RESUMO SIMPLES - ÁREA DAS ENGENHARIAS E TECNOLOGIAS DA INFORMAÇÃO

GESTÃO DE ACESSOS E SEGURANÇA DA INFORMAÇÃO EM UMA IES PRIVADA: UM ESTUDO DE CASO

Francisca Waleska Costa Da Silva Sousa (waleska.sousa@uniateneu.edu.br)

Mirele Cavalcante Da Silva (mirele.silva@uniateneu.edu.br)

Alisson Silvano De Sousa (asousasilvano@gmail.com)

INTRODUÇÃO:

A segurança da informação torna-se essencial em Instituições de Ensino Superior (IES), que lidam diariamente com dados pessoais e sistemas sensíveis. A ausência de políticas estruturadas de controle de acessos favorece riscos como vazamento de informações, uso indevido de credenciais e descumprimento da Lei Geral de Proteção de Dados (LGPD). Em ambientes acadêmicos, a rotatividade de funções e a manutenção indevida de permissões agravam essas vulnerabilidades, tornando evidente a necessidade de governança institucional.

OBJETIVO:

Analisar os riscos decorrentes da ausência de controle sistemático de acessos em uma IES privada e identificar vulnerabilidades associadas à permanência de permissões após mudanças de função ou desligamento.

MATERIAL E MÉTODOS:

Estudo de caso qualitativo, com abordagem exploratório-descritiva, baseado em observação direta, registros pessoais e análise de acessos mantidos após desligamento formal. Os achados foram confrontados com normas e boas práticas de segurança da informação, como ISO/IEC 27001 e LGPD.

RESULTADOS:

Foi identificada a permanência ativa de acessos a sistemas acadêmicos, e-mails setoriais e documentos sensíveis mesmo após o desligamento do colaborador analisado. Constatou-se ausência de políticas formais, inexistência de integração entre os setores de TI e RH e acúmulo de permissões ao longo do tempo. As vulnerabilidades observadas revelam riscos operacionais, legais e reputacionais, incluindo possibilidade de exposição de dados pessoais de alunos.

CONCLUSÃO:

A falta de governança na gestão de acessos compromete a segurança institucional e viola princípios fundamentais da LGPD. Recomenda-se a implantação de políticas formais de controle, auditorias periódicas, integração entre setores e adoção de ferramentas de Identity and Access Management (IAM). Fortalecer a cultura de segurança é essencial para prevenir incidentes e garantir a conformidade legal.

REFERÊNCIAS:

ABNT. NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro, 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

WHITMAN, M. E.; MATTORD, H. J. Segurança da informação: princípios e práticas. Boston: Cengage Learning, 2022.

Palavras-chave: segurança da informação; gestão de acessos; instituição de ensino superior.