E-DIMAS: Jurnal Pengabdian kepada Masyarakat, 15(2), 211-219
ISSN 2087-3565 (Print) dan ISSN 2528-5041 (Online)
Available Online at https://journal.upgris.ac.id/index.php/e-dimas

Pelatihan dan Pendampingan Kegagalan Teknologi Terkait *Brainware* dan Bencana Alam pada Distributor Sepatu

Johanes Fernandes Andry[1], Kevin Christianto[2], Steven Winata[3], Wensen Anggara[4], Angie Wiyani Putri[5], Bolly Oscar Mario Tinambunan[6]
[1,2,3,4,5,6]Program Studi Sistem Infomasi, Fakultas Teknologi dan Desain, Universitas Bunda Mulia
[1]jandry@bundamulia.ac.id

Received: 22 Mei 2023; Revised: 21 Mei 2024; Accepted: 17 Juni 2024

Abstract

Brainware plays a role in the operation of the system. Brainware consists of various roles such as System Analyst, Programmer, Engineer, and others. Brainware performs data input and data output, as well as preparing computer software and hardware. Community service related to information security is carried out at one of the shoe distributors. The problems faced by the company include differences in stock data between the Head Office and stores, as well as loss of CCTV data due to external disturbances. This service activity includes presentations, questions and answers, and feedback with the aim of helping solve existing problems and increase awareness of information security threats. Materials cover various topics related to information security policies, brainware, policies on the use of computers and printers, and natural disaster management. The results show the existence of information security policies, the use of computers and printers, as well as natural disaster management.

Keywords: *brainware; disater; information security policies*

Abstrak

Brainware berperan dalam pengoperasian sistem. *Brainware* terdiri dari berbagai peran seperti *System Analyst*, *Programmer*, *Engineer*, dan lainnya. *Brainware* melakukan input data dan output data, serta menyiapkan perangkat lunak dan perangkat keras komputer. Pengabdian masyarakat terkait keamanan informasi dilakukan di salah satu distributor sepatu. Permasalahan yang dihadapi perusahaan antara lain perbedaan data stok antara Kantor Pusat dan toko, serta hilangnya data CCTV karena gangguan eksternal. Kegiatan pengabdian ini meliputi presentasi, tanya jawab, dan umpan balik dengan tujuan membantu memecahkan masalah yang ada dan meningkatkan kewaspadaan terhadap ancaman keamanan informasi. Materi mencakup berbagai topik terkait kebijakan keamanan informasi, *brainware*, kebijakan penggunaan komputer dan printer, serta penanggulangan bencana alam. Hasil menunjukkan adanya kebijakan keamanan informasi, penggunaan komputer dan printer, serta penanggulangan bencana alam.

Kata Kunci: *brainware*; bencana alam; kebijakan keamanan informasi

A. PENDAHULUAN

Dalam era perkembangan teknologi informasi (Harjoseputro & Sidhi, 2021) serta komunikasi memberikan dampak kepada perkembangan informasi di dalam masyarakat, yang di mana kegiatan komunikasi berlangsung secara elektronik yang membuat kita dapat melakukan jual beli menggunakan internet sehingga perputaran informasi berlangsung secara cepat, di mana informasi

sendiri merupakan hal penting dalam meningkatkan nilai dan kepercayaan publik (Ramadhani, 2018). Dalam kemudahan mendapatkan informasi, tentunya ada ancaman secara langsung dan tidak langsung, maka keamanan informasi harus diperhatikan dalam mendukung proses bisnis (Putra & Tjahjadi, 2018). Ancaman dapat menyebabkan jika kejadian itu terjadi maka dapat mengancam sistem, seperti kerahasiaan yang hilang dan ancaman kepada integritas, ancaman berhubungan erat dengan bagaimana sebuah sistem bisa tereksploitasi (Matondang et al., 2018).

Brainware adalah komponen manusia yang terlibat langsung dalam proses pengoperasian komputer serta menjalankan kegiatan yang berhubungan dengan *hardware* dan *software*. *Brainware* dapat digolongkan menjadi *System Analyst, Programmer, Engineer,* dan *Operator* (Gani, 2019). Integrasi komponen *brainware* harus dapat berkerjasama secara harmonis dalam mendukung proses pengoperasian sistem. Adapun fungsi dari *Brainware* yakni seorang pengguna, melakukan pemasukan dan pengeluaran data, serta penyusunan *software* dan *hardware* komputer (Wahono & Ali, 2021).

