sustainability

MDPI

Article

Analysis of Territorial Risks and Protection Factors for the Business Continuity of Data Centers

Veronica Gazzola [1,*], Scira Menoni [1], Paolo Ghignatti [2], Andrea Marini [2], Roberto Mauri [2] and Giovanni Oldani [3]

[1] Department of Architecture, Built Environment and Construction Engineering, Politecnico of Milan, 20133 Milan, Italy; scira.menoni@polimi.it
[2] Kyndryl, 20054 Segrate, Italy
[3] IBM, 20054 Segrate, Italy
* Correspondence: veronica.gazzola@polimi.it

Abstract: The increasing trend towards the global use of Information Technology (IT) is currently determining the need for more and better infrastructures (both physical and digital) for processing, storing and transferring large amounts of data. As Critical Infrastructure (CI) that is potentially exposed and vulnerable to the impact of different types of phenomena (natural, technological, na-tech, etc.), data centers have to guarantee higher levels of security (physical, logical and operational), reliability and efficiency in the provision of services. Starting from a discussion of the main evidence related to this topic, considering both the most recent cases of failure and serious damage to data centers and the evolution of international and European regulation and standards, the authors propose an analytical methodology to assess the territorial risk factors for data centers by a multirisk, multi-dimensional and systemic approach. This proposal leads not only to a more explicit definition of exposure and vulnerable components, but also to the recognition of resources that—in the case of accidental events involving (directly or indirectly) data center infrastructures—may be implemented at different territorial levels as "protection" factors to ensure business continuity by considering the entire resilience cycle, from the prevention phase to the response and recovery phases.

Keywords: data centers; territorial risks; business continuity

Citation: Gazzola, V.; Menoni, S.; Ghignatti, P.; Marini, A.; Mauri, R.; Oldani, G. Analysis of Territorial Risks and Protection Factors for the Business Continuity of Data Centers. *Sustainability* **2023**, *15*, 6005. https://doi.org/10.3390/su15076005

Academic Editor: Anna Mazzi

Received: 24 November 2022
Revised: 23 March 2023
Accepted: 25 March 2023
Published: 30 March 2023

1. Introduction

In this paper, a methodology for assessing multiple risks to data centers is presented and applied in the context of the metropolitan area of Milan, Italy.

A 2018 report of the World Bank defines a data center as "a location with networked computers providing remote storage, processing, and distribution of data" [1]. Variable in size, these data centers host the servers, mainframes and cables necessary for storing and processing data. Independent data centers external to businesses, designed to provide data storage and processing services to multiple customers, are relatively new nodal points of the complex digital network that characterizes telecommunication systems nowadays. Telecommunications are part of Critical Infrastructures (CIs), intended as assets that are vital for the functioning of several businesses, services, for the functioning of our society and economy and entailing aspects of national security [2]. Telecommunication has grown in importance as other CIs, services, and economic activities are nowadays dependent on digital services and data transmission and processing. While in the past the power system was considered essential for most other systems [3], analyzing failures to critical infrastructures in the last twenty years shows that the Internet and telecommunication have become much more central than used to be the case in the past. Disruption to the Internet has provoked significant cascading impacts in several other interconnected services and critical infrastructures.

Data are the core asset that is transferred and processed by telecommunication services; therefore, there has been an increasing demand for standards of high performance to guarantee that data are not lost and that operations that rely on data processing are maintained as smoothly and safely as possible. In fact, costs related to service interruption, and even worse to data loss, explain why private operators are extremely worried about any threat that may disrupt data centers operational capacity. As an order of magnitude, following the results of surveys conducted by operators, data unavailability costs on average USD 5500 per minute, reaching amounts of USD 500,000 for a 90 min outage, which is considered the average time of a significant disruption of service [4].

Governments have only recently understood the relevance of data center protection as a key component of digital services and telecommunication, as evidenced, for example, by the new European Directive NIS 2 [5]. Not only malicious attacks, but also environmental and natural risk factors may cause "vertical" failures in data centers, causing extended damage to virtual networks and, through the latter, to various systems, including those very far from the site at which the physical damage has actually occurred.

Given the stakes associated with data management, particularly in some sectors such as health, banking, logistics, it has become increasingly relevant to safeguard data centers against potentially disruptive threats, be they cyber attacks or natural and man-made hazards. In fact, there has been a shift over the years from a concept that considered data centers as fortress-type assets that could be completely sealed from external threats to a wiser recognition of the importance the territorial and environmental context in which data centers are located in defining the type of risks and vulnerabilities that could affect them directly or indirectly. The newer trends consider that environmental and territorial risks should be fully considered and assessed in order to better plan not only protective measures, but also to make the overall telecommunication system more resilient, meaning capable of absorbing, responding and overcoming the impact from multiple threats in a way that minimize losses of data and disruption of services. As will be discussed in the following sections, despite the existence of standards, the professional literature and the experience of experts in the field, methods for assessing risks comprehensively arising from multiple threats still need to be developed, and what is available on the market is not fully satisfactory, at least in the view of the authors. Some of the latter, in fact, have been working in data centers for many years now and have witnessed themselves the evolution in thinking about risks from the inside of firms managing data centers as part of their (and later as their core) business. As will be thoroughly discussed later, the same scope of risk assessment is rapidly shifting over time from an exercise focusing on one facility at a time to a group of data centers that function to cover each other in case of emergencies.

Given this state of affairs, it is no wonder that in 2019, IBM asked a group of researchers at the Politecnico di Milano to develop a full multirisk assessment methodology for their data centers to then be applied to two facilities located in the Metropolitan area of Milan. Following that first seminal experience, in 2021 the IBM spin-off Kyndryl requested that the methodology be further developed to fully appraise different configurations of primary and recovery sites to be applied to all of their data centers in the Metropolitan area of Milan (including the first two that were already assessed in 2019). The methodology was therefore developed in two consequent stages: at first, a skeleton of the method, including the procedures for appraisal, was developed and applied in 2019; the method was subsequently refined in 2021 to fully account for multihazard conditions and the potential impact of climate change as a hazard and as a driver of other hazards triggered by meteorological extremes.

It can be said that the development of the methodology and its application resulted from a collaborative effort by the research team of the Politecnico di Milano and experts working for IBM and Kyndryl, who are co-authors of this article. The former contributed with their knowledge and prior work on developing methods for assessing territorial risks, in particular those to critical infrastructures [6,7], in developing emergency plans and territorial risk evaluations for industrial sites under the Seveso Directive [8]. The

experts working for the IBM formerly and for Kyndryl later contributed with their in-depth knowledge of the vulnerabilities of data centers to multiple threats, on the countermeasures that could or should be taken to minimize the impact. Their contribution was essential for the researchers of the Politecnico to better understand the functioning of data centers, the more recent development of both the technology and service configuration in the context of the digital services provided to the public sector, and to the banking system in Italy and Europe.

Following the framing of the problem in Section 2, a literature review, an analysis of international and European regulations and standards, and case studies of data centers disrupted by natural and man-made hazards are presented in Section 3. The methodology described in Section 4 builds on the former sections, on research on territorial risks and systemic vulnerabilities developed by the Politecnico team over years, and on the real-life experience of the managers of the Kyndryl data centers. The application of the methodology in the metropolitan area of Milan is then illustrated in Section 5. The exact location of the data centers is kept confidential, and therefore the application is shown in areas selected at random with no reference to the real plants. This does not represent an issue, though: the exemplification is in fact useful to appraise the applicability of the method to any context in which a data center is already located or could be located. In the latter case, the methodology may prove helpful to guide the selection of more suitable areas in terms of risk minimization. Section 6 discusses the obtained results.

2. Problem Framing

Telecommunication systems are complex [9], as they are constituted by different components that are interconnected in different technical ways and with rather diverse organizational and governance arrangements. According to [10], the relevance of data centers as key nodes of telecommunication systems has evolved in recent decades. From a purely in-house facility in the early times of computerization, when companies could relatively easily manage data for their business and did not need extensive sharing through a period of highly distributed systems in the early 1990s, data centers have grown again in importance in more recent years. Nowadays, companies and administrations prefer to rely on external highly specialized providers for data management and maintenance that require dedicated skills and large resources.

Data centers can be classified as critical infrastructures depending on the type of data, type of services and type of functions. For example, data centers managing data of hospitals, banks or logistics are considered critical, and are accordingly required to provide the maximal protection and security to both information storage and processing. External providers who are highly specialized can guarantee a level of reliability that would be impossible or extremely costly to host in house. The problem of avoiding the loss of data or the interruption of critical transactions is now entrusted to data center providers who are asked to guarantee high reliability even in case of incidents and disasters, natural and man-made.

While data recovery was initially ensured physically via tapes that were stored at another site to guarantee redundancy, new information technologies now permit the full duplication of datasets in an easier and more reliable way in different locations that mirror each other [11]. The duplication of data and processes to manage them can be synchronous or asynchronous, meaning by that the possibility to retrieve full operations in the site where data are duplicated or instead requiring sometime for full retrieval [12]. The site at which data are duplicated is referred to as the "recovery" site of a primary one where the operations and data storage take place under normal conditions. However, this configuration should not be thought of in a rigid way; nor should the designation of primary or recovery site be considered as a fixed inherent feature of data centers. In fact, the decision regarding which to consider as the primary or secondary site is dynamic and may change given new needs or different circumstances. As technology evolves and possibilities for replicating data and processes faster and more easily become available, the

connotations of primary and recovery sites blur. Furthermore, as the cost of replication diminishes, multiple site architectures depending on the nature of data and processes to be guaranteed can be considered, featuring a real "ecosystem approach" for safe and secure data management.

