

Analisis Manajemen Sekuriti di Badan Pengembangan Sumber Daya Manusia (BPSDM) Provinsi Jawa Barat

Rizky Hakiki ¹, Ahmad Taufik Riyadi Sanusi ¹, Muhammad Ardika Putra Maulana ^{1*},
Muhammad Akmal Dzulfikar ¹, Muhammad Fahrel Aditya ¹

¹Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya,
Bekasi Utara Jawa Barat, 17143, (021) 88955882; e-mail:

202210715302@mhs.ubharajaya.ac.id, 202310415300@mhs.ubharajaya.ac.id,
202210715323@mhs.ubharajaya.ac.id, 202210715327@mhs.ubharajaya.ac.id,
202210715328@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715323@mhs.ubharajaya.ac.id

Diterima: 17 Jan 25; Review: 17 Jan 25; Disetujui: 18 Jan 25; Diterbitkan: 18 Jan 25

Abstract

This report presents an analysis of security management at the West Java Province Human Resources Development Agency (BPSDM) with the aim of evaluating and improving the existing information security system. In the era of globalization and advances in information technology, information security has become an important part of the economy, especially in the field of natural resource management. This research will use qualitative and quantitative approaches to collect data through interviews, questionnaires, observations and document studies. The survey found that although employees have a good understanding of the information security policy, there are challenges in its implementation, including lack of resources, inadequate training and barriers to change. Suggested recommendations include enhancing information security training programs, better policy implementation, strengthening access controls, and periodic evaluation of security management practices. We hope this report can make a positive contribution to the sustainable and secure management of natural resources.

Keywords: security management, information security, bpsdm, resource management, risk analysis

Abstract

Laporan ini menyajikan analisis manajemen keamanan di Badan Pengembangan Sumber Daya Manusia (BPSDM) Provinsi Jawa Barat dengan tujuan mengevaluasi dan meningkatkan sistem keamanan informasi yang ada. Di era globalisasi dan kemajuan teknologi informasi, keamanan informasi telah menjadi bagian penting dalam perekonomian, terutama di bidang pengelolaan sumber daya alam. Penelitian ini akan menggunakan pendekatan kualitatif dan kuantitatif untuk mengumpulkan data melalui wawancara, kuesioner, observasi dan studi dokumen. Survei menemukan bahwa meskipun karyawan memiliki pemahaman yang baik tentang kebijakan keamanan informasi, terdapat tantangan dalam penerapannya, termasuk kurangnya sumber daya, pelatihan yang tidak memadai, dan hambatan terhadap perubahan. Rekomendasi yang disarankan meliputi peningkatan program pelatihan keamanan informasi, penerapan kebijakan yang lebih baik, penguatan kontrol akses, dan evaluasi berkala praktik manajemen keamanan. Kami berharap laporan ini dapat memberikan kontribusi positif bagi pengelolaan sumber daya alam yang berkelanjutan dan aman.

Kata kunci: manajemen sekuriti, keamanan informasi, bpsdm, pengelolaan sumber daya, analisis risiko

1. Pendahuluan

Di era globalisasi ini, dunia mengalami perkembangan yang pesat, membawa banyak perubahan di berbagai bidang kehidupan, termasuk keamanan informasi (Putri et al., 2022), keamanan informasi telah menjadi komponen penting bagi setiap organisasi, termasuk Biro Pengembangan Sumber Daya Manusia (BPSDM). BPSDM berperan strategis dalam pengelolaan dan pengembangan kualitas sumber daya manusia di sektor pemerintah dan swasta. Seiring meningkatnya penggunaan teknologi digital dalam mengelola dan mengadministrasikan data, meningkat pula risiko terhadap keamanan informasi (Jerry et al., 2024).

BPSDM Jawa Barat mengelola berbagai aset informasi, seperti data kepegawaian, dokumen pelatihan, dan sistem informasi berbasis teknologi. Dalam melaksanakan tugasnya, lembaga ini juga memanfaatkan berbagai perangkat dan infrastruktur teknologi informasi yang mendukung operasionalisasi pelatihan dan pengelolaan data. Dengan semakin banyaknya ketergantungan pada teknologi, ancaman terhadap keamanan informasi menjadi semakin kompleks, mulai dari risiko serangan siber hingga gangguan fisik seperti bencana alam atau kerusakan perangkat keras. Keamanan informasi yang lemah dapat berdampak serius, seperti kebocoran data, gangguan operasional, hingga kerugian finansial dan reputasi. Oleh karena itu, diperlukan manajemen keamanan yang baik untuk melindungi aset-aset penting yang dimiliki BPSDM Jawa Barat.

Keamanan informasi meliputi perlindungan data pribadi karyawan, data pelatihan, dan data strategis lainnya untuk memastikan bahwa data dan informasi yang disimpan oleh BPSDM tidak jatuh ke tangan yang salah. Ini termasuk perlindungan terhadap ancaman internal maupun eksternal (Soesanto et al., 2023). Analisis kontrol keamanan sangat penting untuk mengidentifikasi potensi ancaman dan kerentanan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan informasi (Nurul et al., 2022). Melalui analisis mendalam, BPSDM mendukung tujuan organisasi dalam mengembangkan strategi keamanan yang efektif, melindungi aset informasi, dan meningkatkan kualitas serta keahlian tenaga kerja (Fathiyah, 2021).

Selanjutnya, sangat penting untuk mematuhi peraturan dan pedoman keamanan informasi internasional dan hukum untuk memastikan bahwa operasi BPSDM berada dalam kerangka hukum yang berlaku. Penegakan kebijakan keamanan yang ketat dapat meningkatkan kepercayaan publik dan meningkatkan efisiensi manajemen sumber daya manusia. Sumber daya manusia merupakan modal dan aset yang penting (Halisa, 2020). Oleh karena itu, analisis manajemen keselamatan dalam BPSDM merupakan langkah proaktif menuju pencegahan risiko dan bagian penting dari strategi pengembangan sumber daya manusia yang berkelanjutan (Flannero et al., 2022).

2. Metode Penelitian

2.1 Penelitian

Metode penelitian ini menggunakan pendekatan kualitatif dan kuantitatif untuk mendapatkan pemahaman mendalam dan data terukur. Pendekatan kualitatif mengeksplorasi pengalaman, persepsi, dan tantangan pegawai terkait manajemen sekuriti, sedangkan pendekatan kuantitatif mengumpulkan data statistik mengenai tingkat pemahaman dan implementasi kebijakan sekuriti di BPSDM (Romlah et al., 2021).

2.2 Jenis Penelitian

- Deskriptif: Mendeskripsikan praktik manajemen sekuriti yang diterapkan di BPSDM, termasuk prosedur, kebijakan, dan alat yang digunakan.
- Eksploratif: Mengupas masalah dan tantangan yang mungkin belum sepenuhnya dipahami, memberikan wawasan baru dalam pengelolaan manajemen sekuriti.

2.3 Tujuan Penelitian

- Menganalisis kebijakan, sistem, dan infrastruktur keamanan yang ada.
- Mengidentifikasi celah keamanan dan potensi risiko.
- Memberikan rekomendasi peningkatan keamanan.

2.4 Populasi dan Sampel

- Populasi: Pegawai BPSDM yang terlibat dalam pengelolaan program pelatihan dan pengembangan sumber daya manusia, termasuk manajer, staf administrasi, pengelola program pelatihan, dan staf IT.
- Sampel: 10 pegawai BPSDM Provinsi Jawa Barat, terdiri dari:
 - Manajer Program: 3 orang
 - Staf IT: 3 orang
 - Staf Administrasi: 4 orang

2.5 Teknik Pengumpulan Data

- Wawancara: Wawancara semi-terstruktur dengan pegawai BPSDM untuk menggali kebijakan keamanan, tantangan, dan pemahaman individu.
- Kuesioner: Mengumpulkan data kuantitatif mengenai persepsi pegawai terhadap manajemen sekuriti.
- Observasi: Observasi langsung terhadap praktik keamanan yang diterapkan di BPSDM.
- Studi Dokumentasi: Analisis dokumen terkait, seperti kebijakan keamanan informasi dan laporan audit keamanan.

2.6 Analisis Data

- Data Kualitatif: Analisis tematik untuk mengidentifikasi tema, pola, dan kategori dari data yang dikumpulkan.
- Data Kuantitatif: Analisis statistik deskriptif untuk menggambarkan sikap dan pemahaman pegawai terhadap praktik manajemen sekuriti.

