GABRIEL ÂNGELO PEREZ GASPARINI SABAUDO
GABRIELA TIEKO HIRASHIMA
GUILHERME HENRIQUE GONÇALVES SILVA
FERNANDO MORGADO PIRES NETO

POLÍTICAS DE SEGURANÇA – BETA MÓVEIS

LONDRINA
2023

DEFINIÇÕES

As políticas de segurança são um conjunto de normas, diretrizes e objetivos que visam proteger os dados, os sistemas, as pessoas e o patrimônio de uma organização contra ameaças internas e externas. Elas podem ser aplicadas a diferentes áreas, como segurança no trabalho, segurança da informação, segurança pública, etc.

A importância das políticas de segurança está relacionada ao propósito de fornecer orientação e apoio às ações de prevenção ou eliminação dos riscos que podem afetar a integridade, a disponibilidade e a confiabilidade das informações e dos recursos da organização. Além disso, as políticas de segurança contribuem para o cumprimento das leis, regulamentos e normas vigentes, bem como para a melhoria contínua da qualidade e da eficiência dos processos e serviços da organização.

É importante definir alguns aspectos de como implementar políticas de segurança eficazes, como:

- Identificar e avaliar os riscos existentes ou potenciais na organização;
- Definir os objetivos, os escopos, os responsáveis e os recursos das políticas de segurança;
- Estabelecer as regras, os procedimentos, os controles e as medidas de segurança a serem adotados.

A partir das informações dadas, foram criadas 3 políticas públicas relacionadas a empresa Beta Móveis partindo de alguns pontos críticos de segurança que foram notados.

1 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação tem como objetivo proteger os dados e os sistemas da empresa contra ameaças internas e externas, garantindo a confidencialidade, a integridade e a disponibilidade das informações. Algumas diretrizes dessa política são:

- Estabelecer um comitê de segurança da informação responsável por definir, implementar e monitorar as normas e os procedimentos de segurança;
- Classificar as informações de acordo com o seu grau de sensibilidade e definir os níveis de acesso e permissão para cada usuário ou grupo de usuários;
- Criar mecanismos de autenticação, criptografia e controle de acesso para os sistemas e dispositivos da empresa;
- Realizar backups periódicos dos dados e armazená-los em locais seguros e diferentes da origem.

2 – POLÍTICA DE BACKUP

A política de backup tem como objetivo garantir a preservação e a restauração dos dados da empresa em caso de perda, corrupção ou indisponibilidade dos mesmos. Algumas diretrizes dessa política são:

- Definir quais dados devem ser copiados, com que frequência, por quanto tempo e em quais mídias ou locais;
- Utilizar técnicas de compressão, de duplicação e verificação para otimizar o espaço e a qualidade dos backups;
- Criar rotinas automatizadas e agendadas para a execução dos backups, evitando a dependência humana ou o esquecimento;
- Estabelecer um processo de restauração dos dados em caso de necessidade, definindo os responsáveis, os prazos e os critérios para a recuperação.

3 – POLÍTICA DE MANUTENÇÃO DE SOFTWARE

A política de manutenção de software tem como objetivo garantir o bom funcionamento, a atualização e a melhoria contínua dos sistemas utilizados pela empresa. Algumas diretrizes dessa política são:

- Definir um ciclo de vida para os softwares, desde o seu desenvolvimento até o seu descarte, passando pelas fases de implantação, testes, operação, suporte e evolução;

- Estabelecer um cronograma para as atividades de manutenção preventiva, corretiva e evolutiva dos softwares, considerando as prioridades, os recursos e os impactos envolvidos;
- Documentar todas as alterações realizadas nos softwares, registrando as datas, os motivos, os responsáveis e os resultados obtidos;
- Criar um canal de comunicação entre os usuários e os desenvolvedores dos sistemas, para receber feedbacks, sugestões, reclamações e solicitações.