BİLGİ TEKNOLOJİSİ FELAKET KURTARMA PLANLAMASININ FENOMENOLOJİK YAKLAŞIMLA İNCELENMESİ: KAMU ÜNİVERSİTELERİ ÖRNEĞİ

Oğuz ERDEN

Yüksek Lisans Tezi
Yönetim Bilişim Sistemleri Ana Bilim Dalı
Doç. Dr. Ahmet Kamil KABAKUŞ
2024
Her Hakkı Saklıdır.

T.C.
ATATÜRK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

Oğuz ERDEN

BİLGİ TEKNOLOJİSİ FELAKET KURTARMA PLANLAMASININ FENOMENOLOJİK YAKLAŞIMLA İNCELENMESİ: KAMU ÜNİVERSİTELERİ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

TEZ YÖNETİCİSİ
Doç. Dr. Ahmet Kamil KABAKUŞ

ERZURUM-2024

SOSYAL BİLİMLER ENSTİTÜSÜ
Graduate School of Social Sciences

TEZ BEYAN FORMU

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

BİLDİRİM

Atatürk Üniversitesi Lisansüstü Eğitim ve Öğretim Uygulama Esaslarının ilgili maddelerine göre hazırlamış olduğum **"Bilgi Teknolojisi Felaket Kurtarma Planlamasının Fenomenolojik Yaklaşımla İncelenmesi: Kamu Üniversiteleri Örneği"** adlı tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kâğıt ve elektronik kopyalarının aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım.

Gereğini bilgilerinize arz ederim *.

☐ Tezimin/Raporumun tamamı her yerden erişime açılabilir.

☐ Tezimin/Raporumun makale için **altı ay,** patent için **iki yıl** süreyle erişiminin ertelenmesini istiyorum.

09.12.2024

Aslı Islak İmzalıdır

Oğuz ERDEN

---

* **LİSANSÜSTÜ TEZLERİN ELEKTRONİK ORTAMDA TOPLANMASI, DÜZENLENMESİ VE ERİŞİME AÇILMASINA İLİŞKİN YÖNERGE**

.....

ÜÇÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Lisansüstü tezlerin erişime açılmasının ertelenmesi MADDE 6– (1) Lisansüstü tezle ilgili **patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda**, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu **iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.**

(2) Yeni teknik, materyal ve metotların kullanıldığı, henüz **makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış** ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile **altı ayı aşmamak üzere tezin erişime açılması engellenebilir.**

Gizlilik dereceli tezler MADDE 7– (1) Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.

(2) Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

SOSYAL BİLİMLER ENSTİTÜSÜ
Graduate School of Social Sciences

TEZ KABUL TUTANAĞI

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Doç. Dr. Ahmet Kamil KABAKUŞ danışmanlığında, Oğuz ERDEN tarafından hazırlanan bu çalışma 09/12/2024 tarihinde aşağıda isimleri yazılı jüri tarafından Yönetim Bilişim Sistemleri Ana Bilim Dalı'nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Başkan	: Prof. Dr. Handan ÇAM	İmza:	Aslı Islak İmzalıdır
Jüri Üyesi	: Doç. Dr. Ahmet Kamil KABAKUŞ	İmza:	Aslı Islak İmzalıdır
Jüri Üyesi	: Doç. Dr. Serdar AYDIN	İmza:	Aslı Islak İmzalıdır

Prof. Dr. Hanifi ŞAHİN
Enstitü Müdürü

Aslı Islak İmzalıdır

İÇİNDEKİLER

ÖZET ..... **IV**
ABSTRACT ..... **V**
SİMGELER ve KISALTMALAR DİZİNİ ..... **VI**
ŞEKİLLER DİZİNİ ..... **VII**
TABLOLAR DİZİNİ ..... **VIII**
ÖNSÖZ ..... **IX**
GİRİŞ **1**

BİRİNCİ BÖLÜM
BT FELAKET KURTARMA PLANLANMASI

1.1. FELAKET KURTARMA PLANLAMASINA TARİHSEL BAKIŞ **4**
1.2. BT FELAKET KURTARMA PLANI METODOLOJİSİ **6**
1.2.1. Felaket Kurtarma Planı Kapsam ve Hedeflerinin Belirlenmesi 7
1.2.2. Risk Analizi ve Risk Yönetimi 8
1.2.3. Önceliklerin Belirlenmesi 18
1.2.4. Altyapının Sağlanması 19
1.2.5. Verilerin Toplanması ve Planın Belgelendirilmesi 20
1.2.6. Planın Test Edilmesi ve Gözden Geçirilmesi 21
1.2.7. İş Birliği ve İletişim 23
1.3. BT FELAKET KURTARMA PLANI VE İŞ SÜREKLİLİĞİ PLANI KAVRAMALARININ DOĞRU TANIMLANMASI **24**
1.4. BT FELAKET KURTARMA PLANI **26**
1.4.1. BT Felaket Kurtarma Planı Seviyeleri 27
1.4.2. BT Felaket Kurtarma Planı Türleri 29
1.4.2.1. Ağ Kurtarma Planı 30
1.4.2.2. Sunucu Sistemlerini Kurtarma ve Sanallaştırma Planı 32
1.4.2.3. Felaket Kurtarma Merkezi Planı 34
1.4.2.4. Hiper Bütünleşik Mimari ve Bulut Bilişim Kullanım Planı 40
1.5. BT FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ STANDARTLARI **43**
1.6. BT FELAKET KURTARMA PLANI ÖRNEĞİ **47**
1.6.1. BT Altyapı Haritasının Çıkarılması 47

1.6.2. Kurtarma Mimarisinin Belirlenmesi 52
1.6.3. Risk Değerlendirmesi 52
1.6.4. Öncelik Listelerinin Belirlenmesi 54
1.6.5. Olay Müdahale Tablosu 55
1.6.6. Kurtarma ve Yönetim Ekibi 57
1.6.7. Felaket Kurtarma Zaman Çizelgesi 58
1.6.8. Veri Yedekleme ve Kurtarma Planı veya Tablosu 59

İKİNCİ BÖLÜM

ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

2.1. EDMUND HUSSERL VE FENOMENOLOJİ 63
2.1.1. Teknoloji ve Fenomenoloji Arasında İlişki 66
2.2. PLANLI DAVRANIŞ TEORİSİ 69
2.2.1 Planlı Davranış Teorisi ve Felaket Kurtarma 71

ÜÇÜNCÜ BÖLÜM

KAMU ÜNİVERSİTELERİNİN BT FELAKET KURTARMA PLANI GELİŞTİRME SÜREÇLERİNDE ETKİLİ TEMALARIN FENOMENOLOJİK DESENLE TESPİTİ

3.1. ARAŞTIRMANIN METODOLOJİSİ 73
3.1.1. Araştırmanın Amacı ve Önemi 74
3.1.2. Evren ve Örneklem 75
3.1.3. Veri Toplama Yöntemi ve Aracı 77
3.1.4. Verilerin Analizi 77
3.1.5. Araştırmanın Sınırlılıkları 80
3.1.6. Araştırmanın Varsayımları 81
3.2. ARAŞTIRMANIN BULGULARI 81
3.2.1. Katılımcılara İlişkin Demografik Bulgular 82
3.2.2. Güncel Bir BT Felaket Kurtarma Planına Sahip Olunmasına Yönelik Bulgular 83
3.2.3. Görüşme Analizi Bulguları 84

SONUÇ VE TARTIŞMA **108**
KAYNAKÇA **116**
EKLER **135**
EK 1. Araştırmada Kullanılan Ölçek 135
EK 2. Ayrıntılı Tema Şeması 136
ÖZGEÇMİŞ **137**

ÖZET

YÜKSEK LİSANS TEZİ

BİLGİ TEKNOLOJİSİ FELAKET KURTARMA PLANLAMASININ FENOMENOLOJİK YAKLAŞIMLA İNCELENMESİ: KAMU ÜNİVERSİTELERİ ÖRNEĞİ

Oğuz ERDEN

Tez Danışmanı: Doç. Dr. Ahmet Kamil KABAKUŞ

2024, 137 Sayfa

Jüri: Prof. Dr. Handan ÇAM
Doç. Dr. Serdar AYDIN
Doç. Dr. Ahmet Kamil KABAKUŞ

Bu tezin amacı, kamu üniversitelerinde bilgi teknolojileri (BT) felaket kurtarma planlarının geliştirilmesine yönelik stratejiler hakkında bilgi sağlamaktır. Araştırmanın temel hedefi, kamu üniversitelerinin felaket durumuna hazırlık süreçlerini daha iyi anlamak ve bilgi teknolojileri açısından felaket kurtarma planlarının etkinliğini, olumlu veya olumsuz yönde etkileyen faktörleri fenomenler yardımıyla tespit etmeye çalışmaktır. Bu kapsamda hazırlanan çalışmamız, Türkiye'deki kamu üniversitelerinden rastgele örneklemeyle seçilen, en az üç yıl BT felaket kurtarma planı geliştirme deneyimine sahip, bilgi teknolojileri alanında faaliyet gösteren, tamamen gönüllülük esasına dayalı olarak katkı sağlayan on kişiden oluşmaktadır. Araştırmada, nitel araştırma desenlerinden biri olan fenomenoloji kullanılmıştır. Veriler, katılımcılara uygulanan görüşme formu aracılığıyla toplanmıştır. Verilerin analizi, tematik analiz yöntemi ile yapılmıştır. Katılımcıların gözlemleri ve deneyimleri analiz edilerek, elde edilen bulgulara göre, BT felaket kurtarma planı oluşturma sürecinde akademik ve teknik bilgi birikiminin faydalı olduğu sonucuna ulaşılmıştır. Ayrıca, felaket kurtarma planı geliştirme sürecini zorlaştıran en önemli faktörlerin başında mali kaynaklarla ilgili kısıtlamalar yer almaktadır. Bu bulgular, literatüre felaket kurtarma planlarının geliştirilmesi sürecine dair nitel verilerle katkı sağlamaktadır. Son olarak elde edilen bulgular, literatürdeki diğer teorik verilerle karşılaştırılarak benzerlikler ve farklılıklar tartışılmıştır.

Anahtar Kelimeler: Felaket kurtarma, Bilgi Teknolojileri, Fenomenoloji, Deneyim.

ABSTRACT

MASTER'S THESIS

A PHENOMENOLOGICAL APPROACH TO INFORMATION TECHNOLOGY DISASTER RECOVERY PLANNING: THE CASE OF PUBLIC UNIVERSITIES

Oğuz ERDEN

Advisor: Assoc. Prof. Dr. Ahmet Kamil KABAKUŞ

2024, 137 Pages

Jury: Prof. Dr. Handan ÇAM
Assoc. Prof. Dr. Serdar AYDIN
Assoc. Prof. Dr. Ahmet Kamil KABAKUŞ

The purpose of this thesis is to explore strategies for developing Information Technology (IT) disaster recovery plans in public universities. The primary objective is to deepen the understanding of disaster preparedness processes in these institutions and to identify factors, through phenomenological analysis, that influence the effectiveness of IT disaster recovery plans. Ten IT staff members from public universities in Turkey, selected via random sampling, participated in the study, all with at least three years of experience in developing IT disaster recovery plans. A qualitative research design, specifically phenomenology, was used to collect data through interviews, which were analyzed using thematic analysis. The findings suggest that both academic and technical expertise are essential in the IT disaster recovery planning process. Financial resource limitations were also identified as a major challenge. These results contribute to the existing literature on disaster recovery planning. Lastly, the findings were compared with theoretical data in the literature to highlight similarities and differences.

Keywords: Disaster recovery, Information Technology, Phenomenology, Experience, Strategy.

SİMGELER ve KISALTMALAR DİZİNİ

BT : Bilgi Teknolojileri

FKM : Felaket Kurtarma Merkezi

GDPR : General Data Protection Regulation

IoT : Internet of Things

ISO : International Organization for Standardization

KVKK : Kişisel Verilerin Korunması Kanunu

LAN : Local Area Network

NIST : National Institute of Standards and Technology

RPO : Recovery Point Objective

RTO : Recovery Time Objective

VPN : Virtual Private Network

WAN : Wide Area Network

vd. : ve diğerleri

ŞEKİLLER DİZİNİ

Şekil 1.1. Risk Derecelendirme Grafiği. 17
Şekil 1.2. Örnek Risk Değerlendirme Grafiği. 18
Şekil 2.1. Planlı Davranış Teorisi. 69
Şekil 3.1. Nitel Veri Analizinde İzlenen Aşamalar. 79
Şekil 3.2. Katılımcı Görüşmeleri Sonucunda Oluşturulan Temalar. 87
Şekil 3.3. Ekonomik Faktörler Temasına Ait Oluşturulan Alt Temalar. 88
Şekil 3.4. Ekonomik Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı. 88
Şekil 3.5. Eğitim Faktörleri Temasına Ait Oluşturulan Alt Temalar. 90
Şekil 3.6. Eğitim Faktörleri Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı. 91
Şekil 3.7. Çevresel Faktörler Temasına Ait Oluşturulan Alt Temalar. 94
Şekil 3.8. Çevresel Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı. 94
Şekil 3.9. Teknolojik Faktörler Temasına Ait Oluşturulan Alt Temalar. 95
Şekil 3.10. Teknolojik Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı. 96
Şekil 3.11. Sosyal Faktörler Temasına Ait Oluşturulan Alt Temalar 99
Şekil 3.12. Sosyal Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı. 99
Şekil 3.13. İdari Faktörler Temasına Ait Oluşturulan Alt Temalar. 101
Şekil 3.14. İdari Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı. 101
Şekil 3.15. Katılımcıların Tema Görüş Sıklıkları. 107

TABLOLAR DİZİNİ

Tablo 1.1. Örnek Güvenlik Açıklıkları Ölçeği. 13
Tablo 1.2. Örnek Olasılık Derecelendirilmesi. 14
Tablo 1.3. Örnek BT Risk Senaryoları. 15
Tablo 1.4. Örnek Ekonomik Etkiler. 16
Tablo 1.5. Örnek Operasyonel Etkiler. 16
Tablo 1.6. Örnek Manevi/İtibar Kayıp Etkileri. 16
Tablo 1.7. UPTIME INSTITUTE Enerji ve İklimlendirme Standartları 39
Tablo 1.8. Örnek Sunucu Felaket Kurtarma Bilgi Çizelgesi. 49
Tablo 1.9. Örnek Ağ Cihazı Felaket Kurtarma Bilgi Çizelgesi. 50
Tablo 1.10. Örnek Risk Değerlendirmesi Çizelgesi. 52
Tablo 1.11. Tehditler-Riskler, Potansiyel Etkileri ve Alınması Gereken Önlemler. 54
Tablo 1.12. Önceliklerin Belirlenmesi Örneği. 55
Tablo 1.14. Kurtarma ve Yönetim Ekibi Örneği. 57
Tablo 1.15. Felaket Kurtarma Zaman Çizelgesi 59
Tablo 1.16. Sistem ve Uygulamalar Bazında Yedekleme ve Kurtarma Planı Örneği. 60
Tablo 1.17. Cihaz ve Sistemler Bazında Veri Yedekleme ve Kurtarma Planı Örneği. 61
Tablo 1.18. Felaket Türü, Kurtarma ve İyileştirme Süreçleri. 62
Tablo 3.1. Katılımcı Demografik Bilgileri. 82
Tablo 3.2. Katılımcıların Felaket Kurtarma Planlaması Hakkında Tecrübe Yılları. 83
Tablo 3.3. Katılımcı Güncel BT Felaket Kurtarma Planına Sahiplik Sonuçları. 83
Tablo 3.4. Kurumların BT Felaket Kurtarma Planı Güncelleme Sıklığı. 84
Tablo 3.5. Temalara İlişkin Kısaltmalar ve Tema İsimleri. 85
Tablo 3.6. Ekonomik Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri. 89
Tablo 3.7. Eğitim Faktörleri Teması İçin Alt Kodlar ve Katılımcı Görüşleri. 91
Tablo 3.8. Çevresel Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri. 94
Tablo 3.9. Teknolojik Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri. 96
Tablo 3.10. Sosyal Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri. 100
Tablo 3.11. İdari Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri. 102
Tablo 3.12. Tüm Temalara Ait Frekans ve Yüzde Değerleri. 106

ÖNSÖZ

Bu çalışmada, konu belirleme aşamasından takdim sürecine kadar bana yol gösteren danışmanım, saygıdeğer hocam Doç. Dr. Ahmet Kamil KABAKUŞ'a teşekkürlerimi sunarım. Ayrıca, tez sürecindeki katkılarından dolayı değerli hocalarım Prof. Dr. Atilla Halil ELHAN, Prof. Dr. Handan ÇAM, Doç. Dr. Serdar AYDIN, Doç. Dr. Esra ÖZMEN, Dr. Öğr. Üyesi Bilal USANMAZ ve Dr. Öğr. Üyesi Erdoğan Serdar ÇALIK başta olmak üzere, tüm hocalarıma özellikle teşekkür ederim.

Çalışma süresince yardımlarını esirgemeyen başta eşim Şeyda Nur olmak üzere, her zaman varlıklarıyla gurur duyduğum aileme teşekkürü bir borç bilirim.

Erzurum – 2024 **Oğuz ERDEN**

GİRİŞ

Bilgi teknolojileri, eğitim uygulamaları başta olmak üzere, askeri, sağlık, ulaşım ve ticaret gibi çeşitli alanlarda, bilgi temelli işlemlerin büyük bir kısmında etkin bir şekilde kullanılmakta ve bu teknolojik gelişmeler, günlük yaşamın her alanında etkisini göstermektedir. Temel bilgi teknolojileri işlemlerinden, kritik öneme sahip altyapılarda kullanılan işlemlere kadar BT kullanımı hemen her alanda yaygınlaşmaktadır. Bu durum sonucunda altyapılar, zaman zaman daha karmaşık hale gelebilmektedir. Bilgi teknolojilerinin yaygın kullanımı, bilgi sistemlerini felaketlere karşı koruma konusunda yöneticileri ve diğer çalışanları daha bilinçli olmaya yöneltmektedir. Özellikle kritik altyapı barındıran kurum, kuruluş veya organizasyonlarda görev yapan yöneticiler ve BT çalışanları, felaket öncesi ve sonrası için etkili bir BT felaket kurtarma planı oluşturmak amacıyla büyük bir çaba sarf etmektedirler. Bu nedenle, etkili bir felaket kurtarma planı, organizasyonların, doğal afetler başta olmak üzere, olası felaketlere karşı hazırlıklı olmalarını ve operasyonlarını hızlı bir şekilde yeniden başlatabilmelerini hedeflemelidir. Etkili bir felaket kurtarma planlaması, beklenmedik olaylar ve doğal afetler karşısında, özellikle eğitim kurumları olmak üzere, tüm kurum, kuruluş ve organizasyonların sürekliliğini temin etmek için hayati öneme sahiptir. Yetersiz veya hatalı tasarlanmış bir felaket kurtarma planı, organizasyonun temel operasyonlarını zamanında yeniden başlatamayacak bir plandır.

Üniversiteler, toplumların önemli bir parçasıdır. Eğitim-öğretim faaliyetlerinin yanı sıra, bulundukları şehirlere ve topluma katkı sağlayan organizasyonlar olarak kabul edilen üniversiteler, organizasyon şemalarında yer alan fakülteleri, enstitüleri, daire başkanlıkları, araştırma merkezleri gibi birimlerle birlikte, kritik öneme sahip Yükseköğretim Kurulu Başkanlığı'na bağlı yapılardır. Bazı üniversiteler, hizmetleri arasında hastane hizmetlerine de yer vermekte olup, toplumsal katkı sağlamada önemli bir rol üstlenmektedir. Üniversiteler, bilimsel araştırma faaliyetleri yürütür ve endüstriyel iş birlikleriyle bulundukları toplumlara katkı sağlarlar. Gerçekleştirdikleri kamu hizmetleri, sağlık hizmetleri ve kültürel etkinliklerle toplumsal sorunlara çözüm arayışları vardır. Sunulan bu hizmetler, üniversitelerin temel misyonunu oluşturan asgari hizmetlerdir. Yaşanması muhtemel bir felaket sonrasında üniversitelerin sunacağı hizmetlerin aksaması, bilgiye geç erişim, bireysel gelişimde gecikme, ekonomik kayıplar

ve kültürel kayıplarla birlikte itibar kaybına yol açacaktır. Bunun yanı sıra, sağlık hizmetleri sunan üniversitelerin hizmet verememesi, bulundukları şehirlerdeki diğer sağlık kuruluşları üzerinde ek bir baskı oluşturarak çevresel, sosyal ve toplumsal etkilere neden olabilir. Sonuç olarak, üniversiteler, toplumun sosyal ve ekonomik yapısında kritik bir rol üstlenmektedir. Üniversitelerde gerçekleştirilen tüm faaliyetler büyük ölçüde BT kullanımını gerektirmektedir. Bilgi teknolojileri, bilişim hizmetleri sağlayan daire başkanlıkları, araştırma merkez müdürlükleri, dijital dönüşüm ofisleri, araştırma-geliştirme merkezleri, teknoloji transfer ofisleri ve belge yönetim koordinatörlükleri gibi organizasyon şeması içerisinde yer alan birimler tarafından, ilgili görev ve sorumluluklar çerçevesinde etkin ve verimli bir şekilde yönetilmektedir. Üniversitelerin, felaket sonrasında hizmet sunamaması hem maddi hem de manevi açıdan ağır sonuçlara yol açabilir. Bu nedenle, üniversitelerin felaket kurtarma planlarını dikkate alarak, olası bir felaket durumunda asgari düzeydeki hizmetlerini en kısa sürede yeniden faaliyete geçirebilecek şekilde tasarlamaları ve yönetmeleri gerekmektedir.

Üniversiteler için başlıca felaket senaryoları arasında sel, kasırga, yangın ve deprem gibi doğal afetler yer almaktadır. Bunun yanı sıra, terör saldırıları, sabotajlar, hırsızlıklar ve insan hataları da önemli riskler oluşturmaktadır. Bu tür durumlarda, kritik verilerin bilinçli ya da bilinçsiz bir şekilde ifşa edilmesi, silinmesi veya bütünlüğünün bozulması, ciddi sonuçlara yol açabilmektedir (Okeagu vd., 2021). Bilgi teknolojisi hizmetlerini aktif bir şekilde kullanan üniversitelerde, afetlerin meydana gelmesi çalışma yeteneğini olumsuz etkileyebilir ve maddi ile manevi kayıplara yol açabilir. Özellikle hastane hizmeti sunan üniversiteler ile diş hekimliği fakültelerine bağlı poliklinik hizmetleri sağlayan üniversitelerde, felaket sonrası hizmetlerin durması veya aksaklıkların yaşanması muhtemeldir. Bunun yanı sıra, nadir eserler barındıran ve köklü bir geçmişe sahip itibarlı üniversitelerimizde, bir felaket sonrası itibar kaybı yaşanması durumunda, yaşanılan kaybın telafisi uzun bir zaman alabilir. Bu tür olumsuzlukların önüne geçmek veya etkilerini azaltmak amacıyla, üniversitelerin özellikle BT açısından felaket öncesi ve sonrası için hazırlıklı olmaları gerekmektedir. Buna bağlı olarak, felaket kurtarma planlarının, felaket durumu gerçekleşmeden önce oluşturulması büyük önem taşımaktadır. Felaket kurtarma planı, bir organizasyonun, kurum veya kuruluşun, felaket ya da olumsuz bir olay sonrası operasyonlarını hızlı bir şekilde yeniden sürdürebilmesi için gerekli prosedürler, yönergeler ve stratejiler içeren yapılandırılmış bir yaklaşıma

sahip belge veya belge niteliğindeki dokümanların tümüdür (Shen vd., 2022). Felaket kurtarma planlaması, yalnızca teknolojik yedeklemeleri kapsamamaktadır. İyi bir plan, insan kaynakları, iş süreçleri ve kurumsal stratejileri de kapsayan bir yaklaşımı içermelidir. Felaket kurtarma planlarının hazırlanmasında, planı geliştiren bireylerin deneyimleri, planın etkinliği ve uygulanabilirliği açısından belirleyici bir faktör teşkil etmektedir. Bu çerçevede, bireylerin deneyimlerini analiz etmek amacıyla nitel araştırma yöntemlerinden biri olan fenomenoloji kullanılarak, üniversitelerde BT alanında görevli bireylerin deneyimleri incelenebilir ve bu veriler doğrultusunda felaket kurtarma planları oluşturulabilir (Jackson vd., 2018).

Bu tezin amacı, kamu üniversitelerinde bilgi teknolojileri felaket kurtarma planlaması ve geliştirilmesine yönelik stratejilerin belirlenmesinde, BT uzmanları veya yöneticilerinin bu planları oluştururken dikkate aldıkları unsurlar, plan geliştirme süreçlerindeki adımlar ve bu planları olumlu ya da olumsuz yönde etkileyen faktörlerin deneyimsel olarak ortaya konmasıdır. Tezin birinci bölümünde felaket kurtarma ve iş sürekliliği konuları ele alınmıştır. İkinci bölümde, fenomenoloji ve planlı davranış teorisi üzerinde durulmuştur. Üçüncü bölümde ise araştırmanın metodolojisi ve bulguları sunulmuş, tez sonuç ve tartışma bölümü ile sonlandırılmıştır.

BİRİNCİ BÖLÜM

BT FELAKET KURTARMA PLANLANMASI

1.1. FELAKET KURTARMA PLANLAMASINA TARİHSEL BAKIŞ

Bilgi teknolojilerinde yaşanan gelişmeler, çeşitli alanlarda olduğu gibi, stratejik planlama süreçlerini ve bu süreçlerin uygulanmasına yönelik yöntemleri de önemli ölçüde dönüştürmüş ve bu alanlarda önemli değişimlere zemin hazırlamıştır. Dijital veri hacmindeki sistematik olarak gözlenen sürekli artış, özellikle kurumlar, kuruluşlar, organizasyonlar ve hizmet sağlayıcılarını hedef alan siber saldırıların yaygınlaşmasına ve olumsuz durumların oluşmasına zemin hazırlamıştır. Bu tür saldırılar genellikle veri kaybına veya hizmet kesintilerine neden olmakta ve bilgi güvenliğine yönelik tehditlerin ciddiyetini artırmaktadır. Bu doğrultuda, kuruluşların bilgi güvenliği tehditlerini önlemeye yönelik yaklaşımları çerçevesinde, felaket kurtarma stratejilerinin önemi giderek daha fazla vurgulanmaktadır (Irmak & Baz, 2019). Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gibi yasal düzenlemeler, bilgi güvenliğini sağlama süreçlerinde temel bir rol üstlenmektedir. Bu düzenlemeler çerçevesinde, veri yedekleme ve felaket kurtarma planlarının geliştirilmesi ve uygulanması, kurumsal düzeyde hem yasal uyumluluğun sağlanması hem de bilgi güvenliğinin temin edilmesi açısından büyük bir önem taşımaktadır (Savaş vd., 2020).

Dijital teknolojiler öncesinde, verilerin kâğıt üzerinde saklanması ve bu verilerin korunmasına yönelik alınan felaket önlemleri, özellikle kamu kurumlarında felaket kurtarma planlamasının ilk örnekleri olarak değerlendirilebilir (Şalcı, 2021). 1960'lı yıllarda dünya genelinde üretilen bilgisayarların büyük boyutları ve yüksek maliyetleri nedeniyle bu teknolojilerin kamu kurumlarında yaygın kullanımı sınırlıydı. John McCarthy tarafından 1960'lı yıllarda öne sürülen *"Bir gün hesaplama işlemleri geniş kamusal ağlar üzerinde gerçekleşecek."* görüşü, çalışma ortamlarında fiziksel yakınlık gereksiniminin azalması ve bulut bilişim teknolojilerinin gelişimiyle büyük ölçüde hayata geçmiştir. Ayrıca bu görüş, bulut bilişim kavramının temellerini oluşturan önemli bir teorik çerçeve sunmaktadır (Selvi & Küçüksille, 2014). Ülkemizde, 1980'li yıllarda dijital depolamanın sunduğu avantajların etkisiyle kamu kurumlarında BT kullanımına başlanmış ve bu durum, kâğıt tabanlı arşivleme, saklama, imha ile felakete karşı önlem

alma stratejilerinde bir dönüşüm sürecini tetiklemiştir. Söz konusu dönüşüm, 1990'lı yıllarda bilgisayarlarda işlenen verilerin yalnızca kullanıldıkları cihazlarda değil, aynı zamanda sunucular ve depolama ünitelerinde saklanmasıyla devam etmiş; bu süreç, son kullanıcı cihazlarının yanı sıra kurumlara hizmet sağlayan veya veri depolayan cihazların da kritik önem kazanmasına yol açmıştır. Aynı dönemde, teknolojinin sağladığı bu avantajlar kamu kurumlarında BT kullanımını yaygınlaştırmış ve bu durum, kurumların iş süreçlerini etkileyen aksaklıklar ve arızalar arasına BT kaynaklı sorunların da eklenmesine neden olmuştur. Bu olumsuz durumlar karşısında, kamu kurumlarının verilerini korumaya yönelik eylem ve planlara olan ihtiyacı artmış, bu tür planların önemi daha belirgin hale gelmiştir. Bu bağlamda, felaket kurtarma planları da gelişen süreçten etkilenmiş; plan içerikleri, son kullanıcı cihazlarını da kapsayacak şekilde genişletilerek üç katmanlı bir mimari yapıya dönüşmüştür. Üç katmanlı mimaride, verilerin saklandığı, işlendiği ve kullanıcı ara yüzlerinin bulunduğu katmanlar ayrıştırılmıştır. Bu yapı sayesinde, kurumlar, kuruluşlar ve organizasyonlar, veri yedekleme ve geri yükleme işlemlerini daha etkin bir şekilde gerçekleştirebilmekte, aynı zamanda verilerin yedeklenmesi ve bakım süreçleri ise daha kolay hale gelmektedir (Liduo & Yan, 2010).