- Triangulasi: Membandingkan hasil dari berbagai sumber data untuk memastikan konsistensi dan ketepatan informasi.

2.7 Kesimpulan dan Rekomendasi

Setelah analisis data, peneliti akan menarik kesimpulan tentang keadaan manajemen sekuriti di BPSDM dan memberikan rekomendasi untuk meningkatkan kebijakan dan praktik manajemen sekuriti.

2.8 Lokasi Penelitian

Penelitian akan dilakukan di kantor BPSDM di Jl. Alun-Alun No. 1, Margahayu, Kec. Bekasi Timur, Kota Bekasi, Jawa Barat.

3. Hasil dan Pembahasan

3.1 Hasil Penelitian

Hasil penelitian ini diperoleh dari analisis data kualitatif dan kuantitatif yang dikumpulkan melalui wawancara, kuesioner, observasi, dan studi dokumentasi.

3.2 Hasil Wawancara

Dari wawancara yang dilakukan dengan 10 pegawai BPSDM, ditemukan beberapa tema utama terkait manajemen sekuriti:

1. Pemahaman Kebijakan Keamanan: Sebagian besar pegawai menyatakan bahwa mereka memiliki pemahaman yang baik tentang kebijakan keamanan informasi yang ada, namun ada beberapa yang merasa kurang mendapatkan sosialisasi yang memadai.
2. Tantangan dalam Implementasi: Pegawai mengidentifikasi beberapa tantangan dalam implementasi kebijakan, termasuk kurangnya sumber daya, pelatihan yang tidak memadai, dan resistensi terhadap perubahan.
3. Perlunya Pelatihan Berkelanjutan: Banyak pegawai menekankan pentingnya pelatihan berkelanjutan untuk meningkatkan kesadaran dan pemahaman tentang keamanan informasi.

3.3 Hasil Kuesioner

Dari 10 kuesioner yang disebar, semua responden mengisi kuesioner dengan baik. Hasil analisis menunjukkan:

1. Analisis data survey

Data yang dikumpulkan dari survei ini melibatkan 50 mahasiswa dan mahasiswi program studi Informatika di Fakultas Ilmu Komputer, yang terdiri dari semester tiga, lima, dan tujuh. Hasil survei ini memberikan wawasan berharga mengenai persepsi dan pengetahuan mereka tentang manajemen sekuriti di Badan Pengembangan Sumber Daya Manusia (BPSDM). Dengan memahami tingkat kesadaran dan pemahaman mahasiswa tentang keamanan informasi, serta frekuensi pelanggaran yang mereka dengar, kita dapat mengevaluasi efektivitas perlindungan

yang dirasakan. Temuan ini menjadi dasar untuk menguji apakah sistem yang diterapkan di BPSDM telah memenuhi tujuan yang ditetapkan dalam penelitian ini.

Tabel 1. Jenis Kelamin Berdasarkan data

	Frequency	Percent	Valid Percent	Cumulative Percent
Perempuan	33	66.0	66.0	66.0
Laki laki	17	34.0	34.0	100.0
Total	50	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Pada tabel 1 menjelaskan Jenis kelamin berdasarkan data.

Tabel 2. Validasi terhadap seberapa tahu tentang manajemen sekuriti

	Frequency	Percent	Valid Percent	Cumulative Percent
ya	39	78.0	78.0	78.0
tidak	11	22.0	22.0	100.0
total	50	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Pada tabel 2 menjelaskan Hasil survei menunjukkan bahwa 78% responden merasa memiliki pemahaman yang jelas tentang manajemen sekuriti, sementara 22% lainnya merasa kurang tahu. Ini menunjukkan bahwa sebagian besar mahasiswa sudah mendapatkan informasi yang memadai mengenai pentingnya keamanan informasi. Namun, masih ada ruang untuk meningkatkan sosialisasi dan edukasi lebih lanjut agar semua mahasiswa dapat memahami aspek-aspek penting dari manajemen sekuriti.

