SOCIETATEA DE INGINERIE SISTEME SIS SA

Aprobat,

Director General SIS

PLANUL DE CONTINUITATE A AFACERII
"BCP"
(Business Continuity Plan)

Scopul acestui plan consta in pregatirea organizatiei in eventualitatea aparitiei unor intreruperi de activitate cauzate de factori necotrolabili (ex. dezastre naturale, atacuri neprevazute, accidente grave, etc.) la revenirea, in cel mai scurt timp posibil, cu pierderi minime, la desfasurarea normala a afacerii.

Planul identifica vulnerabilitatile si recomanda masurile necesare pentru prevenirea intreruperilor activitatilor desfasurate in firma.

Urmatoarele aspecte, procese si proceduri trebuie urmarite de Mangementul SIS SA in cazul unor incidente semnificative de intrerupere a activitatii organizatiei in vederea in vederea reluarii afacerii fara pierderi importante sau cu un minim de consecinte.

Scopul planului este limitat la descrierea problematicii. Este un plan de continuitate a afacerii, nu un document cu proceduri de rezolvare a problemelor cotidiene ale firmei.

Principalele obiective ale planului sunt:

- Este un ghid pentru echipele de salvare.
- Prezinta punctele si locurile datelor critice.
- Indica proceduri si resurse necesare restabilirii situatiei dupa intreruperi.
- Identifica furnizorii si clientii ce trebuie anuntati in caz de dezastre.
- Asista cu documente, date si proceduri de recuperare pe timpul crizelor.
- Identifica surse alternative de alimentare, resurse si locatii.

Asumari:

- Persoanele cheie si echipele disponibile dupa un dezastru
- Dezastrele la nivel national (razboi, etc.) sunt incluse in plan.
- Acest document se pastreaza in loc sigur si este accesibil imediat dupa un dezastru
- Fiecare organizatie-suport are propriul sau plan costand in proceduri unice de recuperare si resurse critice de informatii si proceduri.

Definirea dezastrului

Orice pierdere de utilitati (energie, apa, gaze, etc), conectivitate (locatii de sistem de comunicatii pe diverse medii), sau evenimente catastrofale (meteo, dzastre naturale, vandalism) care cauzeaza o intrerupere in activitatile si serviciile oferite de firma.

CUPRINS

1. Persoane de contact in caz de urgenta

Gheorghe Florea
Director General
Tel.021.252.54.95
Mobil. 0745.01.83.73

Alexandra Ionescu
Director Dezvoltare
Tel.021.252.54.95
Mobil. 0745.08.24.20

Nicolai Fasola
Director Tehnic
Tel.021.252.54.95
Mobil. 0747.50.57.01

Andi Ocheana
Sef compartiment
Tel.021.252.54.95
Mobil. 0749.03.22.06

Ioana Petroman
Asitent Manager
Tel.021.252.54.95
Mobil. 0756.04.66.46

In cazul aparitiei unor evenimente din categoria celor ce se incadreaza in acest plan intra in actiune urmatoarele formatii:

- Echipa pentru situatii de urgenta
- Echipa pentru recuperare dupa dezastru

- Echipa tehnica IT

Componenta si responsabilitatile echipelor este stabilita prin Decizii ale Directorului General SIS.

Responsabilitatile membrilor echipei

- Fiecare membru va avea un inlocuitor.
- Fiecare membru va pastra o lista de apelare a celorlalti membrii ai echipei sale care va contine adresa de acasa si telefoanele personale si de serviciu..
- Fiecare membru va pastra acasa un exemplar al planului de actiune a echipei sale.

2. Sediul firmei

Sediul unic al firmei SIS SA este in Bucuresti, sector 2, sos. Electronicii, 22.

Desi sediul este unic, el se compune din trei corpuri separate de cladire, distantate intre ele, ceea ce permite o organizare a destinatiei acestora ca alternative la pastrarea unor copii de siguranta in anumite situatii de urgenta. Informatiile si datele in format electronic sunt stocate pe serverele din corpul B iar cele pe suporti externi (hartie, suporti optici si magnetici, etc.) se pastreaza in corpul A si/sau C. Bunurile materiale se pastreaza in toate cele 3 corpuri de cladire.

