Segurança da Informação

Implementação De Políticas De Controle De Acesso Aos Sistemas De Dados

- Política de Autenticação Forte: Os usuários devem utilizar autenticação de dois fatores para acessar o sistema, além de uma senha forte com no mínimo 8 caracteres, incluindo letras, números e símbolos.

- Política de Senhas: por inatividade de um período de 6 meses, o usuário tem de realizar a confirmação da senha, ou porventura fazer a alteração após o período de inatividade.

- Política de Revisão de Acessos: Realizar revisões trimestrais dos acessos dos usuários para garantir a conformidade com suas funções.

- Política de Controle de Acesso Condicional: O Acesso a plataforma só será permitido a partir de dispositivos previamente autorizados e dentro das redes IP já cadastradas pela empresa.

- Política de Privacidade de Dados: Apenas colaboradores com a necessidade extrema de acesso a dados pessoais e sensíveis dos clientes terão permissão para visualizar e manipular esses dados, de dados de acordo com a regulamentação de privacidade, de acordo com a Lei Geral de Proteção De Dados (LGPD).

- Política de Desativação de Conta: Conta de Usuários inativos por mais de 24 meses serão automaticamente desativadas. Ex-funcionários terão suas contas desativadas imediatamente após o desligamento.

- Política de Notificação de Acessos Incomuns: Caso haja uma tentativa de acesso fora do padrão de comportamento do usuário, uma notificação será enviada automaticamente ao usuário e ao administrador do sistema.

- Política de Sessão de Inatividade: Sessões de usuários serão automaticamente encerradas após 15 minutos de inatividade para minimizar riscos de acesso indevido.

- Política de Mascaramento de Dados: Informações sensíveis, como números de

cartões de crédito ou CPF, serão parcialmente mascaradas nos relatórios e telas, exibindo apenas os últimos quatro dígitos.

- Política de Auditoria de Acessos: Todo acesso a dados críticos e sensíveis será registrado em logs, com auditorias mensais para garantir que não houve acessos não autorizados.

- Política de Restrição Geográfica: O sistema irá bloquear tentativas de login vindas de regiões geográficas fora das áreas de operação da empresa ou de locais não autorizados.

- Política de Criptografia de Dados em Trânsito: Todos os dados sensíveis transmitidos entre servidores e dispositivos devem ser criptografados utilizando as versões de criptografia mais recentes para proteger contra interceptação.

- Política de Controle de Acesso a Dados Pessoais: Acesso a dados pessoais de clientes será limitado a usuários cuja função exija diretamente essa responsabilidade, e o acesso será monitorado por logs auditáveis.

- Política de Acesso Condicional para Arquivos Sensíveis: Certos arquivos, como relatórios financeiros ou bases de dados de clientes, só estarão acessíveis em condições específicas, como dentro da rede local ou com uma autorização de alto nível.

- Política de Limitação de Compartilhamento de Dados: Proibir o compartilhamento de informações sensíveis fora do sistema sem autorização, como o envio de relatórios por e-mail ou a exportação de grandes volumes de dados.

- Política de Auditoria de Funções Administrativas: Funções administrativas (como root ou administrador de banco de dados) terão suas atividades monitoradas e auditadas regularmente para garantir que os acessos e ações estão em conformidade com as políticas.

- Política de Bloqueio Automático de Acessos Suspeitos: O sistema deve detectar automaticamente acessos suspeitos (login simultâneo de diferentes localidades) e bloquear temporariamente a conta até que o usuário confirme sua identidade.

- Política de Conformidade com Normas de Segurança: Todos os acessos e permissões devem estar em conformidade com normas de segurança reconhecidas, como ISO 27001.

- Política de Acesso Baseado em Risco: dentro da política está presente o sistema de análise de risco em tempo real que avalia o comportamento do usuário durante a tentativa de acesso (por exemplo, horário atípico, local desconhecido) e ajusta as permissões ou solicita autenticação adicional conforme o nível de risco identificado.

- Política de Acesso a Logs de Segurança
Apenas usuários autorizados do time de segurança terão acesso a logs de segurança detalhados, e qualquer tentativa de visualização ou modificação dos logs será registrada e auditada.