Tabel 3. Dari mana anda mengetahui informasi tentang manajemen sekuriti

	Frequency	Percent	Valid Percent	Cumulative Percent
Informasi dan media	17	34.0	34.0	34.0
Mata kuliah	15	30.0	30.0	64.0
Lainnya	18	36.0	36.0	100.0
Total	50	100.0	100.0	

Sumber: Hasil Penelitian (2024)

Pada tabel 3 menjelaskan Ketika ditanya dari mana mereka mendapatkan informasi tentang manajemen sekuriti, responden memberikan beragam jawaban. Sebanyak 34% mengandalkan informasi dari media, 30% memperoleh pengetahuan melalui mata kuliah, dan 36% lainnya mendapatkan informasi dari sumber lain. Variasi ini menunjukkan bahwa mahasiswa mendapatkan informasi dari berbagai saluran, yang mencerminkan pentingnya pendekatan multi-channel dalam penyebaran informasi keamanan.

Tabel 4. Seberapa baik pemahaman anda tentang kebijakan keamanan yang terkait dengan BPSDM

	Frequency	Percent	Valid Percent	Cumulative Percent
Cukup Baik	26	52	52	52
Kurang Baik	12	24	24	76
Tidak tahu sama sekali	7	14	14	90
sangat baik	10	10	10	100
total	50	100	100	

Sumber: Hasil Penelitian (2024)

Pada tabel 4 menjelaskan Hasil bahwa 52% responden merasa memiliki pemahaman yang cukup baik tentang kebijakan keamanan yang terkait dengan BPSDM. Namun, 24% merasa kurang baik, dan 14% tidak tahu sama sekali. Hanya 10% yang merasa sangat baik. Ini menunjukkan bahwa meskipun ada pemahaman yang baik di kalangan sebagian besar mahasiswa, masih ada tantangan dalam memastikan bahwa semua individu memiliki pemahaman yang mendalam tentang kebijakan yang ada.

Tabel 5. Menurut anda,seberapa penting kebijakan keamanan dalam melindungi data dan asset di institusi?

	Frequency	Percent	Valid Percent	Cumulative Percent
Sangat penting	38	76	76	76
penting	10	20	20	96
tidak penting	2	4	4	100
total	50	100	100	

Sumber: Hasil Penelitian (2024)

Pada tabel 5 menjelaskan Ketika ditanya tentang pentingnya kebijakan keamanan dalam melindungi data dan aset di institusi, 76% responden menilai kebijakan tersebut sangat penting, sementara 20% menganggapnya penting. Hanya 4% yang merasa tidak penting. Hasil ini

menunjukkan kesadaran yang tinggi di kalangan mahasiswa tentang peran vital kebijakan keamanan dalam menjaga integritas dan kerahasiaan data.

Tabel 6. Apakah anda pernah mengikuti pelatihan atau sosialisasi mengenai kebijakan keamanan di BPDSM atau institusi lainnya

	Frequency	Percent	Valid Percent	Cumulative Percent
ya	39	78	78	78
tidak	11	12	12	100
total	50	100	100	

Sumber: Hasil Penelitian (2024)

Pada tabel 6 menjelaskan Sebanyak 78% responden mengaku pernah mengikuti pelatihan atau sosialisasi mengenai kebijakan keamanan di BPDSM atau institusi lainnya. Ini menunjukkan bahwa ada upaya yang signifikan untuk meningkatkan kesadaran dan pemahaman tentang keamanan informasi di kalangan mahasiswa. Namun, 12% yang tidak pernah mengikuti pelatihan menunjukkan bahwa masih ada kesempatan untuk menjangkau lebih banyak individu.

Tabel 7. Seberapa sering anda mempraktikkan prosedur keamanan, seperti melindungi data pribadi atau aset akedemik

	Frequency	Percent	Valid Percent	Cumulative Percent
selalu	42	42	42	42
kadang kadang	30	30	30	72
sering	20	20	20	92
tidak pernah	8	8	8	100
total	50	100	100	

Sumber: Hasil Penelitian (2024)

Pada tabel 7 menjelaskan Hasil survei menunjukkan bahwa 42% responden selalu mempraktikkan prosedur keamanan, seperti melindungi data pribadi atau aset akademik. Sementara 30% melakukannya kadang-kadang, 20% sering, dan 8% tidak pernah. Ini menunjukkan bahwa meskipun sebagian besar mahasiswa menyadari pentingnya praktik keamanan, masih ada tantangan dalam konsistensi penerapan prosedur tersebut.