Sebuah peristiwa atau kejadian alam yang menimbulkan kerusakan, rugi, penderitaan, serta gangguan psikologis pada manusia disebut sebagai bencana alam, Pada Indonesia, hal ini, disebabkan karena posisi Indonesia terletak di antara Cincin Api Pasifik dan dikelilingi laut yang menyebabkan Indonesia menjadi negara yang rawan terhadap bencana alam (Simanjuntak et al., 2019). Terletak di antara tiga lempeng membuat Indonesia rawan terhadap bencana alam yang dapat menyebabkan kerugian harta benda, muncul korban jiwa, dan hancurnya fasilitas penting lainnya (Pujianto et al., 2022). Penanggulangan bencana atau disebut juga sebagai mitigasi merupakan usaha untuk mengurangi dampak bencana yang ada terhadap kehidupan manusia sehari-hari, penanggulangan ini termasuk ke tindakan yang dapat dilakukan sebelum bencana (Subekti et al, 2022) yang dapat dilakukan dengan menunggu bantuan dan merencanakan pemulihan dengan cara yang terbaik (Sadewo et al., 2018).

B. PELAKSANAAN DAN METODE

Gambar 1. *Flowchart* Pengabdian kepada Masyarakat

Gambar 1 memperlihatkan kegiatan Pengabdian kepada Masyarakat (PKM) yang dilakukan pada Jumat, 12 Mei 2023 pada jam 08:00 hingga selesai, yang dimulai dengan pembukaan yang dilakukan oleh Johanes Fernandes Andry, S.T., M.Kom. serta Kevin Christianto, S.Kom., MMSI. Dilanjutkan dengan pembahasan terkait dengan kebijakan keamanan informasi, *policy, standard*, *guideline* dan *procedure*, penjelasan terkait brainware, kebijakan *human resource security*, hasil *case study*, dan bencana alam. Setelah sesi pembahasan, dilakukan sesi tanya jawab, dan ditutup dengan mengisi *feedback.*

C. HASIL DAN PEMBAHASAN

Berdasarkan hasil analisa yang dilakukan oleh tim pelaksana PKM, membagi materi, yakni penjelasan terkait kebijakan keamanan informasi, penjelasan terkait *policy*, penjelasan terkait *brainware*, *policy* penggunaan komputer dan printer, penjelasan terkait kebijakan *human resource security*, penjelasan pengujian *SOP*, penjelasan terkait bencana alam, dan penjelasan mengenai solusi

yang ditawarkan oleh pihak tim peneliti yang terdiri dari tahap *preventive, detective,* dan *corrective.* Gambar 2 memperlihatkan proses pelaksanaan kegiatan PKM.

Gambar 2. Proses Pelaksanaan Kegiatan

Kebijakan keamanan informasi merupakan kebijakan yang dibentuk untuk menunjukkan arahan dan peraturan keamanan informasi dalam perusahaan, yang termasuk sistem aplikasi, maupun informasi digital, yang di mana kebijakan yang baik merupakan kebijakan yang melindungi sistem dari seluruh ancaman, sistem yang dimaksud di sini terdiri dari individu, informasi, dan aset fisik. Keamanan informasi ini penting bagi perusahaan dikarenakan dapat melindungi informasi dari ancaman, melindungi kehilangan informasi saat data sedang *transit* dan sedang *rest*, mengendalikan perubahan *IT*, dan melindungi bisnis. Tantangan jika keamanan informasi tidak diterapkan, yakni biaya yang lebih tinggi (pengeluaran biaya tinggi dikarenakan oleh proses yang berulang serta sia-sia), ketidakpuasan pelanggan, dan kurangnya kepatuhan terhadap jaminan keamanan informasi.

Jaminan informasi masih merupakan bagian dari keamanan informasi, yang di mana jaminan informasi merupakan proses untuk memastikan informasi yang ada terlindungi dalam penggunaannya. Jaminan informasi itu sendiri memiliki 5 prinsip, yakni *confidentiality* (kerahasiaan, dengan maksud bahwa informasi adalah rahasia bagi orang-orang yang tidak berwenang atas informasi tersebut, serta memberikan akses untuk pihak yang berwenang atas informasi tersebut), *integrity* (keutuhan, dengan maksud bahwa informasi adalah satu kesatuan yang utuh dan memiliki integritas terkait kepemilikan oleh pihak yang memiliki kewenangan atas informasi tersebut), *availability* (ketersediaan, dengan maksud bahwa informasi mendapat jaminan atas ketersediaannya kepada pihak berwenang atas informasi tersebut, serta dapat diakses dan diambil untuk keperluan pihak pemilik akses informasi), *authentication* (keaslian, dengan maksud bahwa informasi adalah asli atau memuat fakta-fakta yang dicantumkan oleh pihak pemilik informasi dengan menjamin pihak pemilik informasilah yang dapat terhubung dengan informasi tersebut dengan mengumpulkan data-data terkait pihak tersebut untuk mengidentifikasi si pemilik informasi), dan *non-repudiation* (tidak ada penolakan, dengan maksud bahwa tercatatnya semua proses kegiatan individu dalam lingkup teknologi informasi, sehingga ketika ada kesalahan atau ketidaksesuaian pada kegiatan suatu individu secara digital, individu tersebut tidak dapat melakukan penolakan karena terdapat data-data yang terekam mengenai aktivitas yang dilakukan oleh individu tersebut secara terperinci).

