e-ISSN: 2549-7952
p-ISSN: 2580-3336

Sistem Informasi Survey Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Metode Multiple Criteria Decision Analisys (MCDA)

Gadang Putro Bagus Setiyawan[1], Risa Helilintar[2],Resty Wulanningrum[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri
E-mail: [1] gpbase.gp@gmail.com, *[2]risa.helilintar@gmail.com, [3]restyw@unpkdr.ac.id

Abstrak – *Kesadaran terhadap keaanan informasi menjadi salah satu faktor yang sangat penting dalam pemfaatan teknologi dan informasi. Insiden Keamanan informasi akan terjadi akibat dari jika tingkat kesadaran masih rendah. Penelitian ini melakukan pengukuran tingkat kesadaran keamanan informasi terhadap Karyawan Dinas Komunikasi dan Informatika Kota Kediri . Tujuan dari penelitian ini untuk mebangun sebuah tools yang digunakan untuk mengetahui tingkat kesadaraan keamanan informasi karyawan dengan demikian maka dapat digunakan mendukung kebijakan terkait dengan keamanan dan informasi Sehingga harus mendapat perhatian khusus dan perlu suatu tindakan yang nyata untuk mendukung karyawan dalam melakukan peningkatan level kesadaran informasi . Metode yang digunakan adalah metode Multiple Criteria Decision Analysis (MCDA) dengan menggunakan enam area pengukuran dan tiga dimesi pembobotan yaitu pengetahuan, sikap dan perilaku. Bahasa pemrogaman menggunakan PHP dan database MySQL. Dari data yang diperoleh pada penelitian dapat diketahui nilai tertinggi ada pada jawaban Setuju dengan skor 868, Sangat setuju dengan skor 596, Netral dengan skor 343, Tidak Setuju dengan skor 89 dan Sangat Tidak Setuju dengan skor 54. Selain itu kita dapat ketahui kecenderungan dalam 7 area semua user lebih cenderung dan kuat pada Menyadari Konsekuensi setiap tindakan bahwa user menyadarai bahwa dari setiap tindakan yang akan dilakukan maka akan menimbulkan konsekuensi pada dirinya.*

Kata Kunci *— Keamanan Informasi, MCDA, Area, PHP dan MySql*

1. PENDAHULUAN

Keamanan informasi adalah sekumpulan metodologi, praktik, ataupun proses yang dirancang dan diterapkan untuk melindungi informasi atau data pribadi dari akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak sah. Keamanan informasi bertujuan untuk melindungi data pada berbagai tahap, baik itu ketika proses menyimpan, mentransfer, atau menggunakannya. Keamanan informasi merupakan suatu perlindungan informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah untuk memberikan kerahasiaan, integritas, dan ketersediaan informasi. Sedangkan keamanan cyber adalah kemampuan untuk melindungi atau mempertahankan penggunaan cyber space dari serangan cyber. Pada tahun 2018 Pemerintah mengeluarkan Peraturan PresidenNomor 95 Tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), maka untuk mendukung adanya perubhana regulasi dari Pemerintah Pusat, Pmerintah Kota Kediri kemudian merombak kembali Struktur Organisasi pada Dinas Komunikasi dan Informatika sesuai dengan Peraturan Walikota Kediri Nomor 41 Tahun 2019 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi dan Informatika Kota Kediri maka ada perubahan yang terjadi pada Salah Satu Bidang, yang sebelumnya bernama Bidang Penyelenggaraan E-Gov menjadi Bidang Aplikasi Informatika, ada perubahan disalah satu seksi yang sebelumnya yaitu Seksi Sandi dan Telekomunikasi berubah nama menjadi Persandian dan Keamanan Informasi.

Kenapa Keamanan Informasi menjadi salah satu nama seksi karena sesuai dengan Peraturan Presiden Nomor 95 Tahun 2018 Tentang SPBE mengatur khusus terkait tentang arsitektur, road map dan manajemen keamanan informasi yang harus diterapkan baik oleh Pemerintah Pusat dan Pemerintah Daerah. Selain itu untuk mendukung Peraturan Presiden Nomor 95 Tahun 2018 Pemerintah Kota Kediri membuat aturan turunannya yaitu Peraturan Walikota Nomor 42 Tahun 2019 Tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).

2. METODE PENELITIAN

Dalam melakukan penelitian penyusun menggunakan metode-metode sebagai berikut

1. Pendekatan dan Teknik Penelitian

Pendekatan yang sesuai adalah pendekatan kuantitatif. Pemaparan teknik (ragam) penelitian dan pendekatan penelitian yang digunakan. (Teknik penelitian yang sesuai adalah penelitian pengembangan / rekayasa teknologi informasi).

