

PENERAPAN ANALISA RESIKO KEAMANAN INFORMASI PADA LAYANAN APLIKASI PPK KECAMATAN KEMBANGAN: WUJUDKAN JAKARTA TANGGUH DAN BERDAYA SAING

Nungky Awang Chandra^{1*}, Mohamad Yusuf², Inna Sabily³

^{1,2}Teknik Informatika, Universitas Mercu Buana, Jakarta, Indonesia

³Sistem Informas, Universitas Mercu Buana, Jakarta, Indonesia

mhd.yusuf@mercubuana.ac.id

nungky_awang@mercubuana.ac.id

inna.sabily@mercubuana.ac.id

Abstract

In the era of digital transformation, public services such as PPK (District Election Committee) Kembangan in Jakarta are not exempt from information security challenges. This digital transformation involves integrating advanced technology into daily operations and providing services to the public through digital platforms. As the use of digital systems increases, so does the risk of cyberattacks. PPK Kembangan may face attacks such as phishing, ransomware, denial-of-service attacks, or misuse of citizens' personal data, which could disrupt election processes or other district activities. To enhance prevention against threats and vulnerabilities in information security within PPK Kembangan's application services, a community service program was conducted through training for PPK Kembangan members. The results of this program showed that the training was successful, with participants demonstrating high enthusiasm. Participants actively asked questions regarding cases of information security attacks on both web-based and mobile applications. This program is expected to increase awareness of preventing cyber threats and vulnerabilities in PPK Kembangan's service applications, thereby minimizing the occurrence of such attacks.

Keywords:Digital Transformation; Information Security; Cyberattacks; PPK Kembangan ;Training

Abstrak

Di era transformasi digital, layanan publik seperti PPK Kembangan di Jakarta tidak luput dari tantangan keamanan informasi. Transformasi digital ini melibatkan pengintegrasian teknologi canggih ke dalam operasi sehari-hari dan penyediaan layanan kepada publik melalui platform digital. Seiring meningkatnya penggunaan sistem digital, risiko serangan siber juga meningkat. PPK Kembangan dapat menghadapi serangan seperti phishing, ransomware, serangan denial-of-service, atau penyalahgunaan data pribadi warga negara, yang dapat mengganggu proses pemilihan atau kegiatan distrik lainnya. Untuk meningkatkan pencegahan terhadap ancaman dan kerentanan keamanan informasi dalam layanan aplikasi PPK Kembangan, program pengabdian masyarakat dilakukan melalui pelatihan bagi anggota PPK Kembangan. Hasil dari program ini menunjukkan bahwa pelatihan berjalan dengan sukses, dengan peserta menunjukkan antusiasme yang tinggi. Peserta aktif mengajukan pertanyaan terkait kasus serangan keamanan informasi baik pada aplikasi berbasis web maupun aplikasi seluler. Program ini diharapkan dapat meningkatkan kesadaran untuk mencegah ancaman dan kerentanan siber pada aplikasi layanan PPK Kembangan, sehingga dapat meminimalkan terjadinya serangan tersebut.

Kata Kunci: Transformasi Digital; Keamanan Informasi; Serangan Siber; PPK Kembangan; Pelatihan

Pendahuluan

Penggunaan aplikasi layanan teknologi informasi dalam peningkatan layanan pemerintah sangat dibutuhkan saat ini. Layanan menggunakan aplikasi ini dapat di terapkan untuk layanan pemerintah tingkat pusat atau daerah. Layanan aplikasi untuk tingkat daerah seperti di PPK kecamatan akan membantu berbagai layanan. Berbagai layanan aplikasi ini dapat disediakan seperti pengaduan masyarakat, pengelolaan tanah, administrasi pertanahan, pengelolaan bangunan, dan

