INSTRUÇÃO NORMATIVA STI/POSIN 02 – SEGURANÇA FÍSICA E DO AMBIENTE

As informações armazenadas em meios físicos (suportes) como, por exemplo, discos rígidos, fitas magnéticas e até mesmo papel ou microfilmes, assim como aquelas incluídas nos ativos de rede, têm que ser protegidos de acessos indevidos, pois quem tem acesso ao meio pode acessar ou alterar as informações e até mesmo destruí-las.

Um cuidado especial deve ser tomado quanto ao descarte dos meios, uma vez que as informações neles contidas podem ser passíveis de recuperação. É preciso que haja um processo que garanta que as informações em uma mídia não possam ser recuperadas. O descarte de mídia não é descarte de informação, pois esta é objeto de legislação específica.

A informação somente pode ser descartada depois de um processo e autorização, devendo o trâmite ser devidamente registrado. Mídias somente podem ser descartadas se a informação armazenada puder ser descartada ou tiver sido preservada em outro meio.

Os meios físicos (suporte) também devem estar protegidos de deterioração, que pode ser causada pelas condições ambientais, como temperatura e umidade, ou por agentes químicos e biológicos.

Um dos maiores riscos à integridade dos meios inclui os danos causados por fogo e água. Portanto, esses meios devem estar em ambientes seguros, com controle de acesso e condições adequadas de preservação, conforme estabelecido por normas específicas.

Os ambientes devem ser categorizados em:

- **Áreas de segurança:** estes incluem sala de servidores e de arquivos. Deve haver controle de registro de entrada; controle de condições ambientais, biológicas e químicas; mecanismos de segurança contra incêndio e inundações; e garantia contra falhas elétricas.
- **Áreas de equipamentos:** estes incluem a infraestrutura de rede (cabeamento e equipamentos de rede). Deve haver proteção contra acesso indevido e garantia contra falhas elétricas.
- **Uso geral:** escritórios, onde deve haver uma política de mesa e tela limpas. Deve haver registro de movimentação de equipamentos.

O acesso aos ambientes controlados deve ser somente feito por pessoal autorizado e por necessidade de serviço. Deve haver um registro contendo, minimamente, as informações de hora de entrada, hora de saída, identificação, itens acessados e motivo.

1. DIRETRIZES PARA SALAS DE SERVIDORES

Devem ser seguidas normas específicas para este tipo de ambiente. Minimamente, devem ser considerados os itens abaixo:

- Salas seguras
- Paredes sólidas
- Portas de aço
- Controle e registro de acesso
- Proteção contra infiltrações e inundações
- Proteção contra incêndio
- Controle de temperatura e umidade
- Garantias contra falhas elétricas
- Não devassável (sem janelas)

2. DIRETRIZES PARA SALAS DE ARQUIVOS

Devem ser seguidas normas específicas para este tipo de ambiente. Minimamente, devem ser considerados os itens abaixo:

- Paredes sólidas
- Controle e registro de acesso
- Proteção contra infiltrações e inundações
- Proteção contra incêndio
- Controle de temperatura e umidade
- Controle de agentes químicos, físicos e biológicos

3. DIRETRIZES PARA INFRAESTRUTURA DE REDE

Devem ser seguidas normas específicas para este tipo de ambiente. Minimamente, devem ser considerados os itens abaixo:

- Racks com chave

- Garantias contra falhas elétricas

4. DIRETRIZES PARA ARMAZENAMENTO DE CÓPIAS DE SEGURANÇA

Devem ser seguidas normas específicas para este tipo de ambiente. Minimamente, devem ser considerados os itens abaixo:

- Mídia armazenada em cofre
- Cofre fora do local de uso (se possível)
- Replicação remota

5. DIRETRIZES PARA DESCARTE DE MÍDIA

O descarte de mídias deve compreender, entre outros:

- Métodos de controle de classificação de documentos que permitam identificar mídias contendo informações sensíveis, de maneira que sejam guardadas e destruídas de maneira segura;
- Procedimentos para autorização de descarte;
- Métodos e procedimentos de coleta e descarte para cada tipo de mídia;
- Métodos e procedimentos para o controle do descarte de mídias sensíveis de maneira a manter, sempre que possível, uma trilha de auditoria.

Em caso de papel, devem ser usadas fragmentadoras de papel (excepcionalmente, pode ser fragmentado manualmente). Existem diversos modelos de níveis de segurança para fragmentadoras de acordo com a possibilidade de reconstituição do material fragmentado. No caso de CD, DVD, cartões magnéticos, há modelos de fragmentadoras que conseguem destruí-los. Recomenda-se, então, que sejam adquiridas fragmentadoras de papel capazes de destruir CD, DVD, cartões magnéticos de PVC, que atendam, pelo menos, ao Nível 2 de segurança, e que sejam resistentes a grampos e clipes (metálicos ou não).

Em mídias magnéticas ainda em funcionamento, deve ser usado um software específico (formatação não é suficiente!) para apagar fisicamente todo o conteúdo do disco rígido, antes da eliminação. No caso do equipamento não estiver funcional, a unidade deve ser retirada para ser limpa em outro equipamento compatível com uso de software específico. Se a unidade não estiver funcional ela deve ser destruída mecanicamente.