2. Prosedur Penelitian
   a. Studi Pustaka
      Mencari buku-buku, data-data Internet dan Jurnal tentang Keamanan Informasi dan Bagaimana cara untuk melakukan Pengukuran Keamanan Informasi
   b. Pemetaan Data

e-ISSN: 2549-7952
p-ISSN: 2580-3336

Melakukan pemetaan data yang akan digunakan dalam penyusunan perangkat lunak dan penulisan laporan

c. Simulasi dan Penyusunan Perangkat Lunak
Melakukan simulasi sederhana terkait dengan metode yang akan digunakan dalam penelitian dan melakukan penyusunan perangkat lunak yang akan digunakan.
d. Analisa dan Pengujian serta Evaluasi
Melakukan analisa dan pengujian untuk perangkat lunak yang telah dibuat untuk mendapatkan hasil sesuai dengan yang diharapkan oleh penyusun
e. Penulisan Laporan
Melakukan penulisan laporan untuk semua kegiatan yang dilakukan

Kemanan Informasi

Menurut McLeod dan Schell [1] keamanan informasi ditujukan untuk mencapai tiga tujuan utama yaitu kerahasiaan, ketersediaan dan integritas. Menurut Whitman dan Mattord [2] keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut Whitmandan Mattord [2], Security Awareness adalah kontrol/aturan yang dirancang untuk mengurangi insiden pelanggaran terhadap keamanan informasi, akibat dari kelalaian maupun tindakan yang telah direncanakan. Menurut Kruger & Kerney [3], menggunakan teori psikologi sosial membagi tiga komponen untuk mengukur objek yakni cognition, affection dan behaviour. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai Knowledge (pengetahuan seseorang), Attitude (sikap seseorang) dan Behaviour (perilaku seseorang)[4].

Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal terkait informasi atau berusaha meminimalisasi kerusakan akibat tindak kriminal tersebut. Inilah yang disebut dengan keamanan informasi. Sederhananya, keamanan informasi menghargai nilai informasi dan melindunginya. Terkait keamanan informasi, dikenal istilah 4R keamanan informasi yakni: Right Information (Informasi yang benar), Right People (Orang yang tepat), Right Time (Waktu yang tepat) dan Right Form (Bentuk yang tepat). Pengaturan 4R adalah cara paling efisien untuk memelihara dan mengontrol nilai informasi [5].

Right Information mengacu pada ketepatan dan kelengkapan informasi yang menjamin integritas informasi. Right People berarti informasi tersedia hanya bagi individu yang berhak yang menjamin kerahasiaan. Right Time mengacu pada aksesibilitas informasi dan penggunaannya atas permintaan entitas yang berhak, ini menjamin ketersediaan. Sedangkan Right Form mengacu pada penyediaan informasi dalam format yang tepat. Untuk menjaga keamanan informasi, 4R harus digunakan dengan tepat. Ini berarti bahwa kerahasiaan, integritas dan ketersediaan haruslah ditinjau ketika menangani informasi[5].

Keamanan sistem informasi tidak hanya melibatkan kontrol keamanan teknis, namun juga melibatkan kontrol administratif, prosedural dan manajerial [6]. Cara pengguna (karyawan, manajer, personel IT) dalam menggunakan sistem informasi organisasi memainkan peranan penting dalam menjaga kelangsungan aset informasi perusahaan. Kesadaran keamanan adalah bidang ilmu keamanan yang berhubungan erat dengan faktor manusia mengenai keamanan aset informasi. Pengetahuan yang diperoleh dari sekolah adalah elemen utama untuk menciptakan kesadaran keamanan.

Sangat penting untuk mengimplementasikan peraturan keamanan. Chief Security Officer bertanggung jawab untuk melakukan program pembelajaran dan atau mengimplementasikan elemen keamanan pada program pembelajaran Teknologi Informasi. Program pelatihan dan kesadaran keamanan dapat dibagi dalam tiga bagian yang berbeda [7].

3. HASIL DAN PEMBAHASAN

Multiple Criteria Decision Analysis (MCDA). Pada tahun 2011 Warlina, Rusdiyanto, Sumartono, & Sawir telah mengunakan beberapa alternatif untuk mengambil keputusan yang mengambil konsep *MCDA* tersebut. Dalam rangka untuk merancang instrument ini, akan ada beberapa kriteria yang menjadi dasar untuk mengukur nilai total alternatifnya maka penulis menggunakan metode *MCDA* ini.. Metode tersebut sesuai dari penelitian [8] 1) membedakannya menjadi 3 kategori yaitu *Value measurement models*; 2) Model perangkingan; dan 3) *Goal programming[3]*. Dalam melakukan perancangan ini menggunakan penulis akan mencoba menggunakan model *value measurement* (pengukuran nilai) yang akan digunakan untuk mengukur tingkat kesadaran keamanan informasi.
Dalam perancangan ini persamaan yang digunakan adalah berikut sebagai berikut

$$V_{(a)} = \sum_{i=1}^{n} v_{i(a)} w_i \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

4.

Dimana V(a) adalah nilai seluruh alternatif a, v_i (a) adalah nilai skor yang mewakili erformansi alternatifa, dan w_i adalah bobot yang diberikan untuk menggambarkan tingkat kepentingan kriteria i.

Nilai v_i (a) ditentukan berdasarkan kuesioner. Tiga Puluh Lima pertanyaan telah di desain dalam kuesioner untuk menguji pengetahuan, sikap dan perilaku responden berkaitan dengan enam area

e-ISSN: 2549-7952
p-ISSN: 2580-3336

kesadaran keamanan informasi yang memiliki resiko yang sangat kritis yaitu

Tabel 1.1. Enam Area

No	Nama Area
1	Selalu tatat pada aturan
2	Menjaga kerahasian password dan Personal Identity Number(PIN)
3	Menggunakan email dan internet dengan bijaksana
4	Berhati-hati menggunakan perangkat seluler
5	Melaporkan insiden keamanan informasi
6	Menyadari Konsekuensi setiap tindakan
	Dan Ditambahkan1 Area Sesuai Indeks Kami BSSN
7	Selalu membackup data

Setiap pertanyaan diberikan jawaban dengan 5 skala: Sangat Setuju, Setuju, Netral, Tidak Setuju, Sangat Tidak Setuju.

Tabel 1.2. Pembobotan Dimensi

Dimesi	**Bobot**
Penngtahuan	30
Sikap	20
Perilaku	50

Penentuan bobot w_i untuk masing-masing deimensi pengetahuan, sikap dan perilaku ditentukan berdasarkan skala pembobotan yang digunakan oleh Kruger & Kerney[9]. Pembobotan ketiga dimensi tersebut ditunjukkan pada Tabel 2. 2

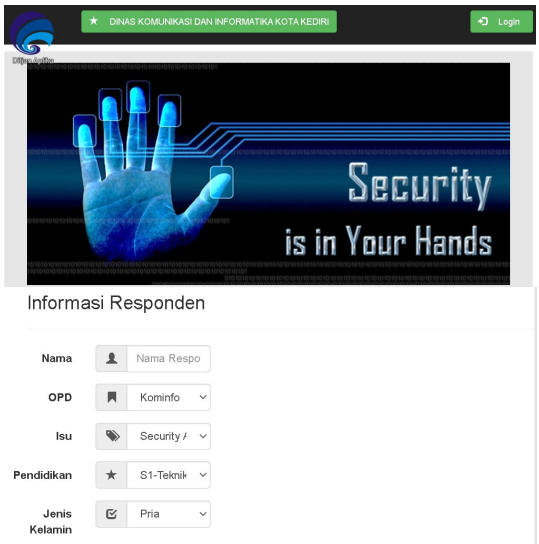
Skala tingkat kesadaran keamanan informasi ditentukan ke dalam tiga tingkatan, yaitu: buruk, sedang dan baik. Penentuan skala ditunjukkan pada Gambar 2.3 Skala ini juga digunakan oleh Kruger & Kerney[10] dalam mengukur kesadaran keamanan informasi di sebuah perusahaan tambang.

Tabel 1.3. Skala Tingkat kemanan Informasi

Nama Skala	**Prosentase Skala**
Baik	80 – 100%
Sedang	60 – 79%
Buruk	0 – 59%

a. Modul Input Data dan Modul Login
   Modul Input Data akan menampilkan tombol untuk login, apabila terjadi proses klik ada tombol login tersebut maka modul login akan melakukan proses sesuai dengan instruksi yang ada pada coding program. Jika terjadi kesalahan pada proses input maka modul login akan memproses notifikasi error
1. Modul Login dan Modul Admin
   Modul login merupakan pintu masuk untuk menuju ke modul admin, jika modul login melakukan proses, sesuai dengan user dan password yang digunakan oleh Admin maka modul login akan memproses dan mengarahkan pada modul admin jika user dan password yang dimasukkan adalah Admin
2. Modul Login dan Modul Super Admin
   Modul login merupakan pintu masuk untuk menuju ke modul super admin, jika modul login melakukan proses, sesuai dengan user dan password yang digunakan oleh Super Admin maka modul login akan memproses dan mengarahkan pada modul admin jika user dan password yang dimasukkan adalah Super Admin
3. Modul Input Data dan Modul Admin dan Super Admin
   Modul Input data akan memproses semua data yang ada, setelah data yang ada di proses kemudian data dan informasi tersebut yang diperoleh akana ditampilkan pada Modul Admin dan Super Admin.

