Universidade Autónoma de Lisboa

Engenharia Informática

Análise de Sistemas

Plano de Recuperação de Desastres e Continuidade de Negócio

Docente: Isabel Alvarez

31 de maio de 2023

Índice

Introdução

No sentido de se aplicar e desenvolver os conceitos adquiridos ao longo do semestre em relação à unidade curricular de **"Análise de Sistemas ",** foi-nos proposto a elaboração de um projeto.

Relativamente a este, como objetivo principal, foi necessário procedermos à **implementação de um plano de recuperação de desastres e continuidade de negócio**.

Desenvolvemos a uma breve descrição de uma empresa que trabalha no setor informático. Em relação a esta, será abordado, o tipo de negócio, os tipos de clientes e produtos comercializados, a dimensão da empresa e também os departamentos existentes.

O escopo da descrição da empresa abrange também uma apresentação detalhada **dos equipamentos e softwares disponíveis**. O departamento de **Tecnologia da Informação e Comunicação (TIC)** e o departamento de **Departamento de Gestão de Aplicações, Desenvolvimento e Apoio a Utilizadores (DGADAU)** têm como principais objetivos, assumir o papel gestor desses recursos, abrangendo áreas como a administração de redes de computadores, a segurança da informação, o desenvolvimento e manutenção de software, o suporte técnico aos utilizadores, a gestão da base de dados e a administração de servidores.

Adicionalmente, o **departamento de TIC** é responsável por garantir o funcionamento e manutenção da infraestrutura de comunicação da empresa, incluindo sistemas de telefonia, videoconferência e internet. Trata-se de uma responsabilidade crucial para a efetividade e competitividade da organização, visto que uma infraestrutura de comunicação eficiente é **fundamental para o sucesso** das operações.

Considerando um plano que incluí todos os riscos de desastres, onde foi necessário identificar as probabilidades de ocorrência, as vulnerabilidade do negócio, *Downtime*, os componentes da equipa de recuperação, que inclui as estruturas, as funções , as responsabilidades de cada elemento, os planos de ensaio, as sequências de ações, o enquadramento organizacional do plano e também as arquiteturas, como *Disaster tolerant* ou outras alternativas consideradas.

Este trabalho foi desenvolvido pelo grupo de alunos do curso de Engenharia Informática, do 2ºano, Pedro Amaral (30008241), Eduardo Araújo (30008290) e João Lucas (30008215).

Descrição da empresa

Este projeto visa desenvolver um caso prático sobre a empresa **Eletroártica**.

A **Eletroártica** é **uma empresa nacional e fictícia**, utilizada em projetos de diversas disciplinas, com forte atuação no ramo da programação. A sua *expertise* é voltada para oferecer soluções terceirizadas a empresas que procuram tipos de serviços relacionados com software. A empresa tem como foco principal fornecer engenheiros de software altamente capacitados e especializados em diversas linguagens de programação, garantindo que os seus clientes possam "contar" com profissionais de qualidade para desenvolver os seus projetos com **eficácia e eficiência**.

A empresa está localizada no centro de Lisboa, próxima da estação de metro "Saldanha".

Relativamente aos departamentos existentes, a nossa empresa conta com um diretor geral, sendo este responsável pelos departamentos. Já os departamentos estão divididos em diversas áreas: administrativa, financeira, recursos humanos, logística, informática e marketing.

O departamento administrativo é responsável por apoiar e aconselhar o diretor geral em situações diárias da empresa, incluindo a supervisão do trabalho desenvolvido nos outros departamentos.

Já **o departamento financeiro** é responsável pela gestão da área financeira, garantindo que os lucros, despesas e dívidas se encontram sob controlo.

Sobre o **departamento de recursos humanos,** é responsável pela gestão do pessoal da empresa, incluindo a contratação e gestão de conflitos.

O **departamento logístico** tem como responsabilidade fundamental, a gestão de material, como expediente, permitindo que todos os funcionários dos respetivos departamentos possam desenvolver o seu trabalho.

O departamento de IT é considerado um dos mais importantes para a estrutura da **Eletroática**, pois é responsável por desenvolver

ferramentas de software e por fornecer apoio técnico aos clientes e funcionários, conforme referido na introdução.

