Política de Segurança de Acesso Físico

PÚBLICO ALVO: AGENTES PÚBLICOS	EMISSÃO:	CODIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

Política de Segurança de Acesso Físico

1. Apresentação

Esta política norteará a implementação de medidas para regular a segurança no acesso físico de pessoas aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI) do Tribunal Regional Federal da 5ª Região (TRF5) e suas Seções e Subseções Judiciárias de forma a minimizarem os riscos à segurança das informações corporativas.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio da instituição, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.2.1 – Política de Segurança de Acesso Físico – do Anexo I da Resolução Nº 6, de 7 de abril de 2008 do Conselho da Justiça Federal que definiu a Política de Segurança da Informação no âmbito do Conselho e da Justiça Federal de primeiro e Segundo graus.

2. Escopo

O escopo deste documento integrante da Política de Segurança da Informação abrange o Tribunal Regional Federal da 5ª Região, suas Seções e Subseções Judiciárias.

3. Público Alvo

Esta Política de Controle de Acesso Físico se aplica aos agentes públicos do Tribunal Regional Federal da 5ª Região, suas Seções e Subseções Judiciárias e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas com a administração.

4. Da Segurança de Acesso Físico

4.1 Devem ser utilizados perímetros físicos de segurança (barreiras tais como paredes e portões de entrada controlados) para proteger as áreas que contenham instalações de processamento, armazenamento e comutação de dados além de controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferências

com o suprimento de energia elétrica, interferência nas comunicações, radiação eletromagnética e vandalismo.

4.1.1 Os perímetros de segurança devem ser claramente definidos e sua localização e a capacidade de resistência dos mesmos devem depender dos requisitos de segurança dos ativos existentes no interior do perímetro.

4.2 A unidade técnica de informática deverá avaliar e providenciar constantemente, com o auxílio das áreas competentes, a melhoria dos recursos de segurança de seus centros de processamento, armazenamento e comutação de dados corporativos.

4.3 As áreas de processamento, armazenamento e comutação de dados devem ser protegidas por controles apropriados de entrada, para assegurar que somente pessoas autorizadas tenham acesso.

4.3.1 Devem ser providos controles de autenticação que utilizem, de preferência, autenticação mínima de dois fatores, para autorizar e validar todos os acessos.

4.3.2 Deve ser mantido, de forma segura, um registro de todos os acessos para fins de auditoria;

4.3.3 A data e hora de entrada e saída de visitantes devem ser registradas, e todos os visitantes devem ser supervisionados, a não ser que o seu acesso tenha sido previamente aprovado.

4.3.4 As permissões de acesso devem ser concedidas somente para finalidades específicas, devendo a pessoa autorizada, receber instruções sobre os requisitos de segurança da área e os procedimentos de emergência.

4.3.5 Os direitos de acesso às áreas seguras devem ser revistos e atualizados em intervalos de tempo regulares, e revogados quando necessário.

4.3.6 Aos terceirizados que realizam serviços de suporte, deve ser concedido acesso restrito às áreas seguras ou às instalações de processamento, armazenamento e comutação da informação sensível somente quando necessário. O acesso deverá ser sempre autorizado e monitorado.

4.4 As áreas de processamento, armazenamento e comutação de dados devem estar localizadas de forma discreta, sem indicação de sua finalidade e sem letreiros evidentes que identifiquem a presença de suas atividades, quando aplicável.

4.5 As listas de funcionários e guias telefônicos internos que identifiquem a localização das instalações de processamento, armazenamento e comutação de dados sensíveis não devem ser de fácil acesso ao público.

4.6 Os equipamentos para contingência e mídias de backup devem ficar a uma distância e local seguros, para que não sejam danificadas por um desastre que afete o local principal.

4.7 Não é permitido, nas localizações dos centros de processamento, armazenamento e comutação de dados, o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado e registrado.

4.8 É proibido o consumo de bebidas, comidas e fumo nas proximidades das instalações de processamento, armazenamento e comutação de dados.

5. Periodicidade de Revisão

5.1 Esta política deverá ser revista anualmente pelo Comitê Local de Segurança da Informação com vistas a adequar a mesma às necessidades atuais.

5.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.