JURNAL CAHAYA NUSANTARA
Vol. 1, No. 2 (2025): 86-92, EISSN: 3093-8113
Journal Homepage: https://jurnal.cahayapublikasi.com/index.php/jcn

Pembinaan peningkatan kapasitas SDM tim tanggap insiden siber pemerintah daerah Provinsi Banten

M. Yusron[1]
[1]*Universitas Primagraha, Indonesia*

Penulis Korespondensi: M. Yusron, **E-mail**: muhammadyusron.albueti@gmail.com

Abstrak
Era transformasi digital selain memiliki manfaat yang dapat membantu memudahkan pekerjaan tetapi juga terdapat dampak negatifnya, Sebagai Sumber Daya Manusia penyelenggara organisasi perlu memiliki kapabilitas dan kompetensi dibidang teknologi untuk dapat melakukan kesiapan yang matang dalam menghadapi tantangan era transformasi dan dampaknya dengan membentuk Tim yang bertugas menangani insiden siber. Hasil kajian menunjukkan bahwa pelatihan berbasis simulasi, sertifikasi profesional, serta program kesadaran keamanan siber secara berkelanjutan berkontribusi signifikan terhadap peningkatan kompetensi kapasitas SDM TTIS.

Kata Kunci
Pembinaan, Peningkatan Kapasitas, SDM

Naskah diterima : Februari 2025 *Naskah disetujui : Februari 2025* *Terbit : Februari 2025*

1. PENDAHULUAN

Saat ini telah memasuki era transformasi digital dimana kehadiran internet segala aktivitas telah dilakukan secara digitalisasi dan online. Keberadaan internet telah menciptakan suatu revolusi tersendiri di berbagai sektor, Para pengguna internet semakin lama semakin meningkat jumlahnya. dan saat ini internet menjadi kebutuhan pokok sebagaimana peran telekomunikasi dalam kehidupan sehari-hari. faktor resiko terbesar adalah terjadinya insiden keamanan siber yang tidak diinginkan baik yang dilakukan secara sengaja maupun tidak disengaja (csirt.bantenprov.go.id yang diakses pada 2025)

SDM adalah kebijakan dan praktik yang dibutuhkan oleh organisasi untuk mengelola aspek-aspek kepersonaliaan, termasuk perekrutan, pelatihan, penilaian, serta kompensasi (Gary Dessler (2013)

Menurut Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional, pembinaan merupakan bagian dari upaya pendidikan untuk meningkatkan kualitas sumber daya manusia. Dalam konteks organisasi atau instansi, pembinaan sering dikaitkan dengan upaya meningkatkan kompetensi dan profesionalisme anggota atau pegawainya.

Peningkatan kapasitas, atau capacity building, adalah proses yang bertujuan untuk meningkatkan kemampuan individu, kelompok, organisasi, atau masyarakat dalam menjalankan fungsi mereka secara efektif, efisien, dan berkelanjutan. Proses ini mencakup pengembangan keterampilan, pengetahuan, sikap, serta penguatan struktur dan sistem organisasi. Pentingnya pengembangan SDM diselenggarakan bukan saja untuk ketahanan organisasi, tetapi juga kepercayaan publik terhadap informasi yang dikeluarkan oleh pemerintah.

Saat ini segala bentuk proses penyelenggaraan pemerintahan sudah berbasis elektronik. Kerentanan terhadap data dan informasi pemerintah dengan mudah di akses secara umum oleh

masyarakat serta penggunaan berbagai layanan pemerintahan sudah secara online dengan hadirnya berbagai aplikasi berbasis web maupun aplikasi dimana tingkat keamanannya harus dijamin. Namun permasalahannya SDM yang menangani hal tersebut sangat minim sehingga hanya mengandalkan beberapa orang saja. Kebanyakan penanganan insiden hanya bergantung pada satu orang admin yang dianggap menguasai sistem. Terkadang dikarenakan keterbatasan pengetahuan dan kapabilitas maka sering kali suatu aplikasi yang terkena serangan siber bukannya dilakukan prosedur penanggulangan dan pemulihan alih-alih dilakukan penonaktifan atau take down, sambil menunggu "bala bantuan" datang, baik menggunakan konsultan keamanan IT atau dari pihak yang dianggap lebih berkompeten (Alfikri & Ahmad, 2022).

Untuk mengantisipasi peningkatan insiden serangan siber di Pemerintah Provinsi Banten, diperlukan pembentukan Tim Tanggap Insiden Siber (TTIS) yang juga dikenal sebagai BantenProv-CSIRT, guna menghadapi dan menangani berbagai ancaman darurat keamanan siber. Sehingga terbit Keputusan Gubernur Banten Nomor 46.05/Kep.151-Huk/2022 tentang Tim Tanggap Insiden Siber Pemerintah Daerah Provinsi Banten. TTIS melaksanakan pemberian peringatan mengenai keamanan siber; perumusan panduan teknis untuk penanganan kejadian siber; Pencatatan setiap laporan atau aduan yang diterima; penyediaan rekomendasi langkah penanganan awal kepada pihak yang terdampak; pemilihan (triage) insiden siber berdasarkan kriteria yang ditetapkan untuk memprioritaskan insiden yang akan ditangani; penyelenggaraan koordinasi penanganan kejadian siber kepada pihak yang berkepentingan; serta pelaksanaan fungsi lainnya sesuai kebutuhan dan kerentanan sistem elektronik. Pembentukan TTIS merupakan amanat Program Prioritas Nasional RPJMN Bapenas 2020-2024 tentang peningkatan keamanan dan ketahanan siber. (csirt.bantenprov.go.id yang diakses pada 2025)

Untuk dapat memberikan kapasitas peningkatan pengetahuan SDM tentang peran nya di bidang penanganan insiden maka perlu mengikuti berbagai kegiatan ketahanan siber baik yang diselenggarakan oleh daerah provinsi banten maupun instansi pusat seperti BSSN dan Komdigi maupun Lembaga-lemabga lainnya seperti pelatihan, bimbingan teknis, workshop dan berbagai kegiatan lainnya.

2. METODE

Kajian ini menggunakan pendekatan metode deskriptif analitik, menurut Ratna (20212) menyatakan bahwa metode deskriptif analitik dilakukan dengan cara mendeskripsikan fakta-fakta, kemudian disusul dengan analisis. Secara etimologis, deskripsi dan analisis berarti menguraikan. Dengan berlandaskan teori dan alat analisis, peneliti menerapkan cara-cara penafsiran dengan menyajikannya dalam bentuk deskripsi. Data yang digunakan yaitu data sekunder yaitu berupa laporan, dokumen dan informasi dari website Diskominfo-SP, serta beberapa kajian ilmiyah dan jurnal penelitian

3. HASIL DAN PEMBAHASAN

Pemerintah Provinsi Banten menyediakan layanan TTIS yang dinamakan BantenProv-CSIRT dan diperuntukan kepada semua konstituen sesuai dengan RFC-2350, yang mencakup Perangkat Daerah se-Provinsi Banten. Adapun Visi TTIS adalah mewujudkan pelayanan keamanan dan ketahanan siber yang responsip dan professional dilingkungan Pemerintah Provinsi Banten. Serta misi yaitu:

a. Membangun, mengkoordinasikan, mengkolaborasikan dan mengoperasionalkan system mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber dilingkungan Pemerintah Provinsi Banten.
b. Membangun kerja sama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber dalam rangka penanggulangan dan pemulihan insiden keamanan siber di lingkungan Pemerintah Provinsi Banten.
c. Membangun kapasitas sumber daya penganggulangan dan pemulihan insiden keamanan siber di lingkungan Pemerintah Provinsi Banten.
d. Optimalisasi layanan dalam rangka penanggulangan dan pemulihan insiden siber.

Dalam penyelenggaraannya, TTIS berkolaborasi TTIS lainnya baik ditingkat pusat maupun daerah serta instansi vertical agar dapat bersama-sama menjaga asset negara dari oknum yang ingin mengambil keuntungan pribadinya. TTIS membuka layanan portal aduan siber dan menghimbau kepada pegawai internal maupun masyarakat luar untuk dapat melaporkan insiden siber jika terdapat gangguan atau tidak berjalannya sistem elektronik milik Pemerintah Provinsi Banten ke alamat https://csirt.bantenprov.go.id/

Penyelenggaraan TTIS di bentuk melalui instruksi dari Badan Siber dan Sandi Negara (BSSN) yang dibentuk dan launching pada tahun 2021 yang berakhir sampai dengan Desember 2021, kemudian diperbaharui dan terbit kembali melalui Keputusan Gubernur Banten Nomor 46.05/Kep.151-Huk/2022 tentang Tim Tanggap Insiden Siber Pemerintah Daerah Provinsi Banten.

Dasar Hukum

Amanah dibentuknya Tim Tanggap Insiden Siber TTIS Pemerintah Daerah Provinsi Banten berdasarkan beberapa dasar hukum sebagai berikut:

1). Peraturan Presiden Nomor 18 Tahun 2020 Rencana Pembangunan Jangka Menengah Nasional 2020-2024
2). Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 Tentang Tim Tanggap Insiden Siber
3). Berdasarkan Surat Kepala Badan Siber dan Sandi Negara:
   a) Nomor: 1959/BSSN/D3/PP.01.07/08/2020 tanggal 28 Agustus 2020 tentang Pemberitahuan Jadwal Kegiatan Asistensi Pembentukan CSIRT
   b) Nomor: T.01/KA.BSSN/PP.01.07/01/2021 tanggal 05 Januari 2021 tentang Penunjukan Instansi Pemerintah dalam Program CSIRT Tahun 2021
   c) Nomor T.02.1/BSSN/D3/PP.01.07/01/2020 tanggal 5 Januari 2021 tentang Persiapan Pembentukan CSIRT Tahun 2021
   d) T.04/BSSN/D3/PP.01.07/01/2021 tanggal 6 Januari 2021 tentang Pemberitahuan Jadwal Kegiatan Persiapan Pembentukan CSIRT Tahun 2021
4). Keputusan Gubernur Banten Nomor 046.05/Ke.96-Huk/2021 tentang Pembentukan Tim Tanggap Insiden Keamanan Komputer Pemerintah Daerah Provinsi Banten.

Fungsi TTIS

Fungsi utama yang diselenggarakan berupa :

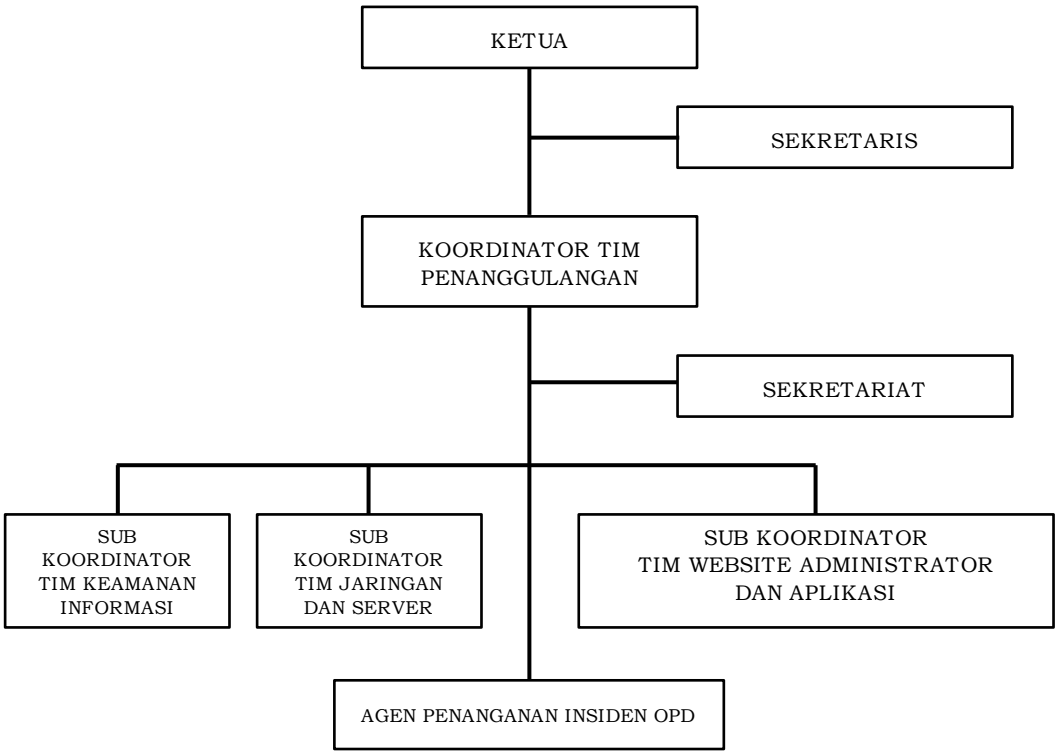
1) Pemberian peringatan terkait keamanan siber untuk penyampaian peringatan mengenai informasi anomali atau ancaman siber kepada seluruh konstituen. Pada pemberian peringatan ini diperoleh berdasarkan:
   a) Notifikasi peringatan dari BSSN.
      BSSN mengirimkan notifikasi melalui email serta alternatif melalui pesan kepada narahubung Banten Prov-CSIRT.
   b) Aduan Siber.
      Terjadi banyak aduan siber dari pengguna Sistem Elektronik, dimana pelapor diharuskan mengisi formulir aduan siber agar dapat diketahui identitas pelapor dan juga jenis serangannya. Aduan siber ini dapat melalui email atau melalui kontak alternatif narahubung.
   c) Monitoring.
      TTIS BantenProv-CSIRT telah rutin memberikan peringatan apabila informasi anomali atau ancaman siber kepada keseluruhan OPD melalui sistem monitoring Wazuh yang sudah terpasang pada semua aset milik OPD. Peringatan tersebut diberikan dalam bentuk laporan dan mewajibkan bagi pemilik aset untuk memberikan feedback berupa tindak lanjut atas peringatan terkait informasi anomali atau ancaman siber yang telah diberikan. Masih terdapat kerentanan pada website dan aplikasi dimana kondisi tersebut dikarenakan belum dilakukannya pentest secara berkala. Dari laporan aduan siber yang diterima langsung

