Plano de segurança da informação

Introdução

O presente documento tendo como base os princípios da segurança da informação que são confidencialidade, integridade, disponibilidade e autenticidade, tem o objetivo de esclarecer e estabelecer regras e procedimentos para reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou organização.

**1. Autenticação**

Visando uma melhor segurança foi estabelecida a utilização de senhas como fator de autenticação. As senhas deverão ser uma mescla de caractere especial junto a numerais e letras maiúsculas e minúsculas. Combinações simples que podem indiciar não serão aceitas. Senhas baseadas em fatos e datas especiais não são indicadas.

Codificar um documento ou arquivo com informações altamente confidenciais é uma atitude muito recomendada, para evitar que pessoas com acesso não autorizado consigam ver seu conteúdo.

A codificação pode ser realizada antes mesmo que o arquivo seja enviado para a nuvem, o mais importante é proteger o conteúdo com um código que só pode ser aberto pelo usuário responsável pelas informações.

Por isso é essencial criar uma senha forte, que não possa ser descoberta facilmente. Misture letras maiúsculas e minúsculas, números e caracteres especiais. Senhas baseadas em acontecimentos e datas especiais que são do conhecimento de terceiros não são indicadas.

# **2. Backups**

Todos os arquivos e sistemas, por mais modernos que sejam, não estão livres de passar por indisponibilidades temporárias de servidores, quedas de energia, problemas em alguma máquina e outros tipos de falhas.

Justamente por isso, é essencial fazer um backup de todos os dados e arquivos importantes da empresa. Para isso, é fundamental contar com profissionais capacitados, que possam efetuar a recuperação de dados no caso de imprevistos.

Permissões e direitos de usuário são requeridos para fazer backup e restaurar dados

# **3. Firewalls**

Com o alinhamento do controle de acesso juntamente com a criptografia, contar com um firewall é fundamental para reforçar a segurança das informações. Ele irá atuar monitorando, toda a comunicação realizada com os bancos de dados do sistema. Resultando rapidamente a identificação e suspensão da comunicação de qualquer tipo de acesso malicioso.

O firewall não irá afetar o funcionamento do software mas restringir o tráfego de informações por determinadas portas, previamente configuradas. Quanto mais sensíveis forem os dados manipulados, mais robustas e criteriosas podem ser as configurações do firewall.

**4. Antivírus**

É obrigatório a utilização de um antivírus, a fim de detectar, anular e eliminar os vírus de computador, analisar os arquivos que estão sendo baixados pela Internet, verificar continuamente os discos rígidos e flexíveis de forma transparente ao usuário, Procurar Vírus e Cavalos de Tróia em arquivos anexados aos e-mails, criar um disco de verificação (disco de boot) que pode ser utilizado caso o Vírus seja mais esperto e anule o antivírus que está instalado no computador.

É altamente recomendável manter o antivírus atualizado, a equipe técnica irá se encarregar disso, porém caso seja detectado que não foi feito, contactar a mesma para que seja feita o mais rápido possível.

.

5. Medidas preventivas

5.1 Políticas de dispositivos

Não traga CD, pen drives, hd externo, mouse de fora da empresa, caso seja necessário informar a equipe técnica para averiguar e registrar.reporte qualquer atitude suspeita no sistema imediatamente

5.2 Políticas de acesso à internet

O uso da internet deve ser destinado somente a trabalho, não para fins recreativos. Acessos a rede sociais, sites pornográficos, sites de compras etc, serão bloqueados e monitorados

5.3 Políticas de e-mails

Os e-mails da empresa não devem ser utilizados para assuntos pessoais, desconfie de todos os e-mails com assuntos ou conteúdos suspeitos. Correntes, anúncios e

Propagandas não devem ser compartilhadas

Evite anexos grandes

5.4 Políticas estação de trabalho

Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de

Segurança

- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria

- Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável.

5.5 Políticas social

Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos.

- Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.

- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.

- Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.

- Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail.

- Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos