API de Gerenciamento de Workloads - Plataforma de Dados

Políticas de Segurança

1. Introdução

Esta política de segurança tem como propósito o estabelecimento de diretrizes e procedimentos para a proteção de dados e do sistema contra acesso não autorizado, divulgação, alteração e destruição, em conformidade com o Regulamento Geral de Proteção de Dados (GDPR) e com as Normas de Segurança

2. Declaração de Política

Proteção de Dados

- Todos os dados sensíveis devem ser criptografados em trânsito por meio de HTTPS/TLS;
- Todos os dado sensíveis em repouso devem ser criptografados;
- Dados não estruturados, como gravações de chamadas telefônicas, devem ser armazenados de forma segura e criptografada, pois podem possuir informações sensíveis;
- Dados pessoais devem ser processados de maneira justa, legal e transparente;
- A API deve garantir a proteção dos dados em todas as operações;
- Dados pessoais sensíveis e credenciais não deverão ser expostos nas respostas da API.
- Backups regulares dos dados críticos devem ser realizados e armazenados de forma segura.

Segurança de Rede

- Os Firewalls devem ser configurados para bloquear o acesso não autorizado à rede da organização, com foco em proteger as interações da API;
- Garantir que todos os recursos estejam em uma mesma rede virtual;
- Utilização de recursos de proteção para garantir resiliência a ataques massivos;
- Scans de rede regulares devem ser realizados para identificar vulnerabilidades;
- Sistemas de detecção de intrusões devem estar em vigor para monitorar o tráfego da rede.

Controle de Acesso

- Definir funções para cada grupo de usuário;
- Todas as requisições deverão ser autenticadas com tokens de acesso seguros (JWT);

- Aplicar o Controle de Acesso Baseados em Funções para controlar o acesso com base nas funções do usuário;
- O permissionamento para a criação de recursos deverá ser granular, seguindo princípios de privilégio mínimo;
- Autenticação multifatorial deve ser implementada para acesso a sistemas críticos;
- A API deve implementar autenticação e autorização robustas para controlar o acesso;
- Revisões regulares dos direitos de acesso dos usuários devem ser realizadas;