Policy merupakan arahan manajemen tingkat tinggi serta jangka panjang yang mengatur pergerakan organisasi yang digerakkan oleh *legal concern*. *Policy* ini harus dilaksanakan oleh seluruh karyawan. *Policy* penting dikarenakan dapat mengembangkan infrastruktur manajemen, mengubah sistem *monitoring* yang pasif menuju manajemen aktif, intervensi permasalahan pada kecepatan komputasi dan tidak bergantung pada waktu reaksi manusia, membolehkan penggunaan kembali, dan perulangan pengetahuan dan proses. *Policy* harus ditulis dengan jelas, singkat, dan bahasa yang mudah dimengerti dan dalam penjelasannya *policy* lebih menjelaskan peraturan bukan cara menjalankannya, dan *policy* melambangkan konsistensi dan *framework* dari pergerakan organisasi.

Standard merupakan proses atau aturan yang digunakan untuk membantu *policy*, dan dapat disebarluaskan secara langsung atau hanya beberapa kelompok saja, *standard* merupakan perintah dan membutuhkan perlakuan khusus jika tidak terpenuhi. *Guideline* merupakan rekomendasi atau pedoman yang membantu dalam mengambil

keputusan atau menjalankan tugas tertentu. *Guideline* umumnya kurang spesifik dan terperinci dibandingkan dengan *standard*, tetapi dapat memberikan panduan yang lebih luas. *Procedure* merupakan instruksi khusus untuk melaksanakan sebuah fungsi atau aksi. *Procedure* merupakan cara bagaimana policy itu sendiri dapat terpenuhi. Keterkaitan antara *policy, standard, guideline,* dan *procedure* yakni *policy* merupakan bagian penting pada perusahaan yang di mana berisi *standard, guideline,* dan *procedure.* Jika *policy* tersebut kurang efektif dalam menghasilkan hasil, maka diperlukan peninjauan ulang terkait hal tersebut.

Brainware merujuk pada manusia sebagai sumber daya intelektual, terdiri dari pengetahuan, keterampilan, dan kemampuan individu atau kelompok. Dalam teknologi informasi, *brainware* digunakan untuk menggambarkan individu atau kelompok yang memiliki kemampuan teknis dan keamanan informasi untuk mengelola sistem komputer dan jaringan. Ciri-ciri *brainware* meliputi pengetahuan tentang keamanan informasi, keterampilan dalam mengelola identitas dan akses, kemampuan merumuskan kebijakan dan prosedur keamanan, serta kemampuan belajar dan beradaptasi. Ada beberapa jenis *brainware*, seperti *brainware* teknis yang memiliki pengetahuan teknis dalam bidang tertentu seperti teknologi informasi, *brainware* keamanan yang memiliki pengetahuan dan keterampilan dalam menjaga keamanan dan kerahasiaan informasi, serta *brainware* keuangan yang memiliki pengetahuan dan keterampilan di bidang keuangan. Tugas-tugas *brainware* termasuk menyelesaikan tugas teknis atau operasional, membuat keputusan strategis dan merencanakan kerja, menjalankan kegiatan pemasaran, dan mengelola keuangan. *Policy* penggunaan komputer dan printer meliputi tanggung jawab karyawan untuk menjaga dan merawat perangkat tersebut agar bebas dari kesalahan, kerusakan, dan penggunaan yang tidak tepat. Standar penggunaan meliputi menjaga kebersihan komputer dan printer dari debu dan kotoran, mematikan perangkat saat tidak digunakan, dan menggunakan satu unit komputer tanpa tambahan yang tidak diizinkan (*CPU, keyboard, monitor, mouse, dan power supply*). Prosedur penggunaan meliputi memperhatikan kebersihan perangkat, tidak menambahkan aplikasi tanpa persetujuan manajer, tidak mengubah tampilan fisik perangkat, tidak menggunakan perangkat untuk keperluan pribadi, mematikan perangkat setelah digunakan, dan hanya menambahkan aplikasi terkait pekerjaan dengan persetujuan manajer. Selain itu, karyawan diwajibkan membersihkan perangkat setelah digunakan, mencuci tangan sebelum menggunakan perangkat, tidak makan saat menggunakan perangkat, dan tidak mengubah atau mengurangi *hardware* internal perangkat. Pelanggaran akan diberikan teguran tertulis, dan setelah beberapa kali pelanggaran, karyawan akan menerima peringatan dan hukuman sesuai ketentuan yang berlaku.

Kebijakan *human resource security* ini didasarkan pada risiko yang sedang dihadapi oleh perusahaan, yaitu adanya perbedaan data dari data *stock* atau adanya *sabotase* sehingga dibuat kontrak kerja, dan pelatihan bersamaan dengan edukasi tentang kesadaran terhadap seberapa pentingnya keamanan informasi. Selain itu, kebijakan ini memiliki keterkaitan dengan prosedur pelatihan dan pengembangan sumber daya manusia, yang di mana prosedur ini yang bertanggung jawab atas semua pelatihan dan edukasi tentang keamanan informasi yang berguna untuk meningkatkan kualitas karyawan, baik secara *intelektual* dan kepribadian, sehingga para karyawan mampu menjaga aset keamanan informasi yang dimiliki oleh perusahaan.

Dalam dokumen prosedur *backup* dan *restore*, terdapat langkah kerja yang diperlukan, khususnya langkah kerja untuk *backup* data. Instruksi kerja ini bertujuan untuk membimbing *administrator* baru dalam mempelajari *proses backup* data dan file. Berikut adalah detail dari instruksi kerjanya:

1. *Backup Database*.

Untuk melakukan *backup* database, pertama-tama buka aplikasi *Putty* dan masuk menggunakan IP database. Isi *port* dengan

angka 22 dan pilih opsi koneksi SSH. Setelah itu, klik tombol *OPEN*. Setelah itu, masukkan *username* dan *password root*. Setelah berhasil masuk, layar akan menampilkan informasi *user* dan data terakhir masuk. Selanjutnya, masukkan *script backup* secara berurutan. Pertama, masukkan *password* yang diperlukan. Kemudian, tentukan lokasi direktori tempat data akan di*backup*. Terakhir, tambahkan pesan yang akan ditampilkan sebagai tanda bahwa proses *backup* berhasil dilakukan. Setelah semua langkah dalam *script backup* telah selesai, *database* akan di*backup* ke file yang telah dibuat sebelumnya. Selanjutnya, lakukan penjadwalan *backup data*. Masuk ke aplikasi Crontab dan isi jadwal penjadwalan secara otomatis sesuai kebutuhan. Setelah mengatur jadwal, tekan tombol *Enter* untuk menyimpan perubahan.

2. *Backup File*

Untuk melakukan *backup file*. Pertama, nyalakan *software* WD SmartWare pada media *backup* yang akan digunakan. Setelah itu, pilih tanda *backup* yang tersedia di dalam *software*. Dengan melakukan langkah ini, proses *backup file* akan secara langsung dimulai dan berlangsung. Setelah *instruksi* kerja *Backup* data, ada juga *instruksi* kerja untuk *Restore* data yang memiliki tujuan yang sama, yaitu untuk membimbing *administrator* baru dalam *proses Restore* data. Berikut adalah rincian *instruksi* kerja untuk *Restore* data.

Pertama, masuk ke aplikasi Putty dan masuk menggunakan IP *database* yang tepat. Isi *port* dengan angka 22 dan pilih opsi koneksi SSH. Setelah itu, klik tombol *OPEN* untuk memulai sesi. Setelah berhasil masuk ke sesi Putty, langkah selanjutnya adalah membuat *database* yang ingin di*restore*. Gunakan perintah yang sesuai untuk membuat *database* baru sesuai kebutuhan. Setelah itu, masukkan *password root* untuk mengakses hak akses administrator. Selanjutnya, masukkan *script restore* yang akan menandakan *file database* yang baru saja dibuat dan *file* yang akan direstore. Pastikan *script* yang digunakan sesuai dengan format dan spesifikasi yang dibutuhkan. Setelah memasukkan *script*, kembali masukkan *password root* untuk memeriksa akses administrator. Terakhir, tekan tombol Enter untuk menjalankan proses *restore* data. Proses ini akan memulihkan database dari *file backup* yang telah ditentukan sebelumnya. Pastikan untuk menunggu proses *restore* selesai dan periksa pesan atau indikator yang muncul untuk memastikan bahwa *restore* data berhasil dilakukan.