Sobre **o departamento de marketing,** é responsável por criar estratégias para promover a companhia em si, bem como os seus serviços.

Cada departamento é liderado por um "**responsável de departamento"**, selecionado de acordo com as suas competências profissionais, currículo e forma de trabalhar. Além de este assumir a responsabilidade de gerir a sua respetiva área, deve também aconselhar o diretor geral, no sentido de **propor ideias inovadoras** de métodos de trabalho.

Tecnologias de Informação e Comunicação (TIC)

O departamento de informática, contêm um subdepartamento, denominado de **Departamento de Sistemas de Informação (DSI),** que tem como principal objetivo apoiar os clientes no uso corrente das **TIC**.

Além disso, é de seu encargo **planear, implementar, configurar e gerir a rede interna de computadores** e os seus respetivos sistemas de comunicação, envolvidos na sua interligação com redes externas à organização. Além da gestão de sistemas informáticos, é da sua responsabilidade detetar e corrigir falhas nos sistemas, assegurando a **operacionalidade** dos mesmos.

De modo, a área de Sistemas de Informação tem como principais objetivos:

- **Implementar, assegurar e gerir as infraestruturas** de suporte (rede, comunicações, parque informático, software e hardware), assegurando o seu correto funcionamento;
- Implementar os mecanismos necessários de **segurança** do sistema informático, garantindo a privacidade e a integridade, quer dos vários componentes que formam os sistemas informáticos e de comunicações, quer da informação constante nos ficheiros centralizados ou que circulem na rede de ligações telemáticas;
- Todo o armazenamento será realizado **na nuvem, com servidores de base de dados, aplicacionais e de backup**, considerando que as medidas de redundância implementadas visam garantir **a segurança e sustentabilidade** dos dados da empresa;
- Os computadores fornecidos a cada funcionário irão conter apenas as especificações/acessos necessários;
- Sobre a gestão de software, utilizarão o **GitHub** como forma de **armazenamento**.

Outro dos subsetores do departamento de informática é o **Departamento de Gestão de Aplicações, Desenvolvimento e Apoio a Utilizadores (DGADAU)** e tem como principais objetivos:

- Promover, assegurar e desenvolver projetos, acompanhando a evolução das tecnologias de informação e avaliando o seu impacto na organização;
- Assegurar a manutenção e boa utilização das aplicações informáticas institucionais e apoiar os **clientes "físicos" e remotos no desenvolvimento de aplicações;**
- Coordenar a integração de meios entre os serviços;
- Gerir os sistemas operativos e aplicações comuns;
- Colaborar com os vários departamentos, particularmente com o de recursos humanos, no levantamento das **necessidades de formação no domínio das TIC**;
- Em articulação com o departamento de Gestão de Recursos Financeiros, **procurar adquirir bens e serviços no domínio das TIC** e colaborar na elaboração de **cadernos de encargos** e acompanhamento da **execução de contratos**;
- Apoiar os funcionários e clientes na exploração das várias aplicações e ferramentas disponibilizadas pela empresa.

Plano de recuperação e Continuidade de negócio

Um dos principais motivos para a existência deste plano é a possibilidade de, em qualquer altura, poderem ocorrer **catástrofes**, levando a **falhas ou mau funcionamento nas infraestruturas** das instalações de apoio aos sistemas operacionais especificados no plano de negócio.

- **Riscos de desastre – Identificação das probabilidades de ocorrência:**

➢ **Terramoto**

A empresa fica situada na região da grande Lisboa, em Portugal. Uma região com um elevado risco de catástrofe natural. Em caso de terramoto, é possível que exista o comprometimento de toda a estrutura de instalações da empresa. Gerando assim um bloqueio completo das atividades de negócio. Um terramoto de grande magnitude poderá causar o **desabamento do edifício**, aonde está situada a empresa, levando a grandes perdas para a empresa. Além das perdas materiais e financeiras, poderá existir a maior perda de todas, a **própria vidas das pessoas.**

➢ **Raios**

Outro tipo de desastre que poderá existir nesta região é a **queda de raios,** que pode causar a interrupção do fornecimento elétrico. Causando o desligamento dos equipamentos utilizados pela empresa e gerando uma quebra das atividades de negócio (causando um enorme prejuízo).