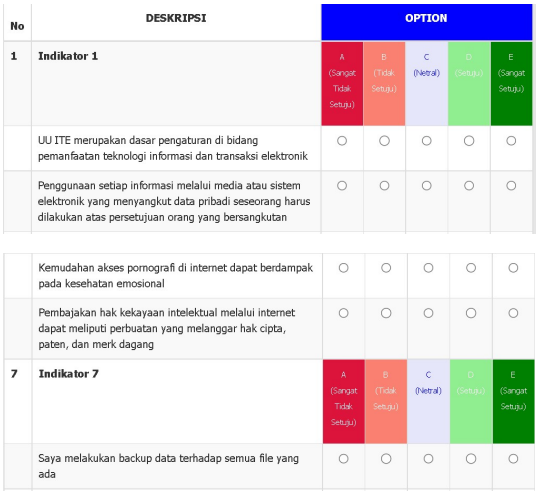
Sistem informasi survey ini akan memproses biodata dan jawaban dari kuisioner yang telah dijawab, selanjutnya akan di proses dan menghasilkan suatu nilai terkait tentang Sikap, Pengetahuan dan Perilaku dari user, kemudian data-data itu bisa diajadikan rujukan untuk mengetahui tingkat kesadaran keamanan informasi buruk, sedang atau baik.



Gambar 1.1 Halaman Utama Bagian 1

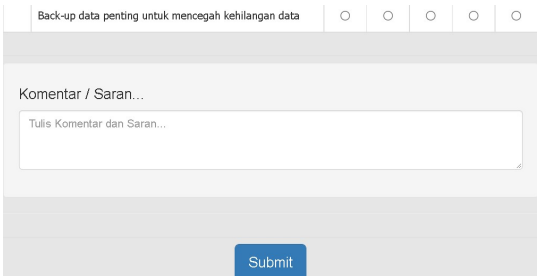
Gambar 1.1 adalah merupakan tampilan utama pada Sistem Informasi Survey pada bagian 1 ini menampilakan Informasi respoden dan tombol login untuk admin. Data dari respoden harus diisi agar bisa diproses.

e-ISSN: 2549-7952
p-ISSN: 2580-3336



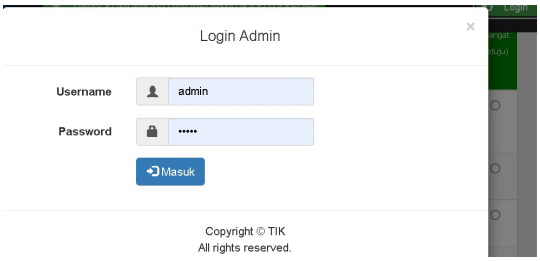
Gambar 1.2 Halaman Utama Bagian 2

Gambar 1.2 adalah merupakan tampilan utama pada Sistem Informasi Survey pada bagian 1 ini menampilakan informasi daftar pertanyaan yang harus dijawab oleh respoden yang merupakan hasil 7 area.



Gambar 1.3 Halaman Utama Bagian 3

Gambar 1.3 adalah merupakan tampilan utama pada Sistem Informasi Survey pada bagian 3 ini menampilakan informasi daftar pertanyaan yang harus dijawab oleh respoden yang merupakan hasil 7 area dan komentar/ saran.

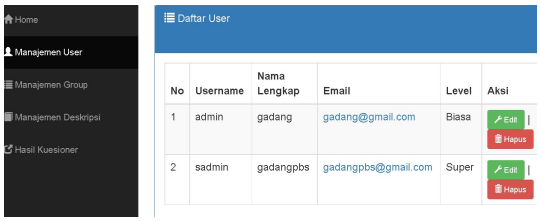


Gambar 1.4 Halaman Utama Bagian 3

Pada halaman utama terdapat tombol login, jika tombol login ditekan maka akan keluar menu untuk melakukan login. Hanya admin dan super admin saja yang bisa melakukan login.