Dalam dokumen prosedur pelatihan dan pengembangan sumber daya manusia, terdapat beberapa formulir yang dapat mendukung pengembangan SDM berjalan dengan maksimal yang di antaranya:

1. Formulir log *backup data*, Tujuan dari formulir ini adalah untuk memverifikasi keakuratan dan kelengkapan hasil eksekusi backup data, serta memastikan keberhasilan data yang telah di*backup* dan data yang belum di*backup*.
2. Formulir log *restore data*, Tujuan dari formulir ini adalah untuk menjaga keaslian data dan memastikan bahwa proses *restore* data telah terdokumentasi dengan baik. Formulir ini juga berfungsi untuk memvalidasi bahwa proses *restore* data telah dilakukan oleh pegawai bagian personalia yang memiliki tanggung jawab atas tugas tersebut.
3. Formulir data pegawai, Formulir ini berguna dalam pelaksanaan pelatihan dan pengembangan sumber daya manusia yang diadakan oleh perusahaan untuk mencatat peserta program pelatihan yang dilakukan terkait dengan keamanan aset informasi.
4. Formulir evaluasi kegiatan pengembangan potensi, Tujuan dari formulir ini adalah untuk mendapatkan hasil evaluasi terhadap pelatihan dan pengembangan pegawai yang dilakukan oleh perusahaan.

Pengujian SOP dalam perusahaan terdiri dari 2 tahap, yaitu validasi dan verifikasi. Tahap validasi melibatkan simulasi SOP untuk memastikan keakuratan prosedur saat diterapkan dalam situasi nyata. Tahap verifikasi dilakukan melalui wawancara untuk memeriksa kesesuaian antara prosedur yang dihasilkan dengan kebutuhan.

Telah dilakukan verifikasi yang melibatkan penambahan kebijakan Keamanan

Sumber Daya Manusia, yang sebelumnya tidak ada kebijakan terkait pengelolaan SDM terkait keamanan informasi. Perusahaan meminta kebijakan yang menjelaskan tanggung jawab pegawai dalam penggunaan hak akses dan pengelolaan keamanan. Selain itu, terjadi pemisahan antara kebijakan pengendalian hak akses dan kebijakan keamanan informasi karena memiliki peraturan dan pedoman yang berbeda. Pada peninjauan kinerja pegawai, sejumlah proses dalam pengelolaan hak akses telah dihapus setelah melalui verifikasi dan koreksi. Hal ini dilakukan karena perusahaan memiliki proses peninjauan kinerja internal yang sudah ada. Sehingga, beberapa proses dalam pengelolaan hak akses dihilangkan. Pelaksanaan pergantian *password* mengalami perubahan di mana tanggung jawabnya telah dipindahkan kepada administrator sistem. Sebelumnya, tugas ini dilakukan oleh pegawai personalia. Perubahan ini dilakukan setelah melalui proses verifikasi dan koreksi. Pada prosedur keamanan kabel, terjadi perubahan setelah melalui verifikasi dan koreksi oleh bagian personalia. Keputusan yang disepakati adalah pelaksana tugas keamanan kabel bukan lagi pegawai dari divisi personalia, tetapi berasal dari divisi keamanan. Perubahan ini telah disetujui oleh kepala bagian personalia. Berdasarkan informasi yang didapatkan, ditemukan masalah yang dihadapi oleh perusahaan, yakni adanya permasalahan data yang ada pada *CCTV* dan *fingerprint*, *data stock* yang dikirimkan oleh *head office* tidak sesuai dengan cabang atau adanya tindakan sabotase. Solusi-solusi yang disarankan oleh tim peneliti terkait *brainware*:

