Qualityclean – Sistemas de Higienização
CNPJ: 06.955.498/0001-22 IE: 554.092.060.110
Telefone: (15) 3261.1906
Visite nosso site: www.qualityclean.com.br

POLÍTICA DE SEGURANÇA FÍSICA

1. Introdução

A proteção do ambiente físico é uma das tarefas mais óbvias e mais importantes, na área de segurança da informação. A falta de controle de acesso físico pode desfazer precauções técnicas mais cuidadosas e potencialmente colocar vidas em risco.

A QUALITYCLEAN SISTEMAS DE HIGIENIZAÇÃO está comprometida em garantir a segurança de seus funcionários, contratados e ativos e leva a questão da segurança física muito a sério. Esta política define as principais precauções que devem ser tomadas e, juntamente com o suporte documentado, forma uma parte significativa do nosso conjunto de controle de segurança da informação.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros do conselho, diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas QUALITYCLEAN SISTEMAS DE HIGIENIZAÇÃO.

2. Áreas Seguras

Informações confidenciais devem ser armazenadas com segurança. Uma avaliação de risco deve ser realizada para identificar o nível apropriado de proteção a ser implementado, para proteger as informações armazenadas.

A segurança física deve começar com o próprio edifício e uma avaliação da vulnerabilidade do perímetro deve ser realizada. Um edifício deve ter mecanismos de controle adequados para as informações sensíveis e equipamentos armazenados nele.

Estes podem incluir, mas não estão restritos, aos seguintes:
- Alarmes instalados e ativados fora do horário de trabalho;
- Fechaduras de janelas e portas;
- Câmeras de CCTV;
- Área de recepção pessoal;
- Proteção contra danos - por ex. fogo, inundação, vandalismo.

A equipe que trabalha em áreas segurança deve interpelar qualquer um que não seja autorizado.

As ferramentas de identificação e acesso (por exemplo, crachás, chaves, códigos de entrada, etc.) devem ser mantidos apenas por pessoas autorizadas a entrar nessas áreas e não devem ser emprestados/fornecidos a qualquer outra pessoa.

Os visitantes das áreas de segurança são obrigados a entrar e sair com os horários marcados.

As chaves para todas as áreas que abrigam equipamentos de TI e gabinetes de TI bloqueáveis são realizadas especificamente pelo encarregado de Dados.

Quando ocorrerem violações ou quando um funcionário fizer a rescisão, todas as ferramentas de identificação e acesso (por exemplo chaves) devem ser recuperados.

3. Papel e Segurança do Equipamento

Informações baseadas em papel (ou similares não eletrônicas) devem receber um proprietário e uma classificação. Controles apropriados de segurança da informação devem ser colocados em prática para protegê-lo de acordo com as disposições dos procedimentos de manuseio de ativos.

A documentação física deve ser protegida pelos controles do prédio e pelas medidas apropriadas que podem incluir, mas não estão restritas, ao seguinte:
- Armários de arquivamento que são bloqueados com as chaves armazenadas longe do gabinete;
- Cofres trancados;
- Armazenado em uma área segura protegida por controles de acesso.

Todo o equipamento informático geral deve estar localizado de forma adequada que:

- Limite os riscos de perigos ambientais - por ex. calor, fogo, fumaça, água, poeira e vibração;
- Limite o risco de roubo - por ex. se necessário, itens como laptops devem estar fisicamente conectados à mesa;
- Permita que as estações de trabalho que manipulam dados confidenciais sejam posicionadas de modo a evitar o risco de os dados serem vistos por pessoas não autorizadas.

Os dados devem ser armazenados em servidores de arquivos de rede, quando disponíveis. Isso garante que as informações perdidas, roubadas ou danificadas por meio de acesso não autorizado possam ser restauradas e sua integridade mantida.

Todos os servidores localizados fora do data center devem ser instalados em um ambiente fisicamente seguro.

Todos os itens do equipamento devem ser registrados no inventário do Provedor de serviços. Os procedimentos devem estar em vigor para garantir que o inventário seja atualizado assim que os ativos forem recebidos ou descartados.

Todos os equipamentos devem ser marcados com segurança e ter um número de ativo exclusivo alocado a ele. Este número de ativo deve ser registrado no inventário.

Os cabos que transportam dados ou suportam serviços de informações importantes devem ser protegidos contra interceptação ou danos.

Os cabos de energia devem ser separados dos cabos de rede para evitar interferência. Os cabos de rede devem ser protegidos por conduítes e, sempre que possível, evitar rotas através de áreas públicas.

4. Gestão do ciclo de vida dos equipamentos

Os fornecedores de serviços e fornecedores terceirizados devem garantir que todos os equipamentos de TI da QUALITYCLEAN SISTEMAS DE HIGIENIZAÇÃO sejam mantidos de acordo com as instruções do fabricante, e quaisquer procedimentos internos documentados para garantir que permaneçam em funcionamento efetivo.

O pessoal envolvido na manutenção deve:
- Identificar quando deve haver manutenção recomendada;
- Ativar um processo de chamada em caso de falha;
- Registrar detalhes de todo o trabalho de reparação realizado;
- Identificar quaisquer requisitos de segurança;
- Registrar detalhes das falhas ocorridas e ações necessárias.

Um registro de histórico de serviço do equipamento deve ser mantido para que as decisões possam ser tomadas em relação ao tempo apropriado para a substituição.

As instruções de manutenção do fabricante devem estar documentadas e disponíveis para uso pela equipe de suporte ao organizar os reparos.

O uso de equipamentos fora do local deve ser formalmente aprovado pelo supervisor do usuário.

O equipamento que deve ser reutilizado ou descartado deve ter todos os seus dados e software apagados/destruídos.

As entregas de equipamento devem ser assinadas por um indivíduo autorizado usando um processo formal. Os ativos reais recebidos devem ser registrados.

As áreas de carregamento e as instalações de armazenamento devem ser adequadamente protegidas contra acesso não autorizado e todo o acesso deve ser registrado.

Os arranjos de segurança da informação devem estar sujeitos a auditorias independentes regulares e melhorias de segurança recomendadas quando necessário.