CHAVE DE RESPOSTA – CARGO 501

O incidente ocorrido no CREA-SE revela fragilidades críticas em diversos pilares da segurança da informação. A confidencialidade foi claramente violada, uma vez que um colaborador terceirizado, sem autorização, acessou dados sensíveis, expondo informações que deveriam ser restritas. A integridade também foi comprometida pelas tentativas de alteração indevida nos registros profissionais, colocando em risco a fidedignidade das informações mantidas pelo sistema. Embora a disponibilidade não tenha sido diretamente afetada, ela deve ser assegurada para manter o pleno funcionamento dos serviços aos profissionais. No que tange à autenticidade, observa-se que a ausência de controles rigorosos de autenticação facilitou o acesso não autorizado. Por fim, a irretratabilidade ficou prejudicada devido à carência de registros detalhados que permitissem atribuir as ações maliciosas aos seus autores.

Diante desse cenário, é imprescindível adotar medidas concretas. A implantação de controle rigoroso de acessos garantirá que apenas usuários devidamente autorizados tenham contato com dados sensíveis, prevenindo acessos indevidos. Além disso, realizar auditorias periódicas e implementar logs de atividade robustos permitirá não só rastrear ações suspeitas, mas também assegurar a irretratabilidade, facilitando a responsabilização por atos ilícitos. Complementarmente, a realização de programas contínuos de capacitação e conscientização é fundamental, abrangendo todos os colaboradores, inclusive terceirizados, para reforçar práticas seguras e alertar sobre os riscos.

A importância da capacitação não pode ser subestimada. A segurança da informação vai além das ferramentas tecnológicas, dependendo essencialmente do comportamento ético e responsável dos usuários. Muitas vezes, falhas humanas, como negligência ou desconhecimento, abrem portas para ataques e incidentes de segurança. Por isso, é vital incentivar a criação de uma cultura organizacional voltada para a proteção da informação, em que todos compreendam seu papel na defesa dos dados institucionais e ajam de forma proativa para evitar riscos, sendo a capacitação dos colaboradores uma estratégia possível para o alcance desse objetivo.