliação anual deste plano ou sempre que for feita uma alteração drástica á infraestrutura da empresa, como a criação de um novo setor.

*Threat and Risk Analysis* (TRA)

Na análise de ameaças e riscos (TRA) foi apurado os seguintes incidentes capazes de causar transtornos ao bom funcionamento da empresa:

* Ataque cibernético – Uma vez que a infraestrutura informática não é um sistema isolado do mundo exterior, é necessário assegurar a confidencialidade, a integridade e autorização de acesso aos dados da empresa.
* Inundação – A infraestrutura física da empresa é suscetível a infiltrações quando o nível de precipitação é muito elevado, o que pode dar origem a diversos problemas como curto circuitos e possivelmente, avaria de equipamentos devido a humidade.
* Ameaça interna – Uma vez que a empresa passou por um grande processo de restruturação devido á crise que se instalou em Portugal, não se pode descartar qualquer intenção maliciosa por parte dos funcionários da empresa. O impacto deste incidente é baixo.
* Incêndio – A empresa opera com muitas máquinas, sendo previsível ter em conta este incidente. O impacto deste incidente é alto.
* Falha de energia – O sistema energético da empresa é fundamental para o seu bom funcionamento, uma vez que todos os equipamentos não conseguem operar sem energia.
* Falha do sistema – Qualquer falha de equipamentos, sejam eles informáticos ou de costura, são críticas e devem ser resolvidas o quanto antes.
* Invasão de propriedade – Apenas pessoal autorizado deve aceder aos ativos da empresa e qualquer outro individuo deve ser considerado como um intruso. Este incidente parte do princípio de que o invasor não é um funcionário da empresa.

*Business Impact Analysis* (BIA)

|  |
| --- |
| BCP |

Com base na análise de ameaças e riscos feita anteriormente é possível apurar efetuar a *Business* *Impact* *Analysis* (BIA) e para cada risco referido anteriormente foi definido o seguinte:

* Ataque cibernético – O impacto deste incidente é alto, uma vez que o autor do ataque pode adulterar a informação da empresa que no melhor dos cenários apenas causa perda de tempo, mas no pior pode comprometer toda a estrutura de informação, dados de encomendas e valores de vendas. O atacante também pode usar a informação roubada para fornecer dados á concorrência da empresa ou até chantagear funcionários da mesma através das informações recolhidas.
* Inundação – A avaria dos equipamentos por humidade força na maioria dos casos á substituição completa do equipamento, o que constitui um prejuízo muito elevado. O tempo que se demoraria a restaurar os sistemas na totalidade também seria outra consequência gravosa deste incidente. Como tal, o impacto deste incidente é alto.
* Ameaça interna –O impacto deste incidente é baixo. Os funcionários da empresa poderão por motivos diversos tentar sabotar os equipamentos da empresa ou até arranjar informação com que possam chantagear outros funcionários da empresa.
* Incêndio – Um dos incidentes mais prejudiciais para a empresa, uma vez que pode custar toda a infraestrutura da empresa e vidas. O impacto deste incidente é alto.
* Falha de energia – A falha de energia pode causar a paragem completa da empresa uma vez que esta está completamente pendente do funcionamento da rede informática, dos equipamentos de corte e das máquinas de costura. O impacto deste incidente varia consoante o tempo, mas se o tempo for superior a 24 horas, o seu impacto é alto.
* Falha do sistema – Qualquer falha de equipamentos, sejam eles informáticos ou de costura, são críticas e devem ser resolvidas o quanto antes pois podem representar perdas significativas de vendas e produção para a empresa, como por exemplo a varia das máquinas de corte ou falha do servidor de base de dados. O impacto deste incidente é alto.
* Invasão de propriedade – Qualquer acesso de pessoal não autorizado á infraestrutura física da empresa constitui um risco, pois o invasor pode roubar, adulterar informação ou danificar os ativos da empresa. O impacto deste incidente é médio.