1. *Preventive*:
   a. Memilih orang yang kompeten dan dapat dipercaya (profesional) melalui seleksi ketat terkait penerimaan karyawan pada perusahaan.
   b. Membuat peraturan di mana hanya yang bersangkutan dapat mengakses informasi sesuai bagian kerja karyawan. Jika sudah ada, maka pertimbangkan untuk membuat peraturan lain yang bersangkutan dan belum ada demi mencegah adanya kesengajaan pengaksesan informasi tidak sesuai bagian kerja.
   c. Membuat kontrak bagi yang karyawan yang bersangkutan dengan menerapkan prinsip keamanan informasi, misalnya ketika ada masalah, perusahaan ikut menangani masalah dengan kontrak yang diberikan sepihak kepada karyawan tertentu yang memiliki beban kerja yang krusial dalam perusahaan.
2. *Detective*:
   a. Menginterogasi karyawan yang terkait dengan masalah yang terjadi (update informasi perusahaan, apa saja aktivitas karyawan, dan sebagainya.
   b. Mencari informasi melalui dokumentasi/informasi dalam bentuk apapun yang ditulis karyawan beberapa waktu lalu yang berkaitan dengan masalah yang terjadi.
3. *Corrective:*
   a. Memberikan sanksi kepada pelaku sesuai peraturan perusahaan yang berlaku, tanpa diskriminasi dan bersikap objektif.
   b. Mengganti, memperbaiki, dan menambah peraturan berdasarkan kasus yang sudah dialami untuk mengatasi kekurangannya.

Menurut peraturan perundang-udangan nomor 24 tahun 2007, bencana dikatakan sebagai kejadian atau rangkaian kejadian yang dapat merugikan kehidupan masyarakat yang diakibatkan oleh faktor alam dan manusia yang dapat berdampak ke kematian manusia serta lingkungan hidup. Bencana dapat merusak, kehilangan harta benda, gangguan psikologis, hingga yang terparah adalah kematian. Bencana alam dapat dikategorikan menjadi 4 jenis yaitu:

1. Bencana alam merupakan bencana yang dipicu oleh langit dan bumi, seperti gempa bumi, tsunami, dan gunung meletus.
2. Bencana non alam merupakan bencana yang diakibatkan bukan dari alam, seperti gagal teknologi, modernisasi, epidemi.
3. Bencana sosial merupakan bencana buatan manusia yang merugikan suatu kelompok masyarakat.

4. Bencana alam klimatologis merupakan bencana langit dan bumi yang disebabkan oleh faktor angin serta hujan, seperti banjir dan angin topan.

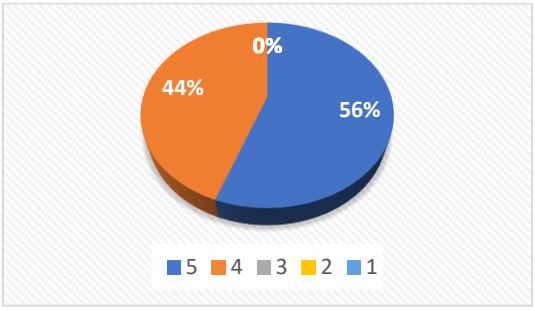
Penanggulangan atau mitigasi bencana alam adalah tindakan yang dilakukan untuk mengurangi efek dari bencana alam terhadap manusia dan hartanya. Ketika berhadapan dengan bencana alam, keamanan informasi dapat mencakup pengamanan informasi di ruang non-fisik atau digital, pendeteksian kemungkinan terjadinya kendala akses data yang terdampak bencana alam melalui fasilitas keamanan pada perangkat *IT* pada perusahaan. *Disaster Recovery Plan* (DRP) adalah kebijakan untuk merespons bencana, menyediakan cadangan selama gangguan, dan kemudian mengelola proses pemulihan dan penyelamatan. ini bertujuan untuk meminimalkan risiko dan optimalisasi kesinambungan entitas. Opsi pemulihan bencana yang umum digunakan termasuk pemulihan bencana virtual, pemulihan bencana jaringan, pemulihan bencana pusat data, dan pemulihan bencana berbasis *cloud*. Tim pelaksana PKM memberikan solusi-solusi terkait bencana alam, yakni:

1. *Preventive* dengan selalu cermat memperhatikan konstruksi ruangan yang berkaitan dengan elektronika di perusahaan, seperti ruangan komputer kerja karyawan, ruangan server dan lain-lain (letak strategis, kekokohan, akses). Selain itu, juga mengadakan *maintenance* setiap beberapa waktu sekali secara rutin untuk mengecek adanya kesalahan pada alat elektronika di perusahaan dan terkait konstruksi ruangan, termasuk pengaman elektronik, perangkat elektronik dan sebagainya.
2. *Detective* dengan mencari sumber-sumber masalah untuk meminimalkan kerusakan pada saat terjadinya bencana alam.
3. *Corrective* dengan membuat laporan terkait bencana alam yang terjadi dan dampaknya sebagai bahan pertimbangan untuk mencegah dampak yang sama terjadi kembali pada saat bencana alam tersebut terjadi. Selain itu, juga mengganti perangkat elektronik dan alat pendukungnya yang rusak akibat dampak bencana alam yang terjadi (pemulihan).

