Plan de continuitate a afacerii

Chisinau, 2025

CUPRINS :

1. Obiectivele planului de continuitate a afacerii

Planul de Continuitate a Afacerii (BCP) pentru **InfoSofTeh SRL** are ca scop principal **asigurarea continuității operaționale** și **minimizarea impactului negativ** al unor posibile incidente asupra activităților esențiale ale companiei.

Obiectivele stabilite de către InfoSofTeh SRL pentru planul pe continuitate a afacerii sunt:

- Asigurarea continuității serviciilor de mentenanță IT oferite pentru programul 1C, inclusiv implementarea actualizărilor de sistem și modificările solicitate de clienți.
- Protejarea integrității și confidențialității datelor stocate și procesate de companie, asigurându-se că informațiile sensibile ale clienților sunt în siguranță în orice moment.
- Reducerea timpului de întrerupere a serviciilor de mentenanță și suport tehnic în cazul unor incidente neprevăzute, pentru a minimiza impactul asupra clienților și afacerii.
- Răspuns rapid și eficient la solicitările clienților, asigurându-se că echipele de suport reacționează prompt la orice problemă tehnică sau contabilă raportată prin apel sau mesaj.
- Respectarea cerințelor legale și reglementărilor de securitate impuse în domeniul IT și al protecției datelor, pentru a evita riscurile juridice și de conformitate.
- Menținerea unui plan de recuperare eficient care să permită reluarea rapidă a operațiunilor critice în caz de dezastre sau evenimente neprevăzute, protejând atât datele cât și serviciile oferite clienților.

Obiectivele specifice stabilite de **InfoSofTeh SRL** în procesul de prestare a serviciilor sunt:

- Implementarea unor soluții avansate de backup și redundanță pentru infrastructura IT utilizată în mentenanța programului 1C, precum și pentru gestionarea datelor sensibile ale clienților, constituie o prioritate strategică. Aceste măsuri vor garanta integritatea, confidențialitatea și disponibilitatea permanentă a informațiilor critice, reducând riscul de pierdere sau compromitere a datelor în contextul unor evenimente neprevăzute.
- Dezvoltarea sistemului securizat de acces la distanță este destinat să permită echipelor de suport tehnic intervenții rapide și eficiente, chiar și în condiții de criză. Acest sistem asigură continuitatea serviciilor, reducând semnificativ timpul de răspuns și impactul asupra clientului.

Accesul este reglementat prin protocoale avansate de criptare, garantând protecția datelor sensibile și prevenind accesul neautorizat. Monitorizarea în timp real și controlul strict al accesului la infrastructura IT contribuie la reducerea riscurilor de securitate, iar verificările constante asigură integritatea conexiunilor.

- Adoptarea unor tehnologii avansate de securitate cibernetică, are ca obiectiv prevenirea accesului neautorizat și protejarea integrității datelor gestionate.

Pentru **creșterea eficienței și flexibilității organizaționale**, se urmăresc următoarele obiective specifice:

- Instituirea unui program continuu de perfecționare profesională a angajaților, prin intermediul unor sesiuni de instruire specializate și simulări periodice, are drept scop pregătirea temeinică a echipelor de mentenanță și suport.
- Optimizarea permanentă a procedurilor de recuperare a infrastructurii și serviciilor critice, prin testări periodice și actualizarea continuă a strategiilor de răspuns, va asigura un grad ridicat de disponibilitate a serviciilor în eventualitatea unor întreruperi neplanificate.
- Elaborarea, actualizarea și menținerea unei documentații operaționale complete privind procedurile de recuperare constituie un pilon esențial în asigurarea continuității afacerii.

În baza celor expuse, **Planul de continuitate a afacerii** al **InfoSofTeh SRL** constituie un cadru operațional pentru asigurarea continuității activităților companiei și pentru reducerea impactului negativ al eventualelor incidente asupra serviciilor și infrastructurii critice. Prin implementarea obiectivelor stabilite, compania își propune să asigure funcționarea neîntreruptă a proceselor esențiale, protejând astfel datele sensibile ale clienților și asigurându-se că intervențiile tehnice se realizează într-un interval minim de timp.