- **Ciberataque**

Hoje em dia, todas as empresas de TI utilizam a internet como suporte às suas ferramentas de trabalho. Considerando esse facto, **os ciberataques em grande escala** são uma possibilidade. Levando à perda de dados, podendo estes ser confidenciais. Além disso, poderá existir o **bloqueio parcial ou completo dos sistemas** utilizados pela empresa.

- **Incêndio**

No edifício onde a Eletroártica está localizada, poderá ocorrer **um incêndio**, seja de que tipo for. Neste caso, o edifício deverá dispor de sistemas **de deteção e combate ao incêndio**. Apesar disso, este tipo de incidente poderá levar à perda ou dano de equipamentos e sistemas de informação importantes, além de poder causar perigo às pessoas que frequentam a empresa.

- **Inundações**

Na região de Lisboa, durante a época das grandes chuvas, existe a forte possibilidade **de ocorrerem inundações**, tal como aconteceu em 2022. Estas inundações podem "chegar" à empresa e causar **grandes perdas em relação a hardware e sistemas de informação**, levando à interrupção das atividades de negócio.

- **<u>Vulnerabilidades do negócio</u>**

Empresas que operam através da internet, mantendo as suas bases de dados na *cloud*, estão sujeitas a diversas vulnerabilidades, principalmente em relação à **segurança dos dados**. As informações armazenadas na "nuvem" podem ser acedidas por utilizadores não autorizados, considerando os riscos de ataques cibernéticos, como **invasões e roubo de informações.** Além disso, **problemas técnicos** na infraestrutura da nuvem, como interrupções de serviço, podem **causar perdas de dados e prejuízos financeiros significativos**.

Além dos riscos já referidos, existem outros aspetos importantes a considerar, que podem comprometer a vulnerabilidade da empresa. Entre estes, podemos mencionar os **desastres naturais**, conforme referido no subcapítulo anterior, que podem causar danos físicos às instalações e aos equipamentos. O próprio software utilizado pela empresa pode **apresentar falhas e erros de compilação (bugs)**. A "sabotagem" é ainda uma das situações a considerar, tendo em conta o elevado nível de **concorrência** presente nos dias atuais. Apresentamos de seguida uma tabela com os diferentes **tipos de catástrofe**, bem como a **sua probabilidade de ocorrência e possível alcance da perda.**

Tipo de Catástrofe	Probabilidade	Alcance da Perda
Destruição de património	30%	$5K - $200K
Desastres naturais	40%	$5K - $200K
Softwares	65%	$50K - $300K
Ataques Cibernéticos	90%	$100K - $500K
Falta de Internet	40%	$5K - $200K

Eletroártica – Imagem dos Potenciais Prejuízos

- **Downtime / Aplicações críticas**

Dos serviços operacionais utilizados, identificamos como sendo os mais críticos: o sistema de *CRM Dynamics 365*, o serviço *.NET* e o *SQL*, em Azure. O sistema ***Microsoft Azure*** assegura um "uptime" de **99.99%,** que se traduz num "downtime" total máximo de 5 minutos por mês. O que na maioria dos casos é considerado pouco tempo, enquanto os sistemas **estão em atualização**.

Entre os hardwares utilizados pela empresa, predominam os **dispositivos móveis e os computadores**. A empresa mantem um stock de peças, de forma a garantir a segurança e a continuidade dos serviços em caso de **imprevisibilidade**. Quando há necessidade, esses itens são instalados. As peças que não estão em stock e são necessárias, são encomendadas, em coordenação com o departamento financeiro.

- **Equipa de recuperação – Estrutura, funções e liderança - Responsabilidades**

Uma equipa de recuperação é um grupo **multidisciplinar de profissionais capacitados,** que prestam assistência técnica e operacional à empresa em caso de ocorrência de eventos naturais adversos, como inundações, terramotos, entre outros, que possam afetar os sistemas de informação e equipamentos. Além disso, esta é responsável por **criar, manter e implementar** o **plano de recuperação de desastres**, que contém instruções detalhadas sobre a forma como responder a este tipo de imprevistos, minimizando os **efeitos negativos** e retomando as operações principais no tempo mais breve possível. Esta equipa pode ser formada por profissionais da própria empresa ou externos (**contratos com outras empresas**).