diteruskan ke tim teknis guna dilakukan pencegahan timbulnya dampak dari insiden tersebut serta dilakukan pemulihan sesuai dengan urutan aduan siber yang masuk.

2) Perumusan panduan teknis penanganan Insiden Siber
TTIS BantenProv-CSIRT melakukan identifikasi dan perumusan panduan teknis yang disesuaikan dengan kondisi saat ini, adapun hasil identifikasi panduan teknis diperoleh 3 panduan teknis yang harus dibuat yaitu, panduan teknis penanganan insiden Web Defacement, Ransomware, dan DDOS. Hal ini dilandasi karena seringnya terjadi insiden siber web Defacement, Ransomware, maupun DDOS pada server. Dari hasil identifikasi tersebut perumusan panduan teknis tersebut sedang dalam tahap penyusunan dan perumusan (dtaft), dan panduan teknis.
3) Pencatan laporan/aduan serta pemberian rekomendasi untuk langkah penanganan awal kepada pihak yang terdampak

Struktur Organisasi Tim Tanggap Insiden SIber

Berdasarkan Keputusan Gubernur Banten Nomor 46.05/Kep.151-Huk/2022 tentang Tim Tanggap Insiden Siber Pemerintah Daerah Provinsi Banten yaitu:



Gambar 1. Struktur Organisasi TTIS (BantenProv-CSIRT)

Langkah-langkah strategis dalam peningkatan kapasitas SDM

Pentingnya meningkatkan kapasitas SDM guna menghadapi ancaman digital yang semakin kompleks. Maka diperlukan Langkah strategis berikut ini:

a. Penyusunan Kebijakan dan Regulasi
Penyusunan kebijakan berupa peraturan tentag Sistem Manajemen Keamanan Informasi, Standar Operasional Prosedur serta aturan lainnya yang diperlukan dalam menetapkan standar kompetensi SDM ketahanan siber.
b. Pelatihan dan Sertifikasi
Agar SDM TTIS memiliki kapasitas pengetahuan dan pengelolaan teknologi diadakan bimbingan teknis, workshop, knowledge sharing rutin. Salah satunya mendorong SDM untuk memperoleh

sertifikasi internasional seperti CEH *(Certified Ethical Hacker),* CISSP *(Certified Information Systems Security Professional),* atau CISA *(Certified Information Systems Auditor).*

Tabel 1: macam-macan peningkatan kapasitas SDM Tahun 2024

No	Nama Kegiatan	Jenis Kegiatan	Penyelenggara
1	Pelatihan Manajemen Risiko keamanan bagi PSE	Pelatihan	Pusbang BSSN
2	Pelatihan Penyusunan Kebijakan Sistem Manajemen Keamanan Informasi bagi PSE Publik	Pelatihan	Pusbang BSSN
3	Pelatihan Audit Keamanan bagi PSE Publik	Pelatihan	Pusbang BSSN
4	Pelatihan dan Sertifikasi Junior Penetration Tester	Pelatihan	Pusbang BSSN
5	Pelatihan dan Sertifikasi Asisten Auditor Keamanan Informasi	Pelatihan	Pusbang BSSN
6	Pelatihan dan Sertifikasi Level 1 Security Operations Center Analyst	Pelatihan	Pusbang BSSN
7	Pelatihan dan Sertifikasi Incident Response Analyst	Pelatihan	Pusbang BSSN
8	Pelatihan dan Sertifikasi Associate Digital Evidence First Responde	Pelatihan	Pusbang BSSN
9	Pelatihan Cyber Security Fundamental	Pelatihan	Pusbang BSSN
10	Pelatihan Cyber Security Insident Response	Pelatihan	Pusbang BSSN
11	Pelatihan Dark Web Investigation	Pelatihan	Pusbang BSSN
12	Pelatihan Perlindungan Data Pribadi	Pelatihan	Pusbang BSSN
13	Pelatihan dan Sertifikasi Auditor Keamanan Informasi	Pelatihan	Pusbang BSSN
14	Pengelolaan CSIRT/TTIS	Bimtek	BSSN
15	Workshop Cyber security	Workshop	Diskominfo-SP Provinsi Banten
16	Security Awareness pada sector layanan public	Bimtek	Diskominfo-SP Provinsi Banten
17	Ketahanan Insiden	Bimtek	Diskominfo-SP Provinsi Banten
18	Drill test kesiapsiagaan	Bimtek	Diskominfo-SP Provinsi Banten
19	Strategi Kebijakan Diskominfo dalam keamanan Informasi	Bimtek	Diskominfo-SP Provinsi Banten
20	Diskusi pakar The esential	Diskusi pakar / sharing knowledge	Diskominfo-SP Provinsi Banten
21	One trust security	Diskusi pakar / sharing knowledge	Diskominfo-SP Provinsi Banten
22	Zero trust security	Diskusi pakar / sharing knowledge	Diskominfo-SP Provinsi Banten
23	Workshop Cyber Security	Workshop	Swiss German University
24	Pelatihan Keamanan SPBE	Daring	Kemenkominfo

Sumber: Diskominfo-SP Provinsi Banten

c. Pengecekan Keamanan Siber
   Melakukan pengecekan keamanan siber melalui (Cyber Drill test) secara berkala. Serta mengadakan uji coba penetrasi sistem (Penetration Testing) untuk mengidentifikasi celah keamanan.
d. Kolaborasi dengan Pihak-pihak lainnya
   Bekerja sama dengan institusi akademik dan perusahaan serta Mengikuti komunitas dan forum keamanan siber seperti OWASP, FIRST, atau ISACA.

e. Pengembangan Budaya Keamanan Siber
   Meningkatkan kesadaran keamanan siber di kalangan pegawai dengan melakukan penyampaian informasi dan peringatan-peringatan keamanan informasi serta mengedukasi pengguna tentang pentingnya praktik keamanan seperti penggunaan password yang kuat dan deteksi phishing.
f. Pemanfaatan Teknologi AI dan Automasi
   Menggunakan sistem deteksi ancaman berbasis AI dan Machine Learning. Mengembangkan sistem keamanan otomatis untuk menangani insiden siber dengan cepat.

Pelaksanaan pengembangan SDM berupa pelatihan, bimtek, workshop dan kegiatan lainnya.

Tujuan keluaran peningkatan kapasitas SDM

Peningkatan kapasitas Sumber Daya Manusia (SDM) dalam ketahanan siber menghasilkan beberapa dampak positif, antara lain:

1. Peningkatan Kompetensi Teknis: Pelatihan dan sertifikasi yang diberikan meningkatkan pemahaman SDM dalam keamanan siber, seperti deteksi ancaman, respons insiden, dan pemulihan sistem.
2. Kesadaran Keamanan Siber: SDM lebih sadar akan pentingnya keamanan informasi, termasuk penggunaan sandi yang kuat, enkripsi data, serta identifikasi dan mitigasi ancaman.
3. Efektivitas Penanganan Insiden: Dengan pelatihan yang tepat, tim keamanan siber dapat merespons serangan lebih cepat dan mengurangi dampak yang ditimbulkan.
4. Peningkatan Kolaborasi dan Koordinasi: SDM yang terlatih lebih mampu bekerja sama dengan tim internal maupun eksternal untuk mengatasi ancaman siber secara kolektif.
5. Penguatan Kebijakan dan Regulasi: SDM yang memiliki wawasan lebih baik dapat membantu dalam perumusan kebijakan keamanan yang lebih efektif dan sesuai dengan standar industri.