2. Echipa de continuitate a afacerii

Membrii echipei		Titlu/ department	Telefon
1	Demian Dumitru	Departamentul administrativ	+37368941000
2	Contabilitaea	Departamentul administrativ	+37368941000
3	Botnarenco Sergiu	Departamentul de Suport Tehnic și Consultanță Contabilă	+37369778884
4	Girlea Valeria		+37360023735
5	Bercaru Dragomira		+37360052992
6	Ciorap Viorica		
7	Vasilache Evelina		

Descrieri generale ale afacerii/ responsabilități ale departamentelor
Compania oferă consultanță în domeniul contabilității, asigurându-se că toate aspectele tehnice și contabile sunt gestionate eficient. Echipa responsabilă de aceste activități include specialiști în suport tehnic și consultanță contabilă, care răspund prompt la solicitările clienților pentru a asigura continuitatea operațiunilor și a soluționa rapid orice problemă tehnică sau contabilă.

3. Analiza impactului asupra afacerii

IDENTIFICAREA PROCESELOR CRITICE
Suport tehnic și mentenanță IT pentru programul 1C - Asigurarea funcționalității continue și corecte a sistemului 1C, inclusiv implementarea actualizărilor de sistem și a modificărilor solicitate de clienți. Consultanță contabilă - Furnizarea de consultanță financiar-contabilă pentru clienți, inclusiv asistență în respectarea reglementărilor fiscale și a cerințelor legale. Actualizări periodice ale sistemului 1C - Implementarea și gestionarea modificărilor lunare ale programului 1C pentru a asigura compatibilitatea și securitatea acestuia. Răspuns rapid la solicitările clienților - Asigurarea unui răspuns prompt și eficient la problemele tehnice sau contabile raportate de clienți.
EVALUAREA IMPACTULUI
Pentru fiecare dintre procesele critice menționate mai sus, s-au evaluat impacturile potențiale ale întreruperilor și măsurile necesare pentru a le preveni sau atenua: - **Suport tehnic și mentenanță IT pentru programul 1C**: **Impact operațional**: Întârzierile în furnizarea suportului pot conduce la întreruperea activităților clienților, afectând procesarea datelor financiare și contabile. **Impact reputațional**: Deficiențele în furnizarea serviciilor de mentenanță pot afecta încrederea clienților și reputația companiei. - **Consultanță contabilă**:

Impact operațional: Lipsa unui serviciu adecvat de consultanță poate afecta procesarea corectă a datelor financiare și îndeplinirea obligațiilor fiscale ale clienților.
Impact reputațional: Erorile în consultanță pot duce la pierderea încrederii clienților și la deteriorarea relațiilor comerciale.

- **Actualizări și modificări ale sistemului 1C**:

Impact operațional: Lipsa actualizărilor poate duce la vulnerabilități de securitate și incompatibilități care pot afecta stabilitatea sistemului.
Impact reputațional: Neactualizarea sistemului poate afecta încrederea clienților în siguranța datelor lor și în capacitatea companiei de a furniza soluții fiabile.

- **Răspuns rapid la solicitările clienților**:

Impact operațional: Întârzierile în răspunsul la solicitările clienților pot afecta procesul decizional al acestora și pot duce la întreruperea activităților lor.
Impact reputațional: Răspunsurile întârziate pot afecta relațiile pe termen lung cu clienții și pot duce la pierderi de afaceri.

IDENTIFICAREA RESURSELOR CRITICE

InfoSofTeh SRL depinde de următoarele resurse esențiale pentru desfășurarea activităților critice:
Infrastructura IT: Servere, software, rețele de comunicație, sisteme de backup și redundanță.
Personalul calificat: Echipele tehnice pentru mentenanța 1C, personalul de consultanță contabilă, administratori de sistem.
Sisteme de backup: Soluții de backup regulat și redundanță pentru protecția datelor.
Canale de comunicare: Linii de comunicare eficientă cu clienții pentru a răspunde rapid la solicitările acestora.

EVALUAREA RISCURILOR ȘI IMPACTULUI POTENȚIAL

Riscurile majore identificate includ:
Atacuri cibernetice: Riscul de compromitere a sistemelor IT prin atacuri de tip malware, ransomware, sau hacking.
Impact: Pierderi financiare semnificative, daune reputaționale, posibile sancțiuni legale.
Defecțiuni ale infrastructurii IT: Defecțiuni ale serverelor sau rețelelor IT care pot duce la întreruperi de serviciu.
Impact: Pierderi operaționale, afectarea serviciilor oferite clienților, pierderi financiare.
Erori umane: Greșeli în utilizarea sistemelor de suport tehnic sau în procesul de consultanță contabilă.
Impact: Posibilitatea de a compromite datele financiare ale clienților, încălcarea reglementărilor fiscale.