O diretor geral da empresa é o responsável **"máximo"** por decidir como será feito o processo de escolha da equipa de recuperação. Para o auxiliar neste processo, o departamento administrativo terá um forte impacto.
O diretor geral e o departamento administrativo deverão estar sempre em coordenação com todos os departamentos, para que

todos saibam como devem agir em cada caso de catástrofe. Prestando todo o suporte e esclarecimento necessário à equipa de recuperação.

Já a equipa de intervenção é o grupo de profissionais que recebe preparação específica para atuar em situações de catástrofes naturais ou provocadas pelo homem. Esta tem como objetivo prestar socorro às vítimas, minimizar os danos e restabelecer os requisitos mínimos de funcionamento da empresa no período mais breve possível, devendo esta estar preparada para enfrentar todos os diferentes tipos de cenários.

Por fim, a equipa de *Compliance* é um grupo de profissionais que se dedica principalmente às **questões legais** e às **questões políticas internas e externas**. Esta equipa tem como função garantir que a empresa esteja em conformidade legal, em relação aos regulamentos, códigos de conduta e boas práticas no mercado. Além disso, deverá procurar desenvolver e aprimorar os princípios éticos da organização, orientando, capacitando e monitorando os colaboradores sobre as normas e procedimentos que devem ser seguidos, procurando identificar e mitigar os riscos de não conformidade, aplicando sanções legais e administrativas, caso seja necessário.

- **Plano de ensaios**

  Este plano deve estabelecer **os procedimentos a observar por todos os ocupantes do edifício**, relativos à articulação das operações destinadas a garantir uma evacuação da forma mais ordenada possível, de todas as pessoas presentes no edifício. Este plano também costuma ser conhecido como **"Plano de Acidentes em Terra" (PAT).** Importa referir que o **Plano de Ensaios define** que deverão ser feitos **simulacros em relação** aos diversos tipos de catástrofes.

- **<u>Fases de Emergência</u>**

➢ **Emergência Parcial**

- Este tipo de emergência ocorre quando se verifica uma **emergência num local restrito**, que possa ser controlada, sem afetar as unidades contíguas. Neste caso, a situação pode ser controlada utilizando os meios materiais e humanos;
- Uma emergência parcial verifica-se quando:
  - Ocorra um acidente que possa ser dominado com os **meios materiais e humanos,** a nível interno;
  - Obrigue à evacuação parcial das instalações.

➢ **Emergência Total**

- A emergência total verifica-se quando a situação pode **ultrapassar os limites da instalação**;
- Esta situação verifica-se sempre que:
  - Exista um risco potencial de incêndio com proporções imprevisíveis;
  - Ocorra um acidente grave que ponha em risco pessoas e bens;
  - Obrigue à evacuação total das instalações e/ou ponha em risco os meios urbanos vizinhos;
  - Sejam necessários meios de auxílio exteriores;
  - Obrigue à paragem total das instalações.

- **Fases do Plano de Evacuação**

Conforme já referido em parte no "**Plano de Ensaios**", é imprescindível proceder à identificação das saídas de emergência, definição dos caminhos de evacuação, programação da evacuação, identificação dos pontos críticos, seleção dos pontos de reunião e elaboração das plantas de emergência.

➢ Identificação de saídas de emergência

Devem ser identificadas todas as **saídas de emergência,** bem como o trajeto de cada uma, a partir do ponto de vista do visualizador da planta. Cada uma deve ter um corrimão da parte de dentro desta. As saídas normais, cuja utilização faz parte do funcionamento regular do edifício, também poderão ser utilizadas como saídas de evacuação.

Eletroártica – Saída de Emergência – Fonte: Teclusa.pt

➢ Definição dos caminhos de evacuação

Visa encaminhar, de maneira rápida e segura, os ocupantes para o exterior ou para uma zona isenta de perigo, e de preferência para o ponto de reunião. Este mesmo ponto deverá estar sinalizado na planta de emergência. Deve, por isso, ser definido um itinerário normal (percurso a utilizar prioritariamente) e um itinerário alternativo (percurso a utilizar quando o itinerário normal se encontra impraticável).