3. Descrierea afacerii

Societatea de inginerie Sisteme SIS SA detine competenta, capacitatea tehnica si umana necesare pentru a desfasura activitatea in domeniul proiectarii, furnizarii, instalarii sistemelor de automatizare industriala, sistemelor SCADA, sistemelor BMS, de siguranta si de securitate. Principalii clienti sunt constituiti din firme industriale private si de stat, persoane fizice, institutii bancare, etc. Firma are activitati de cercetare in parteneriat cu institutii de invatamant superior, institute si centre de cercetare, precum si cu alte firme private din tara si strainatate.

4. Analiza riscurilor

Avand in vedere relatiile complexe cu alte organizatii ca parteneri, clienti sau furnizori Societatea de inginerie Sisteme SIS SA a impementat si mentine un sistem de management integrat (SMI) care include si sistemul de securitate a informatiilor (SMSI) conform cu standardul **ISO/CEI 27001:2013**, cu scopul de a asigura conditiile si mijloacele necesare prevenirii efectelor riscurilor de securitate si asigurarii conditiilor de revenire cu pierderi minime dupa incidente. In acest sens se efectueaza cu regularitate, cel putin odata pe an,o analizare a riscurilor posibile si probabile in functie de gravitatea urmarilor acestora precum si o clasificare a informatiilor, pe categorii de importanta , astfel incat sa se asigure protectia, integritatea si diponibilitatea acestora conform clasificarii. In acest scop se utilizeaza in special procedurile operationale **POSI 04, POSI 05, POSI 07** din sistem.

Principalele pericole si riscuri sunt:

- Epidemii
- Cutremur
- Incendiu
- Inundatie
- Atac cibernetic
- Sabotaj (intern sau extern)

- Eveniment meteo major. (furtuna)
- Intrerupere utilitati
- Terorism/Piraterie
- Razboi
- Furt (de materiale sau informatii vitale)
- Functionare nepcorespunzatoare a sistemelor vitale

In cazul epidemiilor impactul este asupra oamenilor si poate fi atenuat prin solutii tehnice si de afaceri. Cu toate acestea, daca sunt afectate persoanele cu responsabilitati in aceast plan, pot apare disfunctionaliatati. In aceste situatii se instituie carantine si separarea membrilor echipelor astfel incat sa se poata roti in functie de perioada de incubatie a bolii.

In celelalte situatii, dupa definirea amenintarilor, se intocmesc scenarii si proceduri de salvare a bunurilor si de atenuare a impactului situatiilor de urgenta posibile si probabile in variantele cele mai grave. Astfel de proceduri sunt descrise in sistemul de management integrat al SIS SA.

Dupa faza de analiza , in etapa urmatoare se stabilesc cerintele tehnice si resursele materiale, umane si financiare necesare pentru fiecare solutie in parte. Inventarul bunurilor permite o rapida identificare a resurselor desfasurate. In cazul firmei SIS SA , cu o pregnanta activitate IT , cerintele planului trebuie sa acopereresursele umane, aparatura de specialitate, aplicatiile, bazele de date, manualele de utilizare, computerele, perifericile, suportii electronici de informatie, etc.

Toate aceste cerinte se regasesc in documentatia sistemului de management integrat.

5. Politica de securitate

Societatea de inginerie Sisteme SIS SA defineste in cadrul politicii sistemului de management integrat , intr-un capitol distinct, **POLITICA IN DOMENIUL SECURITATII INFORMATIEI** care este obligatorie pentru toti salariatii organizatiei.

In acest sens conducerea organizatiei aloca resurse financiare si umane si sprijin pentru ducerea la indeplinire a urmatoarelor obiective legate de securitatea informatiei:

- Respectarea obligatiilor contractuale si legale in toate activitatile desfasurate;
- Asigurarea continuitatii prestarii serviciilor catre clienti si minimizarea pierderilor in cazul aparitiei unor incidente de securitate;
- Asigurarea unei protectii corespunzatoare importantei informatiilor procesate si limitarea stricta a accesului la informatii cu caracter special (confidential);
- Protectia integritatii datelor generate de procesele suport si a aplicatiilor software utilizate;
- Protectia impotriva atacurilor informatice si a virusilor de orice natura;
- Demonstrarea conformitatii cu standardul ISO/IEC 27001:2013 Sisteme de management ale securitatii informatiilor;
- Consolidarea reputatiei pe piata a organizatiei si cresterea increderii tuturor partilor interesate

  Pentru aplicarea Politicii sunt implementate proceduri de securitate a informatiilor.