3.4 Hasil Observasi

Observasi langsung menunjukkan bahwa BPDSM telah menerapkan beberapa praktik keamanan yang baik, seperti:

- Penggunaan sistem otentikasi ganda untuk akses data sensitif.
- Prosedur pengelolaan data yang jelas, meskipun ada beberapa area yang masih perlu diperbaiki, seperti pengawasan akses fisik ke ruang server.

3.5 Studi Dokumentasi

Analisis dokumen menunjukkan bahwa BPSDM memiliki kebijakan keamanan informasi yang tertulis, tetapi implementasinya belum sepenuhnya konsisten. Beberapa dokumen penting, seperti laporan audit keamanan, menunjukkan adanya beberapa pelanggaran yang perlu ditindak lanjuti.

3.6 Pembahasan

Hasil penelitian menunjukkan bahwa meskipun BPSDM telah memiliki kebijakan keamanan informasi, masih terdapat tantangan dalam implementasinya. Pemahaman pegawai tentang kebijakan keamanan informasi cukup baik, tetapi ada kebutuhan untuk meningkatkan sosialisasi dan pelatihan (Komedi & Ferianto, 2023).

Tantangan yang dihadapi, seperti kurangnya sumber daya dan pelatihan yang tidak memadai, dapat menghambat efektivitas kebijakan keamanan. Oleh karena itu, penting bagi BPSDM untuk mengembangkan program pelatihan yang lebih komprehensif dan berkelanjutan, serta meningkatkan komunikasi mengenai kebijakan keamanan informasi.

Praktik keamanan yang baik, seperti penggunaan sistem otentikasi ganda, menunjukkan bahwa BPSDM telah mengambil langkah positif, tetapi perlu ada pengawasan yang lebih ketat terhadap akses fisik dan prosedur pengelolaan data.

4. Kesimpulan

Berdasarkan hasil analisis, dapat disimpulkan bahwa meskipun Badan Pengembangan Sumber Daya Manusia (BPSDM) Provinsi Jawa Barat telah memiliki kebijakan dasar terkait keamanan informasi, implementasi kebijakan tersebut masih menghadapi berbagai tantangan yang signifikan. Secara umum, pemahaman karyawan terhadap kebijakan keamanan informasi dinilai cukup baik, menunjukkan bahwa ada upaya dalam memberikan panduan kepada para pegawai. Namun, terdapat kendala utama yang perlu mendapat perhatian, seperti pelatihan yang belum memadai, keterbatasan sumber daya untuk mendukung kebijakan, serta resistensi terhadap perubahan yang masih cukup kuat di beberapa bagian organisasi.

Selain itu, meskipun beberapa praktik keamanan informasi modern, seperti autentikasi ganda, telah diterapkan di beberapa aspek operasional, pengawasan fisik terhadap perangkat dan fasilitas, serta konsistensi dalam penerapan kebijakan, masih perlu ditingkatkan secara signifikan. Kelemahan dalam pengawasan fisik ini dapat membuka celah keamanan yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Dalam mendukung penguatan implementasi kebijakan, penelitian menunjukkan bahwa kesadaran tentang pentingnya keamanan informasi sudah cukup tinggi di kalangan karyawan, fakultas, dan mahasiswa. Namun,

sosialisasi lebih intensif masih diperlukan untuk memastikan semua pihak memahami peran dan tanggung jawab mereka dalam menjaga keamanan data institusi (Daeng et al., 2023).

Lebih jauh, hasil analisis juga mengungkapkan bahwa pelatihan terkait manajemen keamanan informasi yang dilakukan sejauh ini masih belum mencukupi untuk menghadapi tantangan teknologi yang terus berkembang. Oleh karena itu, upaya strategis diperlukan untuk merancang dan mengimplementasikan program pelatihan yang lebih komprehensif, mencakup berbagai aspek teknis dan non-teknis keamanan informasi. Pelatihan ini tidak hanya bertujuan untuk meningkatkan pemahaman teknis, tetapi juga untuk membangun budaya keamanan informasi yang kokoh di seluruh lapisan organisasi.