*Correspondent Author: mhd.yusuf@mercubuana.ac.id

media luar ruang. Dirancang untuk mempermudah proses perizinan dan administrasi, C-Mantap dapat diakses mudah melalui perangkat digital. Melalui layanan dengan menggunakan aplikasi digital di PPK kecamatan dapat memberikan solusi lengkap dan terpadu untuk berbagai kebutuhan yang dapat diakses oleh publik. Proses layanan dari manual ke transformasi digital ini berkembang dengan cepat (Verhoef et al., 2021), terutama dalam sektor pelayanan publik yang semakin mengintegrasikan teknologi informasi ke dalam operasionalnya (Juliyandri Saragih & Darmeli Nasution, 2024). Pertumbuhan ini memang membawa banyak keuntungan seperti efisiensi dan aksesibilitas yang lebih besar, namun di sisi lain juga meningkatkan risiko keamanan siber yang dihadapi oleh infrastruktur digital. Keamanan siber menjadi tantangan kritis karena sistem yang lebih terbuka dan terhubung cenderung lebih rentan terhadap serangan siber (Admass et al., 2024).

Transformasi digital juga membutuhkan infrastruktur yang kompleks dan strategi keamanan yang lebih robust dan adaptif dalam menghadapi ancaman serangan dan kerentanan keamanan siber (Rizvi et al., 2025; Wang et al., 2024). Ancaman yang meningkat ini memerlukan perhatian khusus terhadap cara data disimpan, diakses, dan dilindungi. Kebijakan dan regulasi keamanan siber yang kuat sangat diperlukan untuk melindungi data penting dan memastikan kelancaran layanan publik yang tergantung pada teknologi informasi (Muhammad Alfi et al., 2023; Novera Kristianti & Ririn Kurniasi, 2024). Penelitian yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN, 2012) menunjukkan bahwa pada semester pertama tahun 2024, serangan siber di Indonesia meningkat secara signifikan, yaitu sebanyak enam kali lipat dibandingkan dengan periode yang sama di tahun sebelumnya. Total serangan yang tercatat melebihi 2,4 miliar insiden. Data ini menunjukkan betapa kritisnya keadaan keamanan siber di negara ini.

Peningkatan kesadaran dan edukasi keamanan siber untuk para pemangku kepentingan di sektor pelayanan publik juga penting sebagai bagian dari strategi keamanan yang menyeluruh. Ini termasuk pelatihan reguler, penerapan praktik terbaik dalam keamanan siber, dan investasi dalam teknologi keamanan terus berkembang. Pendekatan ini tidak hanya melindungi infrastruktur tetapi juga membangun kepercayaan masyarakat terhadap layanan digital yang disediakan oleh PPK Kecamatan. Untuk meningkatkan kesadaran akan pencegahan serangan keamanan siber pada aplikasi layanan PPK kecamatan ini, Universitas Mercu Buana menyelenggarakan program Pengabdian kepada Masyarakat (PkM) yang berfokus pada pelatihan penerapan analisa resiko keamanan informasi untuk aplikasi layanan PPK kecamatan Kembangan terutama untuk tim Pemberdayaan dan Kesejahteraan Keluarga (PKK). Dengan program diharapkan dapat memberikan manfaat bagi tim PKK, terutama tim yang menggunakan layanan berbasis aplikasi untuk memiliki kesadaran akan tindakan pencegahan akan bahaya ancaman serangan siber dan ketentanan dalam mengakses aplikasi untuk aktivitas operasional sehari-hari. Pemahaman pencegahan serangan keamanan siber melalui analisa resiko keamanan informasi yang berbasis ISO/IEC 27005 : 2025 ini membantu tim PKK dalam pengelolaan informasi, pengembangan aplikasi, dan peningkatan efisiensi operasional secara aman.