Ağ teknolojilerindeki ilerlemeler ve yüksek bant genişliklerine son kullanıcıların da erişebilmesi, kamu kurumları başta olmak üzere işletmelerin, kuruluşların ve organizasyonların personellerine uzaktan çalışma opsiyonları sunmasını teknolojik olarak mümkün hale getirmiş ve bu durum, BT süreçlerinde bir kez daha dönüşüme yol açmıştır. Bununla birlikte, 2008 yılının başlarında, servis sağlayıcılar ile hizmet alanların, sahip oldukları donanım ve yazılım kaynaklarını servis tabanlı modeller biçiminde kullanmaya başlaması, bulut bilişim teknolojilerinin yaygınlaşmasında önemli bir rol oynamıştır (Yazır, 2018). Günümüzde giderek yaygınlaşan bulut bilişim kavramı, özellikle özel bulut (private cloud) hizmetlerinin kurumlar tarafından benimsenmesiyle birlikte, BT felaket kurtarma planlarının tarihsel dönüşümünde de kritik bir rol üstlenmektedir (Chang, 2015). Bu gelişim, felaket kurtarma planlarının, kurumlar, kuruluşlar veya organizasyonlar tarafından bulut hizmeti sağlayıcılarından dış kaynak olarak temin edilmesini ifade eden ve "Hizmet Olarak Felaket Kurtarma" (Disaster Recovery as a Service - DRaaS) yaklaşımıyla somutlaşmaktadır. Bulut bilişim, BT felaket kurtarma planlarında geleneksel site tabanlı sistemlere kıyasla çeşitli avantajlar sunmaktadır. Bunlar arasında kurtarma süreçlerinin kolaylığı, maliyet etkinliği, kurtarma sürelerindeki

hız, ölçeklenebilirlik ve esneklik gibi unsurlar öne çıkmaktadır (Wood vd., 2010). Yedekleme ortamı aynı tesis içinde, kampüs içinde, ana sistem odası yakınında veya aynı şehirde bulunan yapılarda, ana sistemin yaşadığı riskin aynısına benzer şekilde felaket kurtarma merkezi ya da yedekleme ortamı da maruz kalmaktadır. Bu nedenle geleneksel yedekleme ortamı ve sunucu tabanlı kurtarmalara göre bulut bilişim temelli kurtarma seçenekleri, bir kurumun yedeklemesini farklı coğrafi konumlara dağıtmasına olanak bulur ve böylece olası yerel bir felaketin olumsuz etkisini en aza indirme konusunda kuruma avantaj sağlar (Özdemir & Gökgöz, 2018).

1.2. BT FELAKET KURTARMA PLANI METODOLOJİSİ

Toplumu oluşturan insanların günlük yaşamlarını kolaylaştırmak için bilgi teknolojilerinden yüksek oranda faydalanılmaktadır. Günlük yaşamda herhangi bir eylem gerçekleştirilirken belirli oranda olumsuz bir durumla karşılaşma olasılığı insanlık tarihi boyunca var olmuş ve olmaya devam edecek bir şeydir. Olumsuz olay, sonuçları olumsuz, genellikle beklenmedik bir olaydır (Prasetyo vd., 2020). Bilgi teknolojileri açısından olumsuz bir olay, BT felaketi olarak adlandırılır ve gerçekleşmesi halinde normal BT süreçlerini, BT altyapılarını, donanımları, yazılımları veya verileri etkileyen kesintiye uğratacak veya zarar verecek eylemlerin tümüdür (Prasetyo vd., 2020). Doğal afetler başta olmak üzere, kasıtlı olarak gerçekleştirilen saldırılar, yanlış veya eksik yapılandırma nedeniyle devre dışı kalan elektronik cihazlar, insan kaynaklı hatalardan kaynaklana hizmet kesintileri gibi sebeplerden dolayı BT hizmetlerinin olumsuz etkilenmesi durumu BT felaketi olarak görülmektedir (Doğan vd., 2016).

BT Felaket kurtarma planı, olumsuz bir olaydan veya BT felaketinden sonra, bir kuruluşun BT operasyonlarının nasıl tekrar hizmet vermeye devam edebileceğinin detaylandırıldığı bir belgedir ve kuruluşların varsa genel iş sürekliliği planlarının ayrılmaz bir parçasıdır (Rouhanizadeh vd., 2020). BT felaket kurtarma planı oluşturacak kurum, kuruluş veya organizasyonun, her şeyden önce koruması gereken BT envanterine hakim olması gerekmektedir. Prasetyo arkadaşlarına göre, bir kuruluş bilgisi dahilinde olanı ancak koruyabilir (Prasetyo vd., 2020). Bu nedenle bir kuruluşun BT felaket kurtarma planı geliştirmeden önce neyi korumak istediği kararını kesinleştirmiş olması gerekebilir. Felaket kurtarma planında yer alacak BT varlıklarının ve kritik işlevlerin seçilmesi, risklerin ölçülmesi veya derecelendirilmesi ve BT altyapısının denetlenerek bir

liste oluşturulup tanımlanmasıyla BT felaket kurtarma planı oluşturma işlemi başlatılabilir. Kurtarma planının çıktıları bir dizi kurtarma hedefidir (Mendonça vd., 2019). Doğru bir BT felaket kurtarma metodolojisi seçmek felaket yaşanılmadan önce oluşturulan planların, çalışmaların veya hazırlıkların tamamının sonuçlarına güven duyabilmenin ön koşullarından biridir. Bu bağlamda BT felaket kurtarma metodolojisinde yer alan başlıklar değişiklik gösterebileceği gibi genellikle aşağıdaki alt başlıklardan oluşur (Kasim & Mohamed, 2018; Snedaker & Rima, 2013):

- Felaket kurtarma planı kapsam ve hedeflerinin belirlenmesi,
- Risk analizi,
- Önceliklerin belirlenmesi,
- Altyapının sağlanması,
- Verilerin toplanması ve planın belgelendirilmesi,
- Test etme ve tüm planın gözden geçirilmesi

1.2.1. Felaket Kurtarma Planı Kapsam ve Hedeflerinin Belirlenmesi

BT felaket kurtarma planlarının kapsamları, oluşturuldukları kurumun başta teknolojik altyapısı, finansal durumu, verdiği hizmetlerin kritiklik durumları olmak üzere yöneticilerin ve personellerin tutumlarına kadar birçok faktöre bağlı olarak farklılıklar gösterebilir. Bazı kurumlar planlarının kapsamlarını kısa tutarken, bazılarında ise bu kapsam çok geniş tutulabilmektedir. Tipik bir BT felaket kurtarma planının kapsamı genellikle geri yükleme süreleri ve nelerin felaket sonrası çalışacağına bağlı olarak iş gereksinimlerine göre donanımları, veri ve veri tabanlarını, hizmet veren uygulamaları ve geri yükleme stratejilerini içerir (Abualkishik vd., 2020). Bu durum planın revizyonları içerisinde değişebileceği gibi felaket kurtarma bütçesinin zaman içinde karşılayabileceği ölçeğe göre de değişim gösterebilir. Bu nedenle, BT felaket kurtarma planlarında yer alan kapsamlar ve hedefler değişebilir (Wiboonratr & Kosavisutte, 2009). Bütün BT sistemlerinin BT felaket kurtarma planlarına ve iş sürekliliği çalışmalarına dahil edilmesi bir kurum için kapsamın belirlenmesinde kolaylık sağlayacaktır. Fakat tüm BT sistemlerini ve bu sistemlerin internet, elektrik enerjisi, soğutma vb. gibi altyapılarını BT felaket kurtarma planına dahil etmesi neredeyse imkânsız olarak görülmektedir (Gonzales, 2010). Tüm sistemlerin dahil edildiği bir plan, genellikle maliyet ve kaynak

kısıtlamaları nedeniyle gerçekleştirilemez. Bu nedenle BT felaket kurtarma planı hazırlayan bir kurumun neyi koruyacağına karar vermesi gereklidir. Tipik BT felaket kurtarma planı bileşenleri, kurum için en kritik BT sistemlerini, veri tabanı sistemlerini ve kritik sistemi çalıştıracak nitelikteki ağlarını içerir. Enerji yedekliliğini, ağ hizmetinin felaketten sonra sağlanabilmesini, kritik uygulamaların felaket sonrası en kısa sürede hizmet verir hale gelmesini, felaket halinde ve hemen sonrasında iletişimi, veri merkezi seçimini, yaygın ve deprem gibi doğal afet sorunlarını, siber saldırılar gibi sorunları ele alır (Kenan vd., 2020; Meechang vd., 2020).

BT felaket kurtarma planının geliştirilmesi sürecinde, kurum, kuruluş veya organizasyonun kesinti sürelerini ne kadar tolere edebileceğini (RTO - Recovery Time Objective) ve ne kadar veri kaybını kabul edebileceğini (RPO - Recovery Point Objective) belirlemesi kritik bir gerekliliktir. Bu hedefler, planın kapsamını belirlerken önceliklendirilmesi gereken temel unsurlardır. Ayrıca planın kapsamı, ağ ve sistem bileşenlerinin yazılım ve donanım düzeyinde yeniden başlatılması, gerektiğinde yeniden yapılandırılması veya felaketin türüne uygun şekilde uyarlanması ve kurtarılması için gerekli yönergeleri ana hatlarıyla içermelidir (Snedaker & Rima, 2013).

1.2.2. Risk Analizi ve Risk Yönetimi

Bilgi teknolojileri felaket kurtarma planı oluştururken, risk değerlendirmesi temel adımlardan biridir. Kurumlar, kuruluşlar veya organizasyonlar sahip oldukları bilgi varlıklarına dair ayrıntılı listelere sahip olmalı ve bu listeler, risk değerlendirmesine başlamak için kolaylık sağlamaktadır. Risk değerlendirmesi, olası felaket senaryolarını tanımlamayı, bu felaketlerin gerçekleşmesi durumunda potansiyel etkilerini belirlemeyi ve bu etkilere uygun tepki stratejilerini geliştirmeyi içerir (Kuyumcuoğlu & Başoğlu, 2008). İyi bir plan, kurumların kritik BT sistemlerini ve bu sistemler üzerinde depolanan, işlenen veya paylaşılan verileri korumaya odaklanır ve varsa kurumun iş sürekliliği planlarıyla çelişmeyen önlemleri içerir (Ateş & Güneş, 2016). Bu plan dahilinde; *"Hangi felaket senaryoları kurum adına yaşanılması en olasıdır?"*, *"Hangi sistemler ve veriler kurum adına verilen hizmetlerin tamamı düşünüldüğünde en kritiktir?"* sorularına cevaplar aranır. Kurumlar için olası riskler, bölgesel iklim koşulları, BT operasyonlarının yürütüldüğü coğrafi konum, teknolojik altyapı ve içerisinde bulunan kurum, kuruluş veya organizasyonun ihtiyaçları gibi faktörler göz önünde bulundurularak değerlendirilir.

Ayrıca topluluğun bu yapılardan beklediği özel ihtiyaçlar da risk değerlendirmesine dahil edilir. Riskler belirlendikten sonra, felaket durumunda takip edilecek adımları içeren, mümkün olduğunca sade bir dille yazılmış kapsamlı bir plan oluşturulmalıdır. Bu plan, kurumların ihtiyaçları ve yürüttükleri BT hizmetlerine bağlı olarak farklılık gösterebilir; ancak temelde acil iletişim prosedürlerini, envanterde yer alan veya dış kaynaklardan temin edilecek ekipman ve kaynakların yönetimini, personellerin görev sorumluluklarını, personel eğitimini ve diğer önleyici önlemleri içermelidir (Gregory, 2011).

Risk yönetimi, kurumların, kuruluşların veya organizasyonların tüm risklerini kontrol altına almayı amaçlayan bir konudur. Günümüzde kurumlar, hizmet verdikleri alanlara göre farklı ve çeşitli risklerle karşı karşıyadır. Siber saldırılar gibi riskler, kurumların maddi veya manevi değerini olumsuz etkileyebilir. Bu bağlamda, kurumlara veri sızıntıları veya saldırı sonrası kötü olay yönetimi nedeniyle davalar açılabilir. Buna ek olarak, kurumlar, deprem, sel, yangın gibi afetler sonrası hizmet veremeyecek duruma gelebilirler. Ulusal veya uluslararası maddi, manevi zararların oluşturacağı risklerle karşı karşıya kalabilirler. Bunlar, kurumların değerini, saygınlığını etkileyen bazı ana risklerdir. Risk yönetimi sadece finansal risklere odaklanmaz. Tarihi ve kültürel birikimin kaybolması, sendika sözleşmeleri, paydaşlarla yapılan iş anlaşmaları ve dış kaynak kullanımı anlaşmaları gibi unsurların yanı sıra, eğer hizmet veren kurum yapısında toplumun sağlık ihtiyaçlarına yönelik hizmet veriyorsa can kaybı gibi riskler ile toplumsal veya sosyolojik riskler gibi diğer risk türleriyle de ilgilenir. Bu nedenle, risk yönetimi, bir kurumun tüm risklerini kapsayan bir yaklaşımdır. Risk yönetimi, her kurum için önemlidir. İş sürekliliği ve felaket kurtarma planlarına odaklanmaktan çok, kurum öncelikli olarak mevcut risklere odaklanmalıdır. Risk değerlendirme süreci, değerlendirmenin nasıl yapılacağını belirlerken, değerlendirme yaklaşımının ise nicel ya da nitel bir yöntemle mi yapılacağına karar verilmesi gerekir. Seçilecek değerlendirme yöntemi tutarlı bir şekilde belirlenmeli ve belgelendirilmelidir (Khatavakhotan & Ow, 2012). Risk değerlendirme süreci, tehdit değerlendirmesi ve zafiyet değerlendirmesi gibi kavramlarla karıştırılabilir. Bu kavramlar, risk yönetimi kapsamında alt başlıklar olarak ele alınmaktadır. Risk yönetimi, aynı zamanda, bir güvenlik açığının ortaya çıkma olasılığı ve etkisini dikkate alarak, özellikle kurumsal verilerin işlendiği, depolandığı veya iletildiği BT sistemlerine ait riski tanımlama, değerlendirme ve kabul edilebilir bir seviyeye indirme sürecidir. Bu sürecin amacı, kurumsal bilgi işlem kapasitelerini ve

sistemlerini güçlendirerek yönetimin, risk yönetimi kararları almasını sağlamak ve kurumun misyonunu desteklemektir. İyi tasarlanmış bir risk yönetimi süreci, kurumların BT bütçelerini etkin ve verimli bir şekilde kullanmalarına katkı sunmaktadır. Ayrıca, risk yönetimi faaliyetleri, BT sistemlerinin akredite kuruluşlar tarafından gerçekleştirilen denetimlere uygunluğunu sağlamada kritik bir rol oynar ve yetkilendirme ile sertifikasyon süreçlerine önemli ölçüde destek sağlar (Hash, 2002). Risk değerlendirmesi, temel olarak sonucu ve etkileri belirlenmemiş olayları tanımlamayı amaçlar. Risk yönetimi, belirsizliği yönetmeye çalışmakla ilgilidir. BT alanında, bir kurum için tüm risklerin tamamen ortadan kaldırılması neredeyse imkânsızdır. Bu nedenle, risklerin azaltılması veya etkilerinin en aza indirilmesi için yöntemler ve stratejiler araştırılabilir.

Bir kurumun risk değerlendirmesi yaparken dikkate alabileceği temel riskler değerlendirildiğinde, beş temel risk kategorisi olduğu görülür. Bu kategoriler kurumun BT felaket kurtarma planı geliştirmesine yardımcı olabilir (Gritzalis vd., 2019).

- Doğal afetler,
- Lokal riskler,
- Bilgi riskleri,
- Bölümsel veya departman bazlı riskler,
- Bireysel riskler.

Doğal afetler, BT felaket kurtarma planlarında ele alınan önceliklerden biri olarak öne çıkmaktadır. Bu afetler, kurumların doğrudan veya dolaylı olarak etkilendikleri, sel, su baskını, kasırga, volkanik patlamalar, deprem gibi dışsal riskleri kapsamaktadır. Bu tür afetler, kurumların işleyişini genellikle aksatmakta ve çalışanlar, paydaşlar ve müşteriler üzerinde olumsuz etkiler yaratmaktadır. Dünya genelinde meydana gelen 31 farklı doğal afetten 28'inin meteorolojik afetler olduğu belirlenmiştir (AFAD, 2024). Bu durum, BT felaket kurtarma planı hazırlanırken meteorolojik afetlerin oluşturacağı risklere karşı alınacak önlemlerin ön plana çıkmasının önemini vurgulamaktadır.

Lokal riskler, genellikle kurumun kendisiyle sınırlı kalan risklerdir. Elektrik sorunları, inşaat problemleri, kurum içi veya diğer ağlarla olan bağlantıyı sağlayan iletişim hattı sorunları, terör saldırıları, tehlikeli madde sızıntıları ve tıbbi acil durumların oluşturacağı riskler bu kapsamda ele alınırlar (Özbilgin, 2012).

Bilgi riskleri, bir kuruluşun veri depolama sistemlerini, ağ ve iletişim altyapısını, BT donanımlarını hem içeriden hem de dışarıdan etkileyebilecek risklerdir. Bu tür risklere karşı önlem alınmamasında olası veri kayıpları söz konusudur ve yaşanılacak veri kayıpları operasyonel süreçleri etkileyebileceği gibi yasal prosedürlere uygunsuzluk veya diğer hukuki nedenlerden dolayı kurum adına sorunlar doğurabilirler.

Bölümsel veya departman bazlı riskler, genellikle her departmanın, bölümün veya birimin kendilerine tanımlanmış görevleri başarıyla yerine getirebilmesini engelleyen risklerdir. BT felaket kurtarma planlarının hazırlanmasından genellikle kurumlarda BT birimleri sorumluyken, planın işletilmesinden BT birimleri ve kurum yöneticileri sorumlu olabilmektedirler.

Bireysel riskler, BT felaket kurtarma süreçlerinde personellerin kişisel çalışma alanlarını etkileyen risklerdir. Bu riskler, kurumun iş süreçlerinde personellerin görevlerine göre değişim gösterebilir. Kritik bir işin tek bir personel tarafından yürütülmesi, bazı kurumlar için risk olarak değerlendirilirken bazı kurumların iş süreçleri değerlendirildiğinde birden fazla personelin kritik kararlarda yer alması, karar alma süreçlerini yavaşlatacağı için risk oluşturabilir. Bireysel riskler insan kaynaklı afetlerle karıştırılmaktadır. BT süreçleri için insan kaynaklı afetler; insan kusurları, ihmalkarlık, doğru planlanmamış veya yapılandırılmamış ağ cihazlarının, sistemlerin başarısızlığı ve temel olarak etkisi olumsuz olan, içerisinde insan faktörü bulunduran afetlerdir (Aerts vd., 2018; Özbilgin, 2012; Qadriina vd., 2023). Tipik bir BT felaket kurtarma planı, kurumların iş sürekliliği süreçleri çerçevesinde, mevcut durumlarını ne kadar iyi hazırladıklarını ve gelecekteki olası felaketlere karşı nasıl bir strateji izlemeleri gerektiğini anlamalarına yardımcı olmak için belirli sorulara yanıt arar. Bu sorular, kurumun işleyişi, aldığı veya verdiği hizmetler gibi çeşitli faktörlere bağlı olarak farklılık gösterebilir. Cervone'ye göre sorulması gereken temel sorular şunlardır (Cervone, 2017):

- Kurum içindeki kritik iş süreçleri ve fonksiyonları nelerdir?
- Kritik iş süreçlerinin ve fonksiyonların işlevini yerine getirilmemesinin etkisi nedir?
- Kurum BT verilerini nerede tutuyor, hangi sıklıkla erişim sağlıyor, olası veri kaybında hangi hizmetler etkilenecektir?
- Kurum adına en kritik süreçler hangileridir?

- Birden fazla hizmet veya sürecin felaketten sonra kaybedilmesinin etkisi nedir?
- Belirli hizmetler veya süreçler olmadan kurum ne kadar süre çalışabilir?
- Felaket öncesindeki hizmetleri ve süreçleri çalışır duruma geri yüklemek ne kadar sürer?
- Kurumun BT verileri yedekleniyor mu? Yedekten dönme testleri yapılıyor mu? Olası felaket sonrası veriler ne kadar sürede geri dönebilir?
- Kurumun en fazla zafiyet göstereceği, savunmasız olduğu yerler nerelerdir?
- Kurumun BT verilerine yönelik güvenlik tehditleri nelerdir?
- Kurumun BT verilerine kimler, hangi sıklıkla, nereden ve hangi yetkiyle erişebiliyor? Erişim denetimi var mı? Yetkisiz erişim sonucu hangi veriler ele geçirilebilir?
- Zafiyetlerden kaynaklanacak riskler nasıl azaltılabilir?
- Risk ve maliyet ilişkisi göz önünde bulundurularak, kurum için hangi riskler en önemli risklerdir?

BT riskinin belirlenmesinde güvenlik açıkları, etkiler ve tehdit değerlendirmesi önemli unsurlar arasında yer almaktadır (Snedaker & Rima, 2013).

Güvenlik açığı, bir kurumun BT sistemleri, süreçleri veya varlıklarının tehditlere ya da tehlikelere karşı zayıf, savunmasız ya da sömürülebilir durumda olmasını ifade eder. BT felaket kurtarma planlaması bağlamında güvenlik açıkları, risk analizi kapsamında ele alınır ve daha önce belirlenen tehditlere karşı savunmasız olan ya da bu tehditlere maruz kalma potansiyeli taşıyan süreçler veya BT sistemlerinin belirli alanlarını tanımlar (Snedaker & Rima, 2013). Güvenlik açıklıklarının değerlendirilmesi, zafiyet değerlendirme olarak da adlandırılmaktadır. Bu değerlendirme, bir kurum veya kuruluşun kendisi ve çevresine yönelik tehditleri tespit etmesini, anlamasını ve bunlara karşı tepki vermesini gerektiren bilgi, farkındalık ve risk arka planını sağlar (Şahinaslan vd., 2023). BT sistemleri başta olmak üzere, zafiyetler kasıtlı olarak istismar edilebilir, sömürülebilir veya bilinçsiz bir şekilde tetiklenebilir. İşletim sistemlerinde, yazılımlarda veya ağ bağlantısı sağlayan cihazların yapılandırılmalarında yapılan bir değişiklik, BT yöneticilerinin farkına varmadıkları fakat sistemin, yazılımın veya cihazın başka bir yerinde bir güvenlik açığına neden olabilir. Ayrıca gelişen siber saldırı teknikleri daha önceden tespit edilememiş zafiyetleri, saldırganlar tarafından istismar edilebilir düzeyde

ortaya çıkartabilmektedir. Buna bağlı olarak, BT felaket kurtarma planlamasında güvenlik açıklarının analizi, kuruma ait BT sistemlerini kapsamalıdır, ek olarak, bu kapsam sadece BT sistemleriyle sınırlı kalmayıp, süreçler, teknolojik cihazlar, ağ yapıları, altyapılar hatta insan faktörünü de içermelidir. Kurumlar güvenlik açıklıkları ölçeği kapsamında Tablo 1.1'de belirtildiği gibi örnek ölçekler geliştirebilir.

Tablo 1.1. Örnek Güvenlik Açıklıkları Ölçeği.

Açık Derecesi	Açıklaması	Örnek
1	Düşük seviye, etkisi lokal olarak kuruma yansıyan tehditlerdir.	Yanlış yetkilendirilmiş fakat yetkisinin farkında olmayan ve kritik sistemlere hiç erişim sağlamamış personel.
2	Orta seviye, etkisi birden fazla birimi etkileyen tehditlerdir. Verilen hizmetleri kesintiye uğratmazlar fakat kurum adına düşük öneme sahip bilgilerin ifşasına neden olabilirler.	SNMP public ve private community string değerleriyle sistemler hakkında bilgi toplanabilmesi.
3	Yüksek seviye, etkisi kurumun verdiği hizmetlerin devre dışı kaldığı tehditlerdir. Geri dönüş senaryolarıyla yedeklemelerden faydalanılarak hizmetler tekrar geri getirilebilir.	Yazılımın güncel olamayan ve zafiyet barındıran sürümüme sahip sunucuda uzaktan kod çalıştırarak, sunucunun işleyişinin durdurulması ve sunucu yönetiminin ele geçirilmesi.
4	Kritik seviye, etkisi sistemin tamamen ele geçirilmesi ile sonuçlanan veya hizmetlerin yeniden kurulum yapılana kadar çalışmadığı tehditlerdir.	Ana ve yedek verilerini aynı veri merkezinde tutan bir kurumun, standartlara uymayan veri merkezi güç hattında voltaj yüksekliğinde tüm cihazlarının çalışamaz hale gelmesi.
5	Acil seviye, gerçekleşmesi halinde etkisi kuruma maddi, manevi açıdan en yüksek tehditlerdir. Kuruma ait kritik verilerin bir kısmının ya da tamamının ifşasına neden olabilecek tehditlerdir.	Kuruma ait aktif dizin hizmetinin yönetici parolasının ele geçirilmesi sonucu tüm verilerin ifşası ve geri dönülemez biçimde silinmesi.

Örnek bir BT felaket kurtarma planında, olasılık ve etki dereceleri değerlendirilerek kurumun hangi riskleri göze alabileceği durumu analiz edilebilir. Bu

bağlamda, olasılıklar ve etkiler 1 ile 5 arasında değerlendirilebilir. Örneğin, olasılık derecelendirmeleri 1 ile 5 arasında aşağıdaki gibi yapılabilir ve bu değerlendirme Tablo 1.2'de gösterilmiştir.

Tablo 1.2. Örnek Olasılık Derecelendirilmesi (TBD, 2006).

Olasılık Derecesi	Açıklaması
1	Olması hiç muhtemel olmayan veya imkânsız
2	Olması muhtemel olmayan
3	Olması muhtemel olan veya nadir sıklıkta gerçekleşmiş
4	Olması yüksek muhtemelde olan veya sıklıkla gerçekleşmiş
5	Olması kesin olan veya defalarca kez gerçekleşmiş

Tehdit değerlendirmesi, bir kurumun BT varlıklarına yönelik gizlilik, bütünlük ve erişilebilirliği olumsuz olarak etkileyen faktörlerin tümü olarak tanımlanır. Bu tehditler, doğa kaynaklı olabileceği gibi insan kaynaklı tehditler de olabilir. Doğa kaynaklı tehditler, temel olarak deprem, sel yangın vb. olaylar sonucunda BT varlıklarına zarar verecek, işleyişlerini etkileyecek, erişilebilirliklerini kısıtlayacak tehditler olarak bilinmektedir (Çakır & Yaşar, 2015). İnsan kaynaklı tehditler, kurumların BT süreçlerini, bilgi varlıklarını veya bilgi güvenliğini kaza veya kasıtlı olarak, olumsuz sonuçlar meydana getirecek şekilde etkileyecek, bireylerin oluşturduğu tehdit türleridir. Bu tehditler, kurum içindeki personeller veya bilgi güvenliği kapsamında yer alan envantere ya da BT varlıklarına erişim sağlayan kişiler tarafından, kasıtlı veya kazara gerçekleştirilebileceği gibi, kurum dışından da yine kasıtlı ya da kazara oluşabilecek tehditlerdir (Savaş vd., 2020).

Güvenlik açıkları ve olasılıkları derecelendirildikten sonra, BT alanında kurum için risk senaryoları çalışmaları yapılabilir ve bu senaryoların etki ile olasılıklarına göre risk haritası veya risk matrisinde uygun şekilde konumlandırılması sağlanabilir. Her kurum için senaryolar, kurumun yapısına, sunduğu hizmetlere ve uyması gereken yasal zorunluluklara göre farklılık gösterebilir. Temelde, kurumlar, kendileri için tehdit oluşturabilecek durumlara göre senaryoları belirleyebilir ya da daha önce yapılmış benzer çalışmalardan elde edilen senaryolardan faydalanabilirler. Tablo 1.3'te, BT risk senaryolarına örnekler verilmiştir.

Tablo 1.3. Örnek BT Risk Senaryoları (TBD, 2006).

Senaryo Numarası	Olay
Senaryo-1	Doğru planlanmamış veya yetersiz ağ ve sistem kapasitesi nedeniyle oluşacak riskler.
Senaryo-2	Kurum BT yapısından veya kurum kaynaklarından 3. Şahıslara yönelik anlaşmazlıklar veya iflas.
Senaryo-3	Doğal afetler.
Senaryo-4	Kurum kaynaklarının etkin kullanılamaması veya yanlış kullanılması.
Senaryo-5	Kurum personelleri veya hizmet alım kapsamında kuruma hizmet veren personeller tarafından kaynaklanan sorunlar.
Senaryo-6	Kurumun yasal sorumluluğunda olan verilerinin veya gerçekleştirdikleri hizmetlerin gizliliğini, bütünlüğünü veya erişilebilirliğini tehlikeye sokacak sabotajlar, saldırılar veya kötü niyetli eylemler.
Senaryo-7	Yazılım hataları.
Senaryo-8	Yetersiz veya eksik veri modellemesi.
Senaryo-9	Kurum içi personeller, yöneticiler ve BT personellerinin kendi aralarında eksik, yanlış veya etkisiz iletişim.
Senaryo-10	Kurumsal hafıza eksikliği, yanlış yönlendirilmiş bilgi birikimi, yanlış edinilmiş beceri ve kazanımlar nedeniyle oluşacak riskler.

Senaryolara göre riskler belirlendikten sonra, BT alanında bu risklerin kurumlara olan etkilerinin belirlenmesi de gerekmektedir. BT alanında, risklerin kurumlara olan etkilerinin temel olarak ekonomik, operasyonel ve manevi ya da itibar başlıkları altında olduğu bilinmektedir (Snedaker & Rima, 2013). Bu bağlamda, kurumlar risklerin etkilerini kayıplar olarak değerlendirebilirler. Bu değerlendirmeleri 1 ile 5 arasında derecelendirerek, tablolar halinde ifade edebilirler. Böylece, riskin boyutunu belirlemek için kullanılacak yöntemlere yönelik temel bilgi girişi sağlanmış olur. Tablo 1.4'te örnek ekonomik etkiler, Tablo 1.5'te örnek operasyonel etkiler ve Tablo 1.6'da örnek manevi/itibar kayıp etkileri gösterilmektedir. Bu süreçte, BT felaket kurtarma planı

hazırlıklarında, kurumlar kendi risklerinin etkilerine göre benzer tablolar oluşturarak özelleştirilmiş bir değerlendirme yapmalıdırlar.