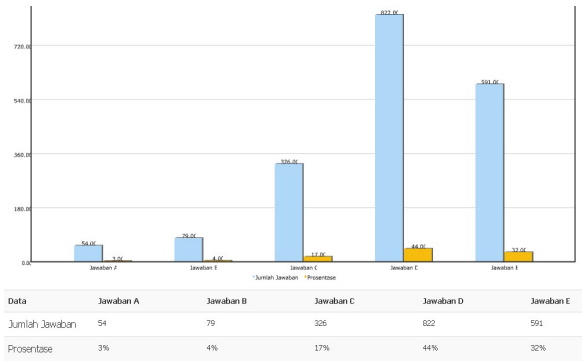
Gambar 1.5 Notifikasi Logout

Gambar 1.5 diatas adalah notifikasi yang akan diperlihatkan saat admin melakukan logout dari aplikasi



Gambar 1.6 Tampilan Menu Admin

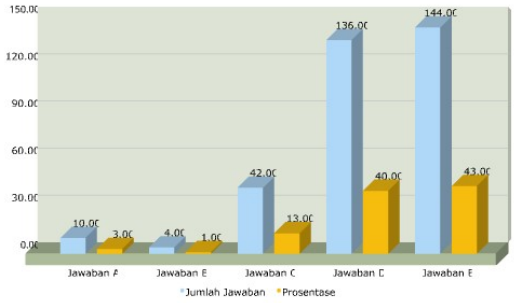
Gambar 1.6 diatas adalah tampilan halaman admin, tugas admin disini hanya bisa menampilkan hasil dari kuisioner dan rekap laporan hasil kuisioner. Seperti yang ditunjukan pada gambar-gambar berikut ini



Gambar 1.7 Grafik Kuisioner Keseluruhan

Gambar 1.7 Diatas adalah tampilan grafik untuk hasil keseluruhan pada Sistem Informasi Survey ini. Dengan rincian jawaban sebagai berikut sangat tidak setuju 54 jawaban dengan prosentase 3%, tidak setuju 79 jawaban dengan prosentase 4%, netral 326 jawaban dengan prosentase 17 %, setuju 622 jawaban dengan prosentase 44%, setuju 591 jawaban dengan prosentase 42%.

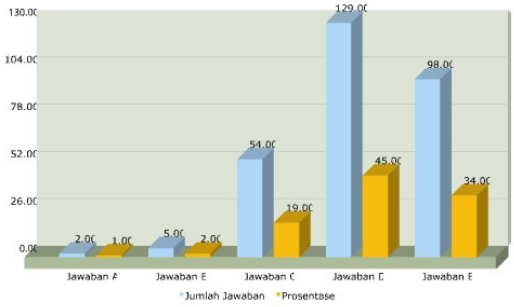
e-ISSN: 2549-7952
p-ISSN: 2580-3336



Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	10	4	42	136	144
Prosentase	3%	1%	13%	40%	43%

Gambar 1.8 Area Aturan

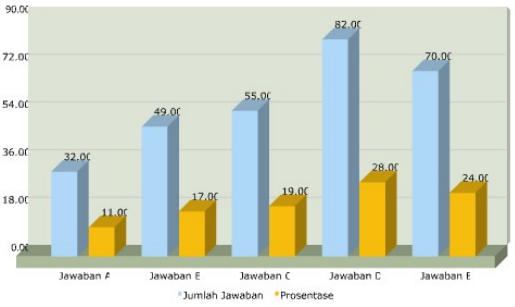
Gambar 1.8 adalah tampilan grafik dari hasil area aturan



Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	2	5	54	129	98
Prosentase	1%	2%	19%	45%	34%

Gambar 1.9 Area Pasword

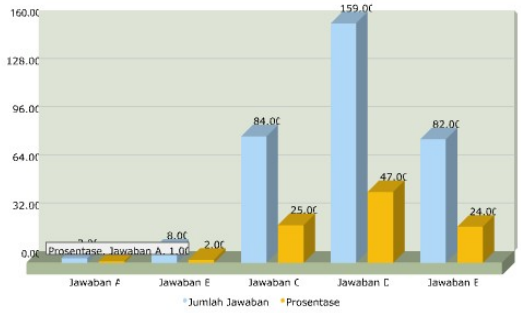
Gambar 1.9 adalah tampilan grafil hasil dari area Pasword



Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	32	49	55	82	70
Prosentase	11%	17%	19%	28%	24%

Gambar 1.10 Area Email dan Internet

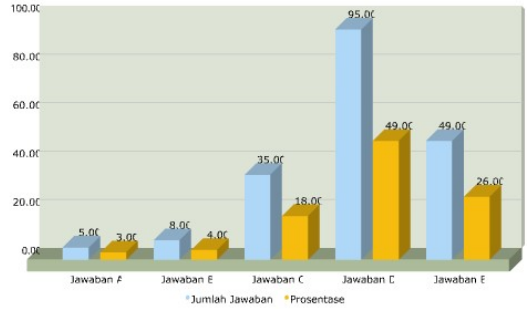
Gambar 1.9 adalah tampilan grafil hasil dari area Email dan Internet



Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	3	8	84	159	82
Prosentase	1%	2%	25%	47%	24%

Gambar 1.11 Area Seluler

Gambar 1.11 adalah tampilan grafil hasil dari area Seluler

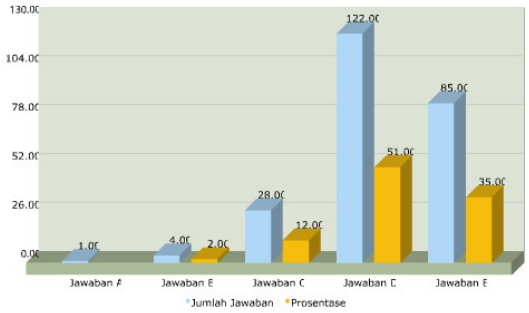


Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	5	8	35	95	49
Prosentase	3%	4%	18%	49%	26%

Gambar 1.12 Area Insiden

Gambar 1.12 adalah tampilan grafil hasil dari area Insiden

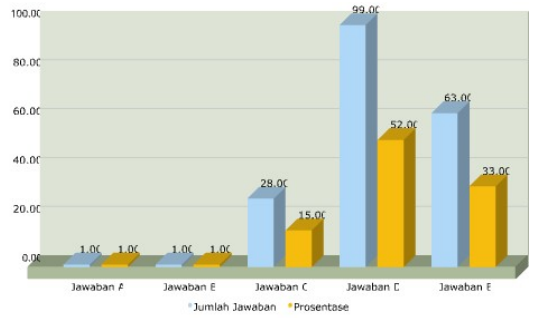
e-ISSN: 2549-7952
p-ISSN: 2580-3336



Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	1	4	28	122	85
Prosentase	0%	2%	12%	51%	35%

Gambar 1.13 Area Kosekuensi Tindakan

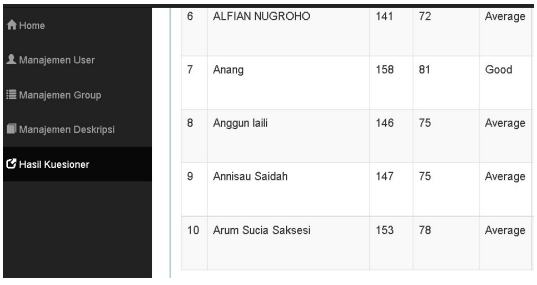
Gambar 1.13 adalah tampilan grafil hasil dari area Kosekuensi Tindakan



Data	Jawaban A	Jawaban B	Jawaban C	Jawaban D	Jawaban E
Jumlah Jawaban	1	1	28	99	63
Prosentase	1%	1%	15%	52%	33%

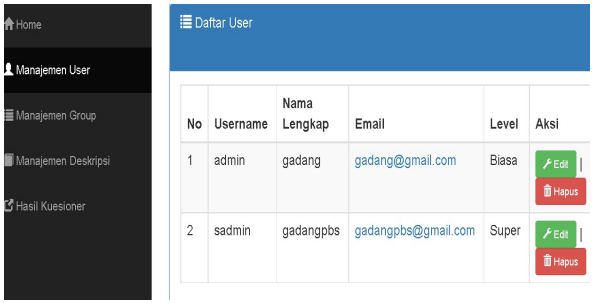
Gambar 1.14 Area Backup data

Gambar 1.14 adalah tampilan grafil hasil dari area Backup data



Gambar 1.15 Hasil Bobot dan Prosentase

Gambar 1.15 diatas adalah gambar yang menampilkan bobot dari hasil jawaban pertanyaan 7 area, prosentase dan level kesadaran keamanan informasi dari masing-masing individu yang melakukan survey.



Gambar 1.16 Manajemen User

Gambar manajemen user berfungsi untuk admin melakukan pengelolaan terhadap user yang ada pada aplikasi ini

Gambar 1.17 Gambar Manajemen Grup

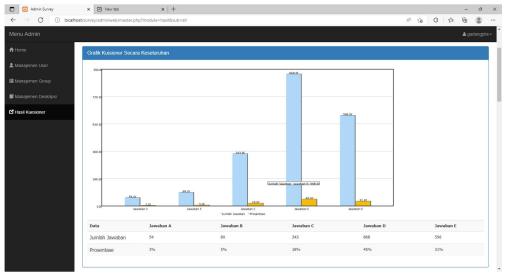
Gambar Manajemen Grup berfungsi untuk admin dapat melakukan pengelolaan untuk 7 area yang dijelaskan diatas.

