Годишник Телекомуникации 2024, том 11, с. 61-67

Yearbook Telecommunications 2024, vol. 11, p. 61-67

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.7

STUDY OF DATA CENTER DISASTER AND EMERGENCY PLAN

Rosen Pasarelski
Alena Dobreva

Abstract: It is extremely important for every data center to have a comprehensive disaster and emergency plan to ensure the continuity of operations and the safety of personnel and data in the facility. The preparation of a disaster and emergency plan should follow a number of points and have clearly formulated goals and objectives. The goals of the plan can be systematized as follows: Data Center Continuity; Personnel Safety; Data and Asset Protection; Timely Recovery; Effective Communication; Compliance and Regulatory Compliance.

The objectives of the plan can be formulated as follows: Risk Mitigation; Emergency Response; Evacuation and Safety; Data Protection and Recovery; Security Measures; Resource Availability; Communication Plan; Training and Exercises; Documentation and Reporting; Plan Maintenance; Regulatory Compliance; Budget Allocation.

By defining these clear goals and objectives, the data center disaster and emergency plan will serve as a strategic framework for addressing a wide range of potential issues and ensuring the resilience of the center's operations.

Keywords: Data center, Plan, Disaster, Emergency, Safety.

1. INTRODUCTION

Every data center should have a well-developed disaster recovery plan to ensure continuity of operations and protection of personnel and data at the site. Creating such a plan requires following specific steps and clearly defined goals and objectives.

The plan’s goals can be summarized as follows:

- Data Center Continuity – Ensure the continued operation of critical data center functions, even in the event of unexpected emergencies or disasters.
- Personnel Safety – Prioritize the safety and well-being of data center employees, visitors, and contractors during emergencies.
- Data and Asset Protection – Protect sensitive data, equipment, and infrastructure from damage, theft, or unauthorized access.
- Timely Recovery – Enable a rapid and effective recovery process to minimize downtime and data loss in the event of an incident.
- Effective Communication – Establish clear and effective communication channels to keep stakeholders informed and coordinated during emergencies.
- Regulatory Compliance and Adherence – Verify that the plan complies with industry and government regulations and standards.

The objectives of the plan can be formulated as follows:

- Risk Mitigation – Identify and assess potential risks and hazards that could impact data center operations and develop strategies to eliminate or reduce them.
- Emergency Response – Establish a well-defined emergency response team with clear roles and responsibilities to effectively manage and coordinate actions during crises.
- Evacuation and Safety – Create comprehensive evacuation plans, including routes and assembly points, to ensure the safety of all staff and visitors during emergencies.
- Data Protection and Recovery – Develop robust data backup and recovery procedures with defined recovery time objectives (RTO) and recovery point objectives (RPO) to minimize data loss and downtime.
- Security Measures – Implement security protocols and access controls to protect the data center's physical and digital assets during incidents.
- Resource Availability – Maintain the necessary resources, such as backup power and supplies, to support operations during emergencies.
- Communication Plan – Create a communication plan that includes contact lists and procedures for notifying and updating internal and external stakeholders.
- Training and Exercises – Conduct regular emergency drills and training to ensure that personnel are prepared to respond effectively to various types of emergencies.
- Documentation and Reporting – Establish clear procedures for documenting incidents, response actions, and reporting to management and appropriate authorities.
- Plan Maintenance – Schedule routine reviews and updates to the plan to reflect changes in the data center environment and emerging risks.
- Regulatory Compliance – Confirm that the plan remains compliant with industry and government regulations and standards and adapt as necessary to meet new requirements.
- Budget Allocation – Allocate appropriate budget and resources to implement, maintain, and continually improve the plan.

By setting clear goals and objectives, a disaster and emergency response plan will provide a strategic framework for addressing various possible issues and ensure the resilience of data center operations.

2. STUDY OF THE MAIN POINTS OF THE DISASTER AND EMERGENCY PLAN

The main points that a disaster and emergency plan should follow can be systematized as follows:

- Meaning of the Plan - Explaining the importance of the plan in ensuring data center resilience. Identifying the most critical functions and assets in the data center.
- Risk Assessment - A comprehensive analysis of potential threats, such as natural disasters, power outages, and cyberattacks. Assessing the likelihood and potential impact of each identified risk to prioritize preparedness efforts.
- Emergency Response Team - Composition of the emergency response team, including roles such as incident commander, communications coordinator, and resource manager. Clear delineation of responsibilities and contact information for team members.

Годишник Телекомуникации 2024, том 11, с. 61-67

Yearbook Telecommunications 2024, vol. 11, p. 61-67

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.7

- Emergency Communications - A detailed internal and external emergency communications plan, including contact lists and procedures for notifying stakeholders. Protocols for escalating communications as the situation evolves.
- Evacuation Plan - Maps showing evacuation routes and assembly points. Special considerations for assisting employees with disabilities or special needs. Training requirements and schedules for personnel to ensure a smooth evacuation.
- Data Center Security - Policies and procedures for controlling physical access to the data center. Security measures to prevent unauthorized access during emergencies, including lockout procedures.
- Data Backup and Recovery - Clear guidelines for regular data backups and procedures for off-site storage of the facility. Defined recovery time objectives (RTO) and recovery point objectives (RPO) for critical systems and data.
- Energy Management - Description of backup power sources (e.g., generators, uninterruptible power systems). Maintenance schedules and procedures for testing backup power systems to ensure their reliability.
- Environmental Control - Explanation of temperature and humidity monitoring systems. Protocols for dealing with environmental issues, such as overheating or flooding, during emergencies.
- Fire Suppression Systems - Overview of fire suppression systems in use, such as sprinklers or fire and cleaning agents. Schedules and procedures for testing and maintaining fire suppression equipment.
- Equipment Inventory - A detailed inventory of all hardware, software, and networking equipment in the data center. Procedures for tagging assets, tracking, and regularly updating inventory.
- Vendor and Supplier Relationships - Contact information for key vendors and suppliers. Contingency plans for supply chain disruptions to ensure critical supplies can be obtained during emergencies.
- Incident Response Plan - Step-by-step procedures for responding to specific types of incidents (e.g., fire, flood, cyberattack). Clearly defined chain of command and decision-making protocols for effective response.
- Training and Exercises - Ongoing employee training programs to ensure they understand their roles during emergencies. A schedule for conducting drills and exercises to test the effectiveness of the plan and familiarize personnel with emergency procedures.
- Documentation and Reporting - Forms and templates for documenting incidents and responses. Reporting procedures for notifying management and regulators, as appropriate.
- Review and Revision - A regular schedule for reviewing and updating the plan to reflect changes in the data center environment and evolving risks. Procedures for incorporating lessons learned from previous incidents to improve preparedness.
- Regulatory Compliance - Ensuring the plan complies with relevant industry and government regulations to avoid legal and operational issues.

- Budget and Resources - Allocation of the necessary resources, including budget, personnel, and equipment, to effectively implement and maintain the plan.
- Appendices - Any additional documents, maps, contact lists, or technical specifications that accompany the plan and provide additional context during emergencies.

It is important to emphasize that a disaster and emergency plan only remains effective if it is regularly reviewed, tested, and updated to reflect changes in the data center environment and evolving risks. Also, all employees must be well-versed in the plan and receive appropriate training to be able to perform their duties effectively in critical situations.

3. ANALYSIS OF THE KEY CRITERIA FOR A SUCCESSFUL DATA CENTER DISASTER RECOVERY PLAN

Analysis of the key criteria for a successful data center disaster recovery plan

To be effective, a data center disaster recovery plan must meet several key criteria. These ensure not only the resilience of operations, but also the safety of personnel and data and can be systematized as follows:

1) Comprehensiveness and scope
- The plan should cover all possible scenarios – from natural disasters (earthquakes, floods) to technical accidents (power outages, hardware failures) and cyberattacks.
- Including a risk analysis will help identify the most serious threats and prioritize them.

2) Clear goals and responsibilities
- Defining the main goals – data protection, rapid service recovery and minimizing losses.
- Clear distribution of responsibilities among employees so that everyone knows their role in an emergency.

