Politicas de TI, empresa **Centermedi.**

Politica de TI da empresa: https://www.centermedi.com.br/site/Politica-de-TI.pdf

Analise geral

A empresa possui uma politica muito completa no que se diz a segurança de acesso e controle de dados e informações, com bons métodos para controlar quem acessa e como acessa estes. No entanto não parece haver o mesmo cuidado para caso toda esta segurança falhe e/ou um erro interno seja causado, é necessário uma revisão no que fazer em caso de crise.

Pontos a melhorar

O principal ponto negativo identificado nas políticas de T.I da empresa Centermedi é a falta de uma política especifica sobre **Disaster Recovery.** Em alguns pontos do documento é falado sobre evitar que dados sejam apagados ou da permissão de acesso aos mesmos, porém não há nenhuma documentação especifica que padronize que ações serão tomadas para recuperar dados perdidos/apagados. Como responsável pelo setor de TI este seria o primeiro ponto que revisaria nesta empresa.

Pontos Positivos

- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantindo o bloqueio de acesso rapidamente a usuários que não mais deveriam ter acesso aos dados e informações diminui a possibilidade de vazar estes mesmos. Sendo assim um bom método de **segurança**.

- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

  >os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

  >os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

- Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra. O uso dos dispositivos

e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Com estas políticas a empresa garante que toda ação tomada nos computadores, sistemas ou banco de dados terá uma pessoa física que poderá ser responsabilizada pelo mesmo, diminuindo o anonimato e possibilidade de boicote interno, um bom método de **segurança**.

- Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Método de **utilização aceitável de tecnologia**, controlando os hardwares e softwares utilizados, garantindo confiança e diminuindo a vulnerabilidade de acesso a propriedades da empresa.