SERRA E COMPANY

POLÍTICA DE SEGURANÇA DE DADOS DA SERRA E COMPANY

A **Serra e Company** se preocupa com seus dados dos quais é controladora ou operadora, estando comprometida com nossos valores corporativos, desenvolveu esta política de segurança de dados baseada na **LGPD (Lei Geral de Proteção de Dados)**.

A Serra e Company mantém um Departamento próprio de Tecnologia da Informação onde os profissionais prestam serviços exclusivos a empresa e monitoram o controle de acesso lógico implantado garantindo que:

1) Apenas usuários autorizados tenham acesso aos recursos;
2) Os usuários possuem acesso apenas aos recursos realmente necessários para a execução de suas tarefas;
3) O acesso a recursos críticos são bem monitorados e restritos a poucas pessoas;
4) Os usuários são impedidos de executar transações incompatíveis com a sua função ou além de suas responsabilidades.

DA IDENTIFICAÇÃO E AUTENTICAÇÃO DOS USUARIOS

A identificação do usuário é única, ou seja, cada usuário tem identificação própria. O processo de logon aos sistemas da Serra e Company envolve a entrada de um ID (identificação de usuário) e uma senha (identificação do usuário).

Os usuários dos sistemas computacionais e aplicativo são identificados e autenticados durante um processo de logon que são usados para conceder acesso e orientam o usuário durante sua identificação e autenticação.

O número de tentativas de logon sem sucesso é limitado a 03 (três) tentativas, posteriormente o usuário é bloqueado necessitando de requerimento ao setor responsável de nova senha, sendo que as tentativas de acesso inválidas ficam registradas;

As identificações são realizada a partir da composição de letras e números sendo cada uma com mais de 5 caracteres e pelo menos uma letra maiúscula.

Todos os usuários são orientados a:

1) Manter a confidencialidade das senhas;
2) Não compartilhar senhas;

3) Evitar registrar as senhas em papel;
4) Selecionar senhas de boa qualidade, dentro dos padrões estabelecidos;
5) Alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
6) Alterar senhas temporárias no primeiro acesso ao sistema;
7) Evitar reutilizar as mesmas senhas;
8) Utilizar senhas diferentes em sistemas diferentes.
9) Evitar senhas compostas de elementos facilmente identificáveis (exemplo: nome, datas, números de telefone, RG...)

DA PROTEÇÃO E CONTROLE DAS SENHAS DE ACESSO

O sistema de controle de senhas é configurado para proteger as senhas armazenadas contra uso não autorizado, sem apresenta-las na tela do computador, mantendo-as em arquivos criptografados e estipulando datas de expiração (normalmente após 90 dias), além de criptografar as senhas, essas informações são guardadas em arquivos escondidos que não podem ser vistos por usuários, dificultando, assim, a ação dos hackers..

O gestor de segurança desabilita contas inativas, sem senhas ou com senhas padronizadas.

Os ex-funcionários têm suas senhas bloqueadas no imediato momento da demissão, também são bloqueados o acesso de usuários após três tentativas de acesso sem sucesso, devendo este fazer requisição de nova senha ao Departamento responsável;

O gestor de T.I. também implementa controle específico restringindo o acesso dos usuários apenas às aplicações, arquivos e utilitários imprescindíveis para desempenhar suas funções na instituição.

DA POLITICA DE CONTROLE DE ACESSO INFORMATIZADO

As regras de controle e direitos de acesso para cada usuário ou grupo foram claramente definidas no documento da política de controle de acesso lógico da instituição, definido quando da implantação da Iso9001, e foi fornecido aos usuários e provedores de serviço para que tomem conhecimento dos requisitos de segurança estabelecidos pela gerência.

DA POLITICA DE CONTROLE DE ACESSO FÍSICO

O prédio da Serra e Company não é aberto ao público, portanto, só possuem acesso ao prédio os colaboradores, diretores e convidados, previamente identificados no porteiro eletrônico e na recepção.

Os arquivos físicos ficam alocados em áreas restritas nos departamentos competentes e seu acesso é restrito aos usuários autorizados.

VPN IPSEC; DNS (Domain Name Service, serviço de nome de domínio); IP Público; Internet de equilíbrio de carga; Firewall