Gambar 1.18 Manajemen Deskripsi

Gambar diatas adalah Jendela Manajemen deskripsi berfungsi untuk melakukan pengelolaan untuk pertanyaan-pertanyaan yang ada ditiap area diatas.

e-ISSN: 2549-7952
p-ISSN: 2580-3336

-



Gambar 1.19 Grafik Kuisioner

Gambar diatas adalah Gambar Hasil kuesioner berfungsi emnampilkan keseluruhan hasil kuesioner baik berupa grafik maupun bisa didowload.

NO	GROUP ID	DESCRIPTION	JAWABAN A	JAWABAN B	JAWABAN C	JAWABAN D	JAWABAN E
1	13	UU ITE merupakan dasar pengaturan di bidang pemanfaatan teknologi informasi dan transaksi elektronik	0	0	4	22	22
2	13	Penggunaan setiap informasi melalui media atau sistem elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan	0	0	3	15	30
3	13	Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.	2	0	6	24	16
4	13	Kode akses adalah angka, huruf, simbol karakter lainya atau kombinasi diantaranya, yang merupakan kunci untuk dapat mengakses komputer dan/atau sistem elektronik	0	0	1	23	24
5	13	Setiap orang dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan UU ini.	0	0	8	17	23
6	13	Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki	8	4	15	10	11
7	13	Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyelahgunaan informasi elektronik dan transaksi elektronik yang mengganggu	0	0	5	25	18
8	14	Password merupakan kata kunci untuk memasuki sebuah sistem	0	0	4	17	27
9	14	Password saya bisa diubah sesuai kebutuhan	0	1	5	22	20
10	14	PIN merupakan identitas yang biasanya bersifat tetap	2	9	14	13	10
11	14	PIN yang saya miliki harus berupa angka	2	9	15	16	6
12	14	Saya menggunakan tanggal lahir atau tanggal yang memiliki kesan khusus sebagai PIN	14	15	7	7	5
13	14	Saya menggunakan satu password dan PIN untuk berbagai keperluan (semua password dan PIN sama)	14	15	10	7	2
14	15	Email merupakan sarana untuk mengirimkan pesan elektronik melalui internet	0	0	8	25	15
15	15	Saya menggunakan email untuk membantu proses pekerjaan	0	2	8	25	13
16	15	Internet merupakan sistem komunikasi global yang menghubungkan komputer dengan jaringannya di seluruh dunia	0	0	3	23	22
17	15	Saya merasa hampa apabila tidak menggunakan internet dalam sehari	2	3	24	11	8
18	15	Dengan internet saya mendapatkan berbagai kemudahan mulai dari informasi pendidikan, sosial, ekonomi-bisnis, agama, hingga pemerintahan	0	0	6	20	22
19	15	Email, www, bbs, ftp, chating merupakan sebagian fasilitas yang ada dalam internet	0	0	5	25	18
20	16	Perangkat seluler (HP) saat ini sudah ditanami fitur komputer	0	0	7	27	14
21	16	Saya memberikan kunci khusus untuk perangkat seluler saya	0	2	8	22	16
22	16	Saya menggunakan perangkat seluler untuk transaksi perbankan	0	2	14	22	10
23	16	saya membatasi konten-konten yang saya akses menggunakan perangkat seluler	1	3	10	24	10
24	16	Aplikasi yang ada dalam perangkat seluler saya berasal dari apps store resmi	1	0	17	20	10
25	16	Saya mengaktifkan debugging (usaha memperbaiki suatu bug atau error dalam suatu progam) dalam perangkat seluler saya	1	1	21	18	7
26	16	saya selalu melakukan pembaharuan sistem perangkat seluler secara berkala	0	0	7	26	15
27	17	Government Computer Security Incident Response Team (Gov-CSRIT) merupakan layanan yang harus dimiliki oleh dinkominfo	0	0	4	25	19
28	17	Saya pernah menggandakan file (copy-paste) dari flashdisk yang membawa virus masuk ke laptop/komputer	5	8	16	14	5
29	17	Spammail, mailbomb yang terjadi sebaiknya dilaporkan kepihak terkait	0	0	13	26	9
30	17	Perkembangan mengenai keamanan informasi penting untuk diikuti	0	0	2	30	16
31	18	Password yang tidak mengandung kombinasi alfanumerik cenderung mudah dibobol	0	1	8	18	21
32	18	Penyebaran virus dari komputer ke komputer dan jaringannya dapat menyebabkan cyber crime	0	1	4	29	14
33	18	Phising mampu menyebabkan kerugian baik finansial maupun non-finansial	0	0	4	28	16
34	18	Kemudahan akses pornografi di internet dapat berdampak pada kesehatan emosional	1	1	7	21	18
35	18	Pembajakan hak kekayaan intelektual melalui internet dapat meliputi perbuatan yang melanggar hak cipta, paten, dan merk dagang	0	1	5	26	16
36	19	Saya melakukan backup data terhadap semua file yang ada	0	0	6	25	17
37	19	Back-up data saya lakukan menggunakan perangkat internet (gdrive, email, dropbox, dab)	1	1	10	26	10
38	19	Backup data saya lakukan dengan menggunakan flashdisk atau harddisk	0	0	8	30	10
39	19	Back-up data penting untuk mencegah kehilangan data	0	0	4	18	26
Total			54	79	326	822	591