*Disaster Recovery Plan* (DRP)

Para cada incidente foram determinadas possíveis ações para minimizar o impacto:

|  |
| --- |
| BCP |

* Ataque cibernético - Tentar perceber se a informação foi adulterada ou apenas copiada. No caso de a primeira tentar perceber, com recurso a backups da base de dados, em que momento a informação foi adulterada e repor os dados originais e na segunda situação, perceber que dados foram copiados e que impacto poderá ter essa cópia. Também será necessário saber como é que o atacante entrou no sistema e resolver o quanto antes essa vulnerabilidade. Por último, recorrer às autoridades e tentar perceber quem foi o responsável pelo ataque, para tentar prevenir futuros ataques por parte dessa entidade.
* Inundação - No caso de uma inundação, imediatamente desligar todos os equipamentos para evitar curto circuitos, e proteger quaisquer dados que sejam crucias e que possam ser afetados pela água, sejam documentos impressos, ou os disco rígidos do servidor. Deve-se também contactar imediatamente os bombeiros.
* Ameaça interna - Imediatamente identificar os responsáveis e ativar todos os mecanismos jurídicos necessários. Questionar o responsável sobre a forma como executou o seu plano e perceber se a pessoa tinha autorização para usar os meios que utilizou e no caso negativo, verificar como proteger esses meios para prevenir futuros incidentes.
* Incêndio - Imediatamente alertar os bombeiros. Evacuar o pessoal do edifício pelas devidas saídas para esta situação e se possível remover e evacuar os discos rígidos do servidor para evitar a perda dos dados críticos da empresa.
* Falha de energia - Após a falha, o técnico informático da empresa tem aproximadamente 20 minutos para desligar o servidor de forma segura, de maneira a evitar perda ou corrupção de dados. Acionar todos os mecanismos necessários para restaurar a energia o mais depressa possível e delegar tarefas em que não seja necessária energia a todos os funcionários de maneira a tentar mitigar os custos da perda de tempo dos funcionários.
* Falha do sistema – Imediatamente contactar o técnico informático ou mecânico para resolver o problema o quanto antes.
* Invasão de propriedade – Solicitar á companhia de segurança os dados necessários para tentar identificar a altura da invasão e o responsável para que se possa alertar as autoridades.

Prevenção de falhas

Para prevenir falhas humanas deve-se realizar um estudo sobre quais são as responsabilidades que cada funcionário deve ter para que se possa dar formação de maneira a mitigar futuros erros e aplicar o princípio de responsabilidade mínima, ou seja, cada funcionário apenas tem acesso ao que

|  |
| --- |
| BCP |

necessita para executar as suas funções dentro da empresa, retirando o acesso a qualquer outro sistema que não seja necessário.

Para prevenir falhas de *hardware* e *software*, fora os equipamentos extra que deveriam de ser obtidos para garantir rápida recuperação do sistema em caso de avaria de equipamentos, deve-se efetuar duplicação total dos discos do servidor com recurso ao mecanismo raid 1, fazer *backups* das configurações dos equipamentos de rede e analise semanal do estado de cada dispositivo para se apurar eventuais quebras de performance e *malwares* no sistema. Esta análise deve ser efetuada depois das 18:00 que é quando a empresa regista menor uso dos serviços.

Para alem da analise semanal, deve-se instalar um sistema de monitorização que permita não só a captura de erros em toda infraestrutura informática, mas também analise de tráfego de rede para se poder verificar se a *firewall* está a usar politicas adequadas para impedir a circulação de trafego malicioso dentro da empresa e se os registos de acesso aos equipamentos apresentam irregularidades com recurso aos registos AAA. Para monitorização de tráfego e alertas da *firewall*, o uso de uma máquina com o sistema operativo Linux Security Onion e software capaz de interpretar alertas gerados pelo syslog e pelos protocolos SNMPv3 e netflow seria o mais indicado. O netflow foi inicialmente introduzido pela Cisco e permite monitorizar tráfego IP á saída e entrada de uma interface e o syslog permite a captura de todas as mensagens geradas pelo equipamento. O *Simple* *Network* *Management* *Protocol* (SNMP) é um protocolo standard da internet e permite capturar e organizar informação dos dispositivos IP, bem como manipular certas variáveis do sistema do mesmo como a velocidade da ventoinha. É proposto o uso de SNMPv3 uma vez que este suporta a autenticação e encriptação dos dados fornecidos quer pelo dispositivo, quer pela entidade de gestão.

Uma vez que a empresa necessita dos dados durante um período médio de 5 anos antes de os poder descartar, o ideal é investir em discos de maior capacidade para evitar a perda de performance do servidor.

Quanto a eventuais catástrofes como incêndios, deve ser elaborado um plano de desastres, de maneira a salvaguardar toda a informação critica da empresa para um sistema remoto. Uma *cloud* poderia ser a solução mais indicada.

*Recovery Point Objective* (RPO)

|  |
| --- |
| BCP |

O RPO permite definir durante quanto tempo é tolerável a perda de informação sem que esta tenha um impacto negativo na continuidade do negócio da empresa. Para os elementos da empresa foi definido:

* Servidor de email – 2 horas.
* Servidor de base de dados – 1 hora.
* Aplicação da empresa – 1 hora.
* *Firewall* – 2 horas.
* Serviço de marcação de faltas dos funcionários – 12 horas.
* *Software* Lectra – 4 horas.
* *Software* SAGE – 1 hora.
* Equipamentos de rede com exceção da *firewall* – 4 horas.
* Gravações do sistema de segurança – 6 horas.

*Recovery Time Objective* (RTO)

O RTO permite definir qual o tempo máximo para o qual se pode restaurar um serviço sem que este prejudique em demasia a continuidade de negócio da empresa.

Para a maioria dos serviços informáticos, com exceção do serviço de marcação de faltas e sistema de segurança, foi estabelecido com a empresa que qualquer tempo de recuperação superior ao tempo de um turno de um funcionário na empresa é inaceitável para a continuidade do negócio. Os turnos têm duração de 4 horas.

O tempo que se definiu para o restauro do servidor e serviços associados (aplicação da empresa, *emails* e base de dados) é de 4 horas. Também se definiu para a internet, Lectra e SAGE este tempo de recuperação.

Para o sistema de segurança definiu-se um tempo de recuperação de 5 horas, que é o equivalente a metade do tempo em que a fábrica fica fechada sem qualquer funcionário por dia.

Para a *firewall* e qualquer outro equipamento de rede definiu-se um tempo de recuperação equivalente a 4 horas.

Para o serviço de marcação de faltas foi definido um tempo de recuperação de 1 dia.

|  |
| --- |
| BCP CONCLUSÃO |

*Recovery Time Objective* (RTO) de Contigência

Uma vez que existem discrepâncias entre RTO e RPO para determinados ativos da empresa, como por exemplo a aplicação da empresa é necessário criar meios alternativos para executar as tarefas enquanto os serviços estão em baixo.

Na eventualidade do servidor que contem os serviços de base de dados, a aplicação da empresa e o servidor de *email*, deve-se recorrer a registos físicos previamente criados com o inventário do armazém de matérias primas, tamanhos e cores das peças para criar as ordens de produção e posteriormente as encomendas. Uma vez restaurado o sistema deve-se transpor os dados criados para o programa de maneira a manter a coerência dos dados. Este procedimento também se aplica para o *software* SAGE.

No caso do *software* Lectra deve-se efetuar a produção de todas as peças cujos moldes já estejam desenvolvidos de maneira a recuperar parte do tempo perdido.

Para terminar, no caso de não funcionamento das máquinas de costura ou corte, deve-se efetuar a confeção de todas as peças possíveis através de costura tradicional, ou seja, agulha e linha.

Conclusão

Com base na infraestrutura existente, foi possível traçar um esboço inicial que depois levou às duas possíveis soluções que aqui apresentamos. Uma delas tem em conta a capacidade de investimento da empresa e foi nessa que se baseou o BCP apresentado. O BCP apresentado está suficiente para manter a continuidade de negócio, mas pode e deve ser melhorado com o passar do tempo de aplicação deste documento na empresa para que fosse possível verificar a sua funcionalidade. Se fosse possível um investimento futuro poderia ser ponderado uma solução virtualizada de toda a infraestrutura da empresa em *cloud* de maneria a mitigar os riscos físicos que se poderiam suceder na infraestrutura informática da empresa e uma duplicação de toda a infraestrutura física dos equipamentos de corte e costura para uma outra fábrica.

Bibliografia:

1. <https://tinyurl.com/y9flmq8m> Custos de dispositivos *refurbished*, UPS’s.
2. <https://tinyurl.com/y8coefxz> Custos de dispositivos *refurbished*, HP ProLiant Servers.
3. <https://tinyurl.com/y7yt53sz> Custos de dispositivos *refurbished,* ASA*.*
4. <https://tinyurl.com/ybvpj3jf> Custos de dispositivos *refurbished*, Cisco 2911 router.
5. <https://tinyurl.com/ybvhkgm6> Custos de dispositivos *refurbished*, DELL 1TB SAS 6G.
6. <https://www.ubnt.com/unifi/unifi-ap-ac-lr/> Access Points Ubiquiti.
7. <https://www.senetic.pt/> Catálogo de produtos *factory new*.
8. <https://www.lectra.com/pt-br/sobre-lectra> Informação sobre o programa Lectra.
9. <https://tinyurl.com/y7jq6zd2> Informação sobre a linguagem Clipper.

|  |
| --- |
| BIBLIOGRAFIA |