Untuk meningkatkan efektivitas implementasi kebijakan keamanan informasi, disarankan agar BPSDM mengambil langkah-langkah strategis, antara lain mengembangkan program pelatihan yang lebih terstruktur dan berkelanjutan, mempromosikan penyebaran informasi terkait kebijakan secara lebih luas, serta melakukan evaluasi berkala terhadap praktik manajemen keamanan informasi yang sudah diterapkan. Evaluasi berkala ini akan membantu mengidentifikasi celah atau kelemahan yang mungkin muncul, sehingga langkah korektif dapat segera diambil untuk meminimalkan risiko.

Selain itu, penting bagi BPSDM untuk meningkatkan alokasi sumber daya, baik dari segi anggaran, tenaga ahli, maupun infrastruktur pendukung keamanan informasi. Pendekatan ini dapat diperkuat dengan melibatkan berbagai pemangku kepentingan dalam penyusunan dan pelaksanaan kebijakan, sehingga tercipta rasa memiliki yang lebih besar terhadap inisiatif keamanan informasi. Dengan langkah-langkah ini, diharapkan institusi dapat memperkuat perlindungan data, mendukung manajemen tenaga kerja yang lebih berkelanjutan, serta membangun kepercayaan publik terhadap kredibilitas dan integritas organisasi secara keseluruhan.

Upaya yang terintegrasi dan konsisten ini juga diharapkan mampu menciptakan ekosistem kerja yang lebih aman dan produktif, sejalan dengan perkembangan teknologi dan tantangan global yang semakin kompleks di era digital saat ini.

Daftar Pustaka

- Daeng, Y., Levin, J., Razzaq Prayudha, M., Putri Ramadhani, N., Imanuel, S., & Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia Yusuf Daeng, A. (2023). Analisis Penerapan Sistem Keamanan Siber TerhadapKejahatan Siber Di Indonesia. *Journal Of Social Science Research*, 3(6), 1135–1145.
- Fathiyah. (2021). Jurnal prajaiswara bpsdm. *Jurnal Prahaiswara*, 2(November), 215–224. <https://prajaiswara.jambiprov.go.id>
- Flannero, F., Ferdinand, F., & Meitiana, M. (2022). Pengaruh lingkungan kerja dan motivasi terhadap kinerja melalui kepuasan kerja pegawai pada BPSDM Provinsi Kalimantan Tengah. *Journal of Environment and Management*, 3(3), 195–206. <https://doi.org/10.37304/jem.v3i3.5685>

- Halisa, N. N. (2020). Peran Manajemen Sumber Daya Manusia “Sistem Rekrutmen, Seleksi, Kompetensi dan Pelatihan” Terhadap Keunggulan Kompetitif: Literature Review. *ADI Bisnis Digital Interdisiplin Jurnal*, 1(2 Desember), 14–22.
<https://doi.org/10.34306/abdi.v1i2.168>
- Jerry, D., Irianto, A., Syauta, J. H., & Thane, S. (2024). *Pengaruh Pelatihan Dan Lingkungan Kerja Terhadap Kinerja Pegawai Dengan Kepuasan Kerja Sebagai Variable Intervening Pada Badan Pengembangan Sumber Daya Manusia Provinsi Papua*. 2(1), 43–49.
- Komedi, K., & Ferianto, J. (2023). Konsep Dan Terapan Pengembangan Sumber Daya Manusia Sektor Publik di Indonesia (Eksistensi Kelembagaan BPSDM). *Musamus Journal of Public Administration*, 6(1), 479–487. <https://doi.org/10.35724/mjpa.v6i1.5317>
- Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(5), 564–573.
<https://doi.org/10.31933/jemsi.v3i5.992>
- Putri, E. Y., Putri, A., Rahma, A. R., & Maolani, F. M. (2022). Penerapan Praktek Manajemen Sumber Daya Manusia Dan Hubungannya Dengan Kinerja Karyawan. *Jurnal Ekobis : Ekonomi Bisnis & Manajemen*, 12(2), 343–356. <https://doi.org/10.37932/j.e.v12i2.618>
- Romlah, S., Tinggi, S., Islam, A., & Bangil, P. (2021). Perbandingan Pendekatan Kualitatif dan Kuantitatif dalam Melakukan Penilaian Operasional. *Jurnal Studi Islam*, 16(1), 1–13.
- Soesanto, E., Saputra, F., Puspitasari, D., & Danaya, B. P. (2023). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher. *Jurnal Ilmu Multidisiplin*, 2(1), 23–29.
<https://doi.org/10.38035/jim.v2i1.221>