3) Regular testing and updating
- Conducting periodic tests (simulations) to verify the effectiveness of the plan.
- Updating the document according to changes in infrastructure, technologies and threats.

4) Flexibility and adaptability
- The plan should allow for adaptation to unexpected events and changing conditions.
- Creating alternative recovery strategies for different types of incidents.

5) Providing backup systems and backup strategies
- Availability of backup power supply systems (UPS, generators) and network connectivity.
- Building reliable backup processes and strategies for rapid data recovery.

6) Good communication and coordination
- Creating a communication plan to ensure rapid and effective exchange of information between employees.

Годишник Телекомуникации 2024, том 11, с. 61-67

Yearbook Telecommunications 2024, vol. 11, p. 61-67

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.7

- Involving external partners and customers in the incident response strategy.

7) Staff training

- Conducting regular training and drills for staff to be prepared for crisis situations.
- Documenting all procedures and providing easily accessible action guides.

A successful data center disaster and accident plan must be well structured, developed in detail and regularly updated. It must provide both technical reliability and clear operational procedures to minimize risk and ensure rapid recovery in emergency situations.

If the above criteria are followed, the data center will be able to ensure high resilience and reliability of its services, even in the event of critical incidents.

4. ANALYSIS OF THE KEY CRITERIA FOR A SUCCESSFUL DATA CENTER DISASTER RECOVERY PLAN

In this part of the article, we will present a real example of implementing a disaster and emergency plan in a data center. A scenario that demonstrates the implementation of response measures in critical situations. Practical application of incident management strategies in a data center.

Scenario: Power outage and hardware failure.

Initial situation: A large data center experiences a sudden power outage due to a failure in the local power grid. Despite the presence of backup power, an unexpected hardware failure of one of the uninterruptible power supplies (UPS) leads to a loss of power for some of the servers supporting critical services.

The process of activating the disaster and emergency plan begins immediately after the detection of a critical incident, and includes coordinated actions to minimize damage, ensure continuity of operations, and protect data and personnel.

Activating the disaster recovery plan:

- Automatic activation of backup power - Diesel generators start automatically, providing temporary power. The operating UPS devices support the servers, but the capacity is limited.
- Immediate notification to the teams - The monitoring system detects the problem and alerts the IT staff. The engineer on duty triggers the response protocol. A notification is automatically sent to key customers about a possible delay in services.
- Diagnosis and localization of the problem - The technical team checks the affected systems and finds that one of the UPSs has failed. The hardware team determines that the problem is in the UPS electronic controller. It is assessed whether the backup generator can support the systems until the UPS is replaced.

Recovery actions:

- Implementation of backup measures - The affected servers are migrated to another working power supply through automated management systems. Critical services are redirected to a backup data center to ensure there is no interruption of work.
- Repair and replacement of the failed UPS - The UPS is safely shut down to prevent additional risk. A backup UPS, previously prepared for emergency situations, is installed and tested.
- Verification and normalization of operations - After power is restored, engineers test the entire system to ensure that it is operating stably. Customers are informed of the successful restoration of services.

Follow-up actions and improvements:

- Documenting the incident - A full report of the failure, the response time and the measures taken is recorded. Why the UPS failed and whether it can be prevented in the future is analyzed.
- Updating the disaster and emergency plan - Tests show that the backup capacity was not sufficient for full coverage. It is decided to add another backup UPS and introduce more frequent system tests.
- Additional staff training - Training is conducted for faster response in similar situations. Communication between the technical and administrative teams is improved.

Thanks to a well-structured disaster and emergency plan, the critical services of the data center are restored with minimal losses. Post-incident analysis leads to additional improvements in infrastructure and processes, ensuring better protection against future incidents.

5. CONCLUSION

The correct and successful implementation of a disaster and emergency plan in data centers requires detailed preparation, clear procedures and coordinated actions. It is critically important that the plan is comprehensive, covering all possible risks – from natural disasters to technical and cyber attacks. Regular testing and updating of the plan ensures its effectiveness and adaptability to the dynamically changing environment. Providing reliable backup systems, such as alternative energy sources and backup solutions, is a key factor in minimizing losses and maintaining the continuity of operations. Good communication between all units and timely training of personnel improve the ability of teams to respond adequately in critical situations. Documentation and analysis of each incident allow lessons to be learned and improvements to be implemented in future versions of the plan. In the long term, effective emergency management increases the resilience of the data center and ensures the reliability of the services provided.