Feedback Pelaksanaan Program Pengabdian Kepada Masyarakat.

1. Apakah kegiatan ini bermanfaat serta edukatif bagi peserta?

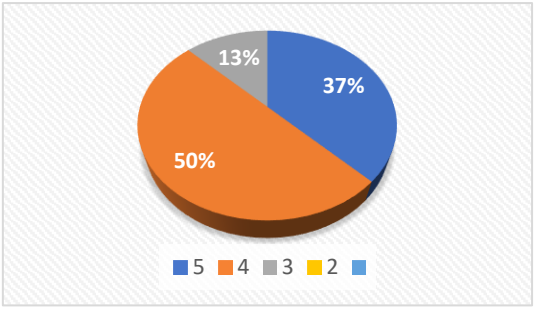
Jawaban responden terlihat telah terbagi tiga dengan poin penilaian poin 4 sebanyak 56%, dan poin 5 sebanyak 44% dari total 8 Responden. Berdasarkan pada hasil tersebut, dapat disimpulkan bahwa kegiatan ini bermanfaat serta edukatif bagi para peserta dengan mayoritas memilih poin 5, yakni sangat setuju terhadap hal tersebut, diperlihatkan pada Gambar 3.



Gambar 3. *Feedback* Bermanfaat bagi Peserta

2. Materi yang disampaikan mudah untuk dipahami?

Jawaban responden terlihat telah terbagi tiga dengan poin penilaian 3 sebanyak 13%, poin 4 sebanyak 37%, dan poin 5 sebanyak 50% dari total 8 Responden. Berdasarkan pada hasil tersebut, dapat disimpulkan bahwa materi yang disampaikan mudah untuk dipahami dengan mayoritas memilih poin 4, yakni setuju terhadap hal tersebut, diperlihatkan pada Gambar 4.



Gambar 4. *Feedback* Materi Mudah Dipahami

3. Materi yang disampaikan sesuai dengan kondisi dan masalah yang sedang dihadapi?

Jawaban responden terkait dengan apakah materi yang disampaikan sesuai

dengan kondisi dan masalah yang dihadapi terbagi menjadi poin 4 sebanyak 38% dan poin 5 sebanyak 62% dari total 8 responden, dan menunjukkan bahwa mayoritas memilih sangat setuju. Dapat disimpulkan bahwa materi yang disampaikan telah sesuai dengan kondisi dan masalah yang dihadapi.

4. Peserta dilibatkan secara aktif dalam pelaksanaan kegiatan?

Jawaban responden terkait dengan apakah peserta dilibatkan secara aktif dalam pelaksanaan kegiatan terbagi menjadi poin 3 sebanyak 38%, poin 4 sebanyak 37%, dan poin 5 sebanyak 25% dari total 8 responden, dan ini menunjukkan bahwa para peserta merasa cukup dilibatkan secara aktif dalam pelaksanaan kegiatan.

Pada Tabel 1 memperlihatkan bahwa pendapat responden tentang kegiatan PKM ini adalah sangat bagus, peserta mendapatkan manfaat terkait isu tentang keamanan Informasi, terutama di bidang *brainware* dan disaster ini. Tabel 1 juga memperlihatkan saran dari peserta PKM terkait kegiatan ini adalah sering melakukan sosialisasi mengenai kebijakan sistem Informasi.

Tabel 1. Pendapat dan Saran dari Responden

Responden	Pendapat tentang kegiatan pengabdian kepada masyarakat yang dilaksanakan	Saran tentang kegiatan pengabdian kepada masyarakat yang dilaksanakan selanjutnya
Responden 1	Sangat bagus.	Jangan terburu.
Responden 2	Baik.	Lebih sering dilakukan.
Responden 3	Good.	Lebih sering lagi.
Responden 4	Sangat bagus.	Service, *Team work.*
Responden 5	Mantap terus dilanjutkan dan dipertahankan.	Terus dilanjutkan.
Responden 6	Menambah wawasan dan informasi seputar keamanan informasi pribadi.	Penyampaiannya lebih jelas dan contohnya ditambah lagi.
Responden 7	Bagus, memberikan informasi terbaru saat ini.	Dalam penjelasan, bisa dibantu berikan contoh kasus yang nyata.
Responden 8	Perlu dilakukan sosialisasi mengenai informasi digital untuk keamanan.	Banyak melakukan sosialisasi mengenai kebijakan sistem informasi.

