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

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

Segurança de Rede

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

Controle de Acesso

1. Definir funções para cada grupo de usuário;
2. Todas as requisições deverão ser autenticadas com tokens de acesso seguros (JWT);
3. Aplicar o Controle de Acesso Baseados em Funções para controlar o acesso com base nas funções atribuídas aos usuários;
4. O permissionamento para o ambiente de produção deverá ser específico para os usuários produtizadores na organização. Caso a função precise ser atribuída a um usuário não definido anteriormente, deverá ser formalizado em documento.
5. O permissionamento para a criação de recursos deverá ser granular, seguindo princípios de privilégio mínimo;
6. Autenticação multifatorial deve ser implementada para acesso a sistemas críticos;
7. A API deve implementar autenticação e autorização robustas para controlar o acesso;
8. Deverão ocorrer revisões regulares do acesso dos usuários.