Faktor Penentu Utama

Beberapa faktor utama yang mempengaruhi peningkatan kapasitas SDM dalam ketahanan siber, melalui pelatihan dan dapat dilakukan melalui berbagai metode, seperti:

a. Workshop dan Simulasi: Menyediakan pengalaman langsung dalam menangani ancaman siber.
b. Sertifikasi Profesional: Seperti CISSP, CEH, atau CISM yang memberikan standar kompetensi di bidang keamanan siber.
c. E-learning dan Webinar: Mempermudah akses bagi SDM untuk belajar secara fleksibel.
d. Simulasi Red Team vs. Blue Team: Latihan serangan dan pertahanan untuk meningkatkan keterampilan teknis dalam keamanan siber.

Tantangan

Beberapa hal yang menjadi tantangan Tim TTIS peningkatan kapasitas meliputi:

a. Kurangnya SDM yang Berkualitas: Kebutuhan tenaga ahli siber semakin meningkat, sementara jumlah tenaga terampil masih terbatas.
b. Perubahan Teknologi yang Cepat: Ancaman dan teknologi keamanan siber terus berkembang, sehingga SDM harus terus memperbarui pengetahuan mereka.
c. Kurangnya Kesadaran Manajemen: Tidak semua organisasi menyadari pentingnya investasi dalam pengembangan SDM ketahanan siber.
d. Anggaran Terbatas: Pelatihan dan sertifikasi sering kali membutuhkan biaya yang tinggi, yang bisa menjadi hambatan bagi organisasi kecil dan menengah.

Untuk mengatasi tantangan di atas diperlukan penerapan strategi berikut:

a. Meningkatkan Program Pendidikan dan Pelatihan: Kolaborasi dengan universitas, lembaga pelatihan, dan industri untuk membangun kurikulum keamanan siber yang relevan.

b. Mendorong Sertifikasi Profesional: Memberikan insentif bagi SDM untuk mendapatkan sertifikasi keamanan siber yang diakui secara global.
c. Membangun Budaya Keamanan Siber di Organisasi: Mengadakan pelatihan rutin bagi seluruh karyawan untuk meningkatkan kesadaran keamanan siber.
d. Memanfaatkan Teknologi AI dan Otomasi: Penggunaan teknologi AI dan otomatisasi dalam deteksi ancaman dapat membantu mengurangi beban kerja SDM keamanan siber.

4. SIMPULAN

Peningkatan kapasitas SDM Tim Tanggap Insiden Siber Pemerintah Provinsi Banten sangat penting untuk menghadapi berbagai ancaman siber yang semakin kompleks dan terus yang dapat mengancam ketenangan dan kenyamanan pegawai dilingkungan Pemerintah Provinsi Banten. Dengan pendekatan pelatihan yang tepat, kebijakan yang mendukung, serta pemanfaatan teknologi yang canggih, SDM dapat lebih siap dalam mengamankan sistem informasi dan data organisasi. Namun, tantangan seperti kurangnya tenaga ahli, perubahan teknologi yang cepat, dan keterbatasan anggaran harus diatasi melalui strategi yang berkelanjutan dan kolaborasi antar sektor.

PUSTAKA ACUAN

Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. Matra Pembaruan: Jurnal Inovasi Kebijakan, 6(1), 1-14.

Diskominfo-SP Provinsi Banten, Tim Tanggap Insiden SIber (BantenProv-CSIRT) www.csirt.bantenprov.go.id

Keputusan Gubernur Banten Nomor 46.05/Kep.151-Huk/2022 tentang Pembentukan Tim Respons Insiden Siber

Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber:

Ratna (2012) Metodologi Penelitian: Kajian Budaya dan Ilmu Sosial HUmaniora pada umum. Yogyakarta: Pustaka Pelajar

Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional