Nome: Yasmin Victória RA: 824210011

Nome: Natasha Melo RA: 82429222

EcoWealth

A *EcoWealth* é uma gestora de ativos focada em investimentos sustentáveis, com o objetivo de promover impacto positivo no meio ambiente e na sociedade. A empresa oferece fundos voltados para setores como energias renováveis, reciclagem e conservação ambiental.

Com a crescente importância da sustentabilidade, a EcoWealth busca alavancar retornos de longo prazo enquanto apoia práticas responsáveis. Operando em um mercado dinâmico, enfrenta desafios como ameaças cibernéticas e mudanças climáticas, tornando crucial a existência de um Plano de Continuidade de Negócios (BCP). Esse plano visa proteger dados, manter a confiança dos investidores e garantir que a empresa esteja preparada para lidar com crises, como falhas em TI e ataques cibernéticos.

Identificação dos Recursos Críticos

1. Infraestrutura de TI:

- Servidores: Sistemas que armazenam dados financeiros e informações dos clientes.

- Soluções de Backup: Mecanismos que asseguram a recuperação de dados em caso de falhas.

2. Equipe de Trabalho:

- Gestores de Investimentos: Profissionais responsáveis pela análise e seleção de ativos sustentáveis.

- Equipe de TI: Especialistas que garantem a segurança dos sistemas e informações.

3. Sistemas e Software:

-Plataformas de Gestão de Ativos: Ferramentas para monitoramento e administração dos investimentos.

- Programas de Segurança Cibernética: Para proteger os dados contra ameaças e ataques.

4. Dados e Documentação:

- Base de Dados de Clientes: Informações sensíveis que devem ser resguardadas.

- Manuais e Protocolos: Documentação que garante a continuidade das operações.

5. Comunicação:

- Canais de Comunicação: Ferramentas para informar investidores e colaboradores em situações de emergência.

- Plataformas de Colaboração: Softwares que permitem a interação da equipe, especialmente em contextos remotos.

6. Recursos Financeiros:

- Capital de Giro: Fundos necessários para manter operações diárias e enfrentar crises financeiras.

Análise de Impacto nos Negócios (BIA)

1. Falha de TI:

- Impacto: Interrupção dos sistemas de gestão de ativos, impossibilidade de acesso a dados financeiros e perda de produtividade da equipe.

2. Ataque Cibernético:

- Impacto: Vazamento de informações sensíveis dos clientes, danos à reputação da empresa e possíveis multas regulatórias.

3. Desastre Natural (ex.: inundações, incêndios)**:

- Impacto: Danos à infraestrutura física, interrupção nas operações e necessidade de realocação da equipe.

4. Problemas Logísticos:

- Impacto: Atrasos nas transações financeiras e dificuldade em manter a comunicação com investidores e parceiros.

5. Mudanças Regulatórias:

- Impacto: Adaptação rápida a novas leis, gerando custos e exigindo atualizações nos processos de investimento.

6. Crises Econômicas:

- Impacto: Redução no volume de investimentos e aumento na inadimplência dos clientes.

Estratégias e recuperação propostas

- Proteção de dados: Estabelecer os imprevistos que podem acontecer para lesionar qualquer tipo de impacto.
- Continuidade operacional: Definir os tipos de área de acordo com a sua categoria operacional, financeira e dados.
- Confiança do cliente: O plano de recuperação de desastres mostra para o cliente, preparo e segurança.
- Conformidade regulatória: o planejamento para recuperação de desastres auxilia a empresa estar de acordo com a proteção de dados de negócios.
- Resposta a emergências: O plano de recuperação de desastres de TI auxilia as equipes na redução dos efeitos sobre as operações da empresa.

O impacto dos desastres de TI

- Perdas financeiras: são os custos relacionados ao tempo de inatividade, à recuperação de dados e à perda de receita.
- Tempo de inatividade operacional: O período de inatividade prejudica os processos e serviços das empresas.

- Danos à reputação: Incidentes de tecnologia da informação podem impactar negativamente a imagem da empresa, resultando na diminuição da confiança dos clientes.
- Falta de conformidade regulatória: Incidentes de TI podem resultar em pesadas multas e implicações legais, caso a empresa não atenda aos critérios de proteção de dados e continuidade operacional. Cumprir com normativas como GDPR, HIPAA e PCI DSS é essencial para prevenir sanções e preservar a confiança de clientes e stakeholders.

Principais componentes de um plano de recuperação de desastres

Avaliação de risco

A fim de compreender os perigos que a empresa enfrenta e determinar quais ações de recuperação devem ser priorizadas, é recomendável realizar uma análise de riscos. Essa análise servirá para identificar ameaças potenciais e fraquezas nos sistemas e na infraestrutura de tecnologia da informação. É importante que a avaliação leve em conta tanto o ambiente físico quanto o data center, possibilitando uma visão abrangente dos possíveis cenários de desastres.

Análise de impacto nos negócios

Uma avaliação do impacto nos negócios (EIN) estabelece a relevância dos sistemas de TI e orienta a priorização das iniciativas de recuperação. Esse processo auxilia a organização a distribuir recursos de forma eficaz, analisando o possível efeito das interrupções nos processos empresariais. A EIN deve reconhecer e classificar os sistemas para a recuperação em situações de desastre.

Plano de continuidade

- Processos alternativos: Consistem em reconhecer e registrar maneiras alternativas de trabalho para garantir a continuidade das funções essenciais.
- Alocação de recursos: Assegura que os recursos necessários, como pessoal e equipamentos, estejam à disposição e possam ser acionados de forma ágil.
- Procedimentos de recuperação: Solicita a especificação das fases necessárias para a recuperação de sistemas de TI e informações.

Backup e recuperação de dados

É fundamental estabelecer processos de backup para assegurar que a empresa realize a cópia de dados importantes de forma consistente e segura. A implementação de backups regulares, tanto no local quanto fora dele, garante a possibilidade de restaurar as informações caso ocorram perdas ou comprometimentos. As abordagens de backup e recuperação de dados, que incluem cópias completas, incrementais e diferenciais, são essenciais para proteger os dados mais valiosos, minimizando o tempo necessário para a recuperação e preservando a integridade das informações.

Plano de comunicação

- Informa os stakeholders sobre a evolução da recuperação.
- Administra as expectativas.
- Preserva a confiança em momentos de crise.

Estratégias para a recuperação de desastres de TI

- Backup e restauração: Realize backups de dados regularmente para que possam ser recuperados quando necessário.
- Recuperação de desastres baseada em nuvem: Utilize soluções em nuvem para alternativas de recuperação que sejam escaláveis e adaptáveis.
- Práticas de DevOps: Incorpore a recuperação de desastres ao fluxo de trabalho do DevOps para tornar o processo de recuperação mais automatizado e eficiente.
- Soluções de alta disponibilidade: Desenvolva sistemas que assegurem a continuidade das operações, mesmo diante de eventuais falhas.
- Resposta a incidentes: Elabore um planejamento claro para a resposta a incidentes, detalhando as fases necessárias para identificar, avaliar, controlar e se reerguer de ocorrências relacionadas à segurança cibernética.
- Redundância: Estabeleça sistemas e componentes redundantes para prevenir pontos críticos de falha.
- Reprodução: copie dados e sistemas, armazenando-os em um local alternativo para facilitar uma recuperação ágil.
- Virtualização: utilize máquinas virtuais para reiniciar os serviços de TI de forma rápida.

Sugestão de teste de plano

Avaliações e atividades de treinamento frequentes confirmam a efetividade do plano de recuperação em situações de desastre e garantem que os colaboradores estejam preparados para tais eventualidades. Exercícios e simulações são essenciais para descobrir deficiências e oportunidades de aprimoramento, garantindo que o plano opere adequadamente em um acontecimento real de desastre.

Use o Jira Service Management para recuperação de desastres de TI

- Compreender as diversas categorias de desastres que podem ocorrer.
- Analisar os riscos envolvidos.
- Colocar em prática estratégias fundamentais, como a realização de backups de dados, a gestão de incidentes e a execução de testes periódicos.
- Empregar ferramentas que ajudam a coordenar ações e a otimizar processos.

REFERÊNCIAS:

- **Recuperação de desastres de TI: estratégias e melhores práticas**
- **Guia completo para Recuperação de Desastres em TI**
- **Software Público — Governo Digital**
- **Análise de Impacto no Negócio (BIA): O que é! Significados e Conceitos**
- **Identificação dos recursos críticos - Documentação da IBM**
- **Guia de PDTIC do SISP - Versão 2.1 — Governo Digital**