  Criteriile pe baza carora se evaluaeaza riscurile SI sunt:
  - pierderi financiare
  - disfuntionalitati ale activitatii
  - pierderi de imagine
  - litigii cu clientii,

toate acestea generand pierderi de Confidentialitate, Integritate si Disponibilitate a informatiilor.

Ducerea la indeplinire a masurilor interne privind asigurarea securitatii informatiei este facuta in cadrul **Comitetului de Securitate a Informatiei (CSI)** din care fac parte: Directorul General, Directorul pentru Dezvoltare, Directorul tehnic si Managerul Sistemului de Management al Securitatii Informatiilor.

6. Organizarea securitatii informatiei

La nivelul organizatiei SIS SA, administrarea securitatii informatiilor se face de catre RMSI sub directa coordonare a Directorului General si a CSI. Responsabilitatile sunt atribuite persoanelor prin decizii ale Directorului General. Se stabileste prin decizii RMSI, Echipa BCP, Comisia de inventariere a activelor SIS, Comitetul de securitate a informatiilor (CSI). Protectia informatiilor este intarita de acorduri de confidentialitate semnate de salariati la angajare. Toata activitatea de securitate a informatiilor se desfasoara coform celor 4 proceduri generale (PGSI01…PGSI04) integrate in PG SMI :

PGSI 01 - Controlul documentelor.doc
PGSI 02 - Controlul inregistrarilor
PGSI 03 - Audit intern
PGSI 04 - Actiuni corective si preventive

a 8 proceduri operationale (**POSI 01…POSI 08**) :

POSI 01 Analiza managementului
POSI 02 Asigurarea continuitatii afacerii
POSI 03 Monitorizarea accesului la resurse
POSI 04 Inventariere
POSI 05 Clasificarea informatiilor
POSI 06 Back-upul informatiilor electronice
POSI 07 Analiza si managementul riscului
POSI 08 Conformitatea

si a 8 proceduri de lucru (**PLSI 01…PLSI 08**)

PLSI 01 -Politica de securitatea a informatiei
PLSI -02-Firewall1
PLSI -03-Servere
PLSI -04-Folosirea resurselor IT
PLSI -05-Utilizare Parole
PLSI -06-Relatiile de munca
PLSI -07-Tratare incidente
PLSI -08-Emitere reglementari interne SMSI

existente in prezent in SMI.

In relatiile cu clientii si partenerii de afaceri se ataseaza, la contractele incheiate, **conventia de confidentialiate a informatiilor comune**.

7. Managementul resurselor

Modul in care se realizeaza gestionarea si monitorizarea resurselor, in detaliu, este descris in procedura operationala **POSI 03**. Principalele aspecte ale procedurii se refera la:

- Zonele de securitate si accesul controlat al angajatilor si a vizitatorilor
- Securitatea echipamentelor
- Accesul utilizatorilor la sistemele de informatii si bazele de date
- Responsabilitatile utilizatorilor sistemelor de procesare informatiilor
- Controlul accesului la reteaua locala sis
- Controlul accesului la sistemele de operare
- Controlul accesului la aplicatii
- Prelucrarea datelor folosind echipamente mobile si lucrul de la distanta
- Controlul accesului la Internet si posta electronica
- Accesul la mijloacele de transport ale firmei se face controlat

Abaterile de la aceste controale se sanctioneaza administrativ sau penal in functie de gravitatea si pagubele pricinuite.

8. Securitatea resurselor umane

Resursa umana este prioritatea maxima in actiunile de salvare in caz de declansare a situatiilor catastrofale, deorece fara aceasta resursa nu se poate pune problema continuarii afacerii. Echipele pentru situatii de urgenta si de salvare dupa dezastru vor incepe actiunile cu salvarea acestei resurse acordand o maxima atentie persoanelor afectate sub aspect fizic si psihic prin apelarea la serviciile institutiilor specializate . Prima masura consta in apelul la serviciul de urgenta 112.

Prevenirea urmarilor grave asupra resursei umane consta si in organizarea de cursuri periodice de instruire asupra comportamentului corespunzator in astfel de situatii.

In programele anuale de instruire ale sistemului managerial integrat se prevad si astfel de tematici.

SIS SA respectă viaţa privată şi datele cu caracter personal pe care utilizatorii le împărtăşesc cu noi în momentul accesării site-ului SIS.

SIS SA respectă legislaţia română în vigoare, respectiv Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, modificată şi completată şi Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

Confidenţialitatea şi protecţia informaţiilor colectate de la clienti/parteneri sunt de o importanţă vitală pentru firma. Firma isi ia angajamentul sa nu diseminеze informaţia colectată unor terţi fără consimţământul expres şi prealabil.

SIS SA este împotriva trimiterii de mesaje comerciale nesolicitate (spam) pentru care nu are acordul explicit al utilizatorului şi da posibilitatea abonării la revista SIS cu noutăţi din domeniu şi informaţii despre serviciile/promoţiile noastre, prin simpla introducere a emailului.

Datele cu caracter personal ale angajatilor vor fi folosite doar in scop strict al businessului iar dreptul de utilizare este rezervat strict departamentului de Salarizare.

9. Securitatea fizica si a mediului de lucru

Securitatea fizica a incintei in care se afla sediul firmei se asigura prin mai multe mijloace si sisteme. Exista un sistem de videosupraveghere cu mai multe camere de luat vederi atat in exterior (perimetral) cat si in interior (in spatiile care gazduiesc bunuri de mare valoare. Accesul pietonal si al masinilor in curtea firmei este controlat prin sistemul de control acces atat la poarta mare cat si la poarta pentru persoane care permite accesul numai prin card de proximitate personalizat sau prin telecomanda radio in cazul masinilor. Vizitatorii sunt admisi numai dupa identificarea prin videointerfon de catre persoanele care au aceste atributii in firma.

In afara programului de lucru, dupa plecarea ultimului salariat se activeaza sistemul de alarmare si intimidare a tentativelor de efractie prin ativarea sistemului de alarmare compus din:

- sistemul de control acces in cladiri
- reteaua de senzori de detectie a inceputului de incendiu (de fum)
- sistemul de proiectoare cu senzori de miscare
- sistemul de detectie a scurgerii de gaze
- formatia de caini de paza ai firmei

Ansamblul acestor sisteme permite alarmarea, in timp-real, a persoanelor cheie, la distanta, prin reteaua de telefonie mobila respectiv prin reteaua INTERNET.

Prin Internet se poate face videosupravegherea de la distanta, de catre persoanele autorizate, vizualizand pe computer imaginile videocamerelor din incinta.

In aceste conditii nu este necesara prezenta permanenta a unei persoane de paza la sediul firmei in afara orelor de program.

Mediul de lucru in incaperile de echipamente respectiv in birouri este asigurat prin mentinerea unui microclimat corespunzator cu ajutorul instalatiei de incalzire cu centrala proprie, respectiv cu ajutorul instalatiilor de aer conditionat de tip split, montate in spatiile de lucru. Conditiile de curatenie si igiena sunt asiguate de personalul auxiliar cu aceste atributii caruia i se pun la dispozitie toate cele necesare.

Securitatea fizica este asigurata si de sistemul de asigurare permanenta a energiei electrice prin comutarea automata pe grupul generator propriu, in cazul caderii tensiunii de alimentaare din reteaua trifazica publica.

In cazul aparitiei unor incidente grave echipele de interventie vor efectua evacuarea persoanelor si bunurilor conform urmatoarelor schite prezentate si afisate in locuri vizibile:

- Planul de interventie si evacuare a persoanelor si bunurilor in SIS SA
- Planul de interventie si evacuare a persoanelor si bunurilor din Corp A
- Planul de interventie si evacuare a persoanelor si bunurilor din Corp B

10. Managementul comunicatiilor si operatiunilor

Pentru a elimina riscul producerii unor disfunctionalitati (in timpul activitatii de recuperare) intre echipe si membrii fiecarei echipe implicate in procesul de asigurare a continuitatii activitatii sunt necesare atat comunicare cat si coodronarea sa fie efciente si eficace. Aceasta presupune o permanenta disponibilitate a tuturor sistemelor de comunicatii de care dispune firma. In principal aceste sisteme sunt:

- comunicatia prin telefonie vocala fixa si mobila
- comunicatia prin SMS
- comunicatia prin FAX
- comunicatia prin e-mail

- comunicatia prin videoimagini pe internet

Toat e aceste sisteme sunt in stare de functionare permanenta si verificate zilnic astfel incat in cazul aparitiei unor incidente sa se poata interveni cu promtitudine si sa se declanseze operatiunile prevazute in procedurile sistemului de management integrat.

11. Controlul accesului la date

Accesul la informatiile si bazele de date ale firmei este permis diferentiat de catre sistemul de protectie a acestora. Mai intai, exista o inventarieire a tuturor bunurilor de acest tip si o clasificare a acestora in functie de nivelul de confidentialitate. Apoi, in functie de suportul pe care acestea se afla , este stabilit modul de protejare. Informatiile pe suport hartie sunt protejate prin pastrarea in incinte si locatii sub cheie si supravegheate prin mijloacele electronice existente. Cheile se pastreaza numai la persoanele autorizate sa aiba acces la aceste date.

Datele si informatiile pe suport electronic sunt protejate in functie de locul, tipul si suportul acestora.

Datele strict confidentiale se pastreaza numai pe suporturi externe (CD, DVD, memory stick) tinute sub cheie si consultate, de persoanele autorizate, numai cu aprobarea expresa a Directorului General.

Datele confidentiale se pastreaza atat pe suporti interni (memorii interne, HDD, etc.) cat si pe supoti externi, pe servere sau pe statii de lucru in LAN (PC-uri, Laptop-uri), accesul la acestea fiind protejat prin parole de acces personalizate, cu privilegii diferite (scriere/citire, numai citire, copiabile/necopiabile, printabile/neprintabile, etc.). Un rol important, in protectia datelor, il are si disciplina angajatilor in utilizarea computerelor conectate sau nu la reteaua locala, care presupune nedivulgarea parolelor proprii si iesire din sesiunea de lucru de fiecare data cand parasesc computerul, chiar si pentru scurte perioade de timp (pauza de masa, mers la toaleta , la locul de fumat, etc.).

Datele publice nu sunt protejate in privinta accesului dar se asigura diponibilitatea si integritatea acestora pentru a nu se crea confuzii sau informatii eronate.

12. Achizitionare, dezvoltarea si mentinerea sistemelor informatice

Componentele hardware si software sunt achizitionate de la firme trecute in “Lista furizorilor acceptati” care comercializeaza produse proprii sau de la producatori recunoscuti prin calitatea produselor. Criteriile de selectie a furnizorilor din lista sunt cele din procedurile sistemului de management integrat.

Componentele software din sistem sunt licentiate sau cu licenta libera atat cele de sistem de operare cat si cele de dezvoltare sau aplicative.

In dezvoltarea in timp a firmei dotarea acesteia permit desfasurarea unei activitati profesionale de inalta tinuta. In prezent firma SIS dispune, in principal, de urmatoarea dotare:

- Servere de retea cu conexiune la Internet: 2 buc
- Calculatoare PC conectate in LAN :16 buc
- Calculatoare Laptop conectabile in LAN: 11 buc
- Sitem de simulare-testare aplicatii SCADA: 1buc
- Echipamente periferice:
  - Imprimanta laserjet : 5 buc

- Imprimanta inkjet : 2 buc
- Multifunctionala : 1buc
- Plotter A0: 1 buc
- Plotter A3 : 1 buc
- Scaner A4 : 1 buc

- Copiator tip xerox: 1 buc
- Fax : 1 buc
- Centrala telefonica digitala 4 ex / 16 int : 1 buc

Mentinerea acestor dotari se face cu forte proprii pentru intretinerea curenta si prin utilizarea unor servicii specializate externe pentru operatii complexe si reparatii.

13. Managementul incidentelor de securitate

SIS SA dispune de suficiente resurse (echipament de comunicatii, configuratii PC, alte configuratii IT, surse de alimentare cu energie electrica etc.) disponibile, testate care pot fi folosite in cazul in care s-ar produce un incident, si reluarea activitatii in conformitate cu BCP presupune o astfel de optiune.

Alimentarea cu energie electrica, infrastructura pentru comunicatii, infrastructura de retea, hardware-ul (servere, desktop-uri, notebook-uri, echipamente de comunicatii, FAX-uri etc.), mediul operational (soft de sistem, soft de aplicatii, baze de date etc.) sunt in stare de functionare astfel incit, in orice moment, in cazul producerii unui incident care ar afecta locatia unde se afla sediul firmei.

Pentru softul de sistem, softul de aplicatii, baze de date si sistemele de gestiune a bazelor de date, se fac salvari la zi, fiind posibila o recuperare coerenta a bazelor de date in cazul producerii unui incident.

In cazul producerii unui incident, reluarea activitatii se va executa conform setului de procese si proceduri prezentat in prezentul plan BCP.

14. Managementul continuitatii afacerii

In SIS continuarea afacerii dupa un incident de intrerupere a activitatii este reglementata de o procedura operationala (POSI 02) care are ca principal scop reluarea activitatilor fara a afecta imaginea SIS SA, reducerea pierderilor, derularea in conditii de siguranta a tuturor proceselor, onorarea obligatiilor organizatiei.

Se are in vedere atingerea urmatoarelor obiective:

-Asigurarea resurselor pentru protejarea sanatatii angajatilor la aparitia unui incident.

- Stabilirea legaturilor de comunicare INTERNA SI EXTERNA.
- Colectarea si evaluarea informatiilor privind gravitatea distrugerilor si a pagubelor.
- Identificarea resurselor disponibile pentre reluarea activitatii.
- Executarea unor actiuni cu scopul continuarii activitatii fara pierderi semnificative.

Etapele principale ale procesului de reluare a activitatii sunt:

- avertizare incident
- identificare incident
- mobilizarea echipelor, revizuirea strategiei
- decizia de relocare, daca este cazul

- reluarea activitatii
- restaurarea activitatilor la nivelul anterior dezastrului

Se are in vedere faptul ca:

- SIS SA dispune de suficient personal calificat pentru a executa setul de procese si proceduri necesar pentru reluarea activitatii.
- personalul care este implicat in procesul de reluare a activitatii este disponibil indiferent de momentul producerii incidentului si de durata implicarii.
- In cazul producerii unui incident, reluarea activitatii se executa conform setului de procese si proceduri prezentat in BCP si SMI.
- Este asigurat un nivel inalt de promptitudine.

Reluarea activitatii in astfel de situatii, intr-o perioada de timp care sa nu ameninte in nici un fel stabilitatea companiei reprezinta o prioritate maxima. Pentru eficacitatea planului se impune :

- elaborarea de planuri alternative (de rezerva) pentru reluarea activitatii in cazul unor intreruperi;
- testarea periodica a planurilor alternative in scopul verificarii disponibilitatii acestora.
- o clasificare a incidentelor care s-ar putea produce in functie de timpul minim necesar pentru reluarea activitatii;
- identificarea activitatilor si proceselor desfasurate;
- identificarea functiilor critice si a locatiilor in care acestea sunt implementate;
- identificarea de locatii de rezerva (alternative) implicand:
    a. surse alternative pentru alimentarea cu energie electrica
    b. conexiuni noi ale retelelor de calculatoare
    c. retele de comunicatii alternative
    d. suport hardware-software
- stabilirea echipelor care ar putea fi implicate in procesul de reluare a activitatii in cazul aparitiei unui incident;
- stabilirea reponsabilitatilor care revin intr-o astfel de situatie fiecarei echipe, reguli de lucru;
- elaborarea formularelor pentru:
    - semnalarea aparitiei unui incident;
    - instiintarea echipelor de producerea unui incident;
    - inregistrarea cheltuielilor generate in procesul de reluare a activitatii;
    - componenta echipei respective;
- redundanta: trebuie pregatite sisteme redundante, care sa preia activitatea in eventualitatea unui dezastru;

Pentru buna desfasurare a actiunilor prevazute in BCP se stabilesc urmatoarele responsabilitati:

Directorul General

-Dispune elaborarea de planuri de rezerva pentru continuarea afacerii in caz de dezastru
-Numeste echipa cu responsabilitati de asigurare a continuitatii activitatilor
-Aloca resursele umane, informationale, financiare, materiale si de timp pentru realizarea activitatilor specificae BCP.
-Dispune intocmirea listelor de contacte si resurse ce vor fi notificate in caz de incidente

RSMSI

- Identifica procesele, activitatile critice, prioritatile echipei in cazul aparitiei unui incident,
- Evalueaza modului de raspuns la aparitia unui incident;
- Evalueaza dimensiunile unui potential impact cauzat de un posibil incident,
- Mobilizeaza personalul;
- Definitiveaza procedurile echipei implicate in procesul de asigurare a continuitatii activitatii;
- Defineste procedurile de urgenta care trebuie urmate in cazul aparitiei unui incident;
- Defineste incidentele care s-ar putea produce, impactul acestora asupra activitatii
- Identifica modul de alertare a echipelor de actiune si obiectivele alocate fiecarei echipe;
- Identifica modul de raspuns al furnizorilor (de hardware, software, servicii, etc.

-Completeaza *Raportul de analiza incident SI*

Echipa de interventie

- Participa la sedintele convocate de RSMSI,
- La dezastru completeaza *Raportul de incident si masuri pentru securitatea informatiei*;
- Da un raspuns partilor interesate dupa ce primeste *Raportul de analiza incident SI*
- Notifica echipele care sunt implicate in procesul de asigurare sau reluare a activitatii
- Solicita departamentului Financiar-contabil un Raport de cheltuieli cu privire la incident
- Utilizeaza listele de contacte si resurse pentru identificarea echipelor implicate in redresarea activitatilor.

15. Conformitatea

Conformitatea cu cerintele legale se face pe baza verificarilor cu Lista de acte normative, care este mentinuta la zi, prin identificarea legislatiei aplicabile.

Organizatia se asigura ca cerintele legale si alte cerinte aplicabile la care organizatia subscrie sunt luate în considerare în stabilirea, implementarea si mentinerea SMI.

Procedura din sistem care care are ca obiect conformitatea este POSI 08 in care se precizeaza in principal urmatoarele aspecte:

RSMSI stabileste si mentine lista cu prevederile legale in domeniul securitatii informationale aplicabile activitatilor, produselor si serviciilor organizatiei, precum si a actelor de reglementare aplicabile (autorizatii, acorduri, contracte etc.).

Lista prevederilor legale si a altor cerinte de securitatea informationala este structurata astfel incât sa poata fi mentinuta pe toata durata functionarii SMSI.

Pentru stabilirea prevederilor legale si a altor cerinte se folosesc urmatoarele surse de informatie:

- Colectia „Monitorul Oficial”;
- Colectia de Acte Normative specifice activitatilor organizatiei;
- Paginile de internet relevante;
- Surse de documentare apartinând autoritatilor centrale si locale de mediu;
- Alte surse de informare

Se actualizeaza lunar *Registrul cerintelor legale si altor cerinte privind SMI*

RSMSI analizeaza textele de reglementare si stabileste noi obligatii de securitate informationala pe care organizatia le ia in considerare pentru activitatile, produsele si serviciile sale.

Registrul cerintelor legale si altor cerinte privind SI, precum si noile obligatii stabilite de RSMSI sunt puse la dispozitia tuturor angajatilor organizatiei in format electronic.

Drepturile de proprietate intelectuala set protejeaza conform reglementarilor in vigoare.

Conţinutul şi design-ul sis.ro, fotografiile, desenele, textele, sloganurile, imaginile, precum şi toate lucrările integrate în acest site, inclusiv bazele de date accesibile prin intermediul său, sunt proprietatea SIS SA şi sunt protejate prin legislaţia română în vigoare cu privire la drepturile de autor şi drepturile conexe. În cazul informaţiilor şi conţinutului postat de utilizatori înregistraţi sau terţe părţi ori parteneri pe site-ul sis.ro, dreptul de autor şi responsabilitatea asupra acestora aparţin în totalitate celor care au publicat acea informaţie. În cazul conţinutului preluat de la parteneri pe baza acordurilor încheiate, acestea sunt identificate prin menţionarea numelui partenerului lângă textul sau imaginea respectivă.

Este interzisă orice utilizare a conţinutului site-ului în alte scopuri decât cele permise expres de prezentul document sau de legislaţia în vigoare. Cererile de utilizare a conţinutului în alte scopuri decât cele permise expres de prezentul document pot fi trimise la adresa de email sis@sis.ro. Excepţie fac informările şi comunicatele de presă, care pot fi preluate parţial sau integral de reprezentanţi ai mass-media, cu precizarea sursei.

Toti angajatii SIS SA au obligatia sa utilizeze doar software licentiat pe statiile de lucru, abterile fiind sanctionate disciplinar.