Gambar 1.20 Gambar Rekap Respoden

Gambar diatas adalah hasil dari rekapitulasi seluruh responden bagian satu yang sudan input kedalam system yang dapat di eksport kedalam Microsoft excel

Evaluasi Hasil

Dari data yang diperoleh diatas dapat diketahui nilai tertinggi ada pada jawaban Setuju dengan skor 868, Sangat setuju dengan skor 596, Netral dengan skor 343, Tidak Setuju dengan skor 89 dan Sangat Tidak Setuju dengan skor 54. Selain itu kita dapat ketahui kecenderungan dalam 7 area semua user lebih cenderung dan kuat pada area Password dan Personal Identity Number (PIN) bahwa user memang tidak akan dengan mudah membagikan password rahasia ke orang lain, karena hal ini sangat memiliki risiko yang sangat tinggi apabila password diketahui oleh orang lain.

4. SIMPULAN

Dengan adanya sistem informasi survey maka telah membantu dalam hal untuk melakukan pengukuran tingkat kesadaran informasi untuk Dinas dan Komunikasi Kota Kediri dengan telah melakukan pengukuran sejumlah 50 Staf, yang untuk selanjutnya akan digunakan untuk ruang lingkup yang lebih luas, khususnya di Pemerintah Kota Kediri.

Dengan adanya Sistem Informasi Survey Kemanan Informasi yang lebih memudahkan untuk melakukan survey dan mendukung digitilasi pemerintah dalam rangka melakukan pelayanan internal untuk seluruh staf. Sistem Inormasi survey ini juga secara otomatis akan melakukan pemeringkatan hasil dari Metode Multiple Criteria Decision Analysis(MCDA) sehingga akan mengethaui level dari masing-masing individu yang telah mengisi survey dalam sistem tersebut.

Setekah mengetahui hasil dan survey maka pimpinan secara bijak akan mengambil keputusan terkait data yang dihasilkan dari survey, bagian di area manakah yang harus diperkuat agar tingkan kesadara informasi dari masing-masing invidu dapat meningkat sehingga insiden keamanan informasi dapat dicegah lebih dini

e-ISSN: 2549-7952
p-ISSN: 2580-3336

5. SARAN

Penyusun mengharapkan penelitian ini bisa dikembangakan lebih baik lagi daripada yang telah disusun saat ini dengan mengembangkan dan menambahkan metode yang lain untuk melakukan pengukuran tingkat kesadaran informasi.

DAFTAR PUSTAKA

[1] McLeod, Raymond & Schell, George P, 2008, Sistem Informasi Manajemen, Edisi 10, Salemba Empat, Jakarta.

[2] Witman, M. E., Mattord, H. J., 2011, Principles of Information security, 4th Edition, Cengage Learning, Atlanta.

[3] Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). An Assessment of the role of cultural factors in information security awareness. ISSA.

[4] Global, S. (2008). Security Awareness: Measuring Attitudes, Knowledge and Behaviour. SAI Global.

[5] APCICT. (2009). Keamanan Jaringan dan Keamanan Informasi dan Privasi. Dalam APCICT, Akadei Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintah. Incheon: Scandinavian Publishing Co., Ltd.

[6] Papagiannakis, K., Pijl, G. v., & Visser, A. d. (2011). An Overview of the current level of Security Awareness in Greek Companies. Erasmus University of Rottersam.

[7] Schlienger, T., & Teufel, S. (2003). Information Security Culture - From Analysis to Change. South African Computer Journal, 638-646.

[8]Belton, V., & Stewart, T. J. (2002). Multiple Criteria Decision Analysis: An Integrated Approach. Kluwer Academic Publishers.

[9] Krugger, H. A., & Kearney, W. D. (2006). A Prototype for assesing information security awareness. Computer & Securitiy, 289 - 296

[10] Kruger, H., & Kerney, W. (2005). Dipetik Februari 2013, dari icsa.cs.up.ac.za: icsa.cs.up.ac.za/issa/2005/Proceedings/Full/018_A rticle.pdf

.