Tablo 1.4. Örnek Ekonomik Etkiler.

Derece	Etki
1	1-100.000 TL arasında potansiyele sahip maddi kayıp.
2	100.001-500.000 TL arasında potansiyele sahip maddi kayıp.
3	500.001-1.000.000. TL arasında potansiyele sahip maddi kayıp.
4	1.000.001-5.000.000 TL arasında potansiyele sahip maddi kayıp.
5	5.000.001 TL ve üzeri potansiyele sahip maddi kayıp.

Tablo 1.5. Örnek Operasyonel Etkiler.

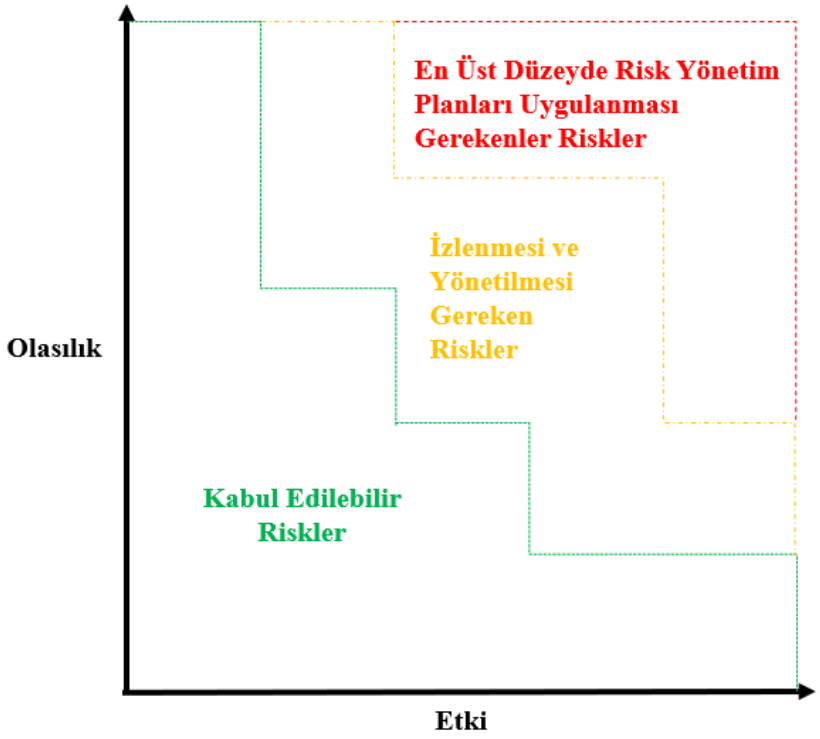
Derece	Etki
1	Operasyonlar hiç etkilenmeyebilir.
2	Operasyonlara etkisi süreçle sınırlı olacaktır.
3	Operasyonların bir kısmı etkilenir, fakat telafi edilebilir düzeydedir.
4	Operasyonlar tamamı etkilenir, kurumu zarara uğratır.
5	Operasyonların tamamen durmasıyla sonuçlanır. Kurum işleyemez hale gelir.

Tablo 1.6. Örnek Manevi/İtibar Kayıp Etkileri.

Derece	Etki
1	Kurumun itibar, saygınlık ya da manevi kayıplarına neden olmaz.
2	Kurumun itibar, saygınlık ya da manevi kayıplarına az bir etkisi olur.
3	Kurumun itibar, saygınlık ya da manevi kayıplarına orta derecede bir etkisi olur.
4	Kurumun itibar, saygınlık ya da manevi kayıplarına ciddi derecede bir etkisi olur.
5	Kurumun itibar, saygınlık ya da manevi kayıpları kurumun kapatılmasıyla sonuçlanır.

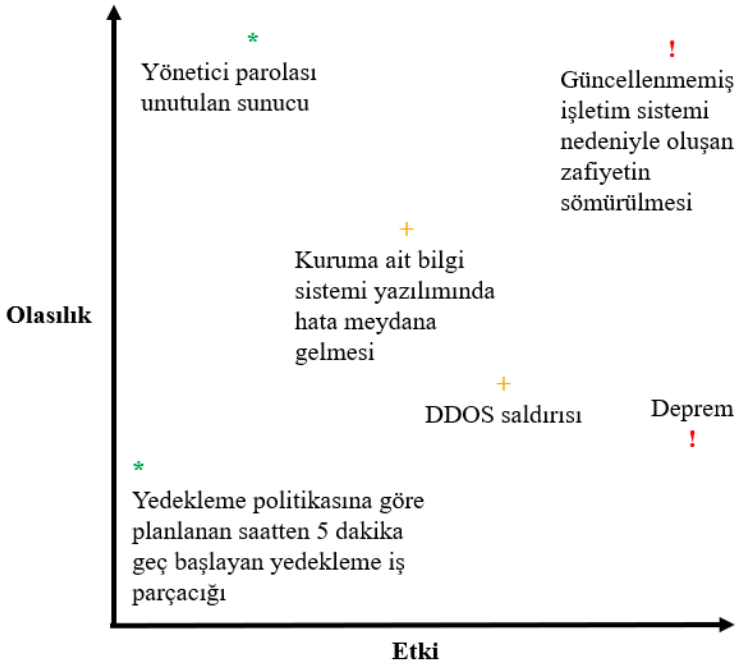
BT felaket kurtarma planlaması kapsamında kuruma ait risk değerlendirilmesi yapılırken senaryoların belirlenmesinden sonra olasılıkları ve bu senaryoların gerçekleşmesi durumunda oluşturacakları etkiye göre bir grafik üzerinde veya risk haritası üzerinden ifade edilmeleri BT felaket kurtarma planlarında önceliklerin

belirlenmesi kapsamında da yardımcı olacaktır. Senaryolara göre riskler, kabul edilebilir, izlenmesi ve yönetilmesi gereken veya en üst düzeyde risk yönetim planları uygulanması gerekenler olarak üç farklı grupta değerlendirilebilirler. Bu değerlendirmeler risk derecelendirme grafiğinde Şekil 1.1'de gösterilen şekilde konumlandırılabilirler. Buna ek olarak, bu konu hakkında Curtis ve arkadaşlarının pratikte risk değerlendirmesi başlıklı çalışmasında örnek ısı haritası üzerinde riskler ve etkileri gösterilmektedir (Curtis vd., 2012).



Şekil 1.1. Risk Derecelendirme Grafiği.

BT alanında, kurumların sundukları hizmetler, personel kabiliyetleri ve yeterlilikleri, maddi/manevi olanakları gibi faktörler, karşılaşabilecekleri riskleri belirlerken farklılık gösterebilir. Ancak, doğal afetler gibi bazı risk türleri, tüm kurumlar için yüksek düzeyde risk oluşturur ve bu nedenle en üst düzeyde risk yönetim planlarının uygulanmasını gerektirir (Özbilgin, 2012; TBD, 2006). Belirlenen BT riskleri, olasılık ve etki derecelerine göre grafiksel olarak ifade edildiğinde, bu risklerin hangi kategoride ele alınacağını belirlemeyi kolaylaştıracaktır. Şekil 1.2'de, bu tür bir risk değerlendirme grafiğine ilişkin örnek bir görsel sunulmaktadır.



Şekil 1.2. Örnek Risk Değerlendirme Grafiği.

Kurumlar, kuruluşlar veya organizasyonlar için BT alanında; personel, teknolojik altyapı, özel riskler, yasal yükümlülükler ve dış etkenlerden kaynaklanan risklere karşı önlem almak ve bu riskleri minimize etmek hayati önem taşımaktadır. Bu çerçevede, risk denetimleri, kuruluşların bu riskleri tespit etmek, değerlendirmek ve etkili bir şekilde yönetmek için başvurabilecekleri temel yöntemlerden biri olarak öne çıkmaktadır. Dünya genelinde bilgi teknolojileri kontrol hedefleri için COBIT (Control Objectives for Information and related Technology) belgeleri kullanılmaktadır (ISACA, 2024). Bu belgelerde belirlenen hedeflere göre, kurumlar iç ve dış bağımsız denetlemeler aracılığıyla riskleri kabul edilebilir seviyelere indirmeyi amaçlamaktadır.

1.2.3. Önceliklerin Belirlenmesi

Afetler ve diğer tehditler sırasında, kurumlar genellikle sınırlı kaynaklara sahiptir ve bu kaynaklara erişim zorluğu yaşanabilir. Ayrıca, belirlenen kaynaklar başka amaçlarla da kullanılabildiği için, önceliklerin belirlenmesinde zorluklar ortaya çıkabilir. Bu nedenle, BT felaket kurtarma planlarında kaynakların durumu göz önüne alınarak önceliklerin belirlenmesi büyük bir öneme sahiptir. BT felaket kurtarma planları, bir kurumun BT altyapısını kullanarak sunduğu hizmetleri ve iş süreçlerini felaket durumlarında tekrar çalışır hale getirmeyi amaçlayan bir yol haritası oluştururken,

öncelikli olarak hangi sistemlerin, donanımların ve süreçlerin kurtarılacağı veya restore edileceği belirlenmelidir. Bu süreç, önceliklerin belirlenmesi olarak tanımlanır. Bu kapsamda, afet anında müdahale ekibinin ilk etapta hangi sistem ve verileri kurtarması gerektiği ve felaket sonrasında hangi sistem ve hizmetlerin geri yüklenmesi gerektiği açıkça tanımlanmalıdır (Timms, 2018). Kurumların genel iş stratejileri ve işleyişleri doğrultusunda kullandıkları teknolojiler farklılık göstermektedir. Bu nedenle, her kurumda kritik öneme sahip BT hizmetleri değişiklik gösterebilir. Bu durum, veri kayıplarını da kurumdan kuruma farklılaştırmaktadır. Veri kayıplarının önlenmesi ve felaket sonrasında kurumun asli işlevlerini yerine getirebilmesi için gereken minimum BT sistemlerinin belirlenmesi büyük önem taşır. Bu bağlamda, kurtarma senaryolarında öncelikli olarak, kurumun faaliyetlerini sürdürebilmesi için gerekli olan BT altyapı ve hizmetlerinin korunmasına yönelik stratejiler geliştirilmelidir (Özdemir & Gökgöz, 2018). Kurumlar için öncelikler farklılık gösterebilse de, kritik iş süreçleri, veri hassasiyeti, süreçlerin kritikliği, dış paydaşlar, verilen hizmetlerin kamu hizmetini içerip içermediği, yasal ve düzenleyici gereksinimler ile kurtarma süreleri hedefleri, bir kurum için öncelik belirlemede etkili olan temel faktörlerdir. Bu unsurlar, kurumun iş sürekliliğini sağlamak için hangi süreçlerin ve hizmetlerin öncelikli olarak kurtarılması gerektiğini belirlerken, aynı zamanda kurumun hizmet vermeye devam edebilmesi için en kritik alanları tanımlar (TBD, 2009).

1.2.4. Altyapının Sağlanması

BT felaket kurtarma planı hazırlarken, hem teorik temellerin hem de pratik uygulamaların dikkate alınması ve altyapı planlamasına özen gösterilmesi gerekmektedir. Bu planların temelini oluşturan altyapılar, teorik açıdan risk yönetimi, iş sürekliliği planlaması ve bilgi güvenliği gibi kavramlar üzerine inşa edilmiştir. Pratik açıdan ise, planın uygulanması ve yürütülmesi önemlidir. Planın pratik kısmı, kritik sistemlerin ve verilerin yedeklenmesini, felaket durumunda yedeklerden hızla geri dönüş yaparak verilerin kurtarılmasını ve iş sürekliliğinin sağlanmasını içerir. Ayrıca, BT altyapılarında kullanılan donanımların, yazılımların ve veri tabanlarının yedeklenmesini; bu yedeklerin sık sık testler ve simülasyonlar yapılarak güncel tutulmasını kapsar. Pratik altyapı sadece donanım ve yazılım boyutuyla sınırlı kalmayıp, felaket anında veya öncesinde hizmet

verecek BT personelinin eğitimi ve felaket kurtarma konusundaki farkındalığını arttırmaya yönelik faaliyetleri de içermelidir (Aksu, 2011; Şahinaslan vd., 2009).

Kurumların, felaket öncesinde ve sonrasında hizmetlerini sürdürebilmeleri için yapacakları tüm çalışmalarda insan faktörü kritik bir öneme sahiptir. BT tabanlı hizmet sunan birçok kurum ve kuruluş için, özellikle BT personelinin ve tüm personelin eğitimlerinin eksiksiz ve güncel olması gerekmektedir. Bu eğitimler, iş sürekliliğini sağlamaya yönelik veya felaket kurtarma konusunda farkındalığı artırmaya yönelik faaliyetler olarak önem taşımaktadır. Bu süreçler, kurumların felaket anlarında ve sonrasında hizmetlerini kesintisiz bir şekilde devam ettirebilmeleri için hayati önem arz eder (Eren, 2013; Rothstein, 2007; Shropshire & Kadlec, 2009). Bu bağlamda, verilecek eğitim içeriğinde kurumun felaket kurtarma planı, acil durum protokolleri ve iletişim planları olmalıdır. Buna ek olarak, personeller felaket kurtarma sürecindeki rol ve sorumlulukları iyi bilmeli ve felaket durumunda kullanılacak teknik araçlar, yazılımlar ve donanımlar hakkında yeterli olmalıdırlar.

1.2.5. Verilerin Toplanması ve Planın Belgelendirilmesi

BT felaket kurtarma planlarının hazırlanması sürecinde, plana dahil edilebilecek tüm verilerin tek bir noktada toplanması ve bu verilerin ayrıntılı adımların oluşturulmasında kullanılması gerekmektedir. Veriler toplanırken iletişim bilgileri, kritik iş süreçleri, kritik kişiler ve felaket durumunda yapmaları gerekenler, varsa paydaşlar, altyapı bilgileri, felaket anında kullanılacak altyapılar ve çizimleri, felaket kurtarma merkezinin yapısal kablolaması, elektrik şebeke çizimleri, mekanik, inşaat, yangın söndürme sistemlerinin çizimlerine ait veriler öncelikli olarak dikkate alınmalıdır. BT felaket kurtarma planında kullanılacak tüm verilerin toplanması sürecinde, kritik BT varlıkları arasında yer alan donanımların kullanıcı kitapları, varsa eğitimlerine ait belgeler ve ileride oluşabilecek sorunlara dair iletişim bilgileri de bu kapsamda ele alınmalıdır. Bu verilerin eksiksiz ve güncel olması, planın etkin bir şekilde uygulanabilmesi için hayati öneme sahiptir (Akıllı, 2016; Kayrak, 2012).

1.2.6. Planın Test Edilmesi ve Gözden Geçirilmesi

Etkili bir planın hazırlanmasının ardından, hayata geçirilmeden önce test edilmesi kritik bir adımdır. Özellikle iş sürekliliği açısından büyük önem taşıyan felaket kurtarma planları, kurumların, kuruluşların veya organizasyonların iş faaliyetlerinin felaketler nedeniyle ciddi şekilde aksamasını engellemeye yönelik hazırlıklar olarak bilinir. Bu testler, planın etkinliğini ve uygulanabilirliğini değerlendirmek için gereklidir, böylece olası aksaklıklar ve zorluklar önceden tespit edilip giderilebilir. Bu sebeple, bir felaket kurtarma planının yalnızca tasarlanmış ve kurum tarafından onaylanmış olması yeterli değildir. Planın sürekli olarak gözden geçirilmesi, güncellenmesi ve periyodik testlerden geçirilmesi, olası zorluklara karşı etkinliğinin sağlanması açısından hayati önem taşır (Sawalha, 2020; Shuvo vd., 2022).

Risklerin belirlenmesi aşamasında oluşturulan senaryoların kurum personeli tarafından benimsenmesi ve olası eksikliklerin tespit edilmesi, test etme süreçlerinin önemli bir parçasıdır. Bu aşamada, acil durum tatbikatlarının düzenlenmesi, yedekleme sistemlerinin veri kurtarma kapasitelerinin değerlendirilmesi, geri dönüş sürelerinin yaklaşık olarak belirlenmesi, personelin felaket durumuna hazırlığının ölçülmesi ve felaket anında yapılacak işlemlerin öncelik sırasının doğru şekilde belirlenip belirlenmediğinin kontrol edilmesi gerekmektedir. Bu başlıkların titizlikle ele alınması, felaket kurtarma planının etkinliğini artırarak, kurumun felaketlere karşı daha hazırlıklı olmasını sağlayacaktır (Gregory, 2011).

Felaket öncesi kadar felaket sonrasının da doğru planlandığını doğrulamak, testler, tatbikatlar ve simülasyonlar gibi süreçlerle mümkündür. Bu bağlamda, sadece bu testler ve tatbikatlardan sonra değil, olası her felaket veya ciddi olaydan sonra da BT felaket kurtarma planının gözden geçirilmesi ve yeniden değerlendirilmesi gerekmektedir. Bu test süreçlerinde elde edilen kazanımlar, BT felaket kurtarma planının gerçek dünya senaryolarını ne kadar kapsadığını ve ne kadar gerçek hayat koşullarına uygun olduğunu göstermektedir. Ayrıca bu süreçler, planın gerçek hayat senaryolarına uygun olmayan kısımlarının düzeltilmesi için de fırsatlar sunmaktadır.

Gelişen teknolojilerin beraberinde getirdiği yeni riskler, BT felaket kurtarma planlarının güncel tutulmasının önemini artırmaktadır. Bu planlar, yeni tehditler ve teknolojik değişikliklere karşı kurumları hazırlıklı tutmak için sürekli olarak gözden

geçirilmeli ve gerektiğinde güncellenmelidir. Her yeni gelişme sonrası planın test edilmesi de önemli bir adımdır. BT felaket kurtarma planının test edilmesi aşağıdaki adımları içermelidir (Demirkasımoğlu, 2018; Drasgow vd., 2006; Mitts, 2005):

- Senaryo tabanlı tatbikatlar,
- Teknoloji testleri,
- Belge inceleme ve iletişim testleri,
- Simülasyon veya rol yapma ile gerçek hayata yakın testler yapılabilir.

Senaryo tabanlı testlerde, BT felaket kurtarma planına farklı felaket senaryoları uygulanarak planın uygulanabilirliği ve etkinliği kontrol edilir. Doğal afetler veya siber saldırılar gibi çeşitli durumlar senaryo tabanlı tatbikatlarda ele alınarak, süreç boyunca plana sadık kalınıp kalınmadığı izlenir. Tatbikat sonunda, eğer gerekli görülürse, plan üzerinde gerekli güncellemeler yapılır. Bu testler, kurumların felaket kurtarma sürecine hazırlıklı olmalarını sağlayarak, gerçek bir felaket durumunda hızlı ve etkili bir müdahale imkânı sunar.

Teknoloji testleri, genellikle iş sürekliliği açısından kritik öneme sahip sistemlerin ve teknolojilerin test edilmesiyle ilgilidir. Bu testler, veri yedekleme ve kurtarma sistemlerinin yanı sıra ağ güvenliği protokollerinin doğru uygulanıp uygulanmadığını kontrol eder. BT felaket kurtarma planları, senaryo tabanlı testlerle birlikte uygulanabilmektedir.

Simülasyon ve rol yapma ile BT felaket kurtarma planlarının hazırlık süreçleri test edilebileceği gibi, gerçek hayata mümkün olduğunca yakın simülasyonlar kurulup çalışanların farklı rollerde nasıl performans sergiledikleri ve planın işleyişi de test edilebilir. Bu test süreçleri, gerçek bir felaket durumunda nasıl davranılacağını anlamada en etkili yöntemlerden biridir.

Belge inceleme ve iletişim testleri, felaket durumunda kurum içi, birimler arası, paydaşlar veya hizmet verilenlerle iletişimin nasıl gerçekleşeceğini BT felaket kurtarma planında yazılı haline sadık kalarak test eder. Bu test türleri, acil durumda belgelere erişim unsurlarını, iletişim protokol ve prosedürlerini kapsar. Bu test süreçleri, BT felaket kurtarma planlarının gerçek dünya koşullarına ne kadar uyum sağladığını ve eksikliklerini

ortaya çıkararak düzeltme fırsatı sunar. Böylelikle kurumlar, felaket anlarında ve sonrasında daha etkili ve hızlı bir şekilde tepki verebilirler.

BT felaket kurtarma planlarının sürekli etkin ve geçerli olabilmesi için değişen iş gereksinimleri, teknolojik, çevresel ve ekonomik koşullar göz önünde bulundurularak güncellenmesi gerekmektedir. Planın her bir alt başlığı, zaman içinde düzenli olarak gözden geçirilmeli ve bütüncül bir değerlendirme süreciyle sürekli iyileştirilmelidir. Bu süreç, aşağıdaki adımlarla izlenebilir (Gregory, 2011; Snedaker & Rima, 2013):

- Değerlendirme ve Analiz: Bu aşamada, planın mevcut durumu değişen koşullar ışığında gözden geçirilir. İş süreçlerinde ve teknolojik altyapıda meydana gelen değişiklikler belirlenir. Yeni tehditler, riskler ve fırsatlar değerlendirilir.
- Güncelleme ve Revizyon: İş süreçlerindeki değişiklikler ve teknolojik gelişmeler doğrultusunda plan revize edilir. Yeni riskler ve tehditler göz önünde bulundurularak planın tüm unsurları yeniden yapılandırılır. Bu adım, planın güncellenmesi ve mevcut gereksinimlere uyum sağlanmasını kapsar.
- Eğitim ve Farkındalık: Güncellenmiş planın tüm personel ve paydaşlarla paylaşılması sağlanır. Eğitimler, yeni revizyonu anlamaları için ilgili personele verilir. Bu sayede çalışanlar, planın en güncel versiyonu hakkında bilgi sahibi olur ve felaket durumunda nasıl hareket etmeleri gerektiğini öğrenirler.
- Yeniden Test Etme: Güncellenmiş plan, çeşitli senaryolarla test edilerek doğrulanır. Bu adım, planın revizyonunun etkinliğini kontrol etmek ve olası eksikliklerin giderilmesini sağlamak için gereklidir.

Bu adımlar, BT felaket kurtarma planlarının sürekli iyileştirilmesini ve organizasyonun yeni koşullara uyum sağlamasını sağlar. Böylece, bu adımlara uyuldukça, kurumun herhangi bir felaket durumunda hızla toparlanabilme yeteneği artar. Bu sürekli iyileştirme süreci, planların etkinliğini artırarak organizasyonun felaketlere karşı daha dayanıklı hale gelmesini sağlar.

1.2.7. İş Birliği ve İletişim

Felaket durumlarında dayanışmanın önemi, günlük yaşamın ötesine geçerek daha kritik bir rol oynamaktadır. Her alanda gerekli olabilecek iş birliği, özellikle BT felaket kurtarma planı oluşturulurken de vazgeçilmezdir. Bu tür bir plan, genellikle tek bir birim

veya ekibin sorumluluğunun ötesine geçerek, çok sayıda paydaşı kapsayan bir yapı içerebilir. Bu nedenle, oluşturulacak planın, farklı departmanlar ve paydaşlar arasında etkili bir iletişimi ve iş birliğini teşvik etmesi gerekmektedir. Başarılı bir BT felaket kurtarma planı, felaket durumunda ekipler arasındaki rol ve sorumlulukları açıkça belirlerken, aynı zamanda iletişim kanallarını da net bir şekilde tanımlar. Felaket durumlarında en büyük sorunlardan biri de iletişimdir. BT felaket kurtarma planında, sorumluluklara göre ulaşılması gereken kişilerin alternatif iletişim bilgileri yer almalı ve bu iletişimin hangi kanallardan gerçekleştirileceği açık bir şekilde belirtilmelidir. BT felaket planına dahil olan ekip üyeleri arasında etkili iletişim ve iş birliği sağlanmalı; herkesin rolü ve sorumlulukları plan içinde açık ve anlaşılır şekilde tanımlanmalıdır. İş birliği ve iletişimde deneyimlerin önemi de göz ardı edilmemelidir. Bu bağlamda, daha önce BT felaket planı hazırlamış kişilerle veya konunun uzmanlarıyla iletişim kurmak büyük önem taşır. Felaket kurtarma planlarından elde edilen deneyimler, yeni planların oluşturulması ve mevcut planların iyileştirilmesinde önemli bir rol oynar. Geçmiş planlardan elde edilen deneyimlerin paylaşılması, benzer felaketlerle karşılaşıldığında uygun tepkilerin ve çözümlerin belirlenmesine yardımcı olabilir. Buna ek olarak, geçmişteki hatalardan ders çıkarılarak planların revize edilmesi sürecinde deneyimli kişilerle iletişim halinde olmak, BT felaket planının daha etkili bir şekilde oluşturulmasını sağlar. Bu tür bir yaklaşım, planın gerçek hayatta karşılaşılabilecek senaryolara daha uygun hale getirilmesine katkıda bulunur.

1.3. BT FELAKET KURTARMA PLANI VE İŞ SÜREKLİLİĞİ PLANI KAVRAMALARININ DOĞRU TANIMLANMASI

Felaketler meydana geldiğinde, kurumlar veya kuruluşlar, verdikleri hizmetleri kesintisiz bir şekilde sürdürebilmek için, öncelikli olarak kritik öneme sahip olan hizmetleri aksatmadan devam ettirmeye çalışır. Olası bir hizmet kesintisi durumunda ise, kesilen hizmetleri en kısa sürede yeniden sağlamak amacıyla kurtarma eylemleri devreye sokulur. Bir organizasyon için, iş süreçlerini, verilen hizmetleri veya üretimi olumsuz şekilde etkileyen, önceden belirlenmiş ya da belirlenemeyen çeşitli nedenlerden kaynaklanan olaylar, iş kesintisi olarak tanımlanır (İzmirli, 2023). Bu kapsamda, iş sürekliliği, bir kurum, kuruluş, organizasyon veya işletmenin, iş kesintisi yaşamadan veya felaket sonrasında temel işlevlerinin, mümkün olan en kısa sürede çalışır durumda

kalmasını ve normale dönmesini amaçlayan süreçtir (Gazdağı & Çetinyokuş, 2020). Buna ek olarak, iş sürekliliği, bir kuruluşun yaşanılacak herhangi bir felaket sırasında, sınırlı bir kapasiteyle de olsa hizmetlerini devam ettirmesine olanak tanır. Bu şekilde aksama süreleri engellenebilir veya tamamen durma riski ortadan kaldırılabilir (Niemimaa vd., 2019). İş sürekliliği tanımlarına dayanarak, bir kurum, organizasyon veya işletme için olası bir felaket durumunda veya rutin işleyişte devreye girecek iş, işlem dizisi veya eylemler bütününe iş sürekliliği planı denir (Kılıç, 2019). Bu planda, kritik hizmetlerin olası bir felaket durumunda durmaması ya da felaketten etkilenmemesi için gerekli eylem ve çalışmalar yer almalıdır. Ayrıca, plan uygulamaya konulduğunda, kritik hizmetlerin felaket durumlarında mümkün olan en az zararla süreci atlatmaları amaçlanmalıdır. İş sürekliliği planları hazırlanırken, yalnızca felaket anı dikkate alınmamalı, aynı zamanda kurum, kuruluş, işletme veya organizasyonların normal işleyişlerinin ve süreklilik süreçlerinin de belirlenmesi gerekmektedir.

BT felaket kurtarma planı, iş sürekliliği planı içerisinde yer alacak bir alt başlık olabilir. BT felaket kurtarma planı, birçok kurumda iş sürekliliği planlarının bir parçasıdır ve genellikle felaket anında ve sonrasında kurumun önceden belirlediği kritik hizmetler başta olmak üzere; BT hizmetlerini yeniden başlatmayı hedefleyen plan türüdür. Tüm BT hizmetlerinin felaket kurtarma planlarına dahil edilmesi, bazı durumlarda ekonomik kısıtlamalar veya kaygılar nedeniyle mümkün olmayabilir. Bu gibi durumlarda, kritik öneme sahip BT hizmetleri önceden belirlenmeli ve felaket kurtarma planlarında, bu hizmetlerin iş sürekliliği planlarının amaç ve hedefleriyle çelişmemesi sağlanmalıdır. İş sürekliliği planları, BT felaket kurtarma planlarını kapsayan bir yapıya sahip olmalı, aynı zamanda BT felaket kurtarma planları da iş sürekliliği planlarını destekleyecek şekilde hazırlanmalıdır (Akıllı, 2016). BT felaket kurtarma planı, olay odaklı, reaktif yaklaşımı benimser, genellikle doğal afetler, siber saldırılar veya donanım arızaları gibi spesifik olayların ardından harekete geçen belirli bir plan ve müdahale süreçlerini içerir.

İş sürekliliği, kurum için stratejik bir yaklaşımı ifade ederken, BT felaket kurtarma planı daha çok reaktif bir süreçtir ve acil duruma odaklıdır. Kurumlar, kuruluşlar veya organizasyonlar genellikle her iki kavramı da kapsayan kapsamlı bir plan geliştirir ve uygular. İş sürekliliği ve BT felaket kurtarma planları arasındaki ilişki şu şekilde özetlenebilir:

- İş sürekliliği planları, kurumların öncelikli olarak kritik öneme sahip iş süreçlerini belirler ve bu süreçlerin olası bir felaket ya da olağanüstü durumda nasıl sürdürüleceğini tanımlar.
- BT felaket kurtarma planları, özellikle kurumların kritik BT sistemlerinin ve bu sistemleri çalıştıran altyapının felaket durumlarında en hızlı ve etkili biçimde nasıl kurtarılacağını belirler.
- İş sürekliliği ve BT felaket kurtarma planları, birbirini tamamlayan bir yapıya sahiptir. Kurumların iş süreçlerinin çoğu, BT sistemlerine bağımlı ya da tamamen bu sistemler üzerinde hizmet verir. Bu nedenle, BT felaket kurtarma planları iş sürekliliği hedeflerinin gerçekleştirilmesinde kritik bir rol oynar.
- İş sürekliliği ve BT felaket kurtarma planlarının her ikisi de kurumların felaket durumlarında hızla başta BT hizmetlerini başlatarak toparlanmalarını ve normal iş faaliyetlerine dönmelerini amaçlar. Birlikte, kurumların sürekliliğini, uzun vadeli dayanıklılığını ve rekabet gücünü artırır.