Among the aspects that must be considered to define a suitable, optimal architecture of primary–recovery data center configurations [13], the siting of the two (or more) facilities is a rather important one. Locational choices must also consider the potential threats to which data center facilities may be exposed to [14]. This is a not trivial problem when a "couple" or multisite configuration is considered. In fact, the recovery site works only on the condition that it is independent from the primary one, meaning that the same event cannot affect and disrupt both simultaneously. On the other hand, there is a limit to the distance that can be kept between two sites where one represents the recovery of the other [12]. The possibility of fully synchronizing data and processes diminishes with increasing distance due to the greater latency, which may induce data losses. In addition, it must be said that distance is not a relevant parameter when it comes to assessing exposure and vulnerability to different types of threat. Fixed predetermined distances are not viable in certain geographic settings and are not supported by clear evidence [13]. For example, the distance from a hazardous installation depends on the damage areas related to likely top even incident scenarios, flooding depends not only on the distance from the main watercourse, but also on the topography, etc. Furthermore, a multihazard, multirisk approach is required, especially in areas that are exposed to multiple threats. Multihazard and multirisk assessments are not trivial either, and not many methods are available for practical application.

Therefore, the locational choice of couple or multisite configurations becomes an exercise of multifactor optimization balancing between the requirement of high reliability, distance at which mirroring is still possible, and the need to avoid the facilities being disrupted by the same hazardous event, or by multiple events occurring simultaneously or cascading. A full classification of multihazard conditions is available in [15]. It builds on research by [16,17] that foresees different types of interaction among hazards. Multihazard conditions, especially in terms of cascading impacts, i.e., where one hazard is triggered by another one, are more likely in complex metropolitan regions or in environmental conditions such as coastal areas [18].

The locational choice or the assessment of already existing data center locations must therefore be split into the following parts: first, a method for assessing the risks posed by multiple hazards to data centers must be provided. In the risk assessment, both direct and indirect damage must be estimated [13]. The former regards the physical integrity of the facilities, the second evaluates the potential data loss. It should be pointed out that data loss is not necessarily only the outcome of physical disruption, it may also occur as a result of extended power or telecommunication outages that may affect external lifelines on which data centers rely for their functioning. Therefore, the problem of assessing risks to data centers cannot be limited to the facility itself and its immediate surroundings; it must instead comprehensively consider the geographic area where the data center is located. Damage to lifelines, vital services, may affect the functionality of data centers in many ways, due to power or telecommunication outages, or impeding the workforce from reaching the site for ordinary or extraordinary operations particularly in case of extreme events. A territorial perspective must be therefore adopted, considering risks at the relevant spatial scale to capture the interconnection between data centers, other critical infrastructures, environmental conditions, the urban fabric. Such a methodology is useful to both decide where to locate a new facility or to assess the risk of existing facilities.

The second part of the problem requires the method to capture the risk of the couple or the multisite configuration of primary and recovery sites. In this latter case, the main question is whether or not an event may affect both sites at the same time, therefore provoking the unserviceability of both, making the redundancy of replicated data and processes ineffective.

3. Knowledge Base for Assessing Data Centers' Exposure and Vulnerability to Multiple Hazards

In order to tackle the problem framed in the previous section, first the existing knowledge base for assessing the environmental and territorial risks to data centers was searched. First, a literature review was carried out, then existing international standards were considered. The latter, in fact, embed the experience gained insofar by data center managers and data management service providers in an attempt to guarantee high-level reliability to their customers. Standards provide a classification of increasingly reliable data centers on the basis of the safety measures they adopt to guarantee business continuity [19], including under adverse circumstances.

3.1. Literature Review

During the development of the methodology described in Section 4, the literature was already consulted, even though it turned out to be rather scarce. To address different aspects, such as the description of incidents, and the reasons for their occurrence, we referred to reports and articles in specialized magazines published by professional associations and by companies that provide standard certification (such as Uptime and Ponemon, see Section 3.3).

A further more in-depth and systematic search for relevant literature representative of the state of current approaches/methodologies to analyze/assess territorial risk conditions (natural and technological) for data centers was carried out in the Web of Science™, Scopus, and ScienceDirect online platforms using key words and Boolean search criteria. The following key words and combination were used (with appropriate inclusion of plural and other derivates where appropriate): "data center/data centre", "risk/hazard/disaster/threat", "analysis/assessment", "territorial/environment", "single/multisite", "availability/security/protection" and "resilience/business continuity". This resulted in 63 references spanning a 15-year period (2007–2022). This database comprises the material for our analysis and is available in File S1. Out of 63 references, only 16 address the issues relevant to the problem as framed in Section 2 (Table 1). About 36% were peer-reviewed scientific journal articles and about 64% were conference proceedings. The database was categorized into three subgroups:

A. "Risks/threats/hazards" subgroup descriptive of the potential disasters and failures (resulting in huge economic loss) faced by data centers as complex systems. This subgroup was used to analyze the main incidents occurring in data centers as a consequence of natural hazards in Section 3.3.
B. "Availability, security and business continuity" subgroup about efficient measures/standards/methods for maintaining protection and service continuity of data centers during failures. This subgroup was used to support the development of the methodology as described in Section 4.
C. "Geographical distribution/Location selection" subgroup discussing strategies for backup of critical business data across multiple data centers (in different geographical locations), avoiding simultaneous failure of backup and primary servers. This subgroup was used to help fine tune the methodology described in Section 4.

Most publications focus on the protection of the asset itself, making the building safe and protecting the storage and processing systems of data from external stressors [14,20,21]. Fewer publications consider the interface between data centers as assets and systems with the environmental and territorial context [22,23] as a potential source of both threats and vulnerabilities, due to the systemic interconnections and interdependencies between data centers, power, telecommunication, and transportation systems [11,13].

Table 1. Classification of the references found in the literature review according to the problem framing.

References	Subgroup A	Subgroup B	Subgroup C
Gomes, R., Lapo, L.V. (2008). The adoption of IT security standards in a healthcare environment. Studies in Health Technology and Informatics 136, pp. 765–770.		x	
Economics of Grids, Clouds, Systems, and Services—8th International Workshop, GECON 2011, Revised Selected Papers (2012)			x
Ceballos, J., Dipasquale, R., Feldman, R. (2012). Business continuity and security in datacenter interconnection. Bell Labs Technical Journal 17(3), pp. 147–155	x		x
Benz, S., De Sousa, L.P., Pedone, F. (2016) Stretching Multi-Ring Paxos. Proceedings of the ACM Symposium on Applied Computing 04–08-April-2016, pp. 492–499.			x
Sengupta S., K.M. Annerva (2014), Multisite data distribution for disaster recovery—A planning framework, Future Generation Computer Systems Volume 41, December 2014, 53–64.	x	x	
Yang C. L., B. J. C. Yuan, C-Y. Huang (2015) Key Determinant Derivations for Information Technology Disaster Recovery Site Selection by the Multi-Criterion Decision Making Method, Sustainability 2015, 7, 6149–6188		x	x
Ferdousi, S., Dikbiyik, F., Habib, M.F., Tornatore, M., Mukherjee, B. (2015). Disaster-aware datacenter placement and dynamic content management in cloud networks. Journal of Optical Communications and Networking 7(7), pp. 681–694.	x		x
Faccioni, M. (2016). Complex Systems: Risk Model Based on Social Network Analysis. IEEE International Symposium on Industrial Electronics 2016-November, 7744859, pp. 22–27.	x		
Proceedings of the 2016 12th International Conference on the Design of Reliable Communication Networks, DRCN 2016	x	x	
Puthal, D., Nepal, S., Ranjan, R., Chen, J. (2016) Threats to Networking Cloud and Edge Datacenters in the Internet of Things. ACM Transactions on Cyber-Physical Systems 4(3), 3351882.	x	x	
Li, X., Wang, H., Yi, S., Liu, S., Zhai, L., Jiang, C. (2019). Disaster-and-Evacuation-Aware Backup Datacenter Placement Based on Multi-Objective Optimization. IEEE Access 7, 6287639, pp. 48196–48208.	x		x
Jha, P., Sharma, A. (2021). Framework to Analyze Malicious Behaviour in Cloud Environment using Machine Learning Techniques. 2021 International Conference on Computer Communication and Informatics, ICCCI 2021 9402671		x	
Das, S., Panda, K.G., Sen, D., Arif, W. (2021). Maximizing Last-Minute Backup in Endangered Time-Varying Inter-Datacenter Networks. IEEE/ACM Transactions on Networking 29(6), pp. 2646–2663.	x		
Liu, Y., Zhou, F., Chen, C., Zhu, Z., Shang, T., Torres-Moreno, J.-M. (2021). Disaster Protection in Inter-DataCenter Networks Leveraging Cooperative Storage. IEEE Transactions on Network and Service Management 18(3), 9459187, pp. 2598–2611.	x	x	
Sharma, A., Jha, P., Singh, S. (2021). Data control in public cloud computing: Issues and challenges. Recent Advances in Computer Science and Communications 14(2), pp. 564–579.		x	
Liu, Y., Zhou, F., Shang, T., Torres-Moreno, J.-M. (2022). Power-efficient and Distance-adaptive Disaster Protection for Service Function Chain Provisioning. 2022 IEEE Global Communications Conference, GLOBECOM 2022—Proceedings pp. 4407–4412		x	

More recently, various publications have focused on climate change as a worrying source of threats to data centers [22–26] and to which they are vulnerable in multiple ways. As they require constant refrigeration due to the heating developed by constantly running servers, they are particularly dependent on energy and water to maintain the

required temperature [12]. During prolonged drought periods or water scarcity, blackouts are likely to increasingly affect data centers, especially those that are located in milder climatic regions, such as Italy. Furthermore, climate change is likely to change the pattern of floods, both riverine and flash, of fires threatening semi-urban areas in periods with combined low precipitation and water scarcity. Such concerns have been explained in reports mandated by the UK Government [22,23]. In the latter, good practices that have been developed by telecommunications providers to counteract the impacts of climate change and increase the resilience of data management services, including specific actions on data centers, are illustrated.