REFERENCES

[1] AKILLI, Yasin and ALI GÜNEŞ. Disaster Recovery Planning for Data Centers and IT Services. *International Advanced Research Journal in Science, Engineering and Technology* [online]. 2016, vol. 3 (6), pp. 145-149 [viewed 24.03.2025]. IARJSET. eISSN 2393-8021. Available from: 10.17148/IARJSET.2016.3627

[2] WALLACE, Michael and Lawrence WEBBER. *The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets*. 2nd edition. AMACOM, 2011. ISBN 978-0814437841.

[3] GENG, Hwaiyu. *Data Center Handbook*. John Wiley & Sons, 2015. ISBN 978-1-118-43663-9.

Годишник Телекомуникации 2024, том 11, с. 61-67

Yearbook Telecommunications 2024, vol. 11, p. 61-67

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

DOI: https://doi.org/10.33919/YTelecomm.24.11.7

[4] ПЕТРОВ, Георги. *Развитие на интернет и отворените системи*. Ч. 1. София: Авангард Прима, 2017. ISBN 978-619-160-834-8. [PETROV, Georgi. *Razvitie na internet i otvorenite sistemi.* Ch. 1. Sofia: Avangard Prima, 2017. ISBN 978-619-160-834-8.]

[5] ANGELOV, Krasen and Stanimir SADINOV. System for Remote Visualization and Control of Data From Low Voltage Power Supply Grids. In: *International Scientific Conference on Communications, Information, Electronic and Energy Systems, CIEES 2021, November 25-27, Ruse, Bulgaria: Conference Proceedings*. 2022, vol. 2570, pp. 1-6. ISSN 0094-243X.

[6] СТЕФАНОВА, Тереза. *Новите технологии: приложения, професии, умения: монография*. София: Аскони-издат, 2024. ISBN 978-954-383-151-7. [STEFANOVA, Tereza. *Novite tehnologii: prilozhenia, profesii, umenia: monografia*. Sofia: Askoni-izdat, 2024. ISBN 978-954-383-151-7.]

[7] IVANOVA, Yoana. Modeling the impact of cyber threats on a traffic control centre of urban auto transport systems. *International Journal on Information Technologies and Security*. 2017, vol. 9(2), pp. 83-95. ISSN 1313-8251.

[8] СИМЕОНОВА, Цветелина Богданова. *Развитие на перспективните технологии в „интернет на свързаните неща“ IoT (Internet of Things)*. София: Асеневци, 2021. ISBN 978-619-758-625-1. [SIMEONOVA, Tsvetelina Bogdanova. *Razvitie na perspektivnite tehnologii v „internet na svarzanite neshta“ IoT (Internet of Things).* Sofia: Asenevtsi, 2021. ISBN 978-619-758-625-1.]

[9] PASARELSKA, Teodora, Plamen TZVETKOV, and Rosen PASARELSKI. Research approach and spectrum allocation analysis for 5G network development. *33rd International Scientific Symposium „Metrology and Metrology Assurance 2023“: Proceedings*. Technical University of Sofia Publishing House, 2023, p. 15-20. ISSN 2603-3194.

[10] PASARELSKA, Teodora and Rosen PASARELSKI. The key moment in the genesis of mobile cellular systems. Control of radio links in Universal Mobile Cellular Systems. *Yearbook Telecommunications* [online]. 2022, vol. 9, pp. 69-77 [viewed 24.03.2025]. eISSN 2534-854X. Available from: https://doi.org/10.33919/YTelecomm.22.9.7

Information about the authors:

Assoc. Prof. Dr. Rosen Pasarelski, New Bulgarian University, Department of Telecommunications, rpasarelski@nbu.bg

Chief Assist. Dr. Alena Dobreva, New Bulgarian University, Department of Telecommunications, alenadobreva@abv.bg

Date of receipt of the manuscript: 28.05.2024

Date of adoption for publication: 30.09.2024