Perlu juga dijelaskan secara eksplisit bentuk partisipasi dan interaksi dengan masyarakat dalam *program community engagement*. Dalam memperkuat latar belakang penelitian atau kegiatan, penulis dituntut untuk menambahkan latar belakang empiris dan kerangka/latar belakang konseptual yang dikonstruksi dari tinjauan studi sebelumnya yang relevan yang diterbitkan selambat-lambatnya 5 tahun. Tujuan dari program PkM Universitas Mercu Buana ini juga dapat meningkatkan partisipasi masyarakat dan memperkuat kerja sama antara akademisi dan komunitas dalam menciptakan solusi berbasis teknologi yang berkelanjutan. Salah satu tri dharma perguruan tinggi Universitas Mercu Buana adalah pengabdian masyarakat maka Universitas Mercu Buana selalu berkomitmen untuk memberikan kontribusi dalam pemberdayaan masyarakat, khususnya di Kelurahan kembangan jakarta barat, melalui pemanfaatan teknologi informasi secara tepat dan sesuai.

Metode Pelaksanaan

Adapun metode kegiatan pelaksanaan pengabdian masyarakat di PPK kecamatan Kembangan Jakarta barat, dibagi beberapa materi sosialisasi penerapan analisa keamanan informasi untuk aplikasi layanan PPK kecamatan kembangan sebagai berikut :

Tabel 1. Metode Pelaksanaan dan Evaluasi Kegiatan Pengabdian Kepada Masyarakat

No.	Kegiatan	Peserta	Metode		Indikator Keberhasilan
			Pelaksanaan	Evaluasi	
1	Melakukan Sosialisasi atau penyuluhan tentang ancaman serangan dan kerentanan keamanan informasi pada aplikasi layanan PPK kecamatan	PKK	Presentasi interaktif dengan menjelaskan materi analisa resiko keamanan informasi pada aplikasi layanan PPK	Diskusi dan tanya jawab kepada peserta	▪ Peserta aktif bertanya atau feedback ▪ Tingkat kehadiran
2	Workshop	PKK	▪ Sesi tanya jawab ▪ Praktek Analisa Resiko Keamanan informasi pada aplikasi layanan	Hasil evaluasi pelaksanaan analisa resiko keamanan informasi pada aplikasi layanan PPK	Peningkatan kemampuan peserta hasil tanya jawab
3	Review pelaksanaan Sosialisasi pada kegiatan PkM	PKK	Survey feedback pelaksanaan sosialisasi	Hasil survey dari peserta tentang pelaksanaan sosialisasi PkM	Jumlah antusias mengisi hasil survey feedback peserta dan hasil positif

Hasil dan Pembahasan

a. Pelaksanaan Kegiatan

Pelaksanaan kegiatan pengabdian masyarakat dilakukan pada tanggal 19-20 Februari 2025 dengan cara sosialisasi dan pelatihan aplikasi dan analisa resiko keamanan informasi untuk aplikasi layanan PPK. Sosialisasi dan Pelatihan dilaksanakan 09.00 WIB sampai pukul 16.00 WIB. Adapun flyer kegiatan pengabdian masyarakat dapat ditunjukkan pada gambar 1.



Gambar 1. Flyer Kegiatan Pengabdian Kepada Masyarakat

Dalam kegiatan pengabdian kepada masyarakat di kecamatan Kembangan Jakarta Barat dihadiri oleh camat kecamatan Kembangan Jakarta barat, tim kader dan Kelompo pembinaan dan kesejahteraan keluarga (PKK). Kegiatan ini dilakukan sesuai jadwal pada gambar 2. Kegiatan PPK kecamatan Kembangan Jakarta Barat.

JADWAL KEGIATAN:

- **Hari/Tanggal** : Rabu & Kamis, 19 & 20 Februari 2025
- **Waktu**
- Day 1
- **Sesi 1 (08.00 – 10.00 WIB) (Inna, Yunita)**
- **Sesi 2 (10.00 – 12.00 WIB) (Mae, Nia)**
- Day 2
- **Sesi 1 (08.00 – 10.00 WIB) (Rushendra, Suhendra)**
- **Sesi 2 (10.00 – 12.00 WIB) (Yusuf, Abdul, Nungky)**

Gambar 2. Agenda Pengabdian Kepada Masyarakat Kecamatan Kembangan

Agenda sosialisasi dan pelatihan analisa resiko keamanan informasi layanan aplikasi PPK dilakukan pada hari ke-2, memakan waktu setengah hari, yaitu terdiri dari:

- 1) Pemaparan materi analisa resiko keamanan informasi layanan aplikasi PPK kecamatan Kembangan Jakarta barat
- 2) Praktek studi kasus analisa resiko keamanan informasi berdasarkan kerangka ISO/IEC 27005 : 2025 layanan aplikasi PPK kecamatan Kembangan Jakarta Barat
- 3) Diskusi dan Tanya jawab terkait kasus ancaman serangan dan kerentanan keamanan informasi pada aplikasi layanan sehari hari di PPK kecamatan Kembangan Jakarta Barat

b. Hasil Kegiatan

Hasil kegiatan pengabdian masyarakat dilakukan pada tanggal 19-20 Februari 2025 adalah sebagai berikut :

- 1) Dari 35 peserta yang diundang 100 % hadir dan aktif dalam berdiskusi
- 2) Peserta mampu memahami cara identifikasi ancaman serangan seperti malware, phishing, ransomware, dan lainnya pada aplikasi layanan PPK kecamatan
- 3) Peserta mampu melakukan analisa resiko kemungkinan, dampak serangan sr serta mitigas pengendalian keamanan infomasi pada aplikasi layanan PPK kecamatan
- 4) Peserta mengisi survey secara positif dan bermanfaat dalam meningkatkan pemahaman dan kesadaran akan resiko keamanan informasi aplikasi layanan PPK
- 5) Dari 35 peserta yang diundang 100 % hadir dan aktif dalam berdiskusi
- 6) Peserta mampu memahami cara identifikasi ancaman serangan seperti malware, phishing, ransomware, dan lainnya pada aplikasi layanan PPK kecamatan

c. Evaluasi Kegiatan

Evaluasi kegiatan pengabdian masyarakat dilakukan pada tanggal 19-20 Februari 2025 adalah sebagai berikut :

- 1) Sesi diskusi dan tanya jawab merupakan salah satu bagian penting dalam kegiatan pengabdian masyarakat ini. Setelah penyampaian materi utama tentang analisa resiko keamanan informasi pada aplikasi layanan publik, peserta diberi kesempatan untuk berdiskusi aktif dan mengajukan pertanyaan secara langsung kepada narasumber. Antusiasme peserta terlihat dari banyaknya pertanyaan dan pendapat yang disampaikan, terutama terkait praktik pengamanan data pada aplikasi layanan PPK Kecamatan. Peserta tidak hanya bertanya, tetapi juga berbagi pengalaman

mereka dalam menghadapi potensi serangan siber, sehingga suasana diskusi menjadi dinamis dan interaktif. Moderator berperan efektif dalam mengatur alur diskusi, memastikan bahwa setiap peserta mendapat kesempatan untuk berbicara, serta membantu merangkum pertanyaan-pertanyaan yang muncul agar dapat dijawab secara komprehensif oleh narasumber. Beberapa poin penting yang dihasilkan dari sesi diskusi dan tanya jawab antara lain:

- a) Peningkatan Pemahaman Praktis: Peserta menjadi lebih memahami langkah-langkah konkret untuk mendeteksi dan mencegah ancaman seperti malware, phishing, dan ransomware di lingkungan kerja mereka.
- b) Identifikasi Kebutuhan Tambahan: Beberapa peserta mengusulkan perlunya pelatihan lanjutan mengenai pengelolaan keamanan data dan penggunaan alat proteksi siber sederhana.
- c) Tantangan Lapangan: Diskusi mengungkapkan bahwa di beberapa kecamatan, masih terdapat keterbatasan dalam hal infrastruktur keamanan teknologi, yang menjadi tantangan tersendiri dalam menerapkan praktik terbaik yang telah diajarkan.