1.4. BT FELAKET KURTARMA PLANI

BT felaket kurtarma planının, felaketlerin ardından uygulanabilmesi, daha karmaşık operasyonların en az kayıpla ve yeniden hizmet verecek şekilde gerçekleştirilmesine olanak tanır. Bu süreçte, farklı ekiplerin veya birden fazla paydaşın koordinasyonu sağlanarak kurum, kuruluş veya organizasyon için operasyonel kolaylık sağlanır. Bir felaketin ne zaman gerçekleşeceği ya da hangi türde olacağının öngörülemez olduğu gerçeği göz önünde bulundurulduğunda, BT operasyonlarının kurtarılmasının karmaşıklığı ve sistemlerin en az hasarla, en hızlı şekilde geri yüklenebilmesi için önceden planlama yapmanın önemi bir kez daha vurgulanmaktadır. Felaketlere hazırlıklı olmak, organizasyonların kesintisiz hizmet sunma kapasitesini artırırken, aynı zamanda olası zararlara karşı daha dirençli olmalarını sağlar. BT felaket kurtarma planına sahip olmak, felaketin maddi hasarlarını tahmin etmek, süreç içerisinde verilemeyen hizmetlerden doğacak maddi kayıpların yaklaşık olarak hesaplanması gibi faydalar sağlamaktadır. BT felaket kurtarmanın bir başka faydası, felaket sonrasında BT hizmetlerinde yaşanılacak olası bir kesintinin hemen ardından, personellerin mümkün olan en kısa süre içerisinde felaket öncesindeki normal sorumluluklarına dönebilmesini sağlamaya yardımcı olmasıdır (Wood vd., 2010).

Felaket durumlarına hazırlık sürecinde planlama yapmak ve düzenli testler gerçekleştirmek, kullanıcı deneyimlerinden ve uzman görüşlerinden faydalanmak kritik bir öneme sahiptir. Felaket sonrasında ise önceden belirlenmiş adımların içinde bulunulan duruma en uygun ve en etkili şekilde hızlıca uygulanması gerekmektedir. Buna ek olarak, BT felaket kurtarma planını uygulayacak personelin veya hizmet alınan paydaşların, felaketin psikolojik etkilerinden en az düzeyde etkilenerek planı uygulayabilmesi, başarılı bir BT felaket kurtarma planının hayata geçirilmesinde önemli bir unsurdur.

Sürekli güncellenen ve iyileştirilen bir plan, kurumların felaket durumlarına karşı hazırlıklı olmasını sağlayarak olası zararları en aza indirir. Başarılı bir felaket kurtarma planının temel bileşenleri, literatürde şu şekilde tanımlanmıştır (Fallara, 2004; Gregory, 2011; Snedaker & Rima, 2013):

- Risk değerlendirmesi ve planlamanın yapılması,
- Yedekleme ve kurtarma stratejilerinin doğru bir şekilde belirlenmesi,
- Test, tatbikat ve sürekli iyileştirme süreçlerinin gerçekleştirilmesi ve takip edilmesi,
- İş birliği ve iletişim süreçlerinin prosedürel olarak ele alınması,
- İş sürekliliği yönetiminin planlama basamağıyla uyumlu olması.

BT felaket kurtarma planlaması, kurum, kuruluş veya organizasyonların mevcut envanterlerini tanımalarına, personelin felaket durumlarına hazırlık düzeylerini artırmalarına ve plan oluşturma süreçlerinde yetkinlik kazanmalarına olanak tanır. Aynı zamanda, felaket anında iş sürekliliğini sağlamak için de kritik bir role sahiptir. Risk değerlendirmesi, yedekleme ve kurtarma stratejileri, düzenli testler ve iş birliği gibi süreçler, başarılı bir felaket kurtarma planının temel bileşenlerini oluşturmaktadır.

1.4.1. BT Felaket Kurtarma Planı Seviyeleri

Bir kurum için BT altyapısının felaket anında ve sonrasında hizmet verme kalitesi önemli bir kriterdir. Bu kriter, felaket sonrası BT altyapısının ne kadar sürede ve hangi kaynaklarla kurtarılabileceğini belirleyen bir derecelendirme sistemini içermelidir. Bu tür bir derecelendirme, genellikle kurumun faaliyet gösterdiği alanlar, paydaşlar, iş gereksinimleri ve risk toleransı gibi faktörlere dayanarak belirlenir. Bu doğrultuda, felaket kurtarma planları genellikle yüksek, orta, düşük ve çok düşük olmak üzere farklı

seviyelerde kategorize edilebilir. Çeşitli çalışmalar, felaket kurtarma süreçlerini farklı seviyelerle ifade ederek, her seviyenin ihtiyaç duyduğu kaynakları ve süreyi belirler. Özdemir ve Gökgöz'e göre geleneksel felaket kurtarma seviyeleri altı gruba ayrılmıştır (Özdemir & Gökgöz, 2018). Buna ek olarak, bir diğer BT felaket kurtarma seviyelendirme türü olarak Uptime Institute'ın belirlediği *"Tier"* kategorizasyonu kullanılmaktadır. Bu kategorizasyona göre dört seviye bulunmaktadır.

Yüksek seviye veya Tier-4 kategorisi, BT felaket kurtarma planları, kritik iş süreçlerinin kesintisiz bir şekilde devam etmesi gereken organizasyonlar, kurumlar veya kuruluşlar için geçerli olan planlardır. Bu düzeyde, veri koruma yöntemleri en yüksek seviyede uygulanarak, sürekli çalışabilme ve otomatik kurtarma imkânı sunulur. Birden çok ikincil veri merkezi veya yedekleme tesisi üzerinde hizmet vermeyi hedefleyen kurumlar, bu plan türünü kullanarak çok katmanlı bir koruma sağlamaktadır. Bu koruma, çoklu güç kaynakları ve ağ bağlantıları gibi unsurlarla desteklenir. Finans kuruluşları ve sağlık hizmetleri sağlayıcıları gibi organizasyonlar, Tier-4 planlarını kullanan kurumlara örnek olarak gösterilebilir. Bu seviyede, olası bir felaket sonrasında sistem, veri tabanı, ağ ve hizmetlerin kurtarılması genellikle yüksek otomasyon desteğiyle yapılır ve kurtarma süreci birkaç saat içinde ya da bir gün içinde tamamlanır (Arno vd., 2010; Turner IV vd., 2006).

Orta seviye veya Tier-3 kategorisi, BT felaket kurtarma planları, BT sistemleri üzerinden hizmet veren iş süreçlerinin kısa süreli kesintilere toleranslı olan kurum, kuruluş veya organizasyonlar için uygun bir çözümdür. Bu seviyede, felaket durumunda hizmetlerin hızlı bir şekilde geri yüklenmesi hedeflenir, ancak kesinti süresinin uzaması kabul edilebilir bir düzeyde kalabilir. Bu tür organizasyonlar, felaketten sonra iş sürekliliğini sağlamak için genellikle belirli bir süreye kadar veri kaybını tolere edebilir ve yedekleme çözümleri ile bu kaybı minimize etmeyi hedefler. Üretim endüstrisi gibi bazı sektörler, bu tür planları tercih edebilir. Bu seviyedeki planlarda veri koruma metodunun, otomatik kurtarma yeteneklerine sahip olması gerekmektedir. Bu sayede felaket sonrası kurtarma süreleri kısaltılabilir. Veri çeşitliliği açısından, bu planlar, konsantrasyonlu yedekleme ve kurtarma sistemleri ile donatılmış ikincil veri merkezi veya yedekleme tesislerine sahiptir ve kritik sistemler ile veriler yüksek seviyede korunur. Olası bir felaket sonrasında, sistem, veri tabanı, ağ ve hizmetlerin herhangi birinin

kurtarılması genellikle bir gün içinde tamamlanır ve manuel müdahale gerektirmez (Arno vd., 2010; Turner vd., 2006).

Düşük seviye veya Tier-2 kategorisi BT felaket kurtarma planları, BT sistemleri üzerinden hizmet veren, iş süreçlerinin bir haftaya kadar kesintiye tahammül edilebileceği kurum, kuruluş veya organizasyonlar için uygun türüdür. Bu tür planlar, küçük ölçekli kamu iştirakleri, işletmeler gibi örneklerde kullanılabilir. Bu seviyedeki planlarda, veri tabanları, sunucu hizmetleri veya ağ hizmetlerinin kurtarma süreleri genellikle birkaç gün ile bir hafta arasında değişir ve manuel müdahale daha yaygın bir şekilde kullanılır. Veri koruma metodları, mevcut yedekleme ve kurtarma sistemleri üzerinden gerçekleştirilirken, tam otomatik kurtarma sağlanamaz. Ayrıca, veri çeşitliliği açısından, ikincil veri merkezi veya yedekleme tesisleri gibi bazı yedeklilik seviyeleri oluşturulsa da, kurtarma sürecinde hala belirli bir manuel müdahale gerekmektedir. Bu tür planlar, daha düşük seviyedeki koruma ve kurtarma ihtiyaçlarını karşılamak için tasarlanmıştır (Arno vd., 2010; Turner vd., 2006).

Çok düşük seviye veya Tier-1 kategorisi BT felaket kurtarma planları, BT sistemleri üzerinden hizmet veren, iş süreçlerinin uzun süreli kesintilere toleransı olan kurum, kuruluş veya organizasyonlar için geçerli olan türleridir ve genellikle bazı araştırma laboratuvarları gibi özel durumlar için uygun görülen planlardır. Bu seviyede, veri tabanları, sunucu hizmetleri veya ağ hizmetlerinin kurtarma süresi genellikle bir haftadan daha uzun sürebilir ve süreç genellikle manuel müdahale gerektirir. Veri koruma metodu, temel bir koruma seviyesinde uygulanır; veriler korunmakta olsa da, kurtarma süreci uzun zaman alabilir veya tamamen manuel olarak gerçekleştirilir. Veri çeşitliliği açısından, düzenli yedeklemeler yapılsa da, yedekleme ve kurtarma işlemleri genellikle sınırlıdır ve kurtarma süreci uzun süreler alabilir veya kısıtlı bir şekilde tamamlanabilir. Bu tür planlar, kritik olmayan sistemlerin kurtarılması için tasarlanmış, daha düşük seviyede koruma sağlayan stratejilerdir (Arno vd., 2010; Turner vd., 2006).

1.4.2. BT Felaket Kurtarma Planı Türleri

Kamu kurumları dahil olmak üzere, BT altyapısının sürekli erişilebilirliği, felaket anında hazırlıklı olması, güvenilirliği ve felaket sonrası en kısa sürede tekrar hizmet verebilir olması, günlük yaşantımızda kritik bir öneme sahiptir. Bu nedenle, BT felaket

kurtarma planlarının doğal afetler, siber saldırılar, donanım arızaları veya insan hataları gibi beklenmedik olaylar dikkate alınarak doğru şekilde planlanması gerekmektedir. Aksi takdirde, kurumlar için meydana gelebilecek felaketler, iş sürekliliği ve veri bütünlüğü açısından ciddi tehditler oluşturabilir (Yurt & Şentürk, 2022). Bu nedenle, bir organizasyonun BT felaket kurtarma planı, sunucu ve ağ sistemlerinin kurtarılması stratejilerini, yedekleme ve yedekten geri dönme planlarını, risk ve öncelik değerlendirmelerini ve felaket halinde gerekli iletişimi sağlayacak iletişim prosedürlerini içermelidir.

1.4.2.1. Ağ Kurtarma Planı

BT kullanımının artması, dijitalleşmenin yaygınlaşması kurumların ağ kullanımını arttırmış ve ağ altyapılarının bağımlılığını sağlamıştır. Kurumların BT tabanlı hizmetlerini kesintisiz bir şekilde yerine getirmeleri için yüksek oranda ağ altyapılarını kullanmaları da ağ altyapılarının önemli olduğunu göstermektedir. Buna ek olarak, felaket durumlarında ağ kurtarma planları, kurumların hizmetlerini veya operasyonlarını sürdürmesini ve hizmet sundukları paydaşlarına kesintisiz hizmet sunmasını sağlamak için hayati bir rol oynamaktadır. Bu bağlamda, ağ kurtarma planlarının önemli unsurlarından biri, ağ altyapısının olası bir felaket sonrasında, hızlı bir şekilde geri yüklenmesi gereken BT altyapısı, kesintisiz hizmetin sağlanabilmesi açısından büyük önem taşır. Ayrıca, veri kurtarma süreçlerinde ağ altyapısına da ihtiyaç duyulabilir. Bu nedenle, ağ kurtarma planları kapsamında veri yedekleme ve geri yükleme stratejileri büyük bir öneme sahiptir. Ağ kurtarma planlarının bir diğer kritik unsuru, kurum personelinin, felaket anında ve sonrasında ağ altyapısının nasıl kullanılacağı, nasıl kurtarılacağı konusunda eğitim alması ve bu konuda farkındalığının yüksek olmasıdır. Personellerin, felaket durumlarında doğru tepkiyi verebilmeleri ve ağ altyapısını etkili bir şekilde yeniden çalışır hâle getirebilmeleri için gerekli yetkinliklere sahip olmaları ve doğru planlama yapılması gerekmektedir (Bradley, 2017). Olası bir felaket durumunda ağ kurtarma süreci, kurumlar için hızlı ve etkili bir şekilde hareket etmeyi gerektirir. Bu nedenle, önceden hazırlık ve planlama, ağ kurtarma süreçleri için büyük önem taşır. Ağ kurtarma planları, ağ altyapısının felaket öncesinde sahip olduğu ve felaket sonrasında kurtarılacak veya kurulacak yeni ağın topolojik haritasını, dokümantasyonunu, ağ cihazlarının yapılandırma dosyalarını da içermelidir. Buna ek olarak, ölçeklenebilir ve

elastik, yedekli, yüksek erişilebilirliğe sahip ağ mimarisi tasarımı, ağ altyapısının dayanıklılığı için önem arz etmektedir. Bu bağlamda, gerçek zamanlı yedeklilik sağlayan ve arıza durumunda yük devreden, coğrafi yük dengeleme ve trafik yönetimi yapabilen, uygun görülmesi halinde bulut tabanlı yedeklenmiş hizmet sunan ağ altyapıları, BT felaket kurtarma planlarında ele alınması gereken başlıklardır. Ayrıca, dinamik kurtarma süreçlerinde yazılım tanımlı ağ (Software Defined Network - SDN) gibi yükselen ağ teknolojilerinden de ağ kurtarma planlarında faydalanılmaktadır. Bu teknolojiler, ağ altyapısının daha esnek bir şekilde yönetilmesini ve hızlı bir şekilde adapte olmasını sağlayarak, felaket durumlarında daha etkin ve verimli bir kurtarma süreci sunmaktadır. SDN, ağ kaynaklarının merkezi olarak kontrol edilmesini mümkün kılarak, ağ yapılandırmalarının hızlı bir şekilde değiştirilmesine ve ağ hatalarına karşı daha hızlı tepki verilmesine olanak tanır (Volvach & Globa, 2016).

Gerçek zamanlı yedeklilik ve yedek ağ cihazlarının kullanımı, kurumsal ağlarda ağ kurtarma planları çerçevesinde yaygın olarak tercih edilen etkili bir yaklaşımdır. Bu strateji ile halihazırda hizmet veren ağ bileşenlerinin yedekleri, çalışır durumda ve hizmete hazır bir şekilde bekler. Ana cihazlarda meydana gelen bir arıza veya felaket durumunda, bu yedekler otomatik olarak devreye girer, böylece kesinti yaşanmaz veya kesinti süresi en aza indirilir. Bu durum, iş sürekliliğinin sağlanmasına da önemli ölçüde katkı sağlar.

Gang ve arkadaşları, yaptıkları çalışmada özellikle endüstriyel alanda hizmet veren Ethernet tabanlı ağlarda, gerçek zamanlı yedekleme sistemlerinin, ağ arızalarında sistemin gecikmeden diğer ağa geçiş yapabilmesi ve ağ güvenilirliğini büyük ölçüde artırması nedeniyle önemli olduğunu sonucuna varmışlardır (Gang vd., 2023). Bu tür yedekleme sistemleri, ağın kesintisiz çalışmasını sağlarken, ağ altyapısının güvenliğini ve sürekliliğini de büyük ölçüde iyileştirmektedir.

Doğal afetler gibi felaket durumlarında, özellikle coğrafi olarak kurtarmanın aynı yerleşkelerde yapılamaması durumu söz konusu olabilir. Bu bağlamda, felaket öncesi ve sonrası sunulan hizmetlerin ağ yüklerinin dağıtılması ve trafik yönetimi amacıyla farklı coğrafyalarda ağ trafiği yük dengeleme ve trafik yönetimi kullanımı, kurumların tercih edebileceği etkili ağ kurtarma stratejilerinden biridir. Bu stratejiye göre, felaket durumunda ağ trafiği otomatik olarak diğer coğrafi lokasyonlara yönlendirilir ve böylece

hizmet kesintisi en aza indirilir. Ancak, bu strateji bazı kurumlar için yüksek maliyetler doğurabilir. Bu nedenle, kurumların bütçe ve ihtiyaçlarına göre bu stratejiyi değerlendirmeleri gerekmektedir. Bu yaklaşım, iş sürekliliğini sağlama ve hizmet kesintilerini minimize etme açısından önemli bir rol oynamaktadır. (Badotra vd., 2023).

1.4.2.2. Sunucu Sistemlerini Kurtarma ve Sanallaştırma Planı

Sunucular, kurumlar, işletmeler veya organizasyonlarda kullanılan, kendilerinden hizmet alan istemcilere hizmet veren gelişmiş sistemlerdir (Lewis, 1995). Günümüzde birçok kurumun BT hizmetleri, özellikle web tabanlı olup, sunucular aracılığıyla istemci-sunucu modeli kullanılarak sunulmaktadır (Zhang, 2013).

Kurumların BT sistemlerinde iş sürekliliğini sağlamak ve operasyonel risklerini minimize etmek için uyguladıkları stratejilerden biri, sunucu sistemlerinin etkin bir şekilde kurtarılmasıdır. Bu amaçla çeşitli yöntemler, metotlar ve teknolojiler kullanılmaktadır. İçinde bulunduğumuz teknoloji dünyasında, kurumlar iş sürekliliğini sağlamak ve yüksek erişilebilirlik elde etmek için sunucu altyapılarını, olası felaketlere karşı korumak amacıyla kümeleme (clustering) yöntemini tercih etmektedirler (Kulaklı & Aslan, 2010). Bu kapsamda, sanallaştırma teknolojileri ve yedekleme teknolojilerinden yüksek oranda faydalanılmakta ve bilişim alt yapıları bu bağlamda yenilenmektedir (İnce vd., 2020). Sanallaştırma platformları, özellikle sunucu sanallaştırma, kurumların BT altyapılarını fiziksel sunucu kaynaklarını paylaştırarak sanallaştırma yazılımı katmanı (hyper-visor) ile soyutlamasını ve sanal makineler üzerinde çalıştırılmasını sağlar. Bu teknoloji, fiziksel sunucuların yerine geçerek kurumların günlük BT işlerinde ve felaket kurtarma süreçlerinde esnek bir yapı sunar. Sanallaştırma, kurumların BT kaynaklarını daha verimli kullanmalarına ve fiziksel donanım bağımlılığını azaltmalarına yardımcı olurken, aynı zamanda felaket durumlarında hızlı ve etkili çözümler sunma yeteneği kazandırır (Akıllı, 2016). Sunucu sanallaştırması haricinde, masaüstü sanallaştırma, uygulama sanallaştırma ve ağ sanallaştırması gibi farklı türden sanallaştırma teknolojileri de yaygın olarak kullanılmaktadır (Bhardwaj & Krishna, 2021). Sunucu sanallaştırmanın, kurumlar için sağladığı önemli avantajlardan birisi, olası bir felaket anında ve sonrasında BT hizmetlerinin barındırıldığı sunucuların kurtarılması süreçlerinde esneklik ve hız sunmasıdır. Felaket sonrasında, kaset ünitelerinden veya soğuk yedek olarak farklı yerleşkelerde saklanan fiziksel sunuculardan, kurtarma yapmak gibi geleneksel sunucu

kurtarma yöntemleri genellikle kuruluşların hizmetlerini eskisi gibi sürdürebilmeleri için uzun süreler alırken, sanallaştırma platformlarının kullanılması sayesinde başta kritik sistemler olmak üzere kurumun tüm BT sistemlerini hızlı bir şekilde kurtarılması mümkün olmaktadır (Bruzzese, 2009). Sunucu sanallaştırmasının ölçeklenebilirliği, sanal sunucularda kullanılan kaynakların ihtiyaç halinde sunucunun kapatılmasına gerek kalmadan arttırılabilmesi ve kullanım oranlarının azalması halinde de düşürülebilmesi olanaklarını sunmaktadır (Rashid & Chaturvedi, 2019). Bunun yanı sıra, sunucu sanallaştırmasının, BT hizmeti veren sunucuların yedeklenmesi ve kurtarılması süreçlerini otomatikleştirme olanağı sunması da olumlu özelliklerinden biridir. Otomatik yedekleme ve kurtarma işlemleri sayesinde, felaket anında ve sonrasında insan müdahalesine ihtiyaç duyulmadan BT sistemlerinin kurtarılması ve tekrar devreye alınıp işletilmesi sağlanabilir. Bu sayede, insan kaynaklı hataların en aza indirilmesi ve kurtarma süreçlerinin daha güvenilir hale gelmesi sağlanır (Adeshiyan vd., 2009). Ancak, sunucu sanallaştırma platformlarının da felaket durumlarında etkilenebileceği göz önünde bulundurulmalıdır. Bu nedenle, kurumların bu platformları farklı yerleşkelerde yedekli bir şekilde kurmaları ve düzenli olarak test etmeleri gerekmektedir. Ayrıca, BT felaket kurtarma planlarında yapılacak güncellemelerde, bu platformların karmaşık yapıları nedeniyle revizyon ihtiyaçları da dikkate alınmalıdır.

Sonuç olarak, BT felaket kurtarma planlarında sunucu sanallaştırmasının kullanımı, sunucu kurtarma süreçlerinin önemini giderek artırmaktadır. Sunucu sanallaştırma ve diğer sanallaştırma platformları, kurumlar, kuruluşlar veya organizasyonlar için BT tabanlı operasyonların kesintilerini en aza indirmek ve iş sürekliliğini sağlamak adına önemli unsurlardır. Bununla birlikte, bu teknolojilerin etkin kullanımı için yeterli personel temini, ayrıntılı planlama, plana sadık kalınması, mali esneklik, yedekleme stratejileri ve sürekli iyileştirme prosedürlerinin benimsenmesi gerekmektedir. Bu bağlamda, potansiyel risklerin doğru şekilde belirlenmesi, sahip olunan tüm sunucu envanterinin ve bu sunucuların kritiklik seviyelerinin doğru bir biçimde tespit edilmesi önemlidir. Envanterin oluşturulmasının ardından sunucuların düzenli olarak yedeklenmesi, yedekleme planlarının oluşturulması ve gerektiğinde güncellenmesi gereklidir. Yedekleme alanlarının depolama ihtiyaçlarının doğru şekilde planlanması ve izlenmesi, olası bir felakette sunucuların nereden ve ne zaman kurtarılacağını belirleyen kurtarma noktalarının tespiti açısından kritik öneme sahiptir. Ayrıca, sunucu kurtarma

süreçlerinde insan faktörünün azaltılması ve süreçlerin mümkün olduğunca otomatize edilmesi gerekmektedir. Felaket durumunda, personelin çeşitli senaryolara nasıl tepki vereceği ve hangi iletişim kanallarını nasıl kullanacağı belirlenmeli; bu doğrultuda etkili bir eğitim ve iletişim planı uygulanmalıdır. Düzenli tatbikatlar, testler ve revizyon süreçlerinin uygulanması, elde edilen sonuçlar doğrultusunda BT felaket kurtarma planının sürekli olarak iyileştirilmesi ve güncellenmesi gerekmektedir.

1.4.2.3. Felaket Kurtarma Merkezi Planı

BT altyapısının temel bileşenlerinden biri olan veri merkezleri, günümüzde kurumların yürütmekte oldukları hizmetlerin veya faaliyetlerin teknoloji temelli bir biçimde sağlıklı ve etkili yürütülmesinde kritik bir öneme sahiptir. Veri merkezleri, içerisinde sunucuları, ağ altyapısını, depolama sistemlerini ve yedekleme ünitelerini barındıran BT hizmetleri sağlamak için özel olarak tasarlanmış alanlardır (Gökmen & Küçüksille, 2013). Veri merkezleri, büyük ölçüde veri depolama, verileri işleme ve verilerin iletimi işlevlerini yerine getiren, aynı zamanda bir kurumun iş sürekliliği ve felaket kurtarma stratejilerinin merkezinde de yer alabilen tesislerdir. Kurumların, dijital varlıklarını çoğunlukla veri merkezlerinde barındırmaları bu merkezlerin önemini bir derece daha arttırmaktadır (Crosby & Curtis, 2021). Felaket kurtarma merkezi (FKM), ana veri merkezinin yedeği veya ayrı bir veri merkezi iken içerisinde felaket durumunda ya da sürekli olarak çalışacak ayrı donanım ve yazılımları bulunan, kurumların felaket durumlarına karşı hazırlıklı olmalarını sağlayacak, iş sürekliliğini yerine getirmek için kullanılabilecek özel tasarlanmış tesislerdir (Dhanujati & Girsang, 2018). Bir başka tanıma göre FKM, kurumların olası bir felaket yaşamaları halinde sunmakta oldukları BT hizmetlerinin en az kayıp ile tekrar aktif bir şekilde hizmet verebilir hale getirmeleri için hazırlanmış merkezlerdir (TÜBİTAK, 2017a). Felaket kurtarma merkezleri, kurumların olası felaket senaryolarına karşı hazırlıklı olmaları konusunda önem arz etmektedirler. Ayrıca bulut tabanlı veya yerleşik bir felaket kurtarma merkezlerinin kurumlar açısından başlıca işlevleri şu şekildedir (Gabriel, 2015; Wood vd., 2010):

- Yedekleme ve kurtarma planları açısından ana veri merkezindeki başta kritik verilerin periyodik olarak saklanabileceği yerlerdir. Olası bir felaket sonrasında bu yedeklerden geri dönüşler sağlanabilir.

- Alternatif çalışma olanağı sağlaması, FKM'ler, ana veri merkezinde yapılacak planlı ve plansız çalışmalarda veya felaket durumlarında kurumun faaliyetlerini sürdürebilmesi için alternatif bir lokasyon olacaktır.
- Test ve simülasyon süreçlerinde; kurtarma planının etkinliğini, kurumun mevcut işleyişini bozmadan değerlendirme imkânı sunarlar.
- Veri güvenliği ve ölçeklenebilirlik açısından kurumun ihtiyaçları doğrultusunda esneklik sağlarlar.

Felaket kurtarma merkezlerini veri merkezlerinden ayıran başlıca unsurlar bulunmaktadır. Veri merkezleri temel işlev ve amaç bakımından büyük miktardaki verileri saklamak, işlemek ve dağıtmakla ilgilenirken; FKM'ler bir kurum veya işletmenin BT operasyonlarının olası felaket durumuna karşı dirençli olmasını amaçlamaktadır. Kullanım senaryosu olarak veri merkezleri, genellikle günlük BT operasyonlarıyla ilgilenirken, FKM'ler, genellikle felaket anında devreye girerek BT hizmetlerini devam ettirmek için tasarlanırlar. Bu durum, kullanım yoğunluğu konusunda da FKM'lerin, çoğu zaman boşta bekleyen sistemler olmasıyla sonuçlanmaktadır. Sonuç olarak, veri merkezleri, BT faaliyetlerinde kullanılan veri yönetimini bir kurum için temel alt yapı olarak sağlarken, FKM'ler, başta iş sürekliliğini sağlamak ve felaket durumlarında kurumların en az kayıpla en hızlı şekilde BT hizmetlerini tekrar verebilmeleri için bir altyapı sunmayı amaçlarlar. Başta kritik altyapı hizmeti sunan kurumlar olmak üzere üniversiteler, hastaneler ve kamu iştirakleri gibi kuruluşlar, genellikle hem veri merkezine hem de FKM'ye ihtiyaç duymaktadır. Bu merkezler, BT tabanlı günlük operasyonların kesintisiz bir şekilde yönetilmesini sağlarken, aynı zamanda olası felaket durumlarına karşı hazırlıklı olunmasını mümkün kılar. Bu bağlamda, bulut tabanlı veya yerleşik FKM çözümlerinin kullanımı, hem esneklik hem de erişilebilirlik açısından önemli bir rol oynamaktadır.

Temel bir FKM hizmeti için cevaplanması gereken sorular aşağıdaki gibidir (TÜBİTAK, 2017a):

- Felaket kurtarma planı FKM'yi dahil edilerek hazırlandı mı?
- FKM'de barındırılacak uygulama veya hizmetlerin belirlenmesi ve değerlendirilmesi yapıldı mı?

- Eğer FKM hizmet olarak dış kaynaklardan sağlanacaksa hizmet sağlayıcının değerlendirilmesi yapıldı mı?
- Eğer FKM hizmet olarak dış kaynaklardan sağlanacaksa hizmet sözleşmesi, gizlilik sözleşmesi ve görev dağılımı yapıldı mı?
- FKM, hizmet alımı veya kurum iç kaynaklarıyla yapılacaksa alt yapı değerlendirilmesi yapıldı mı?
- Yasal zorunluluklar, tabi olunması gereken kanuni düzenlemelere uygunluk kontrol edildi mi?
- FKM'de kullanılacak replikasyon çözümleri nelerdir?
- Yedekleme ve replikasyon raporları oluşturuldu mu veya hizmet alımı ise talep edildi mi?

Kurumların yerleşik FKM kullanımı talepleri, beraberinde kapsamlı denetim, planlama ve durum değerlendirme faaliyetlerini gerektirmektedir. Bu doğrultuda, FKM hizmetinin sağlanması veya FKM'nin kurulumu sürecinde, kurumların uyum sağlaması gereken yasal düzenlemeler ve zorunluluklar bulunmaktadır. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, KVKK, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) gibi kuruluşların hazırladığı rehberler ve düzenlemeler, ilgili kurumlar tarafından dikkatle incelenmeli ve belirlenen gereklilikler yerine getirilmelidir. Kurumlar, ana veri merkezlerinde yer alan verilerini FKM'de yer alacak şekilde uygulama ve servisler bazında değerlendirirler ve yedeklemek veya işletmek için FKM'ye taşınacak verilerini çeşitli yöntemlerle taşırlar. Bu taşıma seçeneklerinden biri de replikasyondur. Replikasyon, dağıtık depolama sistemlerinin önemli bir teknolojisidir (Wang & Li, 2006). Replikasyon, bir sunucu veya veri depolama ünitesinden verilerin neredeyse gerçek zamanlı olarak başka bir sunucuya veya depolama sistemine taşımasına denir (Gregory, 2011). FKM'de kullanılacak replikasyonun genel amacı, iş sürekliliğini sağlamak ve bir felaket durumunda ana sistemlerde oluşabilecek hasar veya veri kaybını en aza indirerek kurumun BT hizmetlerinin devamlılığını sağlamaktır. Bu bağlamda ana sistemlerde bulunan veriler FKM'ye farlı yöntemlerle taşınabilirler. Bu yöntemler seçilirken kurumun maliyet beklentileri seçilecek çözümün performansı ve taşınacak sistemlerin birim ihtiyaçları göz önüne alınarak RPO (Recovery Point Objective – Kurtarma Noktası Hedefi) ve RTO

(Recovery Time Objective – Kurtarma Zaman Hedefi) değerleri incelenerek karar verme gerçekleştirilebilir (TÜBİTAK, 2017a).

RPO, kurum, kuruluş veya organizasyonun olası bir felaket durumunda yaşanılacak veri kaybının ne kadarına tolerans sağlanabileceğinin ölçütüdür. RPO, aynı zamanda kurumun felaket sonrasında kabul edebileceği maksimum veri kaybını ifade etmektedir (TÜBİTAK, 2017a). Replikasyon süreçlerinde kurumların FKM ile asıl veri merkezleri arasında gerçek zamanlı veri replikasyonunu sağlamaları durumunda, veriler anlık olarak yedeklendiği için kaybedilen veri miktarı en aza indirilir ve RPO süresi minimize edilebilir (Zgureanu, 2022).

RTO, kurum, kuruluş veya organizasyonun olası bir felaket durumunda sistemlerinin veya IT tabanlı iş süreçlerinin ne kadar sürede tam olarak çalışır hale getirilmelerini belirten değerdir. RTO, aynı zamanda felaket sonrası kesinti yaşanan BT tabanlı hizmetlerin kurum tarafından kabul edebileceği en yüksek kesinti süresini ifade etmektedir (TÜBİTAK, 2017a). Replikasyon süreçleri doğru kullanılarak felaket anında en kısa sürede FKM' nin devreye girmesi sağlanır ve RTO değeri minimize edilebilir (Zgureanu, 2022).

Sonuç olarak RPO ve RTO kavramları, bir kurumun iş sürekliliği ve felaket kurtarma planlarının temel yapı taşlarındandır. İyi bir felaket kurtarma planı, RPO ve RTO hedeflerini mümkün olduğu sürece en kısa sürelerde gerçekleştirilecek bir şekilde belirleyerek bu hedeflere ulaşmak için uygun stratejiler geliştirmek üzerine kurgulanmalıdır. Replikasyon ise bu stratejilerde yer alan hedeflere ulaşılmasında önemli bir araç olarak kullanılır, doğru replikasyon stratejileri ve doğru replikasyon teknolojilerinin tercih edilmesi ile RPO ve RTO hedeflerine daha yüksek oranda uyum sağlanabilir. Bu bağlamda, FKM'lerde kullanılacak replikasyon çözümleri farklılık gösterebilir. Senkron replikasyon, asenkron replikasyon ve multi-site replikasyon olmak üzere üç farklı replikasyon türü kurumun planlama ve ihtiyaçları doğrultusunda kullanılmaktadır. Senkron replikasyon, veri tutarlılığının ve bütünlüğünün yüksek düzeyde gerekli olduğu sistemlerde, kaynak ya da ana sistemde veri değişikliğinin gerçekleşmesinden sonra FKM'de ya da ikinci olarak belirlenen veri depolama sisteminde yer alan hedef sisteme, bu değişikliklerin aynı anda iletildiği ve aynı anda kaynak ve hedef sistemin eşitlendiği replikasyon türüdür ve bu tür bir replikasyon da

gecikme minimum düzeye çekilmek istense de, gecikme, kaynak ve hedef sistem arasındaki ağın bant genişliğine ve birbirleri arasındaki coğrafik mesafeye bağlıdır (Singh & Shanker, 2016). Asenkron replikasyon, veri değişikliğinin kaynak ya da ana sistemde yapılması tamamlandıktan sonra, gerekli görülmesi halinde, işlem kuyruğuna değişiklik kısımlarının yazıldığı, ardından belirlenmiş aralıklarla ya da tetikleyiciler vasıtasıyla, hedef sisteme iletimi ve eşitlenmesinin sağlandığı bir replikasyon türüdür ve bu tür bir replikasyon da, performans değerleri yüksek olsa da, kaynak ve hedef sistemler arasında anlık eşitleme olmadığı için, eşitleme bitene kadar, iki sistem arasında veri tutarsızlıklarının yaşanmasının söz konusu olduğu replikasyon türlerdir (Singh & Shanker, 2016). Multi-site replikasyon, birden fazla coğrafi konumda bulunan sistemler arasında veri senkronizasyonu sağlayan, kaynak sistemde yapılan veri değişikliklerinin, senkron veya asenkron olarak birden çok hedef sisteme eşitlendiği replikasyon türüdür (Sartakov & Kapitza, 2017; Sengupta & Annervaz, 2014).

FKM hizmetini bulut ortamından ya da dış kaynaklardan temin etmek istemeyen ve bu hizmeti kendi imkanlarıyla gerçekleştirmek isteyen kurumlar için FKM kurulumu büyük bir önem taşımaktadır. Bu süreçte, FKM kurulumu gerçekleştirilirken dikkate alınması gereken ve cevaplanması gereken temel sorular şunlardır (TÜBİTAK, 2017b):

- FKM kurulumu için uygun yer seçimi yapıldı mı ve raporlandı mı?
- FKM için mimari ve mekanik konsept dizaynları hazırlandı mı?
- FKM için ağ alt yapısı planlandı mı?
- FKM için enerji altyapısı planlandı mı?
- FKM için iklimlendirme sistemi planlandı mı?
- FKM için ortam izleme sistemleri planlandı mı?
- FKM için doğal afetlere karşı önlemler alındı mı?
- FKM için fiziksel güvenlik önlemleri alındı mı?
- FKM için personel sayısı yeterli mi ve personel eğitimleri sağlandı mı?
- FKM kullanımı hakkında eğitim dokümanları, yönergeler ve kitapçıklar var mı?

FKM'lerin coğrafi olarak yer seçimleri, olası doğal afetler açısından da önemlidir. Deprem bölgeleri, sel ve heyelan riskinin yüksek olduğu bölgeler, FKM'ler için son tercih noktaları olmalıdır. Ayrıca felaket kurtarma merkezlerinin enerji, iklimlendirme ve veri hattı açısından coğrafi konumu da özellikle dikkat edilmesi gereken özelliklerin başında

gelmektedir. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun hazırlamış olduğu rehbere göre FKM'lerin mümkün olduğu sürece ana sistem merkezleriyle aynı il sınırları içerisinde kurulmamaları önerilmektedir (TÜBİTAK, 2017b). FKM'ler mimari açıdan da kurulum aşamasında dikkat edilmesi gereken bazı temel bakış açılarına ihtiyaç duymaktadırlar. FKM içerisinde yer alacak beyaz alanların yükseltilmiş taban özellikleri ve ölçüleri, kabin yükseklikleri ve kabin yönleri, mekanik ve elektronik açıdan iklimlendirme ve kesintisiz güç ünitelerinin yerleşimleri ve yapısal kablolamanın kabinler arasında nereden ve nasıl yapılacağının titizlikle planlanması ve alan uzmanları tarafından değerlendirilmeleri gerekmektedir (Günal vd., 2017). Günümüzde ister FKM olsun, isterse ana veri merkezi olsun, yapısı içerisinde hizmet veren sunucuların, depolama ünitelerinin, ağ ve diğer cihazların, kesintisiz hizmet verebilmeleri için; güç kaynaklarının yedeklenmesi, en az iki farklı kaynaktan elektrik enerjisinin sağlanması ve uzun süreli şehir şebeke kesintilerine karşı jeneratörle beslemeli bir önlem alınmasına ihtiyaç duyulmaktadır (Günel, 2014).

Dünya genelinde kabul gören, veri merkezi standartlarının belirlenmesi üzerine ABD'deki Uptime Enstitüsünün belirlediği, Tier sertifikasyon çalışmalarına göre, veri merkezlerinin kesintisizlikleri ve erişilebilirlik sürelerine göre dört seviyeden oluşan bir sınıflandırma söz konusudur (Uptime Institute, 2024). Bu sertifikasyon programına göre Tablo 1.7'de verilen Uptime Institute standart değerlerine göre FKM ya da ana veri merkezileri kurulum süreçleri planlanabilmektedir.

Tablo 1.7. UPTIME INSTITUTE Enerji ve İklimlendirme Standartları (Uptime Institute, 2024).

TIER	Kesintisizlik	Kesinti Süresi	Klima	Güç Beslemesi	Jeneratör	UPS
I	%99,671	1680 dakika	N	Tek	Yok	N
II	%99,741	1320 dakika	N+1	Tek	N	N+1
III	%99,982	90 dakika	N+1	Çift, biri aktif	N+1	N+1
IV	%99,995	26 dakika	2N	Çift, aktif aktif	2N	2N

**Bu tabloda N kurumun ihtiyaç miktarını gösterirken, N+1 ihtiyaca ek bir adet yedeği, 2N tüm bileşenlerin yedekli olduğu anlamını taşımaktadır.*

FKM'ler ve veri merkezleri yapılarında bulundurdukları sunucular, depolama cihazları ve ağ cihazları gibi yüksek miktardaki elektronik aygıtlardan dolayı nem ve sıcaklık gibi değişkenlere yüksek oranda duyarlıdırlar ve bu merkezlerde optimum çalışma koşullarını sağlamak için doğru iklimlendirme şarttır (Arregoces & Portolani, 2003; Geng, 2014). FKM'lerde ve veri merkezlerinde ideal iklimlendirme kullanılarak uygun soğutma kapasitesinin belirlenmesi; sunucuların, depolama ünitelerinin ve ağ cihazlarının ürettikleri değerlere, merkezde yer alan kabinlerin sayısına, diğer bileşenlerin yerleşim planlarına, merkezin metrekare cinsinden boyutuna, varsa yükseltilmiş taban ve alçaltılmış tavana, perfore karoların yerleşimine, perfore oranlarına ve buna benzer birkaç hava akışını etkileyebilecek tüm bu bilgilerin hesaba katılması ile yapılabilir. Buna bağlı olarak da, büyük veya orta ölçekli veri merkezi ya da FKM'lerde, soğutucu sistem tasarımlarının CFD (Computational Fluid Dynamics) analizi kullanılarak yapılması bir gerekliliktir (Yüzgeç & Günel, 2016).

Veri merkezleri ve FKM'ler için önemli unsurlardan bir diğeri de fiziksel güvenliğin sağlanmasıdır. Kurumlar için başta hassas veriler olmak üzere BT tabanlı süreçlerin merkezinde yer alan veri merkezleri ve felaket anında iş sürekliliğini sağlayacak ve en az kesintiyle hizmetleri devam ettirecek FKM'lerin hırsızlık, sabotaj, terör saldırıları, yetkisiz erişimler veya art niyetle gelişecek saldırılara karşı hazırlıklı olmaları gerekmektedir. Bu bağlamda ortam izleme sistemlerine sahip olma, kartlı geçiş sistemleri veya biyometrik okuyucular ile erişim yetki kontrollerinin sağlanması, güvenlik personeli bulundurma, alarm sistemlerinden faydalanma gibi birtakım önlemler alınması veri merkezleri ve FKM'lerin fiziksel güvenliklerine katkı sağlamaktadır (Günel, 2014). Günümüzde IoT sensörlerinin kullanılmasıyla ortam izleme ve hareket algılama ile fiziksel güvenlik sağlanmasında olumlu yönde gelişimler gözlenmektedir (Baz & Uludağ, 2021).

1.4.2.4. Hiper Bütünleşik Mimari ve Bulut Bilişim Kullanım Planı

Modern veri merkezi yaklaşımlarından biri olan hiper bütünleşik mimari (Hyper-Converged Infrastructure, HCI) sistemleri, geleneksel sunucu ve veri depolama sistemleri mimarilerinden farklı olarak kaynakları entegre bir biçimde ve yazılım odaklı bir yapıda sunar. Bu mimaride, iş yükleri optimize edilir ve bu sayede kurumların operasyonel verimlilikleri artar, kaynak yönetiminde iyileşmeler sağlanır. Hiper bütünleşik mimaride,

sunucu, veri depolama ünitesi, SAN anahtarı gibi veri merkezi bileşenleri, ayrık yapılar yerine entegre bir sistem olarak sunulmaktadır. Bu yapı, kaynakların daha verimli kullanılmasını ve yönetimini kolaylaştırırken, aynı zamanda sistemlerin esnekliğini ve ölçeklenebilirliğini artırır (Veiga, 2017). Hiper bütünleşik sistemlerin felaket kurtarma planlarında kullanılması, kurum, kuruluş veya organizasyonlar açısından çeşitli avantaj ve dezavantajları barındırır. Felaket anında hız ve basitlik önem arz etmektedir. Bu bağlamda, hiper bütünleşik altyapıların sunduğu hizmetler, felaket anında daha hızlı bir şekilde toparlanma veya felaket öncesinde Felaket Kurtarma Merkezine verilerin daha hızlı bir şekilde replikasyonunun sağlanması açısından kurum, kuruluş ve organizasyonlara önemli avantajlar sunmaktadır. Bu altyapılar, kaynakların entegrasyonu ve optimize edilmesi sayesinde felaket durumlarında hızlı müdahale ve veri kaybının en aza indirilmesini mümkün kılmaktadır. Böylece, organizasyonlar felaket sonrası hizmet sürekliliğini daha etkin bir şekilde sağlayabilir ve operasyonel kesintilerin süresini önemli ölçüde kısaltabilir (Posey, 2019). Buna bağlı olarak, hiper bütünleşik sistemlerde yedeklilik esasına dayanarak, sistemin minimum çalışabilirliğini sağlayan küme sayısının altına düşülmesi durumunda, tüm hizmetlerin kaybedilmesi gibi bir risk bulunmaktadır. Bu nedenle, kritik öneme sahip sistemlerin tek başına hiper bütünleşik yapılarda çalıştırılması tavsiye edilmez. Kritik sistemlerin güvenliği ve sürekliliği açısından, bu sistemlerin daha geniş ve yedekli altyapılarda konumlandırılması gerekmektedir. Böylece, herhangi bir arıza veya felaket durumunda hizmetlerin kesintiye uğramadan devam edebilmesi sağlanabilir (Microsoft, 2023). Hiper bütünleşik sistemlerle tasarlanmış altyapılarda, depolama ve işlem kaynakları sistemin küme yapısına entegre bir biçimde yer aldığı için, felaket kurtarma planları hazırlanırken yedekleme ve kurtarma stratejilerinin bu entegrasyonu dikkate alarak tasarlanması gerekmektedir. Hiper bütünleşik sistemlerin bu yapısal özellikleri, veri yedekleme ve replikasyon mekanizmalarının farklı lokasyonlar veya bulut ortamlarında uygulanmasıyla aşılabilir. Ayrıca, hiper bütünleşik sistemlerin sunduğu merkezi yönetim arayüzleri sayesinde, felaket durumlarında altyapının durumu izlenebilir, yedekleme işlemleri yönetilebilir ve kurtarma operasyonları koordine edilebilir. Felaket kurtarma planlarının test ve eğitim süreçlerinin, gerçek hayat senaryolarına yakın sonuçlar doğurabilmesi kritik önem taşımaktadır. Bu bağlamda, hiper bütünleşik sistemler, test ve eğitim süreçlerinde kurum, kuruluş ve organizasyonlar tarafından etkili bir şekilde kullanılabilir (Crump, 2024;

Oneal, 2020). Sonuç olarak, hiper bütünleşik mimariye sahip sistemler, felaket kurtarma planlarında yüksek esneklik, ölçeklenebilirlik ve performans gibi avantajlar sunmaktadır. Bu nedenle kurumlar, kuruluşlar veya organizasyonlar, hiper bütünleşik mimari altyapısını felaket kurtarma stratejilerinin temel bir parçası olarak değerlendirebilir ve bu altyapıyı felaket öncesinde ve felaket anında etkili bir şekilde kullanarak iş sürekliliğini sağlamaya yönelik yeterlilik gösterebilirler. Bu yaklaşım, iş süreçlerinin kesintiye uğramadan devam etmesini sağlayarak, kurumların felaket durumlarına karşı daha hazırlıklı olmalarına katkı sağlar.

Bulut bilişim, günlük yaşamda birçok alanda hızla yaygınlaşan teknolojilerden biridir. Bulut bilişimin sunduğu hizmetlerden biri de "Hizmet Olarak Felaket Kurtarma" (Disaster Recovery as a Service - DRaaS) modelidir. Bu hizmet, organizasyonlar ve kurumlar için iş sürekliliğini sağlamak amacıyla kullanılan önemli bir çözüm modelidir. Hizmet olarak felaket kurtarma modelinin temel amacı, felaket kurtarma süreçlerini bulut bilişim altyapısını kullanarak gerçekleştirmektir. Bu hizmet modelinin sunduğu avantajlar arasında, maliyetlerin düşürülmesi, daha esnek ve ölçeklenebilir çözümler sağlanması ve karmaşıklığın azaltılması yer alır. Olası bir felaket anında, iş sürekliliğini sağlamak ve kritik iş süreçlerinin kesintisiz devamlılığını temin etmek, hizmet sağlayıcılarının temel sorumlulukları arasında bulunmaktadır (Rebah & Sta, 2016). Bulut tabanlı felaket kurtarma hizmeti, geleneksel felaket kurtarma planlarından farklılık göstermektedir. Bu farklılık, genellikle kurum kaynaklarının dışında bulunan başka bir hizmet sağlayıcıdan sağlanan sunucu ağ altyapısı, işletim sistemi, kuruma özel yazılımlar ve cihaz yapılandırmalarının, geleneksel sistemlerde tek tek kurtarılması için planlama yapılmasının yerine, hizmet olarak felaket kurtarmada tek bir başlık altında ele alınmasıdır. Bu yaklaşım, kurumların felaket kurtarma süreçlerini daha merkezi ve bütüncül bir şekilde yönetmelerine olanak tanır. Ayrıca, farklı coğrafi noktalarda bulunan kaynakların entegrasyonunu kolaylaştırarak, hizmet kesintilerinin en aza indirilmesini sağlar ve iş sürekliliğini destekler (Rashid & Chaturvedi, 2019). Bunun yanı sıra, hizmet olarak felaket kurtarma, kurumların, başta kritik uygulamaları olmak üzere, veri ve uygulamalarının düzenli olarak güncel yedeklerini bulutta tutarak, veri kaybı riskini en aza indirgemeyi ve olası felakette kurtarma sürecini hızlandırmayı amaçlar. Bu amaçlar doğrultusunda, hizmet olarak felaket kurtarma modelinde, önceden belirlenmiş prosedürler çerçevesinde sistemlerin otomatik olarak kurtarılması sağlanmaktadır. Olası

uygulama sorunlarında, yük devretme (Failover) yetenekleri sayesinde hizmet olarak felaket kurtarma, kurum ve kuruluşlara esneklik sunmaktadır. Bu hizmet, genellikle bir abonelik modeli olarak sunulduğundan, maliyet avantajı ve ölçeklenebilirlik sağlar. Ayrıca, felaket kurtarma planları açısından değerlendirildiğinde, hizmet sağlayıcılar, düzenli olarak felaket kurtarma planlarını test edebilir veya simüle edebilir. Bu süreçler, felaket senaryoları üzerinden yapılan değerlendirmeler ile kurum, kuruluş veya organizasyonların felaket durumlarına karşı ne kadar hazır olduklarını belirlemek için kullanılır (Andrade vd., 2017; Wood vd., 2010).

Sonuç olarak, bulut bilişimin sunduğu hizmet kapsamında felaket kurtarma modeli, kurumlar, kuruluşlar veya organizasyonlar için iş sürekliliği hedeflerini sağlamak ve süreçleri modernize etmek adına güçlü bir olanak sunar. Bu model, başta kritik hizmetler olmak üzere birçok hizmetin esneklik, ölçeklenebilirlik ve maliyet etkinliği kazanmasını sağlar. Böylece, kurumların operasyonel risklerini azaltırken, kullanılabilirlik ve güvenlik açısından da alternatif yaklaşımlar sunar. Ancak, bulut bilişim tabanlı bu hizmetin dezavantajları da vardır. Hizmet almak isteyen kurumların, servis sağlayıcıya sorunsuz bir şekilde bağlanabilmeleri için, sundukları hizmetlerin gerektirdiği en az bant genişliğine sahip olmaları gerekmektedir (Tan vd., 2018). Ayrıca, yasal yükümlülükler bu hizmetin kullanımını engelleyebilir veya kritik öneme sahip ya da hassas verilerin, üçüncü taraf bir sağlayıcıda saklanması durumunda, mahremiyet ve veri güvenliğinin sağlanması için ciddi çalışmalar ve teminatlar gerekebilir. Bu bağlamda, kurumların bu hizmet modelini değerlendirirken avantaj ve dezavantajları dikkatlice göz önünde bulundurmaları önemlidir.

1.5. BT FELAKET KURTARMA VE İŞ SÜREKLİLİĞİ STANDARTLARI

Kamu kurumları başta olmak üzere birçok kurum, kuruluş ve organizasyon, felaket kurtarma ve iş sürekliliği planlarını geliştirirken, bu süreçlerde bir yol haritası oluşturmak amacıyla ulusal ve uluslararası standartlara ihtiyaç duymaktadır. Bu bağlamda, uluslararası standartlar ve yönergeler, özellikle kurumsal bilgi güvenliğinin sağlanmasında, felaket kurtarma planlarının ve iş sürekliliği planlarının geliştirilmesinde önemli kolaylıklar sunmaktadır. Bu standartlar, planların yapılandırılmasını, uygulanabilirliğini ve etkinliğini artırarak, organizasyonların felaketlere karşı daha

hazırlıklı olmasına katkı sağlar (Nurhanudin, 2021; Puspitaningrum, 2022; Vural & Sağıroğlu, 2013).

Uluslararası standartlardan biri olan ISO 27031 standardı, bilgi ve iletişim teknolojilerinin iş sürekliliği ve felaketten kurtarma planlaması başlıklarını içeren, bu doğrultuda bir kuruma rehberlik etmek amacıyla geliştirilmiş kılavuz niteliğinde bir standarttır (Puspitaningrum, 2022). Günümüzde hemen hemen her kurum, kuruluş veya organizasyon iş yüklerinin çoğunu bilgi teknolojileri kullanarak gerçekleştirmektedir. Bunun yanı sıra, teknolojinin gelişimi de bilgi ve iletişim teknolojilerinin kurumlar tarafından yoğun bir şekilde kullanılmasını sağlamıştır. Ancak, siber tehditler bu bağlamda önemli bir artış göstermiştir. Siber saldırılar, doğal afetler, donanım veya yazılım arızaları gibi olaylar, bilgi ve iletişim teknolojilerinin kullanımını ciddi şekilde etkileyerek, kurumların işleyişlerinde aksaklıklar veya durmalar meydana getirebilmektedir. Bu nedenle, felaket kurtarma planlaması ve iş sürekliliği çalışmaları, kurumlar için büyük bir önem taşımaktadır. ISO 27031 gibi uluslararası standartlar, özellikle iş sürekliliğinin sağlanması ve felaket kurtarma planlarının oluşturulması, uygulanması ve sürdürülmesi aşamalarında, kurumlara ortak bir dil ve yaklaşım sunarak rehberlik sağlamaktadır. Bu standartlar, kurumların olası felaketlere karşı hazırlıklı olmasına yardımcı olur ve sürecin daha etkili bir şekilde yönetilmesini mümkün kılar (Groenendaal & Helsloot, 2020). ISO 27031 standartları kapsamında, kurumlar planlama, uygulama, kontrol ve denetleme süreçlerinden geçmektedirler. Planlama aşamasında kuruma ait BT hizmetleri, iş sürekliliği adımları, riskler belirlenir ve bu kapsamda politikalar oluşturulur. Bu adımda ayrıca, varsa ilgili paydaşlar, standart gereklilikleri ve standarda uyumun faydaları hakkında bilinçlendirilir (Arief & Putra, 2020). Uygulama ve altyapı hazırlığı basamağında, gerekli teknik ve organizasyonel önlemler alınarak, kuruma ait BT altyapıları, ISO 27031 standartlarına uygun hale getirilir. Bu adımda, kurumun odak noktası kesinti öncesi, kesinti anında ve sonrasında uygulanacak prosedürler, kurum personellerinin bireysel rolleri ve sorumlulukları konusunda bilgilendirilmelerini ve varsa paydaşların sorumlulukları hakkında bilgilendirmelerini içermelidir (Meilani vd., 2019; Muparadzi & Rodze, 2021). Kontrol ve denetleme aşamasında, standartlar tarafından belirtilen maddelere uyum sağlanıp sağlanmadığı tespit edilir. Kurumun planlama aşamasında tanımladığı prosedürler, yönergeler ve planlar gibi iş sürekliliği yönetim sistemi bileşenlerine uyulup uyulmadığı denetlenir ve

bu bileşenlerin performansları kurum açısından değerlendirilir. Bu aşamada, kesinti risklerini azaltmak için kontroller gerçekleştirilir. Buna ek olarak, bu aşamada elde edilen çıktılar, planın geliştirilmesi ve belgenin güncel tutulması açısından kurum için büyük önem taşır. Böylece, planın etkinliği artırılır ve sürekli iyileştirilmesi sağlanır (Das, 2023; Muparadzi & Rodze, 2021).

ISO 27031 standartlarına uyum kapsamında, bir üniversitenin yürütebileceği proje örneği şu adımları içerebilir:

- Proje Ekiplerinin Kurulması: İlk adımda, üniversite yönetimi, bilgi işlem birimi, varsa hastane ve diş hekimliği fakülteleri yönetimi, öğrenci işleri ve belge yönetim birimleriyle bir araya gelerek kritik hizmetlerin tespit edilmesini sağlar. ISO 27031 standartlarını incelemek ve süreci yönetmek amacıyla bir proje ekibi oluşturulur.
- Altyapı ve Plan Değerlendirmesi: Proje ekibi, üniversitenin mevcut bilgi ve iletişim sistemleri altyapısını, felaket kurtarma senaryolarını ve iş sürekliliği planlarını değerlendirir. Bu aşama, mevcut durumun analiz edilmesi ve eksikliklerin tespit edilmesi açısından kritik bir adımdır.
- Risk Analizi ve Kritik Sistemlerin Belirlenmesi: Proje ekibi, ilgili paydaşlarla bir araya gelerek risk analizi yapar. Bu süreçte, bilgi ve iletişim teknolojileri başta olmak üzere, üniversiteye ait kritik sistemler belirlenir ve bu sistemlerin ne kadar kritik olduğu analiz edilir.
- Yeni Politika ve Prosedürlerin Oluşturulması: İş sürekliliği için, belirlenen kritik bilgi ve iletişim sistemlerinin yürütülmesine yönelik yeni politika ve prosedürler oluşturulur. Bu politikalar, felaket kurtarma süreçlerinde izlenecek adımları ve müdahaleleri kapsar.
- Planların Oluşturulması ve Test Edilmesi: Oluşturulan politikalar ve prosedürler doğrultusunda, iş sürekliliği ve felaket kurtarma planları hazırlanır. Bu planlar test edilir ve testler sonucunda ortaya çıkan eksiklikler düzeltilmek üzere not edilir.
- Eksikliklerin Giderilmesi ve Eğitimler: Testler sonucu belirlenen eksiklikler giderilir. Ayrıca, personel için eğitim ve farkındalık çalışmaları düzenlenerek,

çalışanların felaket durumlarında nasıl tepki verecekleri konusunda bilgi sahibi olmaları sağlanır.

- Uygulama ve İzleme: Bu süreçte ISO 27031 standardına uyum süreci izlenir. Gerekli düzeltici önlemler alınır ve yasal belgelendirme süreci başlatılır. Bu süreç, sürekli izleme ve iyileştirmeyi gerektirir.

Bu adımların başarılı bir şekilde uygulanması, üniversitenin iş sürekliliği sağlamasını ve olası felaket durumlarına karşı hazırlıklı olmasını temin eder. İş sürekliliğinin sağlanması adına uluslararası takip edilecek bir diğer belgede *"NIST Special Publication 800-34"* belgesidir. ABD Ulusal Standartlar ve Teknoloji Enstitüsü tarafından yayımlanan bu belgede, felaket kurtarma planlarının oluşturulması ve yönetilmesi konularında rehberlik yapma niteliği vardır (Swanson vd., 2010). Bu belgenin içerdiği yönergeler, stratejiler ve süreçler, kurumlara BT altyapılarının dayanıklılığını artırma konusunda yardımcı niteliğindedir. Bunun yanı sıra, bu belgede bir kurum için, kuruma ait üç temel platformun, özel kurtarma planlaması önerilerini ele alınmaktadır. Bunlar; ağ ya da telekomünikasyon sistemlerinin tamamı, istemci-sunucu sistemleri ve mainframe sistemleridir.