3.2. State of the Art of the Main Standard in the Context of Territorial, Environmental and Climate Change Risk Assessment of Data Centers

Given the growing number of data driven sectors, from finance to healthcare [27] and public administration, extremely high levels of security (physical, logical and operational), reliability and efficiency in the provision of services are demanded. To satisfy the latter, both legislative and standardization efforts are constantly reshaping the market. As for legislation, in Europe for example Network and Information Security Directive (EU 2016/1148) [5], best known as NIS2, established measures aimed at achieving a common high-level security of network and information systems to improve the functioning of the internal market. In the Directive, which replaces a previous one passed only a few years ago (in 2016), for the first time, an explicit reference to the safety of data centers is made. Contextually, there is also the new European Directive (EU) 2022/2557 on the Resilience of Critical Entities [28], which shifts from the concept of protection to that of resilience management. The new directive calls for a systemic consideration of the multiple risks to which infrastructures are potentially exposed and vulnerable in a comprehensive manner, indicating the responsibility of operators as the key element complementary to the physical integrity of assets.

Entities are required to undertake actions aimed not only at preventing incidents but also at enhancing their capacity to restore and recover information services following a proactive approach that is not limited to defining the response to an adverse event, but extends to adopting procedures to ensure business continuity even in case of exceptional events.

The NIS 2 Directive explicitly calls for the adoption of standards that have been developed by the private sector over time to ensure increasing levels of reliability in the telecommunications sector. For more than 30 years, the reliability of data centers has been certified in order to define their ability to cope with possible unforeseen events (i.e., blackouts, fires, etc.) and guarantee business continuity in service provision. Adherence to the standards is voluntary, but the resulting certification is a safety factor and a guarantee for the end user. Currently, the most widely known certification is the Tier Certification by the American Uptime Institute, which distinguishes four classes of data center, assigning each one a different level of "solidity" (Tier I, II, III and IV). In addition, there is another method of certification, the ANSI/TIA-942 [29] standard by the Telecommunications Industry Association, accredited by the American National Standard Institute (ANSI). It specifies the requirements for the design and location of data centers according to four security levels (Table 2). The security levels establish increasingly high degrees of redundancy and reliability in data network, electrical and mechanical systems. In Italy, public administration data centers follow the ANSI/TIA-942.

While the concept of reliability may be relatively simple to define according to the international and European standards mentioned above, the methodological steps to follow to assess the potentially risks that may affect at different territorial levels electricity supply, telecommunications networks, environmental controls and building locations (and their mitigation measures consequently) are less trivial to develop. Over time, several standards have provided some key elements on the topic. Specifically, ISO/IEC 27031 [30] provides specific guidelines for the IT and telecommunications system detailing all issues necessary for supporting IT system recovery, and makes explicit what risk assessment should consist

of, such as a systematic process of risk identification, analysis and assessment. In 2012, CENELEC (Comité Européen de Normalisation Électrotechnique) released the EN 50600 standard [31], providing recommendations for data center design, operational management, energy assurance, and environmental sustainability. Moreover, ISO/IEC 24762 [32] requires natural hazards and the potential impacts of climate change on ITs and telecommunications infrastructures to be taken into account. This is an important standard, as it brings to the attention of the operators the existence of some environmental factors that are external to the data center, potentially impacting it.

Table 2. Data center classification according to levels of availability. Source: [29] modified.

Levels of Availability	Specifications of Protection and Redundancy	Business Continuity	Annual Downtown
Tier I Basic data center	No redundancy in the power supply and mechanical systems (air conditioning and fire protection). Limited protection against physical events. Single redundant components, single distribution path serving equipment.	99.671%	28.8 h
Tier II Data center with limited redundancy	Power supply systems and mechanical systems (air conditioning and fire protection) have their main elements with N + 1 redundancy level. Better protection from physical events.	99.741%	22 h
Tier III Data center with possibility of maintenance without availability interruptions	Multiple independent components and distribution paths to equipment. A part may be subject to maintenance by replacement (removal/overhaul without interruption of plant availability). Protection from most physical events.	99.982%	1.6 h
Tier IV Data center exempt to single failure	Multiple independent components and distribution paths to equipment. Possible simultaneous maintenance without interruption of plant availability. Protection from almost all physical events.	99.995%	26 min

The Uptime Institute [33] stresses the importance of assessing different types of risk, such as:

1. Local site-level risks due to extreme weather events or phenomena (such as sea level rise) that may lead to a prolonged change in site conditions;
2. Territorial (regional/provincial) risks that are not directly related to the site, but which may nevertheless have important impacts on the availability of supplies, services and/or personnel.

With regard to banking and financial services, as an example, the Italian Circular 285/2013 and subsequent updates up on "Supervisory Provision Banks" (18 September 2019) [34] can be considered. The Circular mandates that business continuity plans start from an analysis of possible impacts due to some specific characteristics of the context, such as in terms of probability of disaster: the location of the relevant sites (e.g., seismicity of the area, hydro-geological instability of the territory, proximity to dangerous industrial settlements, proximity to airports or institutions with high symbolic value). The site at which to locate data centers should be chosen on the basis of an assessment of the territorial hazards, climate change and their impacts on the physical infrastructure and on the accessibility. The Circular also requires data be duplicated at two alternative sites, one of which is data disaster recovery. It is, therefore, essential to define conditions that ensure that the two data centers cannot be involved simultaneously in the same adverse or incidental event. Regarding this, the Circular 285/2013 [34] also provides guidance on alternative sites, suggesting they be located at a reasonable distance from

the primary sites in order to ensure a high degree of independence between the two. In addition, they must use services (telecommunications, energy, water, etc.) distinct from those used in production. If this condition is not verified, a rigorous evaluation is required, supported by the opinions of qualified professionals in order to understand the probability of simultaneous unavailability of primary and alternative sites, minimizing the risk that they are impacted by the same event.

According to the newly proposed European Regulation on Digital Resilience for the Financial Sector [35], known as DORA, backup sites must have specific characteristics (art. 11), such as being:

(a) Geographically located at a distance from the primary data processing site to ensure a distinct risk profile and prevent it from being affected by the same event affecting the primary site;
(b) Capable of ensuring the continuity of critical services in an identical manner to the primary site;
(c) Immediately accessible to the staff to ensure the continuity of critical services if the primary data processing site becomes unavailable.

3.3. Analysis of the Main Incidents Occurring in Data Centers as a Consequence of Natural Hazards

Despite constant technological improvements, the number of incidents is currently increasing rather than decreasing, in the form of outages disrupting data center operations and leading to significant costs and data loss. As revealed by an Uptime Institute survey [36], outages have become more frequent and costly in recent years (Figure 1). Moreover, costs associated with data center loss of functionality are set to rise further in the future as an increasing of activities number depend on telecommunication network and digital infrastructures.

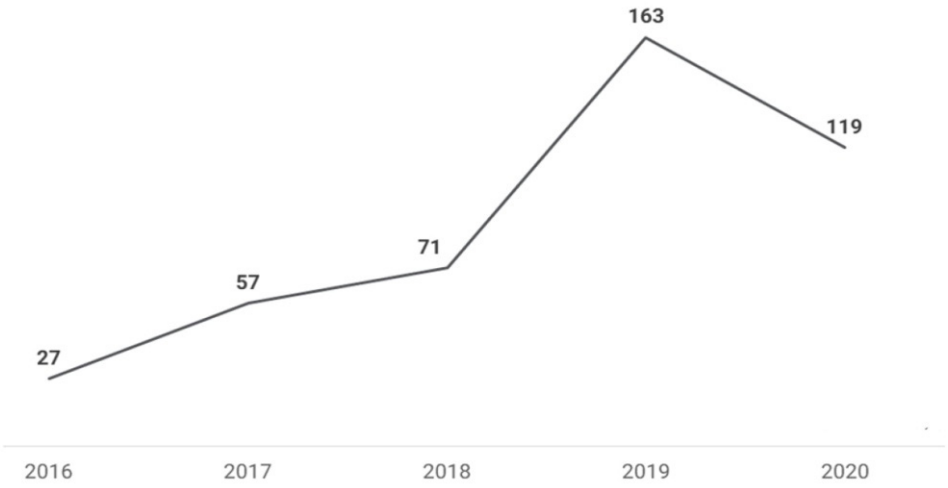

Figure 1. Trend in data center number of outages (y-axis) reported from 2016 to 2020 (x-axis). Source: [36].

In 2019, 34% of 1600 surveyed companies reported a service disruption and severe degradation incidents to IT functions with an increasing of 31% and 25% to 2018 and 2017, respectively. This increase, which could also correspond to an improvement in the capability of tracking down information about outages by consulting more reliable sources (such as public media, surveys, incident reports), also emerges from another study provided by the Ponemon Institute [37]. With regard to the causes, about 70% of incidents were due to failure of uninterruptible power supplies, cyberattacks and human errors; about 20% were due to flooding, heat waves and extreme weather events. In 2020, despite the sharp break in the trend (Figure 1), partly due to the pandemic crisis reducing the business activities globally, 50% of the reported incidents were rated as very serious (catastrophic) or

serious. Power outages (80%) and software and/or network infrastructures problems were identified as the main causes. The average value of downtime was 95 min per year with an average cost of USD 740,357 per activity, roughly equivalent to an hourly cost of downtime of over USD 460,000. Evaluating costs by sector, the highest was reported in the financial sector (USD 994,000) followed by communications (USD 970,000), healthcare (USD 918,000) and e-commerce (USD 909,000) sectors. Indirect effects such as loss of reputation, customer complaints and the high repair cost of IT devices must be also added. In addition to already unfolding trends, the Uptime Institute [38] also reveals the current worrying levels of exposure and vulnerability to future Climate Change as forecast by the IPCC more recent report [39]. From 2018 to 2020, 45% of surveyed operators have experienced at least one extreme weather event that threatened their business continuity; while the majority did not report serious consequences, around 10% reported a serious interruption or disruption.

The analysis of several case studies about accidental events affecting (directly or indirectly) data centers highlights the strong dependence of telecommunication system on power, water, and transport networks. Such dependencies constitute an evident systemic vulnerability, especially due to the possible knock-on effects that may occur during larger-scale disasters, even in cases where the facilities themselves are not physically damaged [40]. For instance, in 2012, Hurricane Sandy provoked significant direct and indirect damage to data centers in New York [41,42], knocking out 25% of cellular antennas of many operators along the East Coast. Moreover, flooding prevented technicians from accessing the damaged facilities hampering the installation of temporary antennas. Similarly, in the aftermath of Hurricane Katrina in August 2005 in the city of New Orleans, flooding provoked leakage of water into a data center through damaged openings, provoking power outage. Power restoration led to an overheating that damaged several components, including the air conditioning system, some switches, and cables. The repair costed USD 3M and took several months.