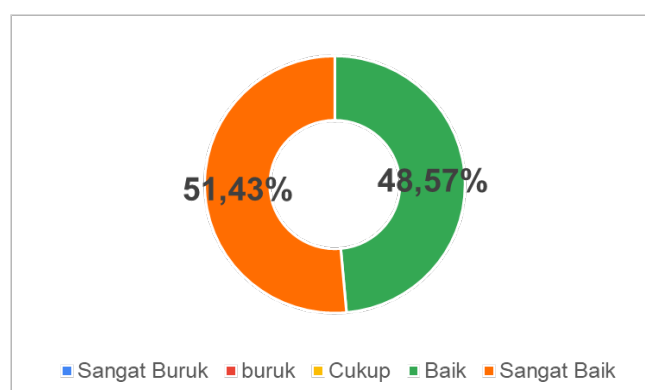
Secara umum, sesi diskusi dan tanya jawab berjalan sangat baik. Keterlibatan peserta tinggi, relevansi pertanyaan sesuai dengan tema yang dibahas, dan waktu yang disediakan hampir seluruhnya dimanfaatkan dengan optimal.

- 2) Workshop analisa risiko keamanan informasi pada aplikasi layanan PPK Kecamatan diselenggarakan sebagai bagian dari upaya meningkatkan kesadaran dan kapasitas pengelolaan keamanan sistem layanan publik di tingkat kecamatan. Workshop ini bertujuan untuk membekali peserta dengan kemampuan dalam mengidentifikasi aset informasi penting, memahami potensi ancaman siber, serta menyusun langkah-langkah mitigasi risiko berdasarkan prinsip keamanan informasi. Workshop dilaksanakan dengan melibatkan 35 peserta yang berasal dari berbagai kecamatan. Kegiatan ini dibagi menjadi dua sesi utama, yaitu penyampaian materi teori terkait analisa risiko keamanan informasi berbasis standar ISO/IEC 27005:2022, dan sesi praktik analisa risiko menggunakan studi kasus nyata pada aplikasi layanan PPK. Seluruh peserta hadir tepat waktu dan menunjukkan partisipasi aktif selama kegiatan berlangsung. Diskusi kelompok, tanya jawab, serta simulasi analisa risiko berjalan dinamis dan produktif. Berdasarkan hasil evaluasi pelaksanaan workshop, diperoleh beberapa poin penting sebagai berikut:
 - a) Tingkat Kehadiran dan Partisipasi: Tingkat kehadiran mencapai 100%, dengan peserta aktif berinteraksi dalam sesi diskusi, simulasi, dan berbagi pengalaman terkait masalah keamanan informasi yang mereka hadapi di lapangan.
 - b) Peningkatan Pemahaman: Sebagian besar peserta mampu memahami konsep dasar analisa risiko, mengidentifikasi aset informasi kritis, serta mengenali berbagai ancaman potensial seperti malware, phishing, ransomware, dan kesalahan internal (human error).
 - c) Kemampuan Praktis: Melalui sesi simulasi, peserta dapat menerapkan teknik analisa risiko sederhana, seperti penilaian dampak dan kemungkinan (impact and likelihood assessment), serta membuat rekomendasi mitigasi risiko.
 - d) Identifikasi Kebutuhan Tambahan: Peserta mengusulkan perlunya pelatihan lanjutan tentang penerapan kontrol keamanan teknis (seperti firewall, enkripsi, dan sistem monitoring) untuk memperkuat hasil analisa risiko yang telah dilakukan.
- 3) Sebagai bagian dari upaya evaluasi dan perbaikan berkelanjutan, dilakukan survei kepada seluruh peserta yang mengikuti kegiatan Pengabdian kepada Masyarakat. Survei ini bertujuan untuk mendapatkan umpan balik terkait efektivitas pelaksanaan kegiatan, relevansi materi, metode penyampaian, serta kepuasan peserta secara keseluruhan. Survei dilakukan menggunakan kuesioner yang disebarkan kepada seluruh peserta di akhir kegiatan. Kuesioner terdiri dari pertanyaan pilihan ganda dan isian terbuka yang mencakup beberapa aspek berikut:
 - a) Kualitas materi yang disampaikan
 - b) Keterampilan fasilitator/pemateri