PLANURI DE MITIGARE A RISCURILOR

Pentru a preveni sau reduce impactul riscurilor, InfoSofTeh SRL va implementează măsuri specifice, cum ar fi:
Sisteme de securitate cibernetică avansate: Soluții antivirus, criptare a datelor și monitorizare continuă a infrastructurii IT.

Backup regulat și redundanță: Implementarea unor soluții de backup zilnic și soluții de redundanță pentru asigurarea continuității serviciilor.
Formarea continuă a personalului: Sesiuni periodice de instruire și simulări pentru echipele de suport tehnic și consultanță contabilă.
Planuri de recuperare în caz de dezastru: Crearea și implementarea unui plan detaliat pentru recuperarea rapidă a activităților critice în cazul unui incident major.

4. Domeniile cheie de afaceri și funcțiile critice

- **Suport Tehnic IT** – Asistență și troubleshooting pentru clienți care utilizează softuri contabile.
- **Mentenanță și Actualizări Software** – Instalarea patch-urilor și actualizarea aplicațiilor pentru conformitate legală și optimizare.
- **Consultanță și Training** – Instruirea utilizatorilor privind utilizarea softurilor de contabilitate.
- **Administrare Sisteme și Infrastructură IT** – Gestionarea serverelor și a platformelor utilizate de clienți.
- **Managementul Relației cu Clienții (CRM)** – Interacțiunea cu clienții și gestionarea contractelor de suport tehnic.

Funcții ale afacerii critice	**Descrierea funcțiilor critice**
Suport tehnic	Asistență pentru utilizatorii softului contabil
Gestionarea incidentelor software	Identificarea și remedierea problemelor software
Mentenanță și actualizări software	Implementarea actualizărilor critice
Consultanță și instuire utilizatorilor	Oferirea de training și suport personalizat pentru clienți.
Backup și recuperare date	Protejarea și restaurarea datelor clienților în caz de incident.
Monitorizarea infrastructurii IT	Prevenirea întreruperilor prin supravegherea sistemelor.

Având în vedere importanța serviciilor oferite, identificarea și gestionarea punctelor critice ale activității sunt esențiale pentru asigurarea continuității afacerii. Oferirea de asistență rapidă și eficientă clienților care întâmpină probleme în utilizarea software-ului de contabilitate.

Dacă această funcție este întreruptă, clienții pot întâmpina dificultăți majore în desfășurarea activității contabile, ceea ce poate duce la întârzieri în raportările financiare și la insatisfacția utilizatorilor. La fel asigurarea actualizării continue a softurilor utilizate, corectarea erorilor și optimizarea performanței acestora. Neefectuarea actualizărilor poate duce la probleme de compatibilitate, vulnerabilități de securitate și neconformitate cu legislația fiscală.

Supervizarea serverelor, bazelor de date și rețelelor pentru a detecta și preveni eventualele probleme tehnice. Dacă infrastructura IT nu este monitorizată eficient, pot apărea întreruperi neașteptate care afectează toți clienții.

Măsuri de prevenire și asigurare a continuității

- **Utilizarea sistemelor de monitorizare** care să alerteze echipa IT în timp real în cazul apariției unor probleme tehnice.
- **Implementarea unui plan de mentenanță preventivă**, pentru a reduce riscul apariției defecțiunilor și pentru a menține performanța optimă a infrastructurii IT.
- **Crearea de servere de backup**, cu scopul de a asigura redundanța serviciilor și continuitatea activității în caz de avarii sau pierderi de date.
- **Protejarea datelor clienților** împotriva atacurilor cibernetice, virușilor și accesului neautorizat. Un atac informatic poate compromite datele financiare ale clienților, ceea ce ar putea duce la pierderi financiare semnificative și la deteriorarea reputației companiei.
- **Oferirea de training și suport personalizat utilizatorilor**, pentru a optimiza utilizarea software-ului de contabilitate. Lipsa unei instruiri adecvate poate duce la erori în operare, generând probleme contabile și nemulțumirea clienților.

5. Identificarea punctelor dureroase și dependențele

În orice afacere, **identificarea punctelor dureroase și dependențelor critice** este crucială pentru dezvoltarea unui plan eficient de continuitate. Aceste puncte reprezintă acele zone vulnerabile care pot afecta operațiunile zilnice ale companiei și care pot duce la întreruperi semnificative în cazul unui incident neașteptat. În cazul unei companii care furnizează **mentenanță IT** și **suport software** pentru **evidența contabilă** la rândul nostru **InfoSofTeh SRL**, este esențial să se identifice toate resursele critice și dependențele care ar putea interfera cu serviciile oferite clienților. O întrerupere a oricărei dintre aceste resurse sau dependențe poate avea un impact considerabil asupra continuității afacerii. Un punct dureros este o **componentă critică** care, dacă devine indisponibilă, poate cauza întârzieri sau chiar oprirea activităților esențiale ale companiei. Acestea pot include resurse tehnologice, procese interne sau furnizori de servicii esențiali.

În cazul **InfoSofTeh SRL**, câteva exemple de puncte dureroase includ:

Puncte dureroase	**Descriere**
Dependența de sistemul 1C	InfoSofTeh SRL furnizează software de evidență contabilă bazat pe 1C, iar orice defecțiune a acestui sistem poate provoca întreruperi semnificative pentru clienți. Astfel, **deteriorarea aplicațiilor 1C sau pierderea accesului la datele de evidență contabilă** poate afecta grav fluxurile de lucru ale clienților.
Furnizori de infrastructură IT	Orice problemă cu serverele, rețelele sau serviciile de cloud necesare pentru **mentenanța IT** și **suportul continuu** al software-ului poate duce la pierderea temporară a accesului la aplicațiile critice. De asemenea, un atac cibernetic care compromite securitatea datelor poate afecta reputația și poate duce la costuri financiare semnificative.
Resursele umane	**Dependența de personalul tehnic calificat** care se ocupă de întreținerea software-ului și soluționarea problemelor tehnice pentru clienți poate fi un alt punct dureros. O **lipsă de personal sau absența acestora** poate duce la întârzieri în rezolvarea problemelor și poate afecta nivelul serviciilor oferite.

Într-o companie de mentenanță IT și consultanță software, dependențele critice reprezintă acele resurse externe sau interne care sunt esențiale pentru livrarea serviciilor de calitate și pentru asigurarea continuității. Aceste dependențe includ, dar nu se limitează la:

- **Furnizori de software și hardware**: InfoSofTeh SRL depinde de furnizori pentru **actualizările lunare de software** și pentru **întreținerea echipamentelor hardware** necesare pentru operarea aplicațiilor software. Un **furnizor de software sau hardware care nu mai poate furniza actualizările** sau produsele necesare poate afecta grav operabilitatea serviciilor.
- **Furnizori de servicii de cloud sau backup**: **Serviciile cloud** și soluțiile de **backup externe** sunt vitale pentru protejarea datelor clienților și pentru asigurarea recuperării rapide în caz de dezastru. O întrerupere a acestor servicii ar putea duce la pierderi de date și la întreruperea accesului la informațiile critice ale clienților.
- **Sistemele interne de monitorizare**: Sistemele interne de **monitorizare a stării aplicațiilor și hardware-ului** sunt esențiale pentru a anticipa defecțiunile și pentru a interveni rapid în cazul în care apar probleme. Lipsa unor astfel de sisteme poate duce la neidentificarea unor erori critice la timp.
- **Conectivitatea internet**: Atât pentru **comunicarea cu clienții**, cât și pentru **accesul la datele critice din cloud** sau la software-ul folosit de clienți, **internetul stabil** este esențial. O problemă la nivelul conectivității poate întrerupe complet activitățile companiei.

Măsuri de Prevenire

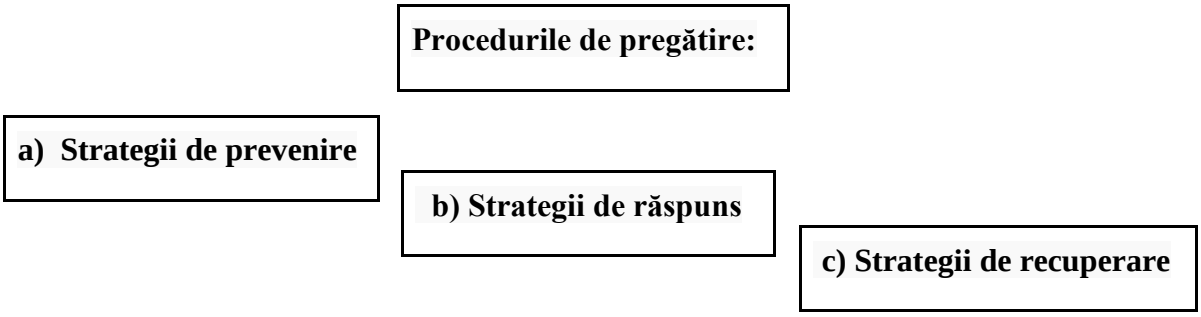
După ce punctele dureroase și dependențele critice au fost identificate, este esențial să se implementeze măsuri specifice pentru **a reduce riscurile** și **a asigura continuitatea operațională**. Aceste măsuri pot include:

- **Diversificarea surselor de aprovizionare**: Compania ar trebui să evite dependența de un singur furnizor pentru servicii esențiale și să implementeze strategii de backup pentru software și hardware.
- **Implementarea unui plan de backup robust**: Asigurarea unui plan de backup pentru datele critice ale clienților și crearea unor copii de rezervă la locații externe.
- **Formarea continuă a personalului**: Să asigurăm că toți angajații sunt instruiți în utilizarea corectă a sistemelor, pentru a reduce erorile umane și a îmbunătăți eficiența în gestionarea incidentelor.

- **Testarea regulată a planurilor de continuitate**: Planurile de continuitate și recuperare trebuie testate periodic pentru a asigura că sunt eficiente în fața riscurilor identificate.
- **Audituri Regulate de Continuitate.** Pentru a asigura că măsurile de prevenire sunt aplicate corect și funcționează așa cum este planificat, este necesar:
- **Realizarea de audituri interne și externe**: Aceste audituri pot identifica eventualele lacune în planurile de continuitate și pot adresa punctele slabe care necesită îmbunătățiri.
- **Evaluarea performanței planului**: După fiecare incident, trebuie evaluată eficiența planului de continuitate, astfel încât să se identifice ce măsuri au funcționat bine și ce trebuie îmbunătățit.
- **Managementul Comunicării în Criză.** Este esențial să fie implementate strategii eficiente de comunicare, atât intern, cât și extern:
- **Plan de comunicare pentru clienți**: Dezvoltarea unui plan detaliat de comunicare cu clienții, pentru a-i ține informați despre statusul serviciilor și despre eventualele întreruperi. Acesta poate include notificări prin email, SMS sau prin portaluri dedicate.
- **Formarea unui echipe de răspuns rapid**: Definirea unei echipe de răspuns rapid pentru crize, care să fie instruită să gestioneze atât incidentele de securitate cibernetică, cât și problemele operaționale, și să comunice rapid cu toate părțile implicate (clienți, furnizori, autorități).

6. Realizarea un plan pentru a menține operațiunile

Un plan de continuitate a afacerii este un instrument esențial pentru asigurarea că o companie poate să își mențină operațiunile chiar și în fața unor incidente neprevăzute. În contextul InfoSofTeh SRL, care oferă servicii de mentenanță IT și suport software pentru evidența contabilă, menținerea operațiunilor continue este vitală pentru a proteja datele clienților și a asigura continuitatea serviciilor esențiale. Acest plan trebuie să fie cuprinzător și să abordeze toate aspectele critice ale afacerii, inclusiv prevenirea riscurilor, răspunsul la crize și recuperarea rapidă a operațiunilor. Prin implementarea unui astfel de plan, InfoSofTeh SRL va fi în măsură să răspundă prompt și eficient la orice provocare care ar putea afecta serviciile sale.



Scopul strategiilor de prevenire este de a reduce riscurile și de a împiedica apariția unor incidente care ar putea perturba activitatea companiei. Aceste măsuri sunt esențiale pentru a asigura o protecție proactivă a sistemelor și a datelor critice, reducând astfel probabilitatea apariției unor situații de criză.

1. **Evaluarea și monitorizarea continuă a riscurilor**:

- Implementarea unui program regulat de evaluare a riscurilor pentru a identifica vulnerabilitățile și pentru a asigura că infrastructura IT și software-ul sunt actualizate constant.
- Utilizarea unor instrumente avansate de monitorizare a performanței sistemelor și rețelelor pentru a detecta eventualele erori sau defecțiuni înainte ca acestea să devină probleme majore.

2. **Securitatea cibernetică**:

- Instalarea și actualizarea constantă a soluțiilor antivirus, firewall-urilor și altor măsuri de securitate pentru a proteja infrastructura IT de atacuri cibernetice.
- Implementarea unor politici stricte de acces și criptarea datelor pentru a preveni accesul neautorizat la informațiile critice ale clienților.

3. **Backup-uri și stocare redundantă**:

- Crearea de copii de rezervă ale tuturor datelor critice ale clienților și ale sistemelor interne ale companiei. Aceste backup-uri trebuie să fie stocate într-o locație externă, preferabil într-un mediu cloud, pentru a asigura protecția acestora.
- Implementarea unor soluții redundante pentru servere și rețele, pentru a asigura că, în cazul unui incident, infrastructura esențială poate continua să funcționeze.

4. **Formarea continuă a personalului**:

- Instruirea constantă a personalului tehnic și non-tehnic în ceea ce privește procedurile de securitate, utilizarea corectă a sistemelor și reacția la incidente.
- Dezvoltarea unui plan de pregătire pentru angajați, care să includă sesiuni periodice de simulare a crizelor pentru a pregăti echipele în fața unor evenimente neprevăzute.

Strategiile de răspuns sunt esențiale pentru gestionarea eficientă a unui incident în momentul în care acesta apare. Acestea sunt destinate să asigure o reacție rapidă și coordonată, pentru a minimiza impactul crizei asupra activităților companiei.

1. **Activarea echipei de răspuns rapid**:

- Formarea unei echipe dedicate care va lua măsuri imediate în cazul unei crize, precum o defecțiune majoră a sistemului sau o breșă de securitate.
- Echipa de răspuns rapid va avea responsabilitatea de a evalua situația și de a implementa procedurile necesare pentru a limita pagubele, inclusiv de a opri temporar accesul la aplicațiile critice dacă este necesar.

2. **Comunicarea eficientă cu părțile implicate**:

- Menținerea unei comunicări clare și eficiente cu toți factorii implicați: clienți, furnizori și autorități. În acest sens, InfoSofTeh SRL va dezvolta un protocol de comunicare, care să includă mesaje predefinite pentru diferite scenarii de criză.
- Asigurarea că informațiile sunt actualizate constant și că există canale de comunicare deschise pentru a răspunde întrebărilor clienților și altor părți interesate.

3. **Izolarea și protejarea resurselor critice**:

- În cazul unui atac cibernetic sau al unei defecțiuni majore, este esențial să se izoleze sistemele afectate pentru a preveni extinderea problemei și pentru a proteja datele sensibile.
- Implementarea unui plan de izolare a rețelelor și a aplicațiilor afectate până când problema poate fi identificată și rezolvată.

4. **Asigurarea unui suport continuu pentru clienți**:

- Crearea unui sistem de suport dedicat clienților care să asigure asistență rapidă în cazul unor incidente care afectează serviciile. Acesta poate include linii telefonice dedicate, sesiuni online de live chat și un portal de suport pentru client.

După gestionarea inițială a incidentului, **strategiile de recuperare** sunt esențiale pentru a restaura operațiunile companiei și pentru a minimiza timpul de inactivitate. Aceste strategii asigură că InfoSofTeh SRL va putea să-și revină rapid la capacitatea normală de lucru.

1. **Restabilirea accesului la datele critice**:

- Restaurarea rapidă a datelor din backup-uri externe, pentru a asigura continuitatea activităților critice ale clienților.
- Implementarea unui plan de recuperare a aplicațiilor software esențiale, precum 1C, și asigurarea că acestea sunt funcționale și accesibile pentru clienți în cel mai scurt timp posibil.

2. **Reconfigurarea infrastructurii IT**:

- În cazul în care echipamentele hardware au fost afectate, InfoSofTeh SRL va asigura disponibilitatea unor resurse IT suplimentare sau redundante pentru a susține activitățile companiei.
- Restabilirea conexiunii la rețelele externe și interne pentru a asigura accesul neîntrerupt la software-ul și datele necesare.

3. **Evaluarea post-incident și învățarea din greșeli**:

- După recuperarea completă, InfoSofTeh SRL va efectua o evaluare a incidentului, identificând ce a mers bine și ce aspecte necesită îmbunătățiri.
- Actualizarea și revizuirea planurilor de continuitate pentru a reflecta lecțiile învățate și pentru a preveni apariția unor probleme similare în viitor.

4. **Recuperarea încrederii clienților**:

- Comunicarea transparentă cu clienții despre pașii făcuți pentru a rezolva incidentul și măsurile implementate pentru a preveni recurența acestuia.
- Oferirea de compensații sau măsuri corective pentru a menține relațiile pozitive cu clienții și a proteja reputația companiei.