tecnologia a serviço da cidade
procempa

Política de Segurança Física

Julho, 2022

Política de Segurança Física

1. Todo o indivíduo nas dependências da companhia deverá usar crachá de identificação fornecido pela PROCEMPA ou por órgão da Administração Municipal comprovando seu vínculo ativo. Visitantes, clientes, fornecedores ou terceiros deverão ser identificados, autorizados e acompanhados por funcionário da PROCEMPA por toda a duração da visita.
2. Portas das áreas de acesso restrito, inclusive datacenters, salas seguras, salas de comunicação, laboratórios e depósitos, devem ser mantidas fechadas e trancadas sempre que os funcionários responsáveis autorizados não estiverem no local.
3. A PROCEMPA deverá exigir via cláusulas contratuais das suas prestadoras de serviços terceirizados, a total responsabilidade das mesmas pelas ações ou prejuízos causados por seus colaboradores ao patrimônio da PROCEMPA, bem como manter confidencialidade das informações acessadas.
4. Os equipamentos e seus componentes internos serão inventariados periodicamente e somente funcionários autorizados podem fazer remanejo de equipamentos e peças.
5. Os notebooks não devem ser deixados desprotegidos quando não acompanhados por seu responsável, mesmo por poucos minutos. Em escritório, pode-se usar cabo e trava de segurança específica com chave que impeça sua retirada do local ou armazená-los em armários ou gavetas chaveados.
6. Ferramentas e equipamentos portáteis da PROCEMPA, tais como notebooks, podem ser levados por seus responsáveis autorizados, para fins de trabalho, e quando possível, deve ser usada forma de registro automático dessas movimentações. Os demais equipamentos, entrando ou saindo da PROCEMPA, deverão estar acompanhados da respectiva nota fiscal e autorização do setor de Patrimônio, com registro de data, hora, identificação do portador e do equipamento.
7. A entrega de documentos com informações confidenciais pode ocorrer apenas com registro e a garantia de identificação de quem recebe.
8. Devem ser tomados cuidados para não expor desprotegidos documentos, mídias, dispositivos ou equipamentos em mesas de escritório, armários ou gavetas, conforme a Politica de Mesas e Telas Limpas.
9. Documentos ou papéis contendo informações confidenciais, ao final de seu ciclo de vida, quando não mais necessários, devem ser destruídos nas fragmentadoras disponíveis para essa finalidade.
10. Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc) contendo informações confidenciais, quando não mais necessárias, também devem ser destruídas.
11. Mídias regraváveis (drives HD, SSD, pen drives, cartões SD, fitas, discos CD-RW, DVD-RW ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas antes do descarte com o procedimento seguro adequado indicado pela equipe de Segurança da Informação ou destruídas se não puderem ser reaproveitadas.
12. Equipamentos desmagnetizadores apropriados estão disponíveis e são indicados para zerar fitas magnéticas e disquetes. Também devem ser usados para destruição de drives HD defeituosos, que não podem ser zerados de outra forma e não possuem mais condição de serem reutilizados, vendidos ou doados. Deve-se sempre levar em conta que

Comentado [1]: Como fica no prédio novo

Comentado [2]: não usar cabos com senha, pois a mesma pode ser descoberta ou compartilhada indevidamente de forma mais fácil.

desmagnetizadores podem e costumam danificar permanentemente equipamentos eletrônicos e impossibilitar seu uso posterior.

13. Equipamentos servidores de rede em produção devem ser instalados dentro de Datacenter ou Sala Segura apropriada, nunca em escritório.
14. Unidades de armazenamento em notebooks e estações de trabalho devem ser criptografadas sempre que possível usando recursos do sistema operacional.

Comentado [3]: encaminhar Projeto para uso de Bitlocker/LUKS nas estações de trabalho e notebooks.