Eletroártica – Exemplo de Sinalização de Emergência – Fonte: SandraBruno.Blogspot.com

➢ Programação da evacuação

A evacuação deve ser programada, ou seja, deve ser definida a ordem de saída, de acordo com o local de ocorrência do sinistro e a proximidade das saídas. Deve ser definido um **"Chefe de Fila" e um "Cerra Fila"** e deverá ser feita a contagem de todos os elementos da fila, no início e no fim da evacuação.

➢ Identificação dos pontos críticos

Consideram-se **pontos críticos** os locais de cruzamentos de vias e escadas. É da responsabilidade do "Chefe de fila" **identificar e avisar** os restantes elementos sobre a aproximação dos pontos críticos, de modo a evitar a criação de situações de pânico.

- **Seleção dos pontos de reunião**

Também designados de **pontos de encontro**, devem ser locais amplos e seguros. Devem estar situados no exterior do edifício, mas em proximidade com o mesmo, a uma certa distância de segurança, onde devem convergir e permanecer todas as pessoas que se encontravam no local, no momento do desastre. **Deve existir apenas um ponto de encontro**. Estes “pontos de encontro” devem ser definidos quando é desenvolvido o plano de evacuação.

- **Elaboração das plantas de emergência**

Com base nas plantas de arquitetura do espaço, elaboram-se **as plantas de emergência**, por piso, onde constam os caminhos de evacuação, localização de saídas, conforme já mencionado, ponto de reunião, meios e recursos existentes e ainda outras informações consideradas convenientes. Deverão ser afixadas em pontos estratégicos, de modo a que sejam de **fácil visualização.**

- **<u>Simulações</u>**

- **Simulação de incêndio**

Pessoas com **deficiências físicas, crianças e pessoas mais velhas** deverão ser prioritárias em relação à evacuação. Deverão existir plantas de emergência, pelo menos em cada corredor da área de trabalho da empresa. Com o local aonde se encontra o visualizador da planta, localização dos extintores, localização das bocas de incêndio, casos existam, e localização dos telefones. Deverá existir **sinalização adequada** a indicar a saída de emergência, setas a indicar para onde cada pessoa se deve dirigir e fichas de risco em cada sala. Todos os elementos do edifício deverão dirigir-se para o ponto de reunião de forma organizada, com a existem de um Chefe de Fila e um Cerra Fila. Deverão ser feitos simulacros deste tipo de simulação de forma inopinada.

- **Simulação de falha de energia**

A interrupção pode ser causada **por falha de fornecimento de energia na rede pública.** Esta situação provoca a paragem de todos os **sistemas e equipamentos** que dependem de alimentação de energia elétrica, excetuando aqueles que dispõem de **dispositivos de acumulação de energia de reserva limitada**, que os permite manter o funcionamento e ainda alimentar outros.

Para os “objetos” de evacuação, como sinalização de evacuação, sinalização de saídas de emergência, equipamentos e dispositivos de combate a incêndio, entre outros, a falta de energia não será um problema, considerando que estes objetos possuem luzes de emergência contidos, ou são criados de forma a que sejam visualizados em espaços com pouca ou nenhuma luz. Em relação aos equipamentos informáticos de trabalho, a empresa conta com geradores de energia para **manter o funcionamento dos equipamentos essenciais.** Ao ser verificado que existiu falhas no

fornecimento de energia, é imediatamente acionado o **"grupo X",** que irá ativar o **"gerador X",** até ao regresso da energia exterior. Caso seja verificada a falha do "grupo X", por falha ao ligar o "gerador X", será acionado o **"grupo Y",** para que assim seja ativado o **"gerador Y",** trabalhando por isso em formato de redundância.

- **Simulação de ciberataque**

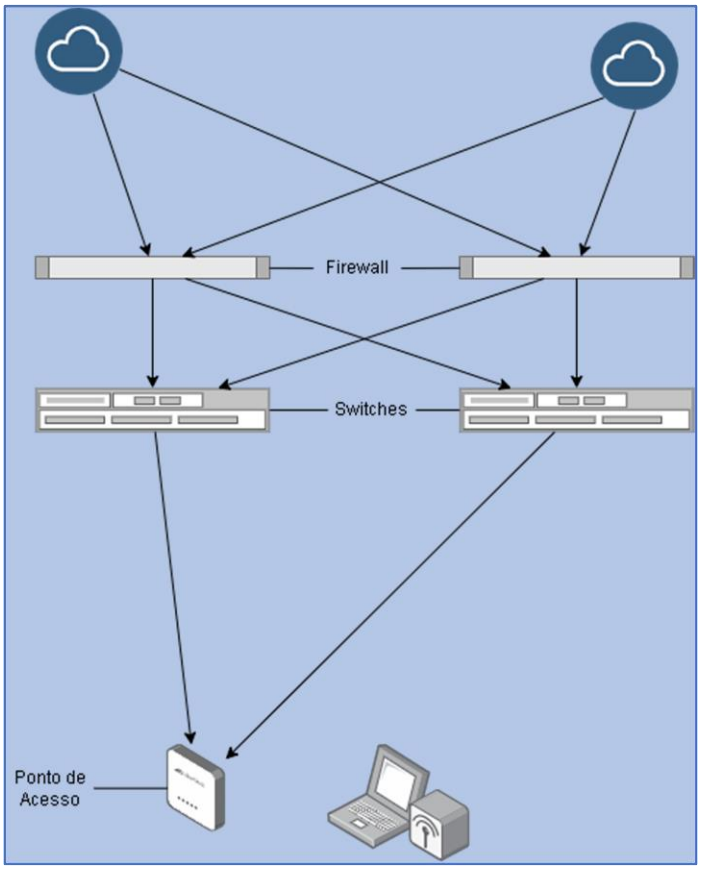
As empresas de testes de intrusão (pentests) são especializadas em simular ataques aos sistemas de empresas, com o objetivo de **detetar e corrigir vulnerabilidades** de segurança. Estas usam ferramentas automatizadas e processos manuais para explorar o sistema em busca de brechas, adotando o papel de um **"intruso".** Assim, estas podem ajudar as empresas a proteger melhor os seus dados. As empresas de testes de intrusão seguem algumas fases para realizar o seu trabalho, desde da recolha de informação sobre o alvo, identificação de vulnerabilidades deste, tentativas de exploração das vulnerabilidades detetadas, relatórios dos trabalhos efetuados com as medidas corretivas e acompanhamento na resolução das vulnerabilidades. As empresas também podem estabelecer acordos contratuais com empresas de **desenvolvimento de Anti-Malware**, de modo a serem analisadas com regularidade. Ainda assim, em caso de perda de dados importantes, a Eletroártica deverá **recorrer à cloud**.

Eletroártica – Fonte: Jivochat.com.br

- **Simulação de falha da conexão à internet**

  - **Arquiteturas *disaster tolerant* e alternativas**

De forma a ser garantida uma estável e segura conexão com a internet, decidimos considerar dois provedores de internet diferentes, de modo que, se um destes falhar**, possamos recorrer ao outro sem interrupções**. Esta redundância também se aplica às firewalls e aos switches que estão conectados ao ponto de acesso, permitindo a conexão dos dispositivos à rede.



Eletroártica – Disaster Tolerant

- **Simulação de catástrofes naturais**

As emergências provocadas por fenómenos naturais, tais como **terramotos, inundações e sismos**, devem-se seguir as seguintes recomendações:

- As primeiras medidas a tomar podem depender do horário em que ocorram os eventos (durante o horário útil ou fora dele);
- No caso de o incidente ocorrer durante o **horário de trabalho,** devem ser ativadas imediatamente três equipas: a equipa de Intervenção, a equipa de Informática e a equipa de Recursos Humanos (RH):
  - A equipa de intervenção tem como principal objetivo evacuar todos os colaboradores das instalações de forma segura e solicitar o apoio das autoridades competentes, **como os bombeiros ou a polícia**, se necessário;
  - A equipa de TI tem como responsabilidade, desde que **não se exponham a riscos**, de desligar todos os equipamentos de comunicação e eletricidade;
  - A equipa de RH tem como função informar todos os presentes sobre a situação e quando tudo estiver controlado, comunicar aos seus familiares, **caso seja necessário.**
  - No caso de o incidente ocorrer fora do horário útil, devem ser ativadas imediatamente as mesmas três equipas;
  - Estas receberão o aviso sobre a situação através do telemóvel, a partir do **diretor geral ou departamento administrativo**, mas só duas destas serão acionadas de imediato:
    - A equipa de intervenção irá solicitar o apoio das autoridades competentes, como os bombeiros ou a polícia, se necessário;
    - A equipa de RH irá comunicar com os funcionários sobre o ocorrido;
    - Depois de um certo período, a equipa de TI será acionada, para verificar os estragos causados.

Após a realização da inspeção dos danos causados num determinado desastre, constata-se que existem **duas situações distintas:**

- Ocorreu a destruição total das instalações e dos equipamentos;
- Ocorreram apenas perdas parciais.

- **<u>Pós-Desastre</u>**

➢ **Destruição Total**

Ocorrendo a **destruição total das instalações e dos equipamentos**, é necessário providenciar um novo local para retomar as atividades. Para isso, serão mobilizadas cinco equipas: a de Recursos Humanos, a Administrativa, a de "Compliance", a de IT e a de Contabilidade e Finanças:

- Os Recursos Humanos devem informar que todos os trabalhadores deverão trabalhar remotamente, até **a normalização das novas instalações**. Assim que forem estabelecidas as novas instalações, esta equipa também ficará responsável por informar a retoma do **trabalho presencial**;
- A equipa Administrativa **encarrega-se de encontrar e preparar o novo local de trabalho**, verificando as condições de infraestrutura, segurança e comunicação. Esta escolha será feita pelo diretor geral, mas coordenada por esta equipa;
- A equipa de "Compliance" irá tratar **das questões contratuai**s do novo local, bem com as questões dos **seguros;**
- A equipa de IT irá ter como principal prioridade o restabelecimento do sistema, com a utilização **do suporte da cloud**. Desse modo, será recuperado **todo o sistema e informações perdidas**, bem como os **acessos** de cada funcionário. Deverão ser instalados os novos equipamentos de comunicação, como os routers e switches;
- A equipa de Contabilidade e Finanças irá ficar responsável por todo o **processo financeiro em relação às novas instalações da empresa**.

- **Destruição Parcial**

Em virtude do incidente que ocasionou somente **perdas parciais**, será solicitada a intervenção imediata da equipa de IT. Esta deverá verificar quais as partes do sistema que se danificaram.

Durante a inspeção ao incidente, poderá ser constatado que o sistema tem **condições de ser restabelecido com os componentes** existentes. Se for verificado que o sistema poderá ser restabelecido, serão mobilizadas duas equipas:

- A equipa da área de Informática irá realizar os procedimentos necessários para restabelecer o sistema, garantindo a segurança e a integridade dos dados e dos serviços;
- A equipa de Recursos Humanos irá informar todos os colaboradores e o diretor geral sobre a normalização do sistema, esclarecendo as possíveis dúvidas e orientando sobre os procedimentos a serem seguidos. Esta equipa irá ter o apoio do **departamento administrativo**.

No caso de se constatar que o sistema não pode ser recuperado com os componentes existentes, serão acionadas as equipas responsáveis pelas áreas **de RH, Informática e Contabilidade e Finanças:**

- A equipa de IT será responsável por fazer o levantamento de todas as necessidades em relação aos **componentes essenciais para o restabelecimento do sistema;**
- Com base nesse levantamento, a equipa de Contabilidade e Finanças providenciará **a liberação de recursos financeiros necessários** para a aquisição imediata dos componentes;
- Após o restabelecimento do sistema, a equipa de RH **comunicará com todos os colaboradores,** de forma a explicar o sucedido e “enviando-os” **para trabalho remoto**.

Enquadramento organizacional do plano

A empresa é gerida por um **diretor geral**, conforme mencionado ao longo do trabalho. Este desempenha um papel fundamental na **liderança estratégica** e supervisão, em relação a todas as operações, tomando decisões em benefício da **organização como um todo.** Este tem como responsabilidade, **garantir a eficiência operacional, a otimização dos recursos e o alinhamento com os objetivos definidos.** Além disso, cada área funcional da empresa é liderada por um "**Chefe de Departamento"**, que tem a responsabilidade de organizar, liderar e gerir as equipas da sua área. Estes são responsáveis por supervisionar as operações diárias das suas respetivas áreas, garantir o cumprimento dos objetivos estabelecidos e promovendo a **eficiência e a produtividade**. Essa **estrutura de liderança** permite uma divisão simples das responsabilidades de cada elemento, garantindo assim um funcionamento alinhado de todas as operações da empresa.

Eletroártica – Business Leadership –Fonte: Iberdrola.com

Conclusão

Em suma, um plano de recuperação de desastres e continuidade de negócios é um componente essencial para garantir a sobrevivência e resiliência das organizações diante de eventos imprevistos que possam interromper as suas operações. Este projeto explorou os principais elementos necessários para desenvolver um plano eficaz, destacando a importância da identificação e análise de riscos, a implementação de medidas preventivas e a criação de estratégias de resposta e recuperação. Ao longo deste estudo, foi possível compreender que um plano de recuperação de desastres e continuidade de negócios deve ser adaptado às necessidades específicas de cada organização, levando em consideração os seus recursos, processos críticos e infraestrutura tecnológica. A colaboração entre diferentes áreas da empresa, a definição clara de responsabilidades e a comunicação efetiva **são fatores-chave** para o sucesso na implementação e execução do plano. Além disso, destacou-se a importância de testar e atualizar regularmente o plano, garantindo sua relevância contínua e a capacidade de lidar com novos desafios e ameaças emergentes. A **conscientização e o treino** dos funcionários também desempenham um papel fundamental na preparação da organização para lidar com incidentes e minimizar o impacto sobre as operações.

Em última análise, um **plano de recuperação de desastres e continuidade de negócios** é um investimento estratégico que pode proteger uma organização contra perdas financeiras significativas, danos à reputação e interrupções prolongadas. Ao implementar medidas preventivas, estabelecer protocolos de resposta eficientes e promover uma cultura de resiliência, as empresas **estarão mais bem preparadas** para enfrentar desafios inesperados e garantir a continuidade das suas operações, salvaguardando os seus interesses e protegendo os interesses de seus clientes e stakeholders.

Agradecimentos

Gostaríamos de expressar os nossos sinceros agradecimentos à nossa Professora, Isabel Alvarez, pela sua orientação e apoio durante a elaboração deste trabalho sobre “Plano de Recuperação de Desastres e Continuidade de Negócio”. A sua experiência e conhecimento foram fundamentais para o bom entendimento dos conceitos e para a construção de um trabalho **sólido e bem fundamentado.** Gostaríamos também de agradecer aos nossos colegas de turma, pelo apoio na realização deste trabalho.

Webgrafia

- Slides do Documento “Os sistemas de informação na empresa” – UAL – Elearning – Disciplina de Análise de Sistemas;
- Slides do Documento “Sistemas de informação, Organizações e Estratégia” – UAL – Elearning – Disciplina de Análise de Sistemas;
- Slides do Documento “Infraestrutura de TI e Tecnologias Emergentes” – UAL – Elearning – Disciplina de Análise de Sistemas;
- Slides do Documento Disaster Recovery - “Avaliando a necessidade de um plano de continuidade” – UAL – Elearning – Disciplina de Análise de Sistemas;
- Imagem da página 10 – “Eletroártica – Imagem dos Potenciais Prejuízos” – Criada pelo nosso Grupo;
- Imagem da página 14 – “Eletroártica – Saída de Emergência” – Fonte: Teclusa;
- Imagem da página 15 – “Eletroártica – Exemplo de Sinalização de Emergência” – Fonte: SandraBruno.Blogspot.com;
- Imagem da página 18 – “Eletroártica” – Fonte: Jivachat.com.br;
- Imagem da página 18 – “Eletroártica – Disaster Tolerant” - Criada pelo nosso Grupo;
- Imagem da página 23 – “Eletroártica – Business Leadership” – Fonte: Iberdrola.com.