D. PENUTUP

Simpulan

Perkembangan teknologi informasi mempengaruhi perkembangan informasi yang beredar di masyarakat. Kemudahan dalam mendapatkan informasi juga menimbulkan ancaman baik secara fisik maupun non-fisik, maka keamanan informasi harus diperhatikan dalam mendukung proses bisnis.

Brainware adalah *user* atau manusia yang mengoperasikan komputer serta menjalankan kegiatan yang berhubungan dengan *hardware* dan *software*. Jadi *brainware* harus bisa bekerjasama dengan *hardware* dan *software* secara baik untuk mendukung proses pengoperasian sistem.

Bencana alam adalah kejadian atau aksi alam yang dapat menghasilkan kerusakan, kerugian, penderitaan, serta gangguan psikologis pada manusia. Maka dari itu harus ada penanggulangan bencana alam atau mitigasi, mitigasi merupakan tindakan berkelanjutan yang dimaksud untuk mengurangi dampak dari bencana yang terjadi.

Saran

Ada permasalahan terkait perbedaan data stok pada *Head Office* dan toko, serta hilangnya data CCTV di distributor sepatu yang dikabarkan adanya sabotase dari pihak luar. Oleh karena itu, tim peneliti melakukan kegiatan pengabdian kepada masyarakat terkait keamanan informasi di distributor sepatu dengan melakukan presentasi dan tanya jawab serta diakhiri dengan *feedback* yang juga bertujuan untuk membantu menyelesaikan masalah yang ada dan meningkatkan kewaspadaan terkait ancaman dalam keamanan Informasi.

Ucapan Terima Kasih

Ucapan terima kasih disampaikan kepada Universitas Bunda Mulia, Jakarta dan kepada Perusahaan distributor sepatu, dan kepada pelaksana kegiatan Pengabdian kepada Masyarakat sehingga acara dapat berjalan dengan baik dan lancar.

E. DAFTAR PUSTAKA

Gani, A. G. (2019). Konfigurasi Sistem Keamanan Jaringan. *Jurnal Sistem Informasi Universitas Suryadarma*, 6(1), 134–149. https://doi.org/10.35968/jsi.v6i1.280

Harjoseputro, Y., & Sidhi, T. A. P. (2021). Pemanfaatan Sistem Informasi Pada Usaha Kecil Menengah Untuk Pencatatan dan Pelaporan Transaksi Penjualan. *Dinamisia : Jurnal Pengabdian Kepada Masyarakat*, 5(5), 1305-1317. https://doi.org/10.31849/dinamisia.v5i5.4209.

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 2(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

Pujianto, A., Faizah, R., & Monika, F. (2022). Mitigasi Bencana Pada Siswa Sekolah Dasar. *Prosiding Seminar Nasional Program Pengabdian Masyarakat*, 2363–2368. https://doi.org/10.18196/ppm.47.727

Putra, M. Y., & Tjahjadi, D. (2018). Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, 6(1), 95–104. https://doi.org/10.33558/piksel.v6i1.1404

Ramadhani, A. (2018). Keamanan Informasi. *Nusantara - Journal of Information and Library Studies*, 1(1), 39. https://doi.org/10.30999/n-jils.v1i1.249

Sadewo, M. G., Windarto, A. P., & Wanto, A. (2018). Penerapan Algoritma Clustering Dalam Mengelompokkan Banyaknya Desa/Kelurahan Menurut Upaya Antisipasi/ Mitigasi Bencana Alam Menurut Provinsi Dengan K-Means. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, 2(1), 311–319. https://doi.org/10.30865/komik.v2i1.943

Simanjuntak, R. H., Tolle, H., & Dewi, R. K. (2019). Pengembangan Aplikasi Mobile Geotagging Fasilitas Tanggap Darurat Bencana Alam Menggunakan Algoritma Polylines sebagai Pencarian Rute Terdekat. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 3(9), 8964–8971. Diambil dari https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6315

Subekti, P., Atwar Bajari, Dadang Sugiana, & Hanny Hafiar. (2022). Peningkatan Pengetahuan Kebencanaan Masyarakat Pangandaran Dalam Mewujudkan Masyarakat Tahan Bencana. *Dinamisia : Jurnal Pengabdian Kepada Masyarakat*, 6(2), 346-352. https://doi.org/10.31849/dinamisia.v6i2.8203

Wahono, S., & Ali, H. (2021). Peranan Data Warehouse, Software Dan Brainware Terhadap Pengambilan Keputusan (Literature Review Executive Support Sistem for Business). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(2), 225–239. https://doi.org/10.31933/jemsi.v3i2.781