- c) Relevansi kegiatan dengan kebutuhan peserta
- d) Tingkat kepuasan secara keseluruhan
- e) Saran dan masukan untuk kegiatan selanjutnya
- f) Jumlah responden yang mengisi survei sebanyak 35 orang atau
- g) 100% dari total peserta.

Hasil survei menunjukkan bahwa kegiatan pengabdian masyarakat ini telah memenuhi harapan sebagian besar peserta. Tingkat kepuasan yang tinggi menunjukkan bahwa materi, metode, dan penyampaian telah sesuai dengan kebutuhan. Namun, terdapat permintaan yang cukup besar untuk memperluas materi pada sesi berikutnya, khususnya terkait praktik pengamanan data dan sistem aplikasi. Adapun hasil survey kepada 35 peserta PkM sebagai berikut :

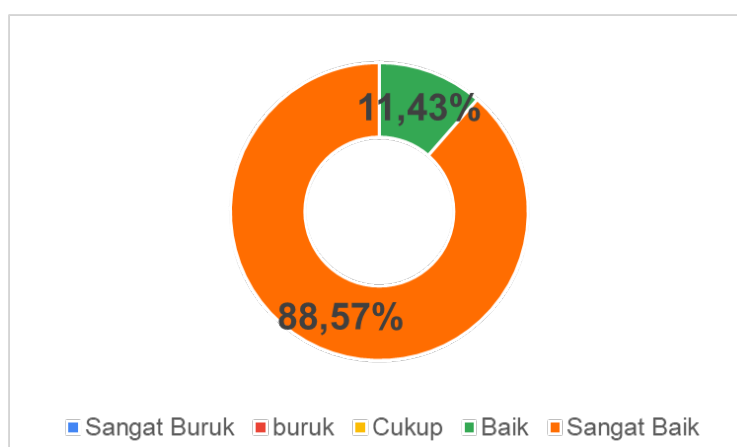
a) Penjelasan Materi Nara Sumber



Gambar 3. Hasil survey ke 35 peserta PPK kecamatan Kembangan Jakarta Barat tentang penjelasan materi yang disampaikan dalam pelatihan pelaksanaan pengabdian masyarakat (PkM)

Hasil survey tentang penjelasan materi pelatihan PkM menunjukan bahwa 51,43 % peserta menyatakan sangat puas dan 48,57 % menunjukkan puas. Tidak ada peserta yang menyatakan pelaksanaan cukup sampai sangat buruk.

b) Kepuasan Pelaksanaan kegiatan Pengabdian kepada Masyarakat (PkM)



Gambar 4. Hasil survey ke 35 peserta PPK kecamatan Kembangan Jakarta Barat tentang kepuasan pelaksanaan pengabdian masyarakat (PkM)

Hasil survey tentang penjelasan materi pelatihan PkM menunjukan bahwa 88,57 % peserta menyatakan sangat puas dan 11,43 % menunjukkan puas. Tidak ada peserta yang menyatakan pelaksanaan cukup sampai sangat buruk.

Pelaksanaan kegiatan pengabdian masyarakat berupa sosialisasi dan pelatihan analisa risiko keamanan informasi di Kecamatan Kembangan menunjukkan keberhasilan dalam meningkatkan kapasitas peserta, khususnya kader PKK, dalam mengenali serta mengelola ancaman keamanan siber. Hal ini sejalan dengan temuan Verhoef et al. (2021), yang menekankan bahwa transformasi digital dalam sektor publik menuntut peningkatan literasi digital dan kapasitas pengelolaan risiko sebagai elemen penting dalam menjaga keberlanjutan layanan. Penggunaan kerangka kerja ISO/IEC 27005:2022 dalam pelatihan memberikan dasar metodologis yang kuat dalam identifikasi aset informasi, penilaian kemungkinan dan dampak, serta penetapan langkah mitigasi, sebagaimana disarankan oleh Rizvi et al. (2025), yang menyatakan bahwa penerapan standar internasional sangat penting untuk penguatan keamanan informasi dalam era digital.

Evaluasi kegiatan juga menunjukkan bahwa interaksi aktif peserta melalui diskusi, studi kasus, dan simulasi praktik menjadi faktor kunci dalam keberhasilan pelatihan. Kegiatan ini tidak hanya meningkatkan kesadaran akan pentingnya keamanan data tetapi juga mendorong partisipasi masyarakat secara langsung dalam perlindungan sistem informasi publik. Seperti dijelaskan oleh Admass et al. (2024), edukasi berkelanjutan dan keterlibatan pengguna merupakan strategi penting dalam membangun budaya keamanan siber yang adaptif dan berkelanjutan. Selain itu, hasil survei yang menunjukkan tingkat kepuasan tinggi memperkuat temuan Muhammad Alfi et al. (2023), bahwa penguatan kapasitas lokal melalui pelatihan berbasis komunitas menjadi pendekatan strategis dalam menghadapi eskalasi serangan siber yang kini semakin kompleks dan masif di lingkungan pemerintahan daerah.

Kesimpulan dan Saran

Sosialisasi dan Pelatihan analisa penilaian resiko keamanan informasi dengan kerangka ISO/IEC 27005 : 2022 untuk aplikasi layanan PPK Kecamatan Kembangan Jakarta Barat berhasil meningkatkan pemahaman dan kesadaran tim PKK tentang identifikasi dan analisa ancaman serangan dan kerentanan serangan keamanan informasi untuk aplikasi layanan PPK. Sehingga resiko ancaman keamanan siber dapat dicegah dan dikurangi. Peserta sangat antusias dan puas atas pelaksanaan PkM dan kedepan peserta meminta ada lanjutan dari program kerja sama dengan pihak terkait.

Ucapan Terimakasih

Puji serta syukur kita panjatkan Kehadirat Allah SWT Tuhan Yang Maha Esa atas segala Rahmat dan KeberkahanNya sehingga kegiatan Pengabdian Kepada Masyarakat ini berjalan lancar dan bermanfaat. Kami juga mengucapkan terima kasih kepada Fakultas Ilmu Komputer Universitas Mercu Buana dan Pusat Pengabdian Masyarakat Universitas Mercu Buana yang telah memberikan support dana kegiatan. Tema yang dipilih dalam kegiatan PkM ini “Transformasi Digital untuk Pemberdayaan Masyarakat : Mewujudkan Jakarta Global yang Tangguh, Inklusif, Berdaya Saing, dan Berkelanjutan”.

Referensi

- Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031. <https://doi.org/10.1016/j.csa.2023.100031>
- Juliyandri Saragih, & Darmeli Nasution. (2024). Boost Public Service Productivity with Effective IT Governance. *International Journal of Industrial Innovation and Mechanical Engineering*, 1(4), 54–68. <https://doi.org/10.61132/ijime.v1i4.103>
- Muhammad Alfi, Ni Putu Yundari, & Ahnaf Tsaqif. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*, 6(2). <https://doi.org/10.7454/jkskn.v6i2.10082>

- Novera Kristianti, & Ririn Kurniasi. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma: Jurnal Ilmu Hukum*, 7(1), 297–310. <https://jurnal.univpgri-palembang.ac.id/index.php/satyadharm/article/view/10759>
- Rizvi, I., Raj, S., & Singh, V. (2025). Cybersecurity in the Digital Age. In *Technology for Societal Transformation* (pp. 131–148). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-1721-0_8
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, 104051. <https://doi.org/10.1016/j.cose.2024.104051>