Üniversiteler, BT ve veri yönetimi alanında karmaşık yapılar barındıran kurumlardır ve bu yapıların sürekliliği, hem akademik hem de idari faaliyetlerin kesintisiz bir şekilde yürütülebilmesi açısından kritik önem taşır. Öğrenci ve personel bilgileri, araştırma verileri, sağlık ve finansal işlemler gibi birçok hassas verinin korunması ve sürekli erişilebilir olması, üniversite yönetiminin en önemli sorumlulukları arasında yer alır. Bu bağlamda, NIST Special Publication (SP) 800-34 belgesi, felaket kurtarma planlarının hazırlanması, uygulanması ve yönetilmesi için detaylı bir rehber sunarak, kurumlara bu alanda sağlam bir temel oluşturur ve yol haritası sağlar. Bu belge, kurumların BT altyapılarını daha dayanıklı hale getirmelerine ve olası felaket senaryolarına karşı hazırlıklı olmalarına yardımcı olabilecek stratejiler, süreçler ve yönergeler içerir. Ancak, her üniversitenin benzersiz bir yapıya ve kendine özgü işleyişe sahip olduğu unutulmamalıdır. Akademik faaliyetlerin doğası, araştırma projelerinin kapsamı ve üniversitenin hizmet sunduğu öğrenci kitlesi gibi faktörler, felaket kurtarma planlarının standart bir çerçeveye uymasını zorlaştırabilir. Bu nedenle, NIST SP 800-34 belgesinde sunulan genel yönergelerin yanı sıra, her üniversitenin özel ihtiyaçlarına yönelik ek gereksinimlerin belirlenmesi ve bu gereksinimlerin dikkate alınarak planların

uyarlanması gerekmektedir. Bu tür bir yaklaşım, üniversitelerin hem genel standartlara uyum sağlamasını hem de kendi operasyonel gerekliliklerini karşılamasını mümkün kılar. Bu doğrultuda, felaket kurtarma planlarının etkinliği artırılabilir, kurum genelinde iş sürekliliği sağlanabilir ve kritik veri kaybı riskleri en aza indirilebilir (Niemimaa vd., 2019). Bu bağlamda, üniversiteler NIST SP 800-34 belgesinden risk değerlendirmesi ve planlaması süreçlerinde faydalanabilir. Özellikle doğal afetler, siber saldırılar, insan kaynaklı hatalar, cihaz kaynaklı teknik arızalar veya yanlış yapılandırmalardan kaynaklanan aksaklıklar gibi olaylara karşı hazırlıklı olunması konusunda bu belge önemli bir rehber niteliği taşımaktadır. Ayrıca, felaket kurtarma planlarının etkili bir şekilde yönetilmesi ve uygulanmasına ilişkin kapsamlı bir çerçeve sunar. Sonuç olarak, NIST SP 800-34, üniversiteler için BT felaket kurtarma planlarını oluşturmak, bu planları etkin bir biçimde yönetmek ve aynı zamanda kamu güvenliği ile ilgili yasalara uyumu sağlamak için bir referans kaynağı olarak değerlendirilebilir.

1.6. BT FELAKET KURTARMA PLANI ÖRNEĞİ

Çalışmanın bu bölümünde, bir kamu üniversitesi örnek alınarak, temel unsurları içeren sade bir felaket kurtarma planı, başlıklar halinde sunulmuştur.

1.6.1. BT Altyapı Haritasının Çıkarılması

BT altyapıları, üniversiteler için sundukları hizmetlerin sürekliliği ve etkinliği açısından hayati bir öneme sahiptir. İş sürekliliğinin sağlanması ve olası bir felaket durumunda etkili bir müdahale gerçekleştirebilmek adına, yapılması gereken temel adımlardan biri, BT altyapı haritasının ayrıntılı bir şekilde oluşturulmasıdır. BT altyapı haritaları, üniversitenin BT tabanlı hizmetlerinde kullandığı bileşenleri ve bu bileşenlerin diğer BT bileşenleriyle ilişkilerini metin tabanlı veya görsel (grafik, topoloji vb.) formatlarda temsil eden dokümanlardır. Bu belgeler, üniversitenin ağ altyapısını, sunucu ve veri depolama sistemleriyle bağlantılarını, sanallaştırma sistemlerini, yedekleme sistemlerini, kullanılan uygulamalar ve uygulamalara ait servisleri içermektedir.

Bir üniversite için BT altyapı haritasının temel bileşenleri şunlardır:

- Ağ altyapısı: Yerel Alan Ağı (LAN), Geniş Alan Ağı (WAN) ve kurum dışı erişim için kullanılan Sanal Özel Ağ (VPN) gibi ağ bileşenlerini; bu ağların hat kapasitelerini ve yapılandırmalarını içerir.
- Sunucular ve veri depolama çözümleri: Fiziksel, bulut veya sanallaştırma platformu üzerinde çalışan sunucuların yerleşim planları, üzerlerinde çalıştırdıkları rolleri ve kurum için olan işlevlerini, veri depolama ünitelerinin kapasitelerini, bağlantılarını, üzerlerinde bulunan disk havuzlarının hangi ortamlara paylaştırıldığını içerir.
- Yedekleme ve veri tabanı çözümleri: Veri tabanlarının, hangi boyutta hangi depolama alanları üzerinden, hangi bilgi sistemi için kullanıldığı ve bu verilerin yedeklenmesi ve replikasyonunun süreç çizelgelerini içerir.
- Güvenlik bileşenleri: Başta güvenlik duvarları olmak üzere, kimlik doğrulama sistemleri, saldırı tespit sistemleri ve varsa siber istihbarat sistemlerinin yapılandırmaları, kapasiteleri ve yedekli çalışma mekanizmalarına ait çalışma prosedürlerini içerir.
- Uygulamalar ve hizmetler: Uygulamaların nasıl ve hangi platformlarda çalıştıkları, bağımlılıkları, servislerle olan ilişkileri varsa bulut hizmetleri ve bunların konumlarını içerir.

BT altyapı haritası oluşturulurken çeşitli yöntemler kullanılabilir. İlk adım olarak envanter listesi hazırlanması ve envanter takibi yapılması, bu sürecin daha verimli bir şekilde yönetilmesine olanak tanır. BT varlıklarının tespit edilmesinden sonra, Her bir varlığın, diğer varlıklarla olan bağlantıları ve bağımlılıkları, aktif ya da pasif olma durumuna bakılmaksızın tespit edilir. Bu bağlantı ve bağımlılıklar analiz edildikten sonra, elde edilen verilere dayanarak ağ, sunucu ve uygulama topolojisi belirlenir ve bu yapı görsel bir harita şeklinde ifade edilir. BT altyapı haritası oluşturulması, yalnızca altyapının detaylı bir şekilde dokümante edilmesini sağlamakla kalmaz, aynı zamanda güvenlik zafiyetlerini tespit etmek, potansiyel riskleri değerlendirmek ve uygun güvenlik önlemlerini belirlemek için de kritik bir araçtır. BT altyapı haritası oluşturulmuş bir üniversitede, felaket kurtarma planına yönelik olarak ağ cihazları, sunucular, veri depolama üniteleri gibi bileşenler için 'Felaket Kurtarma Bilgi Çizelgeleri' hazırlanabilir. Örneğin, Tablo 1.8'de bir sunucu için felaket kurtarma bilgi çizelgesi; Tablo 1.9'da ise ağ cihazları için örnek bir felaket kurtarma bilgi çizelgesi sunulmaktadır.

Tablo 1.8. Örnek Sunucu Felaket Kurtarma Bilgi Çizelgesi.

Sunucu Felaket Kurtarma Bilgi Çizelgesi				
Sunucunun Adı:	SYS_Ag_Izleme_5.25			
Bulunduğu Platform:	Fiziksel (…)	Sanal (.X.)		
Sunucu Modeli: (Sanal ise çalıştığı fiziksel cihaz modeli)	HPE DL380 Gen 10			
Lokasyonu ve Seri Numarası: (Sanal ise bulunduğu lokasyon ve küme ismi)	Merkez-Kampus-HPE-Cluster			
İşlemci:	Intel Xeon Gold 16 çekirdek			
Ram:	16 GB			
Disk Boyutu ve Türü:	10 TB SAS			
İşletim Sistemi:	Debian 12 GNU/Linux			
IPv4 Bilgisi:	10.106.5.25			
Üzerinde çalışan uygulama(/lar) Adı	LibreNMS PHP 8.2 Nginx			
Üzerinde çalışan veri tabanı yazılımı ve sürümü:	MariaDB			
Sorumlu İletişim Bilgileri				
Sunucu Sorumlusu:	Kürşat E. 0312 xxx xxxx			
Paydaş Firma Sorumlusu (yoksa boş bırakınız):				
Yedekleme Bilgisi				
Yedekleme Türü: (Kaset ünitesine yılda 1 defa alınır.)	Aylık (.X.)	Haftalık (…)	Günlük (…)	Saatlik (…)
Yedekleme Başlangıç Zamanı:	Her Ayın 1. Gününde Saat:23:00 da			
Maksimum Geri Dönüş Noktası:	3			

Tablo 1.8. (Devamı)

Felaket Kurtarma Prosedürü	
Senaryo (birden fazla yazılabilir)	**Aksiyon (adım adım yazılmalı)**
1- Bölgesel elektrik kesintisi durumunda	1. Elektrik kesintisi algılandığında otomatik olarak FKM'ye bildirim gönderilir. 2. FKM ekibi, elektrik kesintisi bölgesindeki enerji sağlayıcı ile iletişime geçer ve tahmini onarım süresini alır. 3. Enerji sağlayıcı kesintinin giderilmesi sonrası FKM ekibi, sunucuyu yeniden devreye almak için fiziksel olarak yerinde veya uzaktan erişim aracılığıyla sunucuyu yeniden başlatır ve devreye alır. 4. Sunucunun yeniden başladıktan ve ağ bağlantısının kontrol edilmesi sağlandıktan sonra, sistem normale döner ve ağ izleme süreçleri tekrar aktif hale gelir.

Tablo 1.9. Örnek Ağ Cihazı Felaket Kurtarma Bilgi Çizelgesi.

Ağ Cihazı Felaket Kurtarma Bilgi Çizelgesi	
Ağ Cihazı Host Adı:	SW-Ankara-Hukuk-K3-PoE
Lokasyonu ve Seri Numarası:	Cebeci Kampüsü Hukuk Fakültesi 3.kat SN0001234
İşletim sistemi versiyonu	IOSXE-17.14.1
Yönetim IPv4 Adresi	10.105.06.06

Tablo 1.9. (Devamı)

Sorumlu İletişim Bilgileri				
Ağ Sorumlusu:	Ruhi T. 0312 xxx xxxx			
Ayniyat sorumlusu	Tümay B. 0312 xxx xxxx			
Paydaş Firma Sorumlusu (yoksa boş bırakınız):	Aydın K. Cisco Partner 0312 218 xxxx			
Yedekleme Bilgisi				
Konfigürasyon Yedekleme Türü:	Aylık (...)	Haftalık (…)	Günlük (…)	Manuel (.X.)

Felaket Kurtarma Prosedürü	
Senaryo (birden fazla yazılabilir)	**Aksiyon (adım adım yazılmalı)**
1- Yangın	1. Yangının yayılma durumu değerlendirilir ve yangın alarmı otomatik olarak tetiklenmediyse tetiklenir ve güvenlik amirliğine ve itfaiye derhal olay yerine yönlendirilir. 2. Cihaz ve cihaza bağlı diğer ağ cihazları güvenli bir şekilde kapatılır ve elektrik gücü kesilir. UPS varsa bu sistem devreye alınır. 3. Yangının etkilediği bölgeyi izole etmek için ağ bağlantıları kesilir ve hasarın yayılması önlenir. 4. yangın söndürüldükten sonra ağ anahtarı ve ona bağlı ekipmanlar gözden geçirilir, hasar tespit edilir. Hasarlı ekipmanların onarımı veya değiştirilmesi planlanır. 5. ağ cihazı ve bağlantıları yeniden kurulur ve konfigürasyonu yapılandırılır ve tüm çalışma testleri yapılır. Cihazın sorunsuz çalıştığı kararı verilir. Yoksa eksiklik giderilir test tekrar yapılır. 6. Olayın detayları, alınan aksiyonlar ve süreçler detaylı olarak kaydedilir. Yangın sonrası felaket kurtarma planı gözden geçirilir ve güncellenir.

1.6.2. Kurtarma Mimarisinin Belirlenmesi

BT felaket kurtarma planları, geleneksel ya da ikinci adıyla klasik mimariyle tasarlanabileceği gibi, yasal düzenlemelere uyum sağlanması koşuluyla, bulut bilişim tabanlı olarak da gerçekleştirilebilir. Bu bağlamda, kurtarma planının DRaaS veya klasik mimariyle yapılandırılması kararı verildikten sonra diğer adımlara geçilebilir. Bu iki mimari, belirli koşullarda eş zamanlı olarak da kullanılabilir. Bu tür durumlarda iş etki analizi, risk değerlendirmeleri ve altyapı ile varlık envanteri düzenlemeleri, planda farklı önceliklere ve değerlere sahip olacaktır. Örnek olarak sunulan bu planda, BT felaket kurtarma süreci klasik mimari üzerinden planlanmıştır.

1.6.3. Risk Değerlendirmesi

BT felaket kurtarma planları, iş sürekliliği planlarıyla genellikle benzer doğrultuda hazırlanmakla birlikte, risk değerlendirme başlığı BT felaket kurtarma planlarında daha çok süreçlerden ziyade felaket türlerine odaklanarak oluşturulmaktadır. Bir üniversite için, karşılaşılabilecek olası olaylardan yola çıkarak, hangi felaket senaryolarının daha muhtemel olduğunu belirlemek amacıyla bir risk değerlendirmesi yapılması gereklidir.

Risk değerlendirmesi kapsamında, olasılık değeri, etkisi, risk seviyesi, önerilen eylemler ve olay etkisi gibi başlıklar yer almalıdır. Bu doğrultuda Tablo 1.10'da örnek bir risk değerlendirmesi sunulmuştur.

Tablo 1.10. Örnek Risk Değerlendirmesi Çizelgesi.

Risk No / Açıklama	Olasılık (1-5)	Etki (1-5)	Risk Seviyesi	Olay Etkisi	Önerilen Eylemler
1-Doğal afetler (deprem, sel vb.)	4	5	20	Kritik sistemlerin geçici olarak kullanılamaz hale gelmesi	- Acil tahliye planı oluşturun. - Afet kurumlarıyla iletişime geçin ve varsa ulusal politikalar doğrultusunda hareket edin. - Yedek enerji kaynakları sağlayın. - Veri merkezi dışında yedek tesisler belirleyin ve daha önceden belirlenmiş kritik sistemleri buraya taşıyın.

Tablo 1.10. (Devamı)

Risk No / Açıklama	Olasılık (1-5)	Etki (1-5)	Risk Seviyesi	Olay Etkisi	Önerilen Eylemler
2-Veri merkezi donanım arızası	3	4	12	Kritik sistemlerin geçici olarak kullanılamaz hale gelmesi	- Yedekleme stratejileri güncelleyin. Aktif-aktif veya aktif-pasif mimarilerde çalışan sistemler tasarlayın ve devreye alın - Hızlı donanım değişimi için anlaşmalar yapın. Soğuk yedek cihaz ve kritik donanımları barındırın.
3-Kötü niyetli yazılım saldırıları (virüs, fidye yazılımı)	5	3	15	Veri güvenliği ihlali ve kritik sistemlerin kullanılamaz hale gelmesi	- Güvenlik yazılımlarını güncel tutun. - Sızma testleri yapın. - Fidye saldırılarına karşı kriz planı oluşturun.
4-İnsan hataları (yanlış kullanım, veri sızıntısı vb.)	4	4	16	Kritik veri kaybı veya sistemlerin geçici olarak kullanılamaz hale gelmesi	- Kullanıcı eğitim programları düzenleyin. - Veri sızıntısı yazılımları kullanın ve kurtarma planlarını güncelleyin.
5-İnternet bağlantı sorunları	2	3	6	Erişim sorunları ve kritik sistemlerin geçici olarak kullanılamaz hale gelmesi	- Alternatif internet sağlayıcıları ile anlaşmalar yapın. - Yedek bağlantı yolları oluşturun.

Olasılık başlığı, gerçekleşmesi muhtemel risklerin olasılık düzeyini değerlendiren bir ölçek içermelidir. Örneğin, bu tabloda '1' en düşük olasılığı, '5' ise en yüksek olasılığı temsil etmektedir.

Etki başlığı, risklerin gerçekleşmesi durumunda yaratacağı etkinin büyüklüğünü gösteren bir ölçek içermelidir. Bu tabloda '1' en düşük etkiyi, '5' ise en yüksek etkiyi temsil etmektedir. En yüksek etki, genellikle kurumun hizmet veremez hale geldiği durumlardır.

Risk seviyesi başlığında ise olasılık ve etki değerleri çarpılarak her bir risk için bir risk seviyesi hesaplanabilir. Bu risk seviyesi, farklı matematiksel yöntemler kullanılarak da hesaplanabilir. Ek olarak, tehdit ve riskler basit bir şekilde potansiyel etkiler, alınması

gereken önlemler ve ilgili sorumlular şeklinde başka bir tabloda ifade edilebilir. Bu doğrultuda, Tablo 1.11'de örnek bir tablo sunulmuştur.

Tablo 1.11. Tehditler-Riskler, Potansiyel Etkileri ve Alınması Gereken Önlemler.

Tehdit / Risk	**Potansiyel Etkiler**	**Önlemler**	**Sorumlu Birim**
Doğal Afetler (Deprem, Sel)	Bina hasarı, kesintiler, can ve mal kayıpları	Acil tahliye prosedürleri uygulanmalı, Bina güçlendirme projeleri yapılmalı.	Üniversite Yönetimi
Teknolojik Arıza (Veri kaybı, sistem çökmesi)	Eğitim ve araştırma kesintileri	Yedekleme planları hazırlanmalı ve düzenli kontrolleri sağlanmalı, IT altyapısı güçlendirilmeli.	IT Birimi
İnsan Kaynaklı Arızalar (Kötü amaçlı yazılım, kullanıcı hataları)	Veri güvenliği ihlalleri, sistem aksaklıkları	Güvenlik eğitimleri alınmalı, düzenli güvenlik testleri gerçekleştirilmeli, Kullanıcı rehberleri hazırlanmalı.	Bilgi Güvenliği Birimi

1.6.4. Öncelik Listelerinin Belirlenmesi

BT felaket kurtarma planında önceliklerin belirlenmesi sürecinde, aksiyonlar içerisinden öncelikli olarak ele alınması gerekenler ve bu süreçlerin nasıl yönetileceği gösterilmelidir. Kurumların verdiği hizmete ve hizmet kritikliğine göre öncelikler farklılık göstermektedir. Buna bağlı olarak, öncelikler ciddi bir biçimde belirlenmeli ve düzenli aralıklarla bu öncelik durumlarının devam edip etmediği denetlenmelidir. Üniversiteler açısından değerlendirildiğinde, felaket kurtarma planları, üniversitenin kritik işlevlerini korumayı ve toplumun güvenliğini sağlamayı hedeflemektedir. Bu planlar, yasal gereksinimler, kurumun özel ihtiyaçları ve öncelikleri doğrultusunda ayrıntılı şekilde yapılandırılabilir. Bu bağlamda, Tablo 1.12'de önceliklerin belirlenmesine yönelik bir örnek tablo sunulmuştur.

Tablo 1.12. Önceliklerin Belirlenmesi Örneği.

Senaryo	Öncelik	Açıklama
1. Öğrenci Bilgi Sistemi Çökmesi	**Yüksek**	Öğrenci bilgi sistemi, öğrencilerin akademik bilgilerini, notlarını ve kişisel bilgilerini içerir. Sistemin çökmesi, öğrenci ve yönetim arasındaki etkileşimi olumsuz etkiler.
2. Kimlik Doğrulama Sistemlerinin Çökmesi	**Yüksek**	Üniversiteye ait servislerin tamamına erişimler için kullanılan yetkilendirme ve doğrulama servisidir. Bu servisin çalışmaması durumunda tüm erişimler kısıtlanacağı için hizmetler olumsuz etkilenir.
3. Eğitim Platformu (Öğrenme Yönetim Sistemi) Arızası	Orta	Eğitim platformu, çevrimiçi dersler, materyaller ve öğrenci-öğretmen etkileşimlerini yönetir. Arıza durumunda öğretim sürecinin aksamadan devam etmesi için belirli bir kurtarma süresi belirlenmiştir.
4. E-posta Hizmeti Arızası	Orta	E-posta hizmetleri, akademik ve idari iletişimin temel araçlarından biridir. E-posta sisteminin arızalanması, iletişim kesintisine yol açar, bu nedenle makul bir kurtarma süresi belirlenmiştir.
5. Kütüphane Veri Tabanı Arızası	Düşük	Kütüphane veri tabanları, akademik kaynakların erişimini sağlar ancak diğer sistemlere göre daha az acil durum sunar. Veri tabanının erişilebilirliği önemlidir, ancak acil kurtarma gerektirmeyebilir.
6. Web Sitesi Erişilebilirlik Sorunu	Orta	Üniversite web sitesi, bilgi paylaşımı ve duyurular için kullanılır. Web sitesinin erişilememesi, bilgilendirme süreçlerinde aksamalara neden olabilir ancak acil bir kurtarma gerektirmez.
7. İdari Finans Sistemi Çökmesi	Düşük	İdari finans sistemleri, bütçe yönetimi, maaş ödemeleri ve mali raporlamalar gibi kritik işlevleri destekler. Bu sistemlerin hızlı bir şekilde kurtarılması finansal istikrar için önemlidir.

1.6.5. Olay Müdahale Tablosu

Olay müdahale tablosunda, olası bir BT felaketi ve acil durumlar için atılması gereken adımlar detaylandırılmalıdır. Bu tabloda, sorumlu kişi veya birim, iletişim bilgileri, müdahale adımları, olayın türüne bağlı olarak ilgili kaynaklar ve dokümanlar gibi başlıklara yer verilebilir. Bu bağlamda, Tablo 1.13'te olay müdahalesine yönelik örnek bir tablo sunulmuştur.

Tablo 1.13. Örnek Olay Müdahalesi Çizelgesi.

Olay Numarası	Olay Tanımı	Öncelik Seviyesi	Müdahale Adımları	Sorumlu Birim/Personel
1	Ağ kesintisi	Orta	1. Katman-1ve 7 seviyesinde ağ altyapısını kontrol et. 2. Ağ trafiğini izleme ve sorunun kaynağını belirle.	BT Altyapı Ekibi
2	Veri merkezi yangını	Kritik	1. Yangın alarmını tetikle. 2. İtfaiyeyi ara ve yangınla mücadele edilmesini sağla. 3. Veri merkezi personelini tahliye et ve güvenli alana yönlendir.	Güvenlik ve İtfaiye Ekibi, BT Yöneticisi
3	Köklü yazılım hatası	Yüksek	1. Hatayı tespit etmek için sistem günlüklerini incele. 2. Yazılım sağlayıcısıyla iletişime geç ve sorunu çözmek için adımları belirle.	Yazılım Destek Ekibi, BT Proje Yöneticisi
4	E-posta sunucusu çökmesi	Yüksek	1. Sunucu ve servislerini kontrol et. 2. E-posta iletişiminin yedek sistem üzerinden devam etmesini sağla.	E-posta Yöneticisi, BT Destek Ekibi
5	Doğal afet	Kritik	1. Acil durum ekiplerini harekete geçir ve güvenliği sağla. 2. BT altyapısının zarar görmesini önlemek için önlemler al. 3. Yedekleme sistemlerini kontrol et ve veri kurtarma sürecini başlat.	Kriz Yönetim Ekibi, BT Güvenlik Ekibi
6	Hastane BT altyapısında arıza	Kritik	1. Arızayı tespit etmek için hastane BT sistemlerini incele. 2. Sorunu gidermek için acil müdahale adımlarını belirle. 3. Hasta verilerinin güvenliğini sağlamak için gerekli önlemleri al.	Sağlık Teknolojileri Ekibi, BT Destek Ekibi
7	Web sitesi saldırısı	Orta	1. Saldırıyı tespit et ve saldırıya maruz kalan sistemleri izole et. 2. Saldırının etkilerini minimize etmek için güvenlik duvarı ve filtreleme önlemlerini güçlendir. 3. Olayı SOME ekibine bildir.	BT Güvenlik Ekibi, Web Yöneticisi

1.6.6. Kurtarma ve Yönetim Ekibi

Kurtarma ve yönetim ekipleri felaket anlarında görev yapacak kişileri, bu kişilere erişilememesi durumunda ilgili yedeklerini ve iletişim bilgilerini, görev tanımlarını ve olası felaket türlerine göre sorumluluklarını içermelidir. Buna ek olarak, BT felaket kurtarma planında çeşitli felaket durumları için görevler, sorumlu kişiler, yedek kişiler ve iletişim bilgilerini sistematik bir şekilde yönetmeye yardımcı olmak amacıyla tablo oluşturulması faydalı olacaktır. Bu bağlamda, Tablo 1.14'te kurtarma ve yönetim ekibi belirtilmesine yönelik örnek bir tablo sunulmuştur.

Tablo 1.14. Kurtarma ve Yönetim Ekibi Örneği.

Felaket Durumu	**Görev**	**Sorumlu Kişi**	**Yedek Kişi**	**Kritiklik Durumu**	**İletişim Bilgileri**
Sunucu Arızası	**Sunucu Kurtarma**	Kürşat K..	Ayşe T...	Kritik	kursatk@xuni.edu.tr 0555 xxx xx xx
	Sunucu Yapılandırması	Kürşat K...	Ayşe T...	Yüksek	kursatk@xuni.edu.tr 0555 xxx xx xx
Ağ Arızası	**Ağ Sorun Giderme**	Yaşar K...	Tümay B...	Kritik	kyasar@xuni.edu.tr 0555 xxx xx xx
	Ağ Yapılandırma ve Kontrol	Yaşar K...	Tümay B...	Yüksek	kyasar@xuni.edu.tr 0555 xxx xx xx
	Ağ Güvenlik Önlemleri	Fırat D...	Burak B...	Orta	firat@xuni.edu.tr 0555 xxx xx xx
Veri Kaybı	**Veri Kurtarma**	Ruhi T.....	Şeyda E...	Kritik	ruhit@xuni.edu.tr 0555 xxx xx xx
	Veri Yedekleme ve Geri Yükleme	Ruhi T.....	Şeyda E...	Yüksek	ruhit@xuni.edu.tr 0555 xxx xx xx
Siber Saldırı	**Saldırı Analizi ve Tespit**	Fırat D...	Burak B...	Kritik	firat@xuni.edu.tr 0555 xxx xx xx
	Saldırı Öncesi ve Sonrası Güvenlik	Arif T...	Canan Demirtaş	Yüksek	arift@xuni.edu.tr 0555 xxx xx xx
	Güvenlik Politikaları Güncelleme	Fırat D...	Arif T...	Orta	firat@xuni.edu.tr 0555 xxx xx xx
Felaket Senaryoları	**Felaket Senaryoları Testi**	Burhan S...	Ercan D...	Orta	burhans@xuni.edu.tr 0555 xxx xx xx
	Eğitim ve Senaryo Güncellemeleri	Burhan S...	Ercan D...	Orta	burhans@xuni.edu.tr 0555 xxx xx xx

Tablo 1.14. (Devamı)

Felaket Durumu	Görev	Sorumlu Kişi	Yedek Kişi	Kritiklik Durumu	İletişim Bilgileri
Genel İletişim	**İletişim Koordinasyonu**	Zeynep A...	Kamil K...	Kritik	zeynepa@xuni.edu.tr 0555 xxx xx xx
	Durum Raporlarının Dağıtımı	Zeynep A...	Kamil K...	Kritik	zeynepa@xuni.edu.tr 0555 xxx xx xx
	İç ve Dış Paydaşlarla İletişim	Zeynep A...	Kamil K...	Orta	zeynepa@xuni.edu.tr 0555 xxx xx xx

Felaket anı ve sonrasında belirlenmiş personellerin yapacakları işlere dair bilgiler, kurtarma ve yönetim ekibi başlığında yer almalı ve bu başlık ayrıca olay raporlaması ile üçüncü taraflarla iletişim konularını da kapsamalıdır. Bu başlık altında, felaket durumunda hangi kişilerin yetkili olduğu, bu kişilere ulaşılamadığı takdirde yedek kişilerin kimler olduğu gibi bilgiler de yer almalıdır. Bazı felaketlerden sonra, özellikle BT verilerinin saklandığı tesislerin güvenliğinden, başta fiziksel güvenlik olmak üzere, kimlerin sorumlu olduğu ve felaketin büyüklüğüne göre hangi eylem planlarının devreye gireceği plana dahil edilmelidir. Örneğin, bazı veri merkezlerinin izlenmesi üçüncü taraf hizmet sağlayıcıları tarafından yapılmaktadır. Bu hizmet sağlayıcılarıyla iletişimde yaşanabilecek olumsuzlukları önlemek için iletişim bilgileri yedeklilik esasına dayalı olarak geniş tutulmalı ve iletişim kurulması gereken zaman periyotları önceden belirlenmelidir. Bu sayede, olası iletişim kopuklukları durumunda devreye girecek prosedürler önceden hazırlanabilir. Örneğin, bir deprem felaketi sonrasında, yetkili üç kişiye 48 saat boyunca ulaşılamaması durumunda, ana veri merkezinden FKM veri merkezine hizmetlerin devredilmesi prosedürü devreye sokulmalıdır. Buna bağlı olarak, felaket kurtarma süreçlerinin etkin bir şekilde takip edilebilmesi için bir süpervizörün yetkilendirilmesi gerekmektedir. Planın geliştirilmesi ve düzenli aralıklarla kontrol edilmesi aşamalarında veya planda yer alan herhangi bir personelin kurumla ya da görevle ilişiği kesildiğinde, bu kişinin yerine yeni görevli personel atanarak ilgili yer doldurulmalıdır.

1.6.7. Felaket Kurtarma Zaman Çizelgesi

Üniversiteler başta olmak üzere birçok kamu kurumunda, felaket kurtarma planı, yedekleme prosedürleri ve felaket kurtarma zaman çizelgesi sıklıkla birbirine karıştırılmaktadır. Ancak, BT felaket kurtarma planının bir parçası olan felaket kurtarma

zaman çizelgesi, bir sistem veya uygulamanın önem derecesine göre belirlenen RPO (Recovery Point Objective) ve RTO (Recovery Time Objective) değerlerini içeren ve felaket durumunda uygulanacak yöntemlerle normal işleyişin ne kadar sürede sağlanacağını belirlemeye yardımcı olan bir araçtır. RPO, alınan veri yedekleri arasında kabul edilebilir maksimum veri kaybı süresini ifade ederken, RTO, sistemin tamamen kurtarılması için geçebilecek maksimum süreyi ifade etmektedir. Bu bağlamda, Tablo 1.15'te, felaket kurtarma zaman çizelgesine ilişkin örnek bir tablo sunulmuştur.

Tablo 1.15. Felaket Kurtarma Zaman Çizelgesi

Sistem / Uygulama	Kritiklik Seviyesi	RPO	RTO	Kurtarma Yöntemi
Öğrenci Bilgi Sistemi	Yüksek	1 saat	4 saat	Yedekleme sisteminden geri yükleme ve FKM üzerinden yeniden devreye alma
Elektronik Belge Yönetim Sistemi	Orta	4 saat	8 saat	Yedekleme sisteminden geri yükleme ve FKM üzerinden yeniden devreye alma
Hasta Bilgi Sistemi	Yüksek	1 saat	4 saat	Yüksek erişilebilirlik mimarisi (failover) ve FKM üzerinden yeniden devreye alma
Personel Takip Sistemi	Orta	4 saat	8 saat	Yedekleme sisteminden geri yükleme
Kartlı Geçiş Sistemi	Düşük	1 gün	12 saat	Yedekleme sisteminden geri yükleme
Yemekhane Takip Sistemi	Düşük	1 gün	12 saat	Yedekleme sisteminden geri yükleme
Eğitim Yönetim Sistemi	Orta	4 saat	6 saat	Yüksek erişilebilirlik mimarisi (failover)
Akademik Araştırma Veri tabanı	Yüksek	1 saat	4 saat	Yedekleme sisteminden geri yükleme ve FKM üzerinden yeniden devreye alma

1.6.8. Veri Yedekleme ve Kurtarma Planı veya Tablosu

Felaket kurtarma planları, kurumların iş sürekliliğini sağlamaları, bilgi güvenliği süreçlerini korumaları ve uluslararası standartlara uyum göstermeleri açısından, veri yedekleme ve yedekten geri dönme prosedürlerini içermelerini neredeyse zorunlu kılmıştır. Verilerin düzenli olarak yedeklenmesi, yedeklerin güvenli bir şekilde saklanması ve ihtiyaç durumunda bu yedeklerden hızlıca geri dönülmesi, yalnızca felaket kurtarma süreçleri için değil, aynı zamanda günlük operasyonların kesintisiz

sürdürülebilmesi için de hayati önem taşır. Başta üniversiteler olmak üzere, birçok kurum için verilerin hangi sıklıkla, hangi ortam ve teknolojilerde, hangi güvenlik protokollerine uygun şekilde yedekleneceği, kurumların belirlediği stratejik hedefler ve ihtiyaçlar doğrultusunda planlanır. Bu süreç, yalnızca teknik bir operasyon değil, aynı zamanda iş sürekliliği ve bilgi güvenliğini destekleyen kritik bir yönetim unsurudur. Yedekleme stratejileri, tam yedekleme, artımlı yedekleme veya fark yedekleme şeklinde sınıflandırılabilir (Frisch, 2008; Nakamura vd., 2017). Yedekleme ortamları açısından günümüzde üniversitelerde yaygın olarak kullanılan üç temel depolama ortamı vardır. Bunlar; disk üniteleri, kaset ya da diğer isimlendirmesiyle manyetik şerit üniteleri ve bulut bilişim merkezli depolama ortamlarıdır (Fontana vd., 2012; Moore vd., 2007; Schulz, 2016). Bu bağlamda, Tablo 1.16'da sistem ve uygulamalar bazında bir üniversiteye yönelik örnek bir tablo sunulmuştur. Ek olarak, Tablo 1.17'de cihazlar ve sistemler açısından örnek bir plan yer almaktadır.

Tablo 1.16. Sistem ve Uygulamalar Bazında Yedekleme ve Kurtarma Planı Örneği.

Sistem / Uygulama	**Veri Türü ve Sıklığı**	**Yedekleme Yöntemi**	**Depolama Yeri**	**Kurtarma Zaman Çizelgesi**
Öğrenci Bilgi Sistemi	Günlük	Gün sonu yedekleme	Disk Ünitesi / Bulut depolama	4 saat içinde geri yükleme
Elektronik Belge Yönetim Sistemi	Günlük	Gün sonu yedekleme	Disk Ünitesi / Bulut depolama	8 saat içinde geri yükleme
Hasta Bilgi Sistemi	Anlık	Anlık yedekleme (replication)	Yüksek erişilebilirlik mimarisi (aktif-aktif)	4 saat içinde geri yükleme
Personel Takip Sistemi	Anlık	Anlık yedekleme (replication)	Yüksek erişilebilirlik mimarisi (aktif-aktif)	4 saat içinde geri yükleme
Kartlı Geçiş Sistemi	Günlük	Gün sonu yedekleme	Disk Ünitesi / Kaset Ünitesi	12 saat içinde geri yükleme
Yemekhane Takip Sistemi	Günlük	Gün sonu yedekleme	Disk Ünitesi / Kaset Ünitesi	12 saat içinde geri yükleme
Akademik Araştırma Veri tabanı	Günlük	Günlük yedekleme (transaction logs)	Yüksek erişilebilirlik mimarisi (aktif-pasif)	4 saat içinde geri yükleme
Eğitim Yönetim Sistemi	Haftalık	Haftalık yedekleme	Disk Ünitesi / Bulut depolama	4 saat içinde geri yükleme

Tablo 1.17. Cihaz ve Sistemler Bazında Veri Yedekleme ve Kurtarma Planı Örneği.

Cihaz / Sistem	Yedekleme Sıklığı	Yedekleme Yöntemi	Depolama Yeri	Kurtarma Süresi Hedefi
Veri Merkezi Sunucuları	Günlük	Gün sonu yedekleme	Yedek veri merkezi / Bulut depolama	4 saat içinde sunucuların yeniden kurulumu ve veri geri yükleme
Ağ Anahtarları ve Router'lar	Haftalık	Konfigürasyon yedeklemesi	Konfigürasyon yönetim sistemi / Disk Ünitesi	8 saat içinde konfigürasyonların geri yükleme ve ağ ayarlarının restore edilmesi
Firewall Cihazları	Haftalık	Konfigürasyon yedeklemesi	Konfigürasyon yönetim sistemi / Disk Ünitesi	8 saat içinde firewall konfigürasyonlarının geri yükleme ve güvenlik ayarlarının restore edilmesi
SAN (Storage Area Network)	Günlük	Gün sonu yedekleme	Yedekleme sunucusu / Bulut depolama	4 saat içinde SAN verilerinin geri yükleme ve veri bütünlüğünün sağlanması
DNS Sunucuları	Günlük	Gün sonu yedekleme	Yedekleme sunucusu / Disk Ünitesi	4 saat içinde DNS kayıtlarının geri yükleme ve hizmetlerin restore edilmesi
DHCP Sunucuları	Günlük	Gün sonu yedekleme	Yedekleme sunucusu / Disk Ünitesi	4 saat içinde DHCP yapılandırmalarının geri yükleme ve hizmetlerin restore edilmesi
VPN Sunucuları	Günlük	Gün sonu yedekleme	Yedekleme sunucusu / Bulut depolama	4 saat içinde VPN yapılandırmalarının geri yükleme ve hizmetlerin restore edilmesi

Felaket türleri, önleyici çalışmalar, müdahale planları ve sorumlulukların yanı sıra, yedekleme ve kurtarma planlarının ayrı bir çalışmada ele alınması, olası bir felaket durumunda BT personelinin hazırlıklı olmasını sağlayabilir. Bu bağlamda, Tablo 1.18'de felaket türlerine, kurtarma ve iyileştirme süreçlerine ilişkin örnek bir tablo sunulmuştur.

Tablo 1.18. Felaket Türü, Kurtarma ve İyileştirme Süreçleri.

Felaket Türü	Önleme ve Hazırlık Yapılacaklar	Müdahale Planı	Kurtarma ve İyileştirme Süreçleri	Sorumlu Ekip	Notlar
Doğal Afet (Deprem, Sel vb.)	- Bina güçlendirme çalışmaları ve acil tahliye planları oluşturulmalı.	- Acil durum ekipleri belirlenmeli ve eğitilmeli.	- Hasar tespit ve değerlendirme süreci.	Yönetim Birimi	- Acil durum ekipmanları düzenli kontrol edilmeli.
Yangın	- Yangın alarm sistemleri ve söndürme ekipmanları periyodik olarak test edilmeli.	- Yangın söndürme ekipleri görevlendirilmeli ve eğitilmeli.	- Hasarın onarımı ve yangın sonrası temizlik süreci.	İtfaiye ve Güvenlik Ekibi	- Acil durum çıkışları belirgin olmalı.
Bilgi Güvenliği İhlali	- Güçlü şifre politikaları ve güvenlik duvarı konfigürasyonları oluşturulmalı.	- Olay yanıt planı hazırlanmalı ve güncel tutulmalı.	- Veri kurtarma ve sistemlerin yeniden kurulması.	Bilgi İşlem ve Güvenlik Ekibi	- Sık yedekleme yapılmalı.
Veri Kaybı	- Düzenli veri yedekleme politikaları oluşturulmalı ve test edilmeli.	- Veri kurtarma ekipleri görevlendirilmeli ve eğitilmeli.	- Veri bütünlüğünün sağlanması ve kayıp verilerin geri kazanılması.	Bilgi İşlem	- Kritik veriler için kriptolama kullanılmalı.
Elektrik Kesintisi	- Yedek güç kaynakları (UPS) ve jeneratörlerin düzenli bakımı yapılmalı.	- Acil durum güç ekipleri belirlenmeli ve eğitilmeli.	- Normal işleyişe dönüş süreci ve elektrik kesintisi sonrası sistem testleri.	Tesis Yönetimi	- Elektrik panoları düzenli olarak kontrol edilmeli.
Salgın Hastalık	- Sağlık hizmetleri için acil durum ekipleri oluşturulmalı ve planlar güncellenmeli.	- Sağlık hizmetleri sunan ekiplerin acil durum eğitimi yapılmalı.	- Sağlık hizmetlerinin devamlılığı ve topluluk sağlığının korunması.	Sağlık Hizmetleri Yönetimi	- Hijyen protokolleri düzenli olarak güncellenmeli.

İKİNCİ BÖLÜM

ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

2.1. EDMUND HUSSERL VE FENOMENOLOJİ

İnsanlar, son iki yüzyılda, yaşadıkları dünyayı ve kendilerini anlamlandırmak amacıyla, dünyanın işleyişinin her zaman mantıksal çıkarımlarla açıklanamayacağına ve daha derin, gizli bir işleyiş mantığının varlığına yönelik farkındalık geliştirmiştir. Bu bağlamda, dünyanın işleyişini anlamaya yönelik sabırlı ve detaylı incelemelerin önemi vurgulanmıştır. Ampirizm, bu dönemde baskın hale gelen bilimsel paradigmayı şekillendiren temel felsefi akım olarak öne çıkmıştır. Doğanın ve onun işleyişinin araştırılmasında kullanılan yöntemler, zamanla insanları ve insan davranışlarını incelemek için de uygulanmaya başlanmıştır. Ancak, insanın doğa ile etkileşim içinde olmasına rağmen, doğa bilimleri ile beşerî bilimlerin temel prensipleri arasında önemli farklılıklar bulunmaktadır. Bu çerçevede, psikolojinin inceleme konusu olan anılar, imgeler, bilinç ve halüsinasyonlar gibi birçok fenomen, ampirizmin ölçüm ve doğrulanabilirlik kriterlerini tam anlamıyla karşılamamaktadır. Bu eksikliğin giderilmesi noktasında fenomenoloji, önemli bir yaklaşım olarak devreye girmektedir. Fenomenoloji, bir şeyin gerçek olmaktan ziyade deneyimlenebilir olmasından hareketle, bilgi ya da verilen bir şeyin bilinçle olan ilişkisini açıklamak için kullanılabilir (Giorgi, 2009).

Fenomenoloji, diğer felsefi akımlardan farklı olarak bireylerin deneyimlerine, özellikle de bu deneyimlerin öznel boyutuna odaklanmaktadır. Bu yaklaşımıyla, bilginin duyular aracılığıyla elde edildiğini savunan ampirizm ve pozitivizm gibi felsefi akımlara eleştirel bir tutum sergilemektedir (Yener, 2012). Fenomenolojiye göre deneyimler, bireysel veya öznel olarak nitelendirilir. Fenomenoloji, deneyimlerin nesnel olmadığını savunur. Fenomenoloji, özne-nesne ilişkisini yeniden tanımlamaya çalışırken, insanın deneyimini anlamayı ve bu deneyimleri nasıl edindiklerini, nasıl geliştirebileceklerini açıklayabilmek için önemli bir fırsat sunan felsefe akımıdır (Uğuz & Tekindal, 2020). Bu akımın öncü isimlerinden biri Edmund Husserl'dir.

Fenomenoloji terimi ilk kez Edmund Husserl tarafından kullanılmamış olmakla birlikte, 20. yüzyılda yaşamış olan Husserl, fenomenolojinin kurucusu olarak kabul

edilmektedir (Koçak & Akbel, 2023). Fenomenoloji terimi ilk kez Johann Heinrich Lambert tarafından, Neues Organon adlı eserinde bir bölüm başlığı olarak kullanılmıştır (Moran, 2002).

Fenomenoloji isim kökü bakımından, Yunanca Phainomenon (Fenomen), görünüm veya olgu anlamına gelen bir terimdir (Bal, 2012). Fenomen kelimesi, Osmanlı felsefesinde 'başına olay gelmiş' anlamını taşıyan 'hadise' kelimesiyle ifade edilmiştir. Ancak bu terim, zaman zaman "gerçekleşmiş olan" anlamına gelen "vakıa" kelimesiyle karıştırılmaktadır (Hançerlioğlu, 2000). Fenomenoloji kavramı ikiye bölünecek olursa, Phainomenon ve logos kelimelerinin birleşiminden meydana gelmiş bir kavram olacağı çeşitli araştırmalara konu olmuştur (Hatab, 2013; Schrag, 2006). Fenomenolojinin alan yazında çeşitli tanımları bulunmaktadır. Bu tanımlardan birini yapan Gallagher, fenomenolojiyi insanların yaşamlarından elde ettikleri, anlık veya daha sonra özümseyerek ulaştıkları deneyimi anlamak için kullanılan bir felsefi yöntem olarak tanımlamıştır (Gallagher, 2022). Oxford learners sözlüğüne göre fenomenoloji, *"Dünya hakkında gerçek veya doğru olabilecek şeylerin aksine gördükleriniz, duyduklarınız, hissettikleriniz vb. ile ilgilenen felsefe dalı"* olarak tanımlanmaktadır (Oxford University Press, 2024).

Edmund Husserl, fenomenolojiyi, bilincin özünün bilimi olarak tanımlamaktadır (Husserl, 1975).

Edmund Husserl, çalışmalarıyla yalnızca felsefe tarihçiliği alanında değil, aynı zamanda 20. yüzyıl felsefesinin iki önemli geleneği olan analitik felsefe ve kıta felsefesinin gelişiminde de etkili bir rol oynamıştır (Hartimo, 2008). Logischen Untersuchungen-Mantık Araştırmaları, Fenomenoloji Üzerine Beş Ders gibi çalışmaları Edmund Husserl'in önemli eserlerindendir (Husserl vd., 1968; Smith, 2015). Kıta felsefesinin önemli bir isim olan Edmund Husserl, analitik alanında da çalışmalar gerçekleştirmiştir. Özellikle matematik alanında analitik çalışmalar gerçekleştirdiği bilinmektedir. Bu durum, Edmund Husserl'in erken dönem eserlerinde kendini göstermiştir. Erken dönem eserlerinin çoğunun matematik ve matematik felsefesi hakkında olduğu bilinmektedir. Değişkenler hesabı üzerine yaptığı çalışmayla doktora yapmıştır (Smith, 2019). Husserl, matematiği ve mantığı psikolojiden ayıran bir görüşe sahiptir. Bu bağlamda, matematiğin temel nesneleri olan simgesel sayılar, önermeler ve

tümellerin, psikolojizmin iddia ettiği gibi zihinsel durumlara indirgenemeyeceğini savunmuştur (Zack, 2019). Herhangi bir felsefe veya düşüncenin bilim statüsüne yükselebilmesi için Husserl' e göre bazı şartlar taşıması gerektiği bilinmektedir. "Kesin bir bilim olarak felsefe" adlı çalışmasında, bu şartlardan ilk olarak düşünce veya felsefenin nesnesini gösterebilme yetkinliğinin olmasının gerektiği, İkincisinin ise esaslı bir metodoloji ya da yönteme sahip olabilmesinin olduğu anlaşılmaktadır (Husserl, 2020). Fenomenolojiyi bu bağlamda değerlendirmek gerekirse, temel bilimlerden, nesnesi ve metoduyla ayrıldığı görülmektedir. Öznel fenomenal bilincin yaşam içerisinde uygunluk göstermesinin kategoriyle şemalandırılması, fenomenolojinin bilimsel metodolojisi için temel oluşturmaktadır. Bir kıta felsefesi alanı olan fenomenoloji, temelinde bireyin edinmiş olduğu deneyimi anlama ve açıklama çabasını içerir. Kıta felsefesine özgü olarak net ve kesin tanımlardan ziyade, kavramları daha soyut, eleştirel ve şiirsel bir dil aracılığıyla derinlemesine yorumlama eğilimi, fenomenolojinin de temel yapısında yer almakta ve insan deneyimlerini kapsamlı bir şekilde anlama ve açıklama amacı taşımaktadır (Saei, 2019). Bilinçte yer alan şey, bir nesne, bir kişi, ilişkilerin kompleks bir hali olarak ele alındığında, fenomenoloji, deneyimi yaşayan kişinin bakış açısından, o şeyi kişinin bilincindeki şekliyle açıklamaya çalışan bir felsefedir. Bu bağlamda, deneyimi yaşayan kişinin dışındaki bir objektif analize ihtiyaç duyulmaz; aksine, deneyimlenen şeyin, deneyimleyen kişi tarafından nasıl deneyimlendiği üzerinde odaklanılır. Bu yaklaşımın benimsenmesinin nedeni, hiçbir şeyin bilinç olmadan değerlendirilemeyeceği ve konuşulamayacağı anlayışıdır.

Fenomenoloji çalışmalarında, deneyimi yaşayan kişinin, yani fenomenin bilinç deneyimlerini incelerken ya da analiz ederken, tüm varsayımlardan, ön yargılardan ve dogmalardan uzaklaşılması 'epokhe'ye almak olarak adlandırılır (Walsh, 1988). Epokhe, Antik Yunan Septisizm'ine kökenleri dayanan bir terim olup, temel olarak bir yargının askıya alınması anlamına gelir (Parry, 2010).

Epokhe'ye almak, Husserl'in fenomenolojisinde, olaylara kesin yargılar vermektense, bilgilerin özüne odaklanarak alışılagelmiş ve sürekli ön planda tutulan doğal nesnelerin arka planda bırakılmasını gerektirir (Esen, 2015). Buna bağlı olarak, Husserl'in, bu yöntemi geliştirmesi, araştırmacıların sadece fenomenlerin özlerine odaklanabilmelerini ve bu özleri ön yargılardan uzak, saf bir şekilde inceleyebilmeleri olanağını doğurmuştur.

Sonuç olarak, Edmund Husserl'in fenomenolojisi, nesnelerin saf ve doğrudan gözlemiyle ilgilenerek, bu nesnelerin nasıl deneyimlendiğini anlamak için öznel deneyimleri inceler ve bilincin derinliklerine inerek nesneleri anlamaya çalışır. Fenomenolojinin amacı, şeylerin kendisinin öz yapısını anlamak olup, bunu yaparken varsayımları paranteze alarak veya imgesel çeşitleme yaparak deneyimin farklı varyasyonlarında sabit kalanları ya da değişenleri tespit etmekle mümkün olacaktır, olarak açıklanabilir. Paranteze alma ya da imgesel çeşitleme yapma süreci ise fenomenolojik indirgeme olarak adlandırılmaktadır (Gilstrap, 2007).

2.1.1. Teknoloji ve Fenomenoloji Arasında İlişki

İnsanoğlunun günlük yaşamında her zaman yeri olan teknoloji, çoğu zaman bir sürecin otomatikleştirilmesi veya hayatın idame ettirilmesi noktasında yardımcı bir alet olarak görülmektedir. Ayrıca bunun dışında teknolojinin çeşitli biçimlerde tanımlamaları da yapılmıştır. Bunlar;

Teknoloji, düşünceler, fikirler, yönetim, süreç ve makine insan organizasyonların birbirlerine entegre oldukları karmaşık, komplike bir yapıdır (Hoban, 1965). Bu tanıma göre teknolojinin insan ve makinelerle olan karmaşık ilişkisi sonucu geliştiğinin yapılan bilimsel araştırmalar sonucunda ortaya çıktığı sonucuna erişilirken, Alkan'a göre tüm yaşantılardan kazanımı gerçekleştirilmiş yeteneklerin kullanılmasıyla doğanın egemenliğine sahip olmak için gerekli, işlevsel yapıların oluşturulması teknoloji olarak tanımlanmaktadır (Alkan, 1998). Teknoloji, onu geliştiren, doğuran ve dahil olduğu ortamın ontolojisini algıda değiştiren, insanların yetersiz yeteneklerinin devamı ve becerileridir (Günay, 2017). Teknoloji, daha önceden belirlenmiş amaçlara ulaşmak için, belli sorunları çözmek amacıyla, gözlem ve kanıtlara dayalı bilgilerin kullanımı, uygulanmasıdır (Demirel, 1993). Bu tanımlamalara göre günümüzde genellikle makineler, yazılım ve sistemlerin oluşturduğu aletler ve elektronik cihazlar gibi somut bir şekilde ifade edilse de teknoloji, insan yaşamını kolaylaştıran, süreçleri iyileştiren veya yeni ürün ve hizmetler geliştirmek için kullanılan beceri, bilgi ve araçların bütünüdür.

Fenomenoloji ise, bir olay hakkında deneyime sahip fenomenleri ve deneyimlerini açıklamaya ve anlamaya çalışan felsefi ve psikolojik bir yaklaşımdır. Bir başka açıdan fenomenoloji, bilincin ve insan algının yapısını felsefi bir yaklaşımla inceler. Bu

bağlamda teknoloji insan yaşamını kolaylaştırmaya odaklanırken fenomenoloji deneyimlere odaklanır. Fenomenoloji ve teknoloji arasındaki ilişki karmaşık ve çok yönlüdür, fakat aralarındaki ilişkinin merkezine insan faktörü alındığında, teknoloji ve fenomenoloji arasındaki bağ daha derin bir anlam kazanır. Teknoloji ve fenomenoloji arasındaki ilişki bu iki kavramın birbirleri üzerindeki etkisiyle de değerlendirilebilir. İyi tasarlanmış bir teknoloji, insanların deneyimlerini geliştirebilir, farklı deneyimler edinmesinde kolaylık sağlayabilir. Aynı zamanda fenomenolojik bir bakış açısıyla incelendiğinde, teknolojinin merkezinde insan deneyimini ele almak, teknolojinin insan yaşamını nasıl değiştirdiğini ve anlamını nasıl etkilediğini kavrama noktasında yardımcı olur. Bu nedenle, fenomenoloji ve teknoloji arasındaki ilişkiyi anlamak için insan faktörünü merkeze almak önemlidir. İnsan faktörü, her iki kavram içinde hayati öneme sahiptir. Hem teknolojinin tasarımında, kullanımında hem de fenomenolojik deneyimin anlamında merkezi bir rol oynayan insan faktörü, bu iki kavram arasındaki derin ilişkinin açıklanmasındaki temel faktördür. Bu bağlamda, insan deneyimleri, teknolojinin geliştirilmesinde, teknolojik ürünün tasarımında, teknolojinin ihtiyaç analizinde ve ürün sonrası değerlendirmelerde önem arz etmektedir.

Holmberg ve Bilmes, yaptıkları çalışmada kitap, televizyon, telefon ve bilgisayar gibi teknolojik ortamlar ile insan deneyimi arasındaki ilişkiyi analiz etmek amacıyla McLuhan, Heidegger ve Foucault'un çalışmalarına dayanan teorik bir yol izlemiştir (Holmberg & Bilmes, 2004). Bu çalışmaya göre teknolojinin başlıca etkileri fiziksel değil, deneyimsel olarak değerlendirilmiştir. Bu değerlendirme çerçevesinde, fenomenolojik terminolojinin kullanılarak teknolojinin insan zihni üzerindeki etkilerinin tanımlanmasının faydalı olduğu sonucuna varılmıştır.

Fenomenoloji ve teknoloji deneyimlerin nasıl yapılandırıldığını ve anlamlandırıldığını inceleyebilir. Bu incelemeyi gerçekleştirirken fenomenoloji, bireylerin yaşadıkları dünyayı nasıl algıladıklarını ve nasıl deneyimlediklerini anlamak için iç görüler sunmaya çalışırken, teknoloji; kullanıcıların geliştirilmiş teknolojik araçlarla nasıl etkileşime geçerek deneyimlerini şekillendirdiğini ve deneyimler sonucunda elde edilen çıktıların anlamlarını nasıl oluşturduğunu gösterme cabasındadır. Bunun yanı sıra, her iki kavram da bireylerin çevreleriyle etkileşimini ve bağlantılarını vurgulamaktadır. Ancak, fenomenoloji felsefi bir yaklaşım ve metodoloji olarak insan deneyimini anlamaya odaklanırken, teknoloji daha çok pratik ve uygulamalı bir yaklaşım

benimseyerek, insanların günlük yaşamlarını kolaylaştırmak veya iyileştirmek amacıyla tasarlanmış ürün ve hizmetler sunmaya yönelmiştir.

Teknolojinin fenomenolojik bir bakış açısıyla incelenmesi, temelde teknolojinin insan deneyimini nasıl etkilediği, değiştirdiği, geliştirdiği veya zenginleştirdiği sorularına yanıt ararken, teknolojinin insan ile doğa arasındaki ilişkisini, insanların diğer insanlarla olan bağlarını ve bireyin kendisiyle olan ilişkisini nasıl dönüştürdüğünü ve bu süreçleri nasıl deneyimlediğini araştırmayı amaçlar. Bu bağlamda, örnek olarak, mobil cihaz teknolojisinin insanların bilgiye erişim biçimlerini nasıl etkilediği ve sosyal etkileşimlerini nasıl genişlettiği veya dönüştürdüğü üzerine fenomenolojik bir analiz yapılabilir. Fenomenolojinin teknolojiye bir araç olarak yaklaşması ise, insan deneyiminin zenginleştirilmesi, derinlemesine incelenmesi ve çeşitlendirilmesi gibi soruları gündeme getirmektedir. Bu durum, fenomenoloji ile teknoloji arasındaki ilişkinin, insan deneyimini anlamlandırmak, derinleştirmek, geliştirmek ve zenginleştirmek adına önemli bir fırsat sunduğunu ortaya koymaktadır. Ihde, yaptığı çalışmada fenomenolojinin post modern bağlamda teknolojiyle nasıl etkileşime girdiğini ve nasıl şekillendiğini araştırmıştır (Ihde, 1995). Aynı zamanda teknoloji ve fenomenoloji arasındaki ilişkiyi incelerken, modern ve post modern düşünce arasındaki etkileşimlere de odaklanmaktadır.

Fenomenoloji, deneyimlere ve bu deneyimlerin nasıl algılanıp, nasıl yorumlandığına odaklanırken, teknoloji ve BT felaket kurtarma planlarında insan faktörleri de bilincin rolünü önemli ölçüde etkilemektedir. Teknoloji kullanımında insanlar, bilinçli ya da bilinçsiz bir şekilde kararlar alırlar ve deneyimler elde ederler, olası bir felaket durumunda teknoloji kullanımından elde edilen deneyimler BT felaket kurtarma senaryolarında uygulamaya geçirilebilir. Buna ek olarak, afetleri azaltmaya yönelik teknoloji ve eğitim yoluyla afete yönelik insan bilincinin geliştirilmesi kullanılabilir (Varol, 2007). Bu bağlamda hem teknoloji ve fenomenoloji hem de BT felaket kurtarma süreçlerinin ortak noktalarından biri olarak bilincin rolü olduğu söylenebilir.

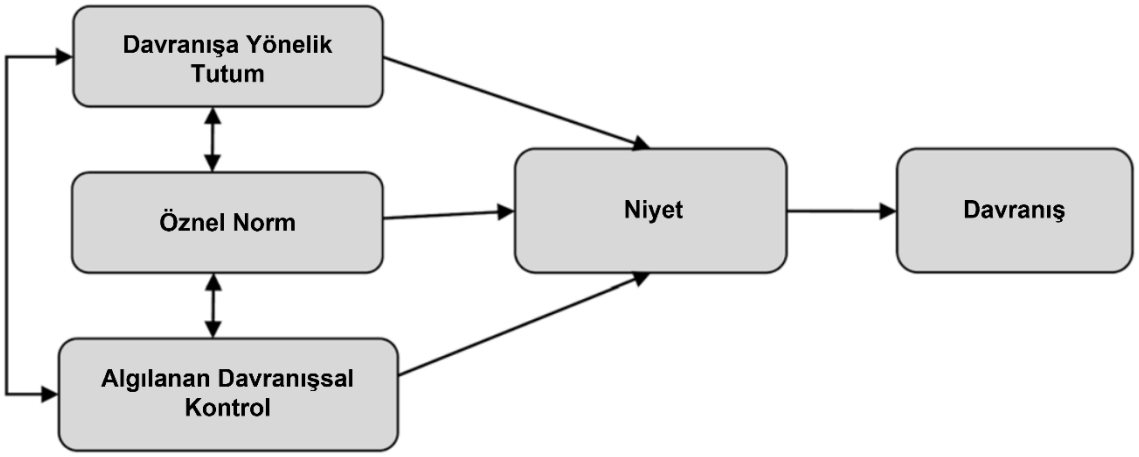
Sonuç olarak fenomenoloji ve teknoloji arasındaki ilişki çok yönlüdür. Bunun nedeni, her iki kavramın da insan deneyimini anlamak için farklı perspektifler sunmasıdır. Aralarındaki bu ilişki, insanın teknolojiyi nasıl deneyimlediğini ve nasıl algıladığını

anlamak için geniş bir çerçeve sunması ve aynı zamanda teknolojinin de insan deneyimini nasıl şekillendirdiğini anlamak için derinlemesine bir bakış açısı ve anlayış sağlamasıyla özetlenmektedir.

2.2. PLANLI DAVRANIŞ TEORİSİ

Bireylerin bir olay karşısındaki niyetlerini, davranışlarını, duygu ve düşüncelerini anlamaya yönelik çeşitli kuramlar ve teoriler bulunmaktadır. Bu teorilerden biri, Planlı Davranış Teorisi'dir. Bu teori, ilk kez 1975 yılında Fishbein ve Ajzen tarafından yapılan öncü çalışmalarla geliştirilmiş, ancak 1991 yılında Ajzen tarafından yeniden düzenlenerek güncellenmiş ve literatürdeki mevcut haliyle kullanılmaya başlanmıştır (Erten, 2002).

Planlı Davranış Teorisi'ne göre, bireylerin sosyal yaşamda bir davranışı gerçekleştirmeden önce, o davranışa yönelik niyetlerini, çeşitli etkileyicilerin kontrolü altında oluşturdukları ve bu niyetlerin davranışlarını şekillendirdiği öne sürülmektedir (Erten, 2002). Bu bağlamda, bireylerin bir eyleme geçme kararlarını belirleyen faktör, niyet olarak tanımlanır (Ajzen, 2005). Bununla birlikte Ajzen, eyleme geçme niyetini, üç temel yordayıcıya dayandırmaktadır: davranışa yönelik tutum, algılanan davranışsal kontrol ve öznel normlar (Ajzen, 2005).



Şekil 2.1. Planlı Davranış Teorisi (Ajzen, 1991).

Tutum, psikolojik bir eğilim olarak bireylerin bir durum karşısındaki olumlu ya da olumsuz değerlendirmeleridir (Eagly & Chaiken, 1993). Davranışsal tutum, bireyin belirli

bir davranışa yönelik olarak yaptığı olumlu ya da olumsuz değerlendirmelerin derecesiyle ifade edilen bir kavramdır (Ajzen, 2002). Tutumların, bireylerin davranışlarını etkilemesi beklenir. Ancak, bir bireyin bir eylemi gerçekleştirmeye karar vermesi veya bu eyleme geçmeye niyetlenmesi, genellikle tutumuna dayanır. Bununla birlikte, bazı durumlarda, bireyde bir eylemi gerçekleştirmeye yönelik olumlu bir tutum bulunmasına rağmen, kişinin ruhsal inançları, içinde bulunduğu şartlar veya diğer dışsal faktörler gibi çeşitli etmenler, bu tutumun niyete dönüşmesini engelleyebilir (Bagozzi vd., 1989).

Öznel normlar, bireyin bir davranışı yapma, eyleme geçirme veya yapmama konusunda hissettiği sosyal etkiyi ifade eder ve aynı zamanda davranışın toplumsal etkisini ifade etmek için kullanılır. Öznel normlar, etki altında bireyin belirli bir davranışı gerçekleştirip gerçekleştirmemesi gerektiği hakkındaki düşüncelerini şekillendirmektedir. Bu bağlamda, Planlı Davranış Teorisi'ne göre, bireylerin sosyal faktörlere bağlı olarak belirli bir davranışı benimseme ya da benimsememe konusundaki kararlarını etkileyen temel unsurlardan biri, hissettikleri öznel normlardır. Bu öznel normlar, bireylerin toplumda kabul edilen değerler ve normlara göre davranışlarını yönlendiren faktörlerdir (Ajzen, 1991, 2005; Armitage & Conner, 2001).

Algılanan davranışsal kontrol, bireyin belirli bir davranışı gerçekleştirme kabiliyetine dair kuvvetli hissi ya da sahip olduğu davranışı gerçekleştirme yeteneğine ait inanç ve güveni ifade eder (Mistry vd., 2015). Bu kontrol algısı, bireylerin davranışlarının her zaman doğru bir biçimde tahmin edilemez olduğunu ve değişkenlere bağlı olarak, çeşitli kısıtlamaların bulunduğunu vurgulamaktadır. Algılanan davranışsal kontrol, bireylerin eyleme geçme isteği veya motivasyonunu artırarak, davranışsal sonuçları öngörebilmelerini sağlıyorsa, bu kontrol değişkeni, hedefe ulaşma olasılığını davranışsal niyetten bağımsız olarak tahmin etmek için kullanılabilir. Bu çerçevede, algılanan davranışsal kontrol, bireylerin niyetlerinden bağımsız olarak hedefe yönelik başarıyı doğru bir şekilde yansıtabilir (Ajzen, 2005; Şaşmaz & Tengilimoğlu, 2024).

Niyet, bireyin bir davranışı gerçekleştirme çabası ve isteğini belirleyen, davranışın gerçekleştirilmesi için gereken olumlu ya da olumsuz motivasyonel faktörleri içeren bir kavramdır. Bireyin bir davranışı gerçekleştirme niyeti, o davranışı yapma konusundaki istekliliğini, sarf ettiği çabayı ve planladığı çabayı ortaya koymaktadır (Ajzen, 1991; Ho & Sae-Jong, 2017; Şaşmaz & Tengilimoğlu, 2024). Buna bağlı olarak, bireyin iradesi ve

bilinçli eylemleri doğrultusunda gerçekleşen davranışlarının yanı sıra, iradesi dışında çeşitli etmenlere bağlı olarak meydana gelen olaylar da Planlı Davranış Teorisi tarafından incelenmektedir (Özer vd., 2015). Felaket kurtarma planı oluşturma süreçlerinde, planın tamamı kadar, katılımcıların davranış niyetleri, risk algısı ve Planlı Davranış Teorisi ile Felaket Kurtarma Teorisi arasındaki ilişki de büyük bir öneme sahiptir.

2.2.1 Planlı Davranış Teorisi ve Felaket Kurtarma

Planlı Davranış Teorisi, temel olarak bir sosyal psikoloji kuramı olmasına rağmen, birçok farklı alanda insan davranışlarını açıklamak için kullanılan bir teoridir (Blue, 1995; Conner, 2020; Özer vd., 2015). Bu çalışmada ana araştırma yöntemi olarak kullanılmamasının nedeni, katılımcıların felaket anında gösterecekleri davranışları veya felaket planı oluşturma süreçlerindeki tutum ve niyetlerini değerlendirmeyi amaçlamamış olmamızdır. Planlı Davranış Teorisi, doğrudan felaket kurtarma süreçlerine uygulanabilir olup, felaket kurtarma hazırlık süreçlerinde bir davranış kategorisi olarak ele alınırsa, afet riskinin azaltılabileceği düşünülebilir (Prasetyo vd., 2020). Bu çalışmada Planlı Davranış Teorisi kullanılmıştır. Bu teori haricinde, BT felaket kurtarma planı hazırlama süreçlerinde başka bir teoriden faydalanılması da mümkün olacaktır. Örneğin, Sistem Teorisi, karmaşık sistemlerin yönetimi ve değişim süreçlerine odaklanarak, felaket kurtarma planlarının oluşturulması için etkili bir çerçeve sağlayabilir. Bu konu hakkında üniversiteler için felaket kurtarma planları hazırlama süreçleri basit ve etkili olmalıdır. Fakat sadece felaket kurtarma planı oluşturmak için karmaşık sistemlerin yönetimi ve değişim süreçleri üzerine odaklanan sistem teorisi bir alternatif olabilmektedir.

Planlı Davranış Teorisi, BT felaket kurtarma planlarıyla ilişkilendirilerek, planlama sürecinin ve niyet oluşturmanın kritik önemini vurgulamak amacıyla birlikte kullanılabilir. Bu sayede, kurumların kriz yönetimi süreçlerini anlamalarına ve yönetmelerine katkı sağlayacak bir bakış açısı kazandırılabilir. İnsan davranışlarının felakete hazırlık sürecinde, davranışsal kontrollerin algılanması, felaket anında ve sonrasında gösterilecek olan davranışsal niyetleri önemli ölçüde etkiler. Bu durum, kurumların felaket kurtarma hazırlık süreçlerini büyük ölçüde etkileyebilir. Najafi ve arkadaşlarının yaptığı bir araştırmaya göre felaket durumlarına hazırlıklı veya hazırlıksız bireyler arasında ciddi farklılıklar bulunduğu belirtilmiştir (Najafi vd., 2017). Buna bağlı olarak, kurumlar BT felaket kurtarma planlarını daha etkili bir biçimde hazırlamak ve

uygulamak için çalışanlarının güçlü niyetlere sahip olmalarını sağlamalıdırlar. Bir başka çalışmada, Zaman ve arkadaşları büyük veri analizi teknolojileri ve planlı davranış teorisi kullanılarak, gecikilmeden ve doğru kararlar almanın sağlanacağını savunmaktadırlar (Zaman vd., 2021). Planlı Davranış Teorisi ile BT felaket kurtarma teorilerinin birlikte kullanılması, kurum personeli, plan geliştiriciler ve planı uygulayacak bireylerin niyetlerini, kritik bir faktör olarak öne çıkarır. Bu bağlamda, öznel normlar ve algılanan davranışsal kontrol, BT felaket kurtarma planlamasının benimsenmesini ve planın etkinliğini artırabilir. Planlı Davranış Teorisi, BT felaket kurtarma planlarının önemli bileşenlerinden biri olan risk değerlendirme süreçlerinde etkin bir şekilde kullanılabilir. Bu teori, kurumların bütünsel risk değerlendirme stratejilerine dayalı olarak daha etkili kriz yönetim yaklaşımları geliştirmelerini sağlamaya yardımcı olabilir (Hagger vd., 2022).

Sonuç olarak, Planlı Davranış Teorisi ve BT felaket kurtarma planı geliştirme süreçleri, bir kurumun felaket anında ve sonrasında etkin bir şekilde toparlanmasını ve hizmetlerini sürdürebilmesini sağlayan önemli kavramlardır. Planlı Davranış Teorisi'nin sunduğu teorik altyapı üzerine inşa edilecek bir BT felaket kurtarma planı, başta üniversiteler olmak üzere kurumların iş sürekliliği ve BT felaketlerine karşı daha hazırlıklı olmalarına katkı sağlayacaktır. Bunun yanı sıra, bu ilişki kriz yönetimini etkileyecek çıktılar elde etmek amacıyla da kullanılabilir. Bu sayede kurumlar, beklenmedik olaylara karşı personel açısından daha dirençli hale gelir ve hızlı reaksiyon gösterme kapasitesine sahip olabilirler.

ÜÇÜNCÜ BÖLÜM

KAMU ÜNİVERSİTELERİNİN BT FELAKET KURTARMA PLANI GELİŞTİRME SÜREÇLERİNDE ETKİLİ TEMALARIN FENOMENOLOJİK DESENLE TESPİTİ

3.1. ARAŞTIRMANIN METODOLOJİSİ

BT felaket kurtarma planlarının geliştirilmesi, süreç içerisindeki çeşitlilik ve karmaşıklık nedeniyle yalnızca teknik veya prosedürel bir çerçeveyle ele alınamayacak kadar komplekstir. Kamu kurumlarının kendine özgü karmaşık yapıları ve sundukları hizmetlerin çeşitliliği, bu tür planların tek bir prosedür olarak uygulanabilirliğini sınırlamaktadır. Etkili bir felaket kurtarma planı oluşturmak için kurumun ihtiyaçları ve imkanları kesin bir biçimde belirlenmelidir. Bunun yanı sıra, kurum kültürü ve beklentileri göz önünde bulundurularak, planların sadece teknik ve prosedürel bir çerçeveyle ele alınamayacağı anlaşılmalıdır. Bu bağlamda, planın etkili bir şekilde geliştirilmesi için insan deneyimlerinin, algılarının ve psikolojik süreçlerinin derinlemesine anlaşılması gerekmektedir. Fenomenolojik bir yaklaşım, insan merkezli verilerin toplanması ve analiz edilmesi için son derece uygun bir metodolojik yaklaşımdır. Bu araştırmada fenomenolojik yaklaşımın kullanılmasının başlıca gerekçeleri, karmaşık süreçlerin insan merkezli yönünü ortaya çıkarmak, teoriyi gerçek dünya uygulamalarıyla ilişkilendirerek derinlemesine içgörüler sağlamak ve öznel deneyimlerin anlamlandırılarak diğer plan geliştiricilere sunulmasını sağlamaktır.

Fenomenolojik araştırmalar, bireylerin deneyimlerini ve bu deneyimlerin anlamlarını keşfetmeye odaklanır. Bu çalışmada kullanılan fenomenolojik yaklaşım metodolojisi ile, katılımcıların BT felaket kurtarma planı geliştirirken edindikleri deneyimlerin özüne ulaşmak hedeflenmiş ve yalnızca teknik süreçler değil, aynı zamanda bu süreçlerin katılımcılar üzerindeki etkileri de incelenmiştir. Böylece, daha bütünsel ve etkili sonuçlar elde edilmiştir.

Bu çalışmada katılımcıların seçiminde, deneyim sahibi olmaları özellikle dikkate alınmıştır. Katılımcıların deneyimlerinden doğru ve güvenilir verilerin toplanabilmesi için yarı yapılandırılmış derinlemesine görüşmeler gerçekleştirilmiştir. Görüşmeler

sonucunda elde edilen bulgular, uzman görüşlerine başvurularak temalaştırılmış ve tematik analiz yöntemi kullanılarak incelenmiştir. Bu süreçte, BT felaket kurtarma planı geliştirme sürecini olumlu ve olumsuz yönde etkileyen kodlar belirlenmiştir.

3.1.1. Araştırmanın Amacı ve Önemi

Bilişim teknolojilerinin hız kesmeden gelişmeye devam etmesi, bu teknolojilerin birçok bilim dalı ve gündelik yaşam süreçleri üzerinde etkili olmasına yol açmıştır (Ersöz & Özmen, 2020; Orhan & Genç, 2018). Felaket durumu, genellikle farkında olmadığımız ve zamanla günlük yaşamın ayrılmaz bir parçası haline gelmiş bir olgudur (Hawkins vd., 2000). Felaket durumu söz konusu olduğunda, özellikle kritik altyapıların, felaket öncesinde sağladıkları hizmetleri en kısa sürede, doğrudan ya da alternatif yollarla yeniden sunabilmesi büyük önem taşımaktadır (Bach vd., 2013; Genco, 2020). Seo ve arkadaşlarına göre, kritik bir bilişim teknolojileri sisteminin hizmet veremez hale gelmesinin olumsuz maliyeti, ilgili kuruluşa günlük operasyonel kapasitesinin %50'sine kadar bir kayıp olarak yansıyabilmektedir (Seo vd., 2022). Buna bağlı olarak, BT felaket kurtarma planının gerekliliği açık bir şekilde anlaşılmalı ve önemle dikkate alınmalıdır (Alhazmi & Malaiya, 2013; Özdemir & Gökgöz, 2018).

Fenomenoloji günlük yaşamda farkında olduğumuz fakat ayrıntılı ve derin bir bakış açısına sahip olmadığımız olgulara odaklanan bir yaklaşımdır (Tekindal & Arsu, 2020). Olası felaketlerin yıkıcı sonuçlarını ortadan kaldırmak veya en aza indirmek amacıyla, teorik ve pratik çalışmalarda deneyim sahibi bireylerin verdikleri geri dönüşler ve deneyimlerine dair bulgular, günümüz BT hizmetlerinin geliştirilmesinde önemli bir rol oynamaktadır. Bu bağlamda, gerçekleştirilen bu çalışmada fenomenolojik bir tasarım tercih edilmiştir. Fenomenolojik tasarımın aşamaları sırasıyla şu şekilde izlenmiştir: olguyu tanımlama, olguya ilişkin ayrıntılı bir açıklama geliştirme, görüşmeler yoluyla katılımcılardan veri toplama, verilerin tematik analiz yoluyla incelenmesi, BT felaket kurtarma planını etkileyen faktörlerle ilgili temalar geliştirilmesi ve nihayetinde sonuçların sunulması. Bu çalışmadan elde edilen bulgular, kamu üniversitelerinin BT felaket kurtarma planlarını geliştirmeleri ve felaket kurtarma bilincini artırmaları için öneriler sunmayı amaçlamaktadır. Buna ek olarak, bu çalışmada, katılımcıların deneyimlerinden yararlanarak bir BT felaket kurtarma planı geliştirmeye yönelik stratejileri belirlemek için fenomenolojik bir yaklaşım benimsenmiştir. Görüşmelerde

katılımcıların bu deneyimleri nasıl anladıklarına dair içgörüler edinmeleri üzerine yapılan çıkarımlar, çalışmanın başlıca amacını yansıtmaktadır.

Yaşanmış veya yaşanması muhtemel felaketlerin tam olarak tahmin edilememesi ya da tahmin süreçlerinin zorlukları, yaşamın birçok alanında felaket durumları ve sonrasında gerçekleştirilecek eylemler için planlar oluşturulmasını gerekli kılmaktadır. Bu bağlamda, özellikle eğitim kurumlarından biri olan üniversitelerin, kritik altyapılarından biri haline gelen bilgi teknolojileri için felaket kurtarma planlarını geliştirmeye yönelik stratejiler belirlemeleri büyük önem taşımaktadır. Felaket, genellikle kritik iş fonksiyonlarında aksamalara neden olan olumsuz bir olay olarak tanımlanabilir. Bilgi teknolojilerinin üniversiteler başta olmak üzere birçok alanda kesintisiz bir şekilde büyümeye devam etmesi, bu kaynakların yönetimini ve güvenliğini zorunlu kılmakta, dolayısıyla felaket kurtarma planlaması bir gereklilik halini almaktadır (Fallara, 2004). Buna bağlı olarak, bilgi teknolojileri felaket kurtarma planı geliştirmeye yönelik belirlenen stratejilere katkı sağlayacak değerli bilgilerin sunulması, bu tez çalışmasının önemini vurgulamaktadır. Buna ek olarak, bu tez çalışmasında, kamu üniversitelerinin felaket durumuna hazırlıklarını daha iyi anlayabilmeleri ve yaygın hatalardan kaçınabilmeleri amacıyla stratejiler edinmeleri hedeflenmektedir. Çalışmada kullanılan araştırma yöntemleri ve elde edilen sonuçlar, literatüre katkı sağlamakla kalmayıp, aynı zamanda BT yöneticileri için bir rehber niteliği taşıyacak şekilde şekillendirilmiştir.

Bu çalışmanın temelini oluşturan araştırma sorusu; Kamu üniversitelerinin iş sürekliliğini sağlamak amacıyla bilgi teknolojileri felaket kurtarma planlarını geliştirme sürecinde, deneyim sahibi uzmanların bu süreçle ilgili yaşadıkları deneyimler ve bu deneyimlerden türetilen stratejik yaklaşımlar nasıl şekillenmektedir? olmuştur. Bu çalışmada, yarı yapılandırılmış görüşmelerde kullanılan açık uçlu sorular aracılığıyla, araştırma sorusuna yanıt aranmaya çalışılmıştır.

3.1.2. Evren ve Örneklem

Fenomenolojik çalışmalarda, katılımcı grubunun homojen bir dağılım temelinde seçilmesi önemlidir. Buna ek olarak, katılımcıların incelenen fenomenle ilgili deneyime dayalı bir perspektife sahip olmaları gerekmektedir (Larkin vd., 2019). Örneklemin belirli bir fenomeni yaşamış, deneyim sahibi bir gruptan oluşturulması, bu çalışmanın

geçerliliğini güvence altına alırken aynı zamanda fenomeni yaşamış grup hakkında daha ayrıntılı bilgi edinme ihtimalini de arttırmaktadır (Frechette vd., 2020). J. A. Smith ve arkadaşları, örneklem büyüklüğünün belirlenmesinde mutlak bir doğru yanıtın olmadığını ileri sürmüşlerdir (Smith vd., 1999). Deneyim odaklı nitel çalışmalarda, ideal katılımcı sayısı genellikle 12-15 arasında önerilmekle birlikte, yorumlayıcı fenomenoloji veya hermenötik çalışmalar için bu sayı 5-10 katılımcı olarak belirtilmektedir (Larsen & Adu, 2021; Pietkiewicz & Smith, 2014). Bu doğrultuda, çalışmanın nihai örneklem boyutunun belirlenmesinde nitel bir yaklaşım benimsenmiş ve olasılıksız örnekleme yöntemlerinden biri olan amaçlı örnekleme tercih edilmiştir. Ancak, evrenin daraltılması genelleme imkânlarının sınırlanmasına yol açabileceğinden, örnekleme dahil edilecek katılımcıların seçiminde kamu üniversitelerinin tamamının kapsanması ve katılımcı homojenliğinin sağlanması hedeflenmiştir. Bu amaçla, Türkiye'nin farklı illerindeki kamu üniversitelerinde çeşitli görevlerde BT hizmetinde çalışan ve belirlenen katılımcı kriterlerine uygun 10 kişi örnekleme dahil edilmiştir. Katılımcıların belirlenmesinde amaçlı örnekleme yönteminin tercih edilmesinin iki temel nedeni bulunmaktadır. Birinci neden, kamu üniversitelerinde felaket kurtarma planı geliştirme deneyimine sahip olunmasıdır. İkinci neden ise katılımcıların, 6 Şubat 2023 tarihinde Kahramanmaraş merkezli ve on bir ilimizi etkileyen deprem gibi doğal afetler veya siber saldırılar gibi BT felaketlerini yaşamış ya da bu tür felaketlerin ardından ilgili üniversitelere kardeş üniversite kapsamında destek sağlamış olmalarıdır. Katılımcıların kimlik bilgilerinin gizliliğini korumak amacıyla, her birine K1, K2, K3, K4, K5, K6, K7, K8, K9 ve K10 şeklinde kodlamalar yapılmıştır.

Bu çalışmanın evreni, Türkiye'deki tüm kamu üniversitelerinde felaket kurtarma ile ilgilenen BT personelinden oluşmaktadır. Ancak, örneklem, on farklı üniversiteden seçilen BT personeli ile sınırlandırılmıştır. Örnekleme dahil edilecek personelin seçimi aşağıdaki kriterlere göre yapılmıştır:

- 18 yaşından büyük olmak,
- Kamu üniversitelerinde BT alanında çalışmış olmak,
- BT felaket kurtarma planlaması hakkında en az üç yıl veya daha fazla deneyime sahip olmak.

3.1.3. Veri Toplama Yöntemi ve Aracı

Bu çalışmada nitel araştırma yöntemi benimsenmiş ve fenomenolojik yaklaşım kullanılarak kamu üniversitelerinde Bilgi Teknolojileri felaket kurtarma planlamasının değerlendirilmesi gerçekleştirilmiştir.

Nitel araştırmalarda, her bir olay veya olgu kendi bağlamı içinde titizlikle ele alınır ve değerlendirilir. Bu tür çalışmalarda, evrensel genelleme yapma amacı güdülmez; bunun yerine, araştırmanın odaklandığı bireylerin veya olayların derinlemesine incelenmesi hedeflenir. Bu yaklaşımla, her bir durumun kendine özgü özellikleri ve iç dinamikleri anlamlandırılarak, daha zengin ve kapsamlı bir perspektif sunulması amaçlanır (Özdemir, 2010).

Fenomenolojik yaklaşımla analiz edilen çalışmalarda, veri toplama yöntemi olarak genellikle yarı yapılandırılmış bireysel görüşmeler, diğer bir ifadeyle yarı yapılandırılmış görüşme formları tercih edilmektedir (Larkin & Thompson, 2011; Smith vd., 2021). Fenomenolojik çalışmalarda derinlemesine görüşmeler gerçekleştirebilmek için, soruların açık uçlu olması ve herhangi bir varsayım içermemesi gerekmektedir. Aynı zamanda, katılımcılara yöneltilen soruların tarafsız olması ve katılımcıları yönlendirmemesi önem taşımaktadır (Dinçer vd., 2023).

Bu çalışmada da verilerin toplanması aşamasında yarı yapılandırılmış görüşme formu kullanılmıştır. Görüşmeler, kamu üniversitelerinde felaket kurtarma planı hazırlama konusunda deneyime sahip BT çalışanlarıyla gerçekleştirilmiştir. Görüşmeler, yüz yüze yöntemle yapılmış; ayrıca, web tabanlı (online-çevrimiçi) platformlar üzerinden de katılımcılara ulaşılmıştır. Kullanılan yarı yapılandırılmış görüşme formu Ek 1'de sunulmaktadır.

3.1.4. Verilerin Analizi

Bu çalışmada, verilerin temalarını, ilişkilerini ve örüntülerini belirlemek amacıyla nitel veri toplama yöntemi uygulanmış ve tematik analiz yöntemi kullanılmıştır.

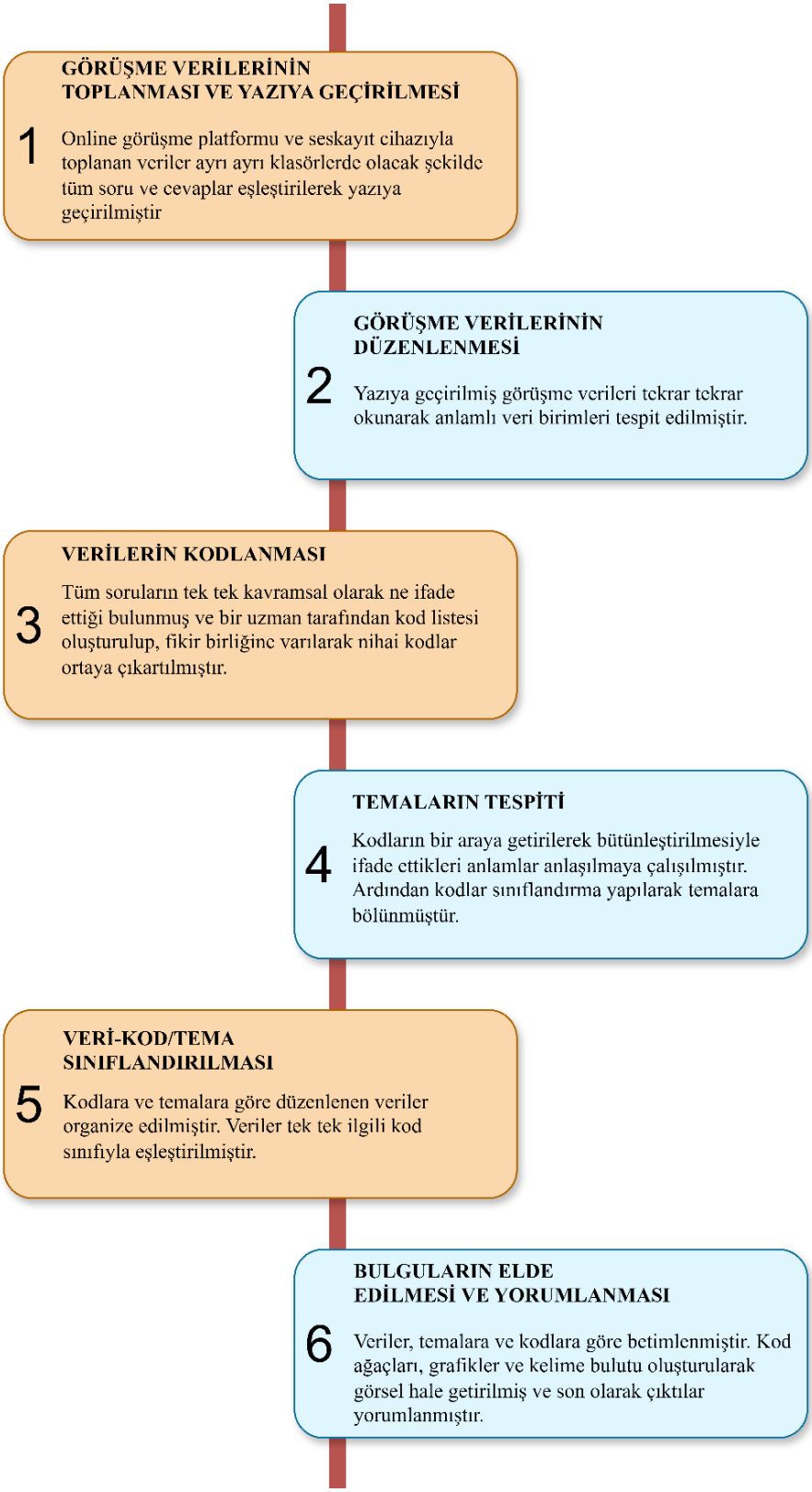
Tematik analiz, özellikle psikoloji alanında yaygın olmakla birlikte, son yıllarda farklı disiplinlerde de kullanım alanı bulan, sınırları tam olarak belirlenmemiş bir nitel analiz yöntemidir (Boyatzis, 1998). Lochmiller'e göre, esnek bir metodoloji olan tematik

analiz, yapılandırılmamış verilerden deneyim ve iç görü elde etmeye odaklanır. Aynı zamanda, bu yöntemle toplanan veriler kolaylıkla geniş temalar altında gruplandırılabilir (Lochmiller, 2021).

Nitel araştırmalarda, veri kavramı ve bu kavramın araçları sıkