ABSTRAK

Keamanan informasi merupakan aspek penting dalam pengelolaan sistem informasi di lingkungan rumah sakit untuk melindungi data pasien dan operasional medis dari ancaman yang terus berkembang. Penelitian ini bertujuan untuk mengevaluasi Sistem Manajemen Keamanan Informasi (SMKI) di RSD Gunung Jati Cirebon berdasarkan standar ISO/IEC 27001:2022, dengan fokus pada analisis kesenjangan, identifikasi risiko, dan pemberian rekomendasi perbaikan yang spesifik.

Metode penelitian yang digunakan mencakup survei kuesioner, wawancara terstruktur, dan analisis dokumen kebijakan yang relevan. Analisis kesenjangan menunjukkan bahwa dari 93 kontrol yang dievaluasi, 25,8% telah memenuhi standar sepenuhnya, 51,6% berada pada tingkat implementasi menengah, dan 22,6% memerlukan perbaikan signifikan. Hasil analisis risiko juga mengidentifikasi ancaman utama pada area pengelolaan akses data dan pembaruan perangkat lunak, dengan mayoritas risiko berada pada kategori menengah hingga tinggi.

Hasil penelitian menunjukkan bahwa RSD Gunung Jati memiliki beberapa area yang membutuhkan perbaikan dalam memenuhi standar ISO/IEC 27001:2022, terutama dalam hal kebijakan keamanan dan pengelolaan akses informasi. Berdasarkan temuan ini, disusun rekomendasi untuk meningkatkan SMKI di rumah sakit, termasuk pelatihan karyawan, pengembangan prosedur keamanan yang lebih jelas, dan peningkatan pengawasan terhadap akses data. Saran bagi RSD Gunung Jati adalah untuk terus memperbarui kebijakan SMKI secara berkala agar dapat mengimbangi perkembangan ancaman keamanan siber. Studi ini diharapkan dapat menjadi acuan bagi rumah sakit lain yang berencana untuk mengimplementasikan SMKI berdasarkan ISO/IEC 27001:2022.

Kata Kunci: Sistem Manajemen Keamanan Informasi, ISO/IEC 27001:2022, Rumah Sakit Daerah Gunung Jati Cirebon, Keamanan Siber, Perlindungan Data Pasien, Analisis Kesenjangan.