In 2014, a major digital network service provider in the UK was deprived of electrical power during a storm, compromising internet services, including e-mail, for many customers. Due to the concurrent failure of telecommunications network customers could neither be alerted nor updated on the recovery process which took several days.

An analysis of the case studies highlights the importance of considering not only the safety and protection of installations, but also their territorial context, as serious emergencies may hinder repair and response actions that would be almost routine in normal conditions. The impossibility of accessing damaged areas is a common factor recalled in many of the selected case studies. Competing organizational factors have further worsened operating conditions, such as the failure to update work files or the unavailability of telecommunication networks in the most affected areas, not allowing key personnel to telework.

Alongside extreme weather events, another source of great concern for data center operators is fires, such as the recent one that destroyed the facility if OVHcloud in Strasbourg in March 2021. French government offices, a British motor vehicle authority, and the European Space Agency (ESA) suffered data disruption as a consequence of the incident. Among the considered causes were reported the innovative technology used to cool the plant, a tower shape that would have caused a sort of "chimney" effect, and the lack of adequate fire prevention measures. It must be also highlighted that a rather large percentage of the incidents that have occurred could have been avoided (76% in 2021 compared to 60% in 2019), according to plants managers interviewed by Uptime Institute [38].

Finally, it is worth mentioning that the COVID-19 pandemic constituted a significant "stress test" for the telecommunications sector as a whole, and more specifically for data centers. Operators had to face and solve multiple challenges to guarantee the presence of the minimum number of staff necessary for business continuity while ensuring the full adoption of health restrictions measures aimed at for example avoiding physical contact between operators, requiring operators living near the sites to go to work premises

to avoid long displacements, ensuring the availability of materials for sanitization and air purification.

In a nutshell, the analysis shows that, despite being a highly innovative sector, telecommunication remains potentially vulnerable to extreme events and to the direct impacts of climate change. Among the analyzed case studies, a very common element triggering enchained failures is inadvertently provoked by emergency interventions that are not always prepared and adequate to deal with exceptionally challenging operational conditions [43].

4. Analytical Methodology for the Assessment of Territorial Risks and Protection Factors for the Business Continuity of Data Centers

International standards and existing guidelines provide a rather generic framework for assessing risk in data centers, referring to the methodologies that are mostly used for other assets and systems. Furthermore, such methods focus on the plants without sufficient consideration of their interaction with the environment and with the territory in which they are located. However, as can be seen from the literature review and the case studies, such interactions have been the cause of several failures. In addition, a paradigm shift has also occurred as a result of safety mangers, who increasingly understand the limitations of an approach that does not consider such complex interactions. Resilience thinking was at the core of the discussions between the plant safety managers and the researchers and inspired the development of the methodological framework. Resilience thinking stems from the understanding that it is impossible to avoid the occurrence of stressful conditions that may lead to an incident, even with the best technologies and organizational practice, particularly in multihazard contexts [44]. As a result, the method considers risk reduction measures ex ante, in order to diminish the potential of failures, even in conditions of environmental stress also induced by climate change, as well as capacities and interventions for recovery so as to minimize data losses [45].

Based on the literature review, on the case studies, on the expert knowledge of the managers of the Kyndryl data centers, and on the experience of the research team [6–8], a framework was developed to account for both physical and systemic vulnerabilities. This framework accounts for both multihazard and multirisk conditions and for the potential impact of climate change. Climate change is intended as a hazard per se (inducing for example heat waves), and as a factor worsening other hazards (such as fires, droughts, and storms).

The core elements of the framework are synthesized in Figure 2. The joint consideration of threats, vulnerabilities, potential impacts, and possible countermeasures takes inspiration from the Dow method, adopted for analyzing risk in hazardous industrial installations [46], as each risk is balanced against the mitigation measures that may be enforced.

In the first two boxes in the upper left part of Figure 2, the hazard factors are considered, namely: i. climate change as both a hazard and a stressor of other hazards; and ii. natural, health and man-made hazards. Along the same lines, the vulnerability of data centers intended as single assets to multiple hazards is considered. The third box in the first line accounts instead for the vulnerabilities to multiple hazards of the territory in which a data center is located.

Following the conceptual framework of the Ensure project [47], the systemic vulnerability represents a second-order factor, as illustrated in the second box in the second line. In the first box in the second line, the physical damage scenario derives from the combination of hazards, the vulnerability of data centers and of their territorial context. Systemic vulnerability depicts the response capacity (or lack of) to the physical damage that has occurred to one or more components of data centers or to systems they depend on for their functioning, as depicted in the second box in the second line. Systemic damage, due, for example, to the disruption of transportation or power system in the area, is derived from the combination of physical damage and systemic vulnerability as depicted in the box in the last line.

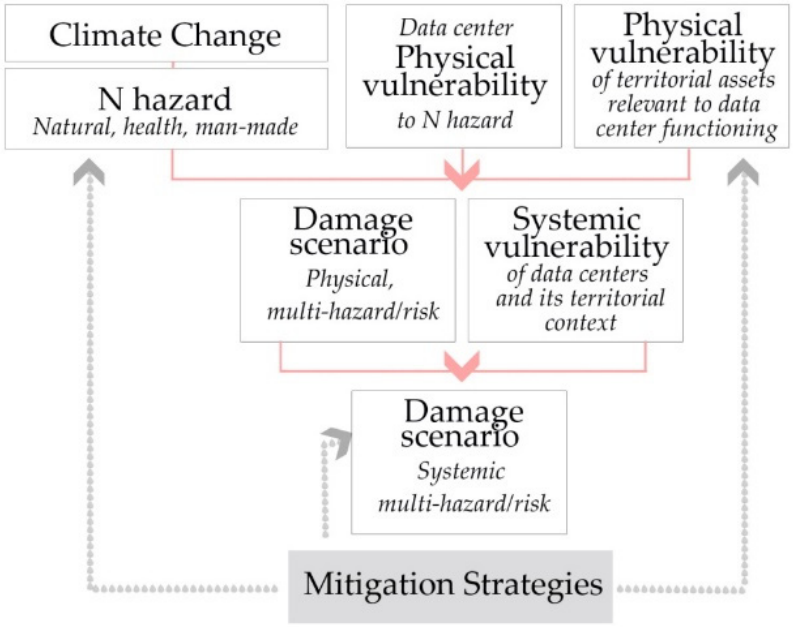

Figure 2. Conceptual scheme of the analytical methodology proposed for multihazard and multirisk assessment of data centers. Source: elaboration by the authors.

Mitigation strategies in the grey box are aimed at contrasting the systemic damage and the various components of both physical and systemic damage scenarios. Such measures are aimed at reducing the hazard potential, making the data centers more robust structurally and less dependent on external services, and increasing the response capacity and the resilience of the territory and critical services. As shown in the figure, mitigation measures are aimed at reducing the potential of systemic failure but also recovering from it, using all resources that can be put in place both internally to the plants and in collaboration with civil protection and rescue organizations.

In order to operationalize the framework in Figure 2, Table 3 lays down the various indicators that should be considered when determining the location of data centers and protecting them from the impacts of hazards.

Table 3. Impacts on data centers, territorial networks, and personnel as a consequence of hazards.

Hazard and Territorial Scale of Event	Climate Change Impact	Multihazard, Multirisk	Impacts -> Mitigation Measures	
			Direct Impact on Data Center (☒)	Indirect Impact on Territorial Networks & Personnel (◎)
Seismic Regional	-	⌘→ Landslides Tsunami	Collapse of walls, damage to plants (including generators) and equipment -> Seismic and anchoring structures	Damage to buildings and infrastructure, difficulties of access and personnel, damage to service networks -> Support of personnel outside the area, electric and water autonomy, radio connections
Volcanic Regional for ash, local for other hazards	-	⌘→ Landslides Tsunami ⌘ Seismic	High temperature plant damage; ash damage to all plant components -> Avoid locating near active volcanoes	Locally inaccessible area until end of phenomena, for ash relevant on accessibility and networks -> At least temporary relocation

Table 3. *Cont.*

Hazard and Territorial Scale of Event	Climate Change Impact	Multihazard, Multirisk	Impacts -> Mitigation Measures	
			Direct Impact on Data Center (⊠)	Indirect Impact on Territorial Networks & Personnel (◎)
Hydraulic Regional, local	⇃↑ It could increase/decrease depending on the area	⌘→ Landslides ⌘ Heavy rainfalls	Damage to plants by water contact or humidity -> Lift the installations with respect to level "0", humidity control	Damage to transport, electricity and telecommunications networks -> Access redundancy, electric/water autonomy, radio connections and mobile devices (switch etc.)
Tsunami Regional	-	⌘→ Flooding	Damage to plants by water contact or humidity -> Avoid localization in at risk areas (coastal areas)	Damage to transport, electricity and telecommunications networks -> Support of personnel outside the area, access redundancy, electric and water autonomy, radio connections
Hydro-geological Local and/or multisite	⇃↑ It could increase/decrease depending on the area	-	Damage to structures by direct impact -> Avoid localization in at risk areas (near or under landslide areas)	Interruptions of transport and electricity network (flooding of rooms) -> Redundancy of transport networks and electric autonomy, radio connections
Avalanche Local and/or multisite	⇃↑ It could increase/decrease depending on the area	-	Damage to structures by direct impact and by water contact or humidity -> Avoid localization in at risk areas	Punctual damage to transport system and control units -> Redundancy or autonomy for a few hours
Heavy rainfall Regional, wide area	⇃↑ Heavy rainfall events	⌘→ Flooding Landslides	Damage due to winds and induced events (rainfall, flooding) -> Resistant structures (roofing) and lightning protection	Damage to transport, electricity and telecommunications networks -> Access redundancy, electric autonomy for a few hours, telecommunications network support
Lightening Local	↑	-	Damage to electrical equipment -> Lightning protection	Punctual damage to telecommunications system and electrical control units -> Devices protection
Heavy snowfall Regional	⇃↑ Decrease in annual average precipitation but occasional extreme events	-	Structural damages -> Resistant structures (roofing)	Damage to transport, electricity and telecommunications networks -> Access network redundancy, electric autonomy for a few hours/days, radio connections
Wind storm Regional	↑	⌘ Flooding Heavy rainfalls	Structural damages, equipment damage due to dust -> Resistant structures (roofing), external ventilation shutdown, filter cleaning, server access blocks	Punctual damage to transport system (trees), electrical, transport and telecommunications control units -> Access network redundancy, electric autonomy for a few hours, telecommunications network support
Drought Regional	Trend in precipitation reduction on the basis of past data	-	Water availability problems -> Water system autonomy	Water deficit -> Autonomy for a few days/months, closed-loop systems

Table 3. *Cont.*

Hazard and Territorial Scale of Event	Climate Change Impact	Multihazard, Multirisk	Impacts -> Mitigation Measures	
			Direct Impact on Data Center (⊠)	Indirect Impact on Territorial Networks & Personnel (◎)
Forest fire Regional, local	↑	⌘→ Landslides	Structural and plants damages -> Avoid localization in at risk areas	Damage to transport, electricity and telecommunications networks, air conditioning and filtration systems -> Electric autonomy and radio connections
Heat wave Regional	↑	-	Plants damages -> Modernization of air conditioning systems and e use of electrical generators for self-production	Power outages due to overcharging of the public network -> Electric autonomy for a few hours/days by electrical generator
Sea level rise Regional	↑	⌘→ Coastal flooding	Plants damages due to water contact and humidity -> Avoid localization in at risk areas	Damage to transport, electricity and telecommunications networks -> Verification of dependence on coastal networks
Epidemic/Pandemic Regional, national	↑ Several studies show a correlation with Climate Change	-	Impact on the availability of staff -> Remote work but need for presence of critical workers on site	Impact on population
Installations at major accident risk Regional, local	-	⌘→Na-tech due to: Flooding Earthquakes Landslides Tsunami Storms	Damage to structures if located in damage areas, dust infiltration and/or toxic substances -> Localization of the plants in damage, verification not Seveso plants	Interruption of the transport network -> Shift to air recirculation system
Transport of dangerous substances Local	-	-	Damage to structures and electrical and telecommunications unit controls in case of proximity of the event -> Avoid location adjacent to high-speed roads	Interruption of the transport network -> On site in case of prolongedstay conditions
Aquifer pollution Regional and local	-	⌘← Flooding ⌘→ Installations at major accident risk	Damage to the cooling system -> Monitoring system of aquifer pollutants	Water supply disruption -> Shift to traditional conditioning, closed-loop systems
Road accident Local	-	-	Damage to structures and electrical and telecommunications unit controls in case of proximity of the event -> Avoid location adjacent to high-speed roads	Interruption of the transport network -> On site in case of prolonged stay conditions
Excavations/ road works Local	-	-	Power supply loss -> Diversification of access routes to data center	Power supply loss -> Redundancy of the networks
Sabotage Local, multisite	-	-	Intentional damage to structures and plants -> Data protection measures and staff monitoring	Vandalism and/or terrorism in sensitive targets close to the data center -> Avoid localization near known sensitive targets

Table 3. *Cont.*

Hazard and Territorial Scale of Event	Climate Change Impact	Multihazard, Multirisk	Impacts -> Mitigation Measures	
			Direct Impact on Data Center (⊠)	Indirect Impact on Territorial Networks & Personnel (◎)
⌘ Multirisk			↓ Climate Change impact: reduction of hazard frequency/severity	
⌘→ Multirisk: event that can be triggered by			↑ Climate Change impact: increase in hazard frequency/severity	
⌘← Multirisk: hazard that can trigger another one			↓↑ Climate Change impact: hazard could increase/decrease depending on the area	

The table is organized as follows: in the first column, all considered hazards are listed and their territorial scale is specified. For example, a landslide is a rather local event, whereas a flood may be regional, a storm can be interregional or even cross-country. The scale is important as a location factor: while it is relatively easy to avoid flood-prone areas or being in the trajectory of an active landslide, it is more difficult to avoid seismic areas, in a country that is almost entirely seismic, or the trajectories of large storms. In the second column, the arrows show the potential impact of climate change on the specific hazard considered. The double arrow refers to the possibility that Climate Change increases or decreases the hazard, while the single-direction arrow indicates either a decrease or an increase. The third column is related to the multihazard condition, showing the types of hazards that may be triggered by other hazards.

The knot symbol (⌘) represents the multihazard condition, while the arrows specify whether the relative hazard is triggered or may trigger those that are named in the third column below the symbols. In the fourth column, the direct impacts of hazards are shown, and the appropriate mitigation measures synthesized. The last column reports the indirect damage intended as systemic disruption and failures, and the mitigation measures that can be put in place to counteract them. For example, in the tenth line, as indicated by the one directional arrow in the second column, windstorms are shown as having increased in recent years in Italy, where they used to be rare events. Windstorms can be associated (albeit not triggered or triggering) with intense precipitation and consequent local flooding (as indicated by the multihazard knot symbol). Direct damage to plants is more likely to occur on some parts of buildings, especially roofs, and due to dust infiltrating through openings. Appropriate mitigation measures consist of reinforcing roofs, shutting down external ventilation, and filter cleaning. The indirect damage may result from the lack of availability of power or transportation systems due to falling trees, falling poles, etc. In this case, mitigation measures include telecommunication and power redundancy, and the autonomous generating capacity of internal plants, at least during some hours.

The table is comprehensive in that it lists all possible threats and vulnerabilities that may affect any region. Its application to a specific case as shown in Section 5 requires the selection of those threats and vulnerabilities that are pertinent to the area at stake. Risk-related information sources are generally available in at least some countries in the form of reports of past events and GIS maps provided via open geoportals of public administrations. Each data center in the primary–recovery couple or multisite configuration must be assessed individually. It may well be that even relatively close facilities are differently exposed and vulnerable to given threats or combination of threats. In large metropolitan areas, hazards, territorial and environmental vulnerabilities maps must be detailed enough and provide information at a sufficient level of granularity to account for differences between one neighborhood and another, and between one part of the city and another. While this is not very easy to do for large-scale phenomena such as storms or regionalized climate change, it is possible for earthquakes, for example, thanks to microzoning studies.

Following the assessment of each data center, the "couple" or multisite configuration must be appraised: a comparative matrix has been used for this purpose, as schematized in Table 4.

Table 4. Comparative assessment of risks of the primary–recovery couple or multisite configuration.

Hazards	Summary of the Assessment for Individual Data Centers	Evaluation of the Direct Impact on the Primary–Recovery Data Center Configuration	Evaluation of Systemic Impacts on the Primary–Recovery Data Center Configuration	Available or Recommended Protection
Natural hazards Climate Change impacts Hazardous installations Health related hazards (epidemics, toxicbcontamination) Accidents in the transportation system	Site 1 Site 2 Site n	Comparison between the hazards levels fo the primary–recovery sites and assessment of the possibility of having both affected by the same event	Comparison between the hazards levels fo the primary–recovery sites and assessment of the possibility of having both affected by the same event	Recommended mitigation for the configuration as a whole

In order to assess the coupled or multisite configuration risk to multiple hazards, taken individually or combined, the process described in Figure 3 must be followed.

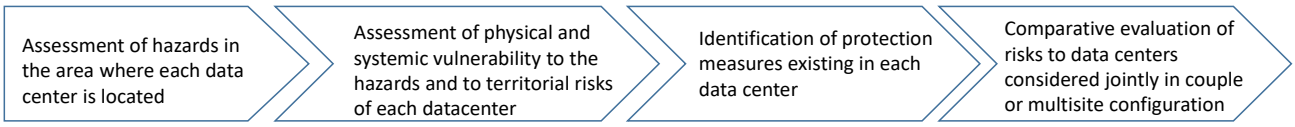

Figure 3. Process to be followed for comparative multirisk assessment of primary and recovery site configurations. Source: elaboration by the authors.

First, both the hazards threatening the data center as a facility and the territorial hazards in the area in which it is located (which is relevant for systemic, indirect impacts) must be assessed; then the physical and systemic vulnerability of each data center is ap-praised, followed by the identification of appropriate protection measures that either exist or can be implemented. Finally, the couple or multisite comparative risk assessment must be carried out to evaluate the actual robustness of the primary–recovery data center con-figurations.

5. Application in the Metropolitan Area of Milan

In this section, the territorial risks of two randomly located data centers (with no reference to the real plants) in two municipalities of the metropolitan area are evaluated following the methodology described in Section 4 (Figure 4). The Milan metropolitan area represents a major data center cluster led by several operators and colocation service providers such as Equinix, Aruba, IBM, Irideos, MIX, BT Italia. The aim is to define the risk to which the plants are subject and to assess to what extent they may be impacted simultaneously by the same event.

As for hazards (natural, health and man-made) that are relevant in the area (Table 3), it is evident that risk scenarios at regional or supra-local levels could simultaneously and similarly damage both locations, particularly in the case of seismic and extreme weather events (i.e., heavy rainfall, windstorms, drought and heat waves). In fact, both sites are located in seismic zone 4 (low probability). On the basis of past events data analysis [48], it can be concluded that the consequences of climate change are increasingly being felt in the metropolitan area of Milan, such as the increasing average temperature, more frequent extreme climatic conditions (due to both the intensification of winds and precipitation), and the reduction in annual average rainfall precipitation. While the direct impact on plants/servers/IT equipment is potentially low, considering the level of reliability required

of current data centers (Section 3), the indirect impact on the power grid and telecommunication systems (responsible for widespread outages at the level of the metropolitan area of Milan) and on the accessibility of sites (limited in the case of trees falling on the roads) is expected to be higher. In this case, the critical indirect impacts could be mitigated by the implementation of several protection factors in terms of the redundancy and efficiency of electrical equipment, telecommunications network connections, and the accessibility of the data center. Moreover, internal procedures and emergency management systems are becoming fundamental to carrying out all of the necessary operations for guarateeing the business continuity of the data center, in addition to the availability and accessibility of territorial resources such as the Regional Fire Department and the Prefecture and Regional Directorate of Civil Protection.

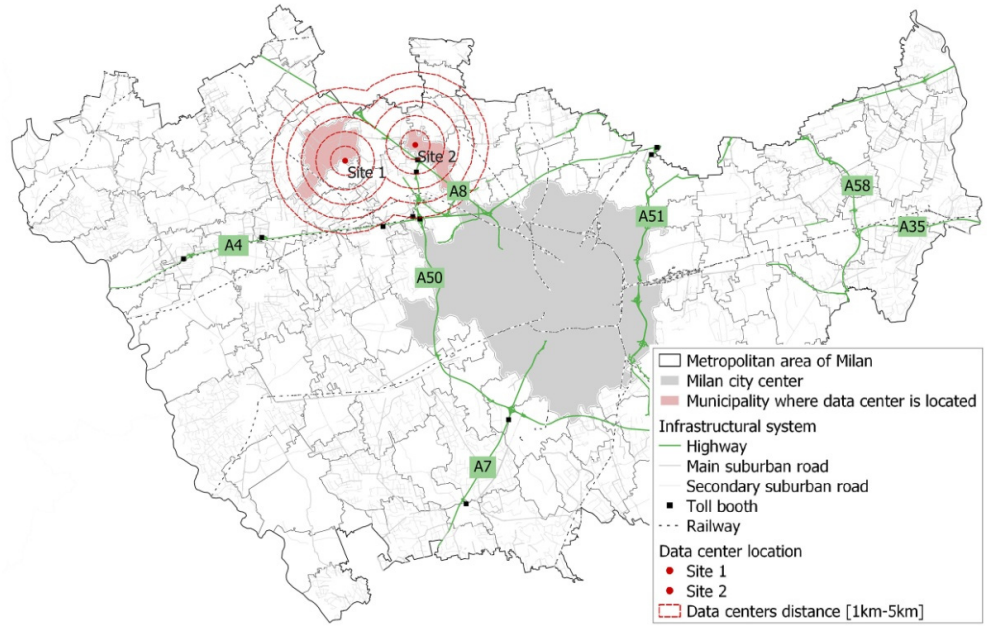

Figure 4. Territorial framework of the application case study. Source: elaboration by the authors.

With regard to pandemic risk, it is a territorial risk potentially impacting an entire region. In particular, it could have a direct impact on the health of workers and/or limit their movement when emergency measures are designed to reduce infections. Therefore, the sites are characterized by the same risk. All data centers must provide a pandemic plan, including all the interventions aimed at containing the spread of infection for instance minimizing the presence of the workers and encouraging smart working. Measures must be defined and diversified in consideration of the evolution of pandemic peaks.

On the other hand, threats with a local potential impact have to be precisely evaluated for both the sites, as synthesized below.

- Flood risk—The areas in which the selected data centers are located are not characterized by the same hydraulic risk. Considering the Flood Risk Management Plan (Figure 5), site 1 is close to flood-prone areas within the main hydrographic system of the Olona river, whereas site 2 is located near minor streams (Lura and Guisa). The direct impact on both data centers is low; but, in the case of a flood event impacting highway A4, accessibility to both sites could be similarly compromised. In this case, the search for alternative routes is crucial.

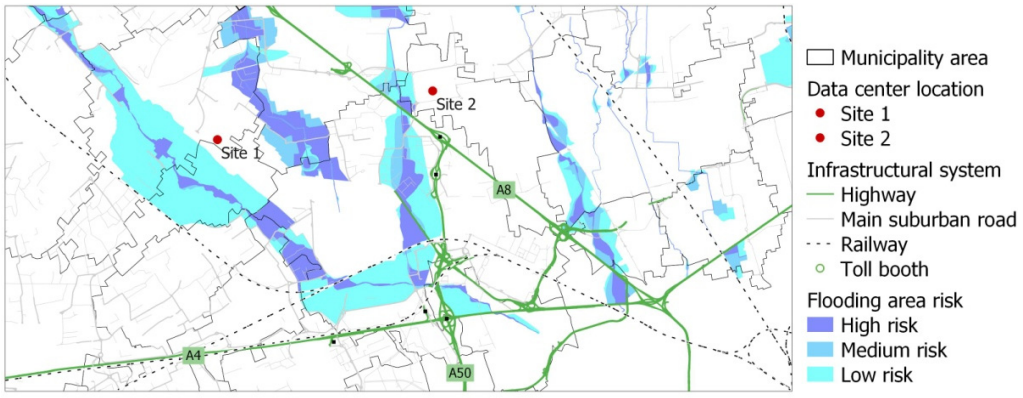

Figure 5. Flood risk areas potentially impacting the territorial context selected as the case study. Source: elaboration by the authors.

- Forest fire risk—The areas where the selected data centers are located are not characterized by the same forest fire risk; however, both sites may be indirectly affected by possible traffic disruptions (highway A4 and ring road A50), limiting the accessibility to the areas. Considering the Integrated Regional Risk Mitigation Program of Lombardia Region [49], site 1 is located in a medium-/high-forest-fire-risk area and site 2 in a medium-forest-fire-risk area (Figure 6). Furthermore, prolonged periods of drought and the presence of temporary storage of waste in/near the site should not be overlooked as possible causes of fire ignition. Mitigation measures should deal with the monitoring of green areas (mainly in summer) and the management of waste containers near/in data center areas.

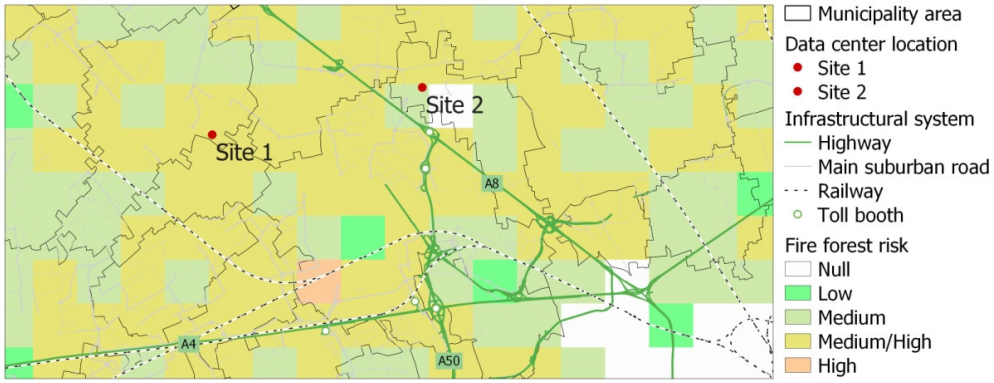

Figure 6. Level of forest fire risk in the territorial context selected as a case study. Source: elaboration by the authors.

- Proximity to hazardous installations—Several hazardous installations are located in the metropolitan area of Milan [50]. With regard to the selected case study (Figure 7), the risk is higher for site 2, which is located close to two chemical plants (~2/3 km). In the case of fires/explosions and as a consequence of the spread of toxic fumes/harmful substances, the location of such installations should be taken into account when assessing the related direct and indirect impacts on both the sites. In fact, highway A4 and ring road A50 may be indirectly affected by a possible traffic disruption, limiting the accessibility to these areas. No installations at major risk of accident are located in the flood risk area (Na-tech risk).

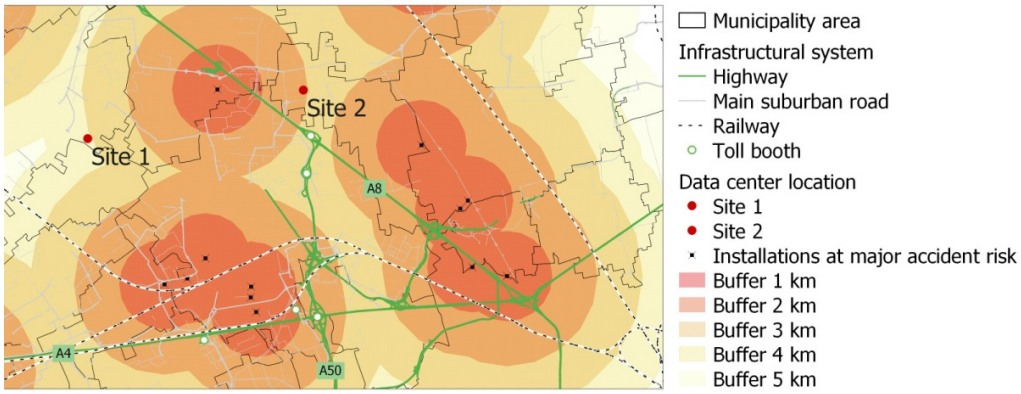

Figure 7. Presence of installations at major risk of accident in the territorial context selected as the case study. Source: elaboration by the authors.

- Transport of dangerous substances risk—In a territory, dangerous substances (flammable liquid material—ADR3) are transported by road and rail networks, as well as through special underground pipelines (oil and gas pipelines). The risk prediction and prevention program of Milan Province [51] describes the related risk level for all of the different transport categories, defining different classes of risk. With regard to the road system, highway A4 (Turin–Trieste) and the A50 ring road are classified as belonging to the R4 class (high risk, 250–1000 daily transits), and highway A8 (Milan-Varese) in the R2 class (moderate risk, 50–100 daily transits). The Milan–Turin railway is classified in R3 (medium risk, 100,000–150,000 tons/year). No pipelines affect the municipalities in which the selected data centers are located. In general, considering the high risk levels defined and the proximity of the data centers to the infrastructural system, potential impacts must be evaluated directly at both the sites, particularly in the case of explosions/fires and the consequent dispersion of harmful substances/fumes and indirectly on territorial networks/personnel as a consequence of the potential disruption of vehicle traffic and the limitation of accessibility to the data center area. The implementation of air circulation systems, alternative road systems, civil protection plans, and cooperation with firefighters are considered to be protective factors.
- *Road accident risk*—The risk prediction and prevention program of Milan Province [51] describes the accident risk level of all main arterial roads in the metropolitan area, classifying the A4 and A8 highways as belonging to the R4 class (high risk) and the A50 ring road to the R3 class (medium risk). As defined above for the transport of dangerous substances risk, both sites are characterized by the same level of risk responsible for potential direct and indirect impacts. Similarly, the implementation of air circulation systems, alternative road systems, civil protection plans, and cooperation with firefighters are proposed as protective factors.

In Table 5, threats, vulnerabilities, potential impacts and possible countermeasures are jointly considered for both selected sites in accordance with the actual spatial distribution of the data centers in the Milan cluster, which are not very distant from one another (~5 km), are serviced by the same main arterial roads (highways A4 and A8, and the A50 ring road) and close to the historic center of Milan (Figure 4).

In conclusion, the selected sites are exposed to similar risks (with different expected levels of impact). The probability of local incidental scenario involving them directly is very low. Moreover, the sites are certified ANSI-TIA 942 [29] respecting several operative standards (Section 3). At territorial level, instead, indirect potential damages could impact simultaneously both sites. Therefore, implementing protective factors is key with particular regard to: (a) accessibility to sites, (b) proximity to the fire stations, (c) availability of independent and redundant power supplies for telecommunications and electricity networks.

Table 5. Risk factors and direct/indirect impact assessment of the data center sites.

Risk	Hazard	Potential Impact Assessment (☒ Direct on Data Center, ◎ Indirect on Territorial System)		Protection Factors
		Site 1	Site 2	
Seismic	Sites are located in seismic zone 4 (low probability)	☒ Low ◎ Medium/low		Seismic resistant buildings, power generators, road system redundancy
Heavy rainfall	Rainy events have been less frequent but more intense in the last 15 years [48]	☒ Medium/low ◎ Medium/low		Resistant structures with sealed roofs, emergency generators, power grid redundancy, alternative traffic
Windstorm	Increasing frequency of wind phenomena daily peaks (v > 100 km/h) [48]	☒ Low ◎ Medium/low		Power supply medium voltage redundancy
Drought	Rainy events have been less frequent in the last 15 years [48]	☒ Low ◎ Medium		Redundancy of air conditioning systems
Heat wave	In recent years, temperature peaks (~30/35 °C) have been more frequent [48]	☒ High ◎ Medium		Advanced/redundant air conditioning system, emergency generators
Pandemic	Sites are characterized by the same risk	☒ Low ◎ Medium/high		Emergency plans, infection spread control measures
Hydraulic	Site 1 is close to potentially flood area of the main hydrographic system; site 2 is located near some minor streams	☒ Low ◎ Medium/high	☒ Low ◎ Medium/high	Organization of alternative roads system
Forest fire	Site 1 is located in a medium-/high-forest-fire-risk area and site 2 in a medium-forest-fire-risk area [49]	☒ Medium/high ◎ Medium/high	☒ Medium ◎ Medium/high	Vegetation maintenance and on-site fire protection systems, civil protection plans, cooperation with firefighters
Installations at major risk of accident	Site 2 is located close to two chemical plants [50]	☒ Low ◎ Medium/high	◎ High ◎ Medium/high	Air circulation systems, alternative road system, civil protection plans, cooperation with firefighters
Transport of dangerous substances	Road Proximity to A4 and A50, classified in R4 class (high risk), and A8, in R2 class (moderate risk) [51]	☒ Low ◎ Medium/high	☒ Medium ◎ Medium/high	Interruption of the vehicular circulation with difficulty in accessibility of the area
	Railway Proximity to railway Milan-Turin classified in R3 (medium risk) [51]	☒ Low ◎ Medium/high	☒ Low ◎ Medium/high	Interruption of the vehicular circulation
	Pipelines No proximity [51]	☒ Low ◎ Low		Interruption of the vehicular circulation with difficulty in accessibility of the area
Road accident	A4 and A8 classified in R4 class (high risk), A50 in R3 class (medium risk) [51]	☒ Low ◎ Medium/high	☒ Low ◎ Medium/high	Interruption of the highways or closure of the ring road junctions

6. Conclusions

Even though risk prevention and security measures against the impacts of extreme events on data centers are currently very effective, it is necessary to further invest in research and applications as risk factors internal to plants, territorial, and environmental are dynamically changing. Hazard and vulnerability factors, both internal to the plants and within the wider territory are dynamic and require protective factors to be continuously adapted: as correctly put by Weick [52], safety is a "dynamic non event".

For this purpose, the paper draws attention to the essential key elements to be considered when carrying out the dynamic assessment of territorial risks and protective factors in order to guarantee the business continuity of data centers. Starting from a discussion of the available evidence related to the topic, considering both recent cases of failure and serious damage to data centers and the evolution of international and European regulations and standards, the authors propose an analytical methodology for assessing the territorial risk conditions according to a multi-dimensional, multirisk and systemic approach.

With respect to the spatial dimension, the proposed methodology considers risk factors and levels of exposure and vulnerability to different threats (i.e., natural, man-made, etc.), assessing their possible interrelationships (i.e., co-concurrence, cause/effect, cascading effects, etc.), also according to the most recent indications provided by the JRC Disaster Risk Management Knowledge Centre of the European Commission [53,54]. Multirisk assessment that takes into consideration the interactions among events triggered by natural or mixed phenomena (Na-tech) is a necessity, given the increasing complexity of urban settlements. Moreover, the pandemic crisis has highlighted even more the need for multirisk approach. During the pandemic, several operators (i.e., civil protection agencies) had to adapt their intervention procedures at different disaster scenes in light of the simultaneous risk of infection with COVID-19.

With respect to the temporal dimension, the entire cycle of an incidental event must be considered, from prevention to the response and recovery phase, in light of the fact that no risk can be completely eliminated, not even in the most favorable situations using the best solutions. In addition, as some reports of incidents in data centers in recent years have also highlighted, damage can be significant. Furthermore, it is not always possible and/or economically feasible to reduce/avoid the so-called "residual risk". The proposed multiphase approach invites the consideration of different prevention and protective measures with the aim of reducing the possibility of an incident degenerating into cascading damage.

In addition to mitigation measures, adaptation strategies are also defined for the telecommunication sector, and specifically for data centers. Good practices related to the advanced level of adaptation of some enterprises of the telecommunications sector have been provided by [26]. Among all case studies, one of the most relevant is by IBM, which created the Smarter Cities project (as part of its Social Corporate Responsibility program) implemented in 2012 after Hurricane Sandy in Suffolk County (not far from New York City, and which suffered from serious problems related to water contamination). The proposed adaptation approach does not apply only to the company itself, but also serves to support the company's customers in the creation and maintenance of advanced information systems capable of improving the management of and access to crucial data. Moreover, IBM proposed the provision of a weather forecast service aimed at making operational decisions towards the safeguarding and management of sensitive data, in collaboration with Twitter.

Currently, the telecommunications sector is subject to a rapid and continuous process of innovation in both mitigation practices [55] and in adaptation measures to climate change. However, as pointed out in [55], mitigation and adaptation strategies must be pursued simultaneously, since it is necessary both to reduce the anthropogenic impact on the climate and to prepare effective measures for coping with the changes already underway and those inevitable in the future. Given the complexity of urban and territorial areas where data centers will have to be located in the future, it is crucial to consider

systemic approaches able to assess risks at the site and territorial levels to better address existing and future vulnerabilities.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/su15076005/s1, File S1 represents the database resulted from systematic search for relevant literature representative of the state of current approaches/methodologies to analyze/assess territorial risk conditions (natural and technological) for data centers was carried out in the Web of ScienceTM, Scopus, and ScienceDirect online platforms using key words and Boolean search criteria.

Author Contributions: Conceptualization, V.G. and S.M.; methodology, V.G. and S.M.; formal analysis, V.G. and S.M.; writing—original draft preparation, V.G. and S.M.; writing—review and editing, V.G. and S.M.; supervision, P.G., A.M., R.M. and G.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. World Bank. *Information and Communications for Development. 2018: Data-Driven Development. Information and Communications for Development*; World Bank: Washington, DC, USA, 2019.
2. OECD. *Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies*; OECD Publishing: Paris, France, 2019.
3. Luiijf, E.; Klaver, M. Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *Int. J. Crit. Infrastruct. Prot.* **2021**, *35*, 100471. [CrossRef]
4. Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to Networking Cloud and Edge Datacenters in the Internet of Things. *ACM Trans. Cyber-Phys. Syst.* **2016**, *4*, 3351882. [CrossRef]
5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 (accessed on 12 December 2022).
6. Menoni, S.; Pergalani, F.; Boni, M.P.; Petrini, V. Lifelines earthquake vulnerability assessment. In *Managing Critical Infrastructure Risks*; Linkov, I., Wenning, R.J., Kiker, G.A., Eds.; NATO Science for Peace and Security Series C: Environmental Security; Springer: Dordrecht, The Netherlands, 2007; pp. 111–132.
7. Bonadonna, C.; Frischknecht, C.; Menoni, S.; Romerio, F.; Gregg, C.E.; Rosi, M.; Biass, S.; Asgary, A.; Pistolesi, M.; Guobadia, D.; et al. Integrating hazard, exposure, vulnerability and resilience for risk and emergency management in a volcanic context: The ADVISE model. *J. Appl. Volcanol.* **2021**, *10*, 7. [CrossRef] [PubMed]
8. Menoni, S. Cities and factories. Special Issue in Urbanistica. *INU J. Urban Plan. Biling. Ital.-Engl.* **2002**, *118*, 63–93.
9. van den Dool, F. Telecommunication system architectures: Dealing with complexity. *Int. J. Commun. Syst.* **1994**, *7*, 1–6. [CrossRef]
10. Gabriel, C. Datacenter disater recovery and high availability. In *Data Center Handbook*; Geng, H., Ed.; Wiley & Sons: Hoboken, NJ, USA, 2015; pp. 641–657.
11. Sengupta, S.; Annerva, K.M. Multi-site data distribution for disaster recovery-A planning framework. *Future Gener. Comput. Syst.* **2014**, *41*, 53–64. [CrossRef]
12. Liu, Y.; Zhou, F.; Shang, T.; Torres-Moreno, J.-M. Power-efficient and Distance-adaptive Disaster Protection for Service Function Chain Provisioning. In Proceedings of the 2022 IEEE Global Communications Conference, GLOBECOM 2022—Proceedings, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 4407–4412.
13. Yang, C.L.; Yuan, B.J.C.; Huang, C.-Y. Key Determinant Derivations for Information Technology Disaster Recovery Site Selection by the Multi-Criterion Decision Making Method. *Sustainability* **2015**, *7*, 6149–6188. [CrossRef]
14. Ferdousi, S.; Dikbiyik, F.; Habib, M.F.; Tornatore, M.; Mukherjee, B. Disaster-aware datacenter placement and dynamic content management in cloud networks. *J. Opt. Commun. Netw.* **2015**, *7*, 681–694. [CrossRef]
15. Zschau, J. Where Are We with Multihazards, Multirisks Assessment Capacities? In Disaster Risk Management Knowledge Centre. SCIENCE FOR DISASTER RISK MANAGEMENT 2017 Knowing Better and Losing Less. 2017. Available online: https://drmkc.jrc.ec.europa.eu/portals/0/Knowledge/ScienceforDRM/ch02/ch02_subch0205.pdf (accessed on 6 June 2022).
16. Gill, J.C.; Malamud, B.D. Reviewing and visualising the interactions of natural hazards. *Rev. Geophys.* **2014**, *52*, 680. [CrossRef]

17. Gill, J.C.; Malamud, B.D. Hazard Interactions and interaction networks (cascades) within multi-hazard methodologies. *Earth Syst. Dyn.* **2016**, *7*, 659. [CrossRef]
18. Menoni, S.; Boni, M.P. A systemic approach for dealing with chained damages triggered by natural hazards in complex human settlements. *Int. J. Disaster Risk Reduct.* **2020**, *51*, 101751. [CrossRef]
19. Ceballos, J.; Dipasquale, R.; Feldman, R. Business continuity and security in datacenter interconnection. *Bell Labs Tech. J.* **2012**, *17*, 147–155. [CrossRef]
20. Sieńko, P. Methods of securing and controlling critical infrastructure assets allocated in information and communications technology sector companies in leading. *Securitologia* **2015**, *22*, 107–123. [CrossRef]
21. Engemann, K.J.; Miller, H.E. Risk and Data Center Planning. In *Engineering and Management of Data Centers*; Marx Gómez, J., Mora, M., Raisinghani, M., Nebel, W., O'Connor, R., Eds.; Service Science: Research and Innovations in the Service Economy; Springer: Berlin/Heidelberg, Germany, 2017; pp. 73–89.
22. Horrocks, L.; Beckford, J.; Hodgson, N.; Downing, C.; Davey, R.; O'Sullivan, A. Adapting the ICT Sector to the Impacts of Climate Change. *AEA Final. Rep.* **2010**, *ED 49926*, 5.
23. Fu, G.; Horrocks, L.; Winne, S. Exploring impacts of Climate Change on UK's ICT Infrastructure. *Infrastruct. Asset Manag.* **2016**, *3*, 42–52. [CrossRef]
24. Adams, P.; Steeves, J.; Ashe, B.; Firth, J.; Rabb, B. *Climate Risks Study for Telecommunications and Data Center Services. Report Prepared for the General Services Administration by Riverside Technology, Inc. and Acclimatise*; Riverside Technology: Cambridge, WA, USA, 2014.
25. Runhaar, A.C.; Uittenbroek, H.F.M.W.; van Rijswick, H.L.P.; Mees, P.P.J.; Driessen, H.K. Gilissen, Prepared for climate change? A method for the ex-ante assessment of formal responsibilities for climate adaptation in specific sectors. *Reg. Environ. Change* **2016**, *16*, 1389–1400. [CrossRef]
26. Goodman, A. *Adapting to Change. The Business of Climate Resilience*; Business Expert Press: New York, NY, USA, 2016.
27. Gomes, R.; Lapo, L.V. The adoption of IT security standards in a healthcare environment. *Stud. Health Technol. Inform.* **2008**, *136*, 765–770.
28. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557 (accessed on 6 June 2022).
29. *ANSI/TIA-942*; Telecommunications Infrastructure Standard for Data Centers. Telecommunications Industry Association: Washington, DC, USA, 2005.
30. *ISO/IEC 27031*; Guidelines for Information and Communication Technology Readiness for Business Continuity. British Standards Institution (BSI): London, UK, 2011.
31. *EN 50060*; Information Technology—Data Centre Facilities and Infrastructures. American Association: Los Angeles, CA, USA, 2019.
32. *ISO/IEC 24762*; Guidelines for Information and Communications Technology Disaster Recovery Services. Canadian Standards Association: Toronto, ON, Canada, 2008.
33. Uptime Institute. The gathering storm: Climate change and data center resiliency. In *UI Intelligence Report 41*; Uptime Institute: New York, NY, USA, 2020.
34. Circular n. 285 of 17 December 2013 on "Supervisory Provision Banks". Available online: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/?dotcache=refresh (accessed on 29 May 2022).
35. Proposal for a Regulation of The European Parliament and of The Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 COM/2020/595 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595 (accessed on 6 June 2022).
36. Uptime Institute. Annual outage analysis 2021, The causes and impacts of data center outage. In *UI Intelligence Report 46*; Uptime Institute: New York, NY, USA, 2021.
37. Ponemon Institute, Cost of Data Center Outages, Data Center Performance Benchmark Series. 2016. Available online: www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf (accessed on 21 June 2022).
38. Uptime Institute. Global Data Center Survey 2021, Growth stretches an evolving sector. In *UI Intelligence 51*; Uptime Institute: New York, NY, USA, 2021.
39. IPCC. *Climate Change 2022: Impacts, Adaptation, and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*; Cambridge University Press: Cambridge, UK, 2022.
40. Peerenboom, J.; Fisher, R. Analyzing Cross-Sector Interdependencies. In Proceedings of the 40th Hawaii International International Conference on Systems Science, Waikoloa, HI, USA, 3–6 January 2007.
41. ASCE. *Adapting Infrastructure and Civil Engineering Practice to a Changing Climate*; Olsen, R., Ed.; American Society of Civil Engineers—Committee on Adaptation to a Changing Climate: Reston, VA, USA, 2015.
42. National Hurricane Center (NHC). Tropical Cyclone Reports. Available online: www.nhc.noaa.gov/ (accessed on 29 May 2022).
43. Cushman & Wakefield. *Italy Data Center Report*; Cushman & Wakefield: Chicago, IL, USA, 2022.
44. Park, J.; Seager, T.; Rao, P.S.C.; Convertino, M.; Linkov, I. Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Anal.* **2013**, *33*, 356–367. [CrossRef]

45. Chen, R.; Xie, Y.; Liu, Y. Defining, Conceptualizing, and Measuring Organizational Resilience: A Multiple Case Study. *Sustainability* **2021**, *13*, 2517. [CrossRef]
46. American Institute of Chemical Engineers. *Dow's Fire and Explosion Hazard Index Guide*; American Institute of Chemical Engineers: New York, NY, USA, 1994.
47. Menoni, S.; Molinari, D.; Parker, D.; Ballio, F.; Tapsell, S. Assessing multifaceted vulnerability and resilience in order to design risk-mitigation strategies. *Nat. Hazards* **2012**, *64*, 2057–2082. [CrossRef]
48. Arpa Lombardia—Regional Agency for the Protection of the Environment. Hydro-Nivo-Meteorological Data Collection. Available online: www.arpalombardia.it/Pages/Meteorologia/Richiesta-dati-misurati.aspx (accessed on 5 June 2022).
49. Integrated Regional Risk Mitigation Program of Lombardia Region. Available online: https://sicurezza.servizirl.it/primviewer/ (accessed on 5 June 2022).
50. Legislative Decree of 17 August 1999, n. 334 "Implementation of Directive 96/82/EC on the Control of Major-Accident Hazards Involving Certain Dangerous Substances". Available online: https://www.agid.gov.it/sites/default/files/repository_files/approfondimentocircolare18062019_0.pdf (accessed on 6 June 2022).
51. Province of Milan—Program of Prevision and Prevention of Risk. 2013. Available online: www.cittametropolitana.mi.it/protezione_civile/ORGANIZZAZIONE/Programma_Previsione_Prevenzione.html (accessed on 6 June 2022).
52. Weick, K. Organizing for Transient Reliability: The Production of Dynamic Non-Events. *J. Contingencies Crisis Manag.* **2011**, *19*, 21–27. [CrossRef]
53. Disaster Risk Management Knowledge Centre. Science for Disaster Risk Management 2017 Knowing Better and Losing Less. Available online: https://drmkc.jrc.ec.europa.eu/knowledge/science-for-drm/science-for-disaster-risk-management-2017 (accessed on 6 June 2022).
54. Disaster Risk Management Knowledge Centre. Science for Disaster Risk Management 2020 Acting Today, Protecting Tomorrow. Available online: https://drmkc.jrc.ec.europa.eu/knowledge/science-for-drm/science-for-disaster-risk-management-2020 (accessed on 6 June 2022).
55. Olsen, R.L.; Balachandran, K.; Hald, S.; Gutierrez Lopez, J.; Pedersen, J.M.; Stevanovic, M. Telecommunication Networks. In *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*; Kyriakides, E., Polycarpou, M., Eds.; Studies in Computational Intelligence; Springer: Berlin/Heidelberg, Germany, 2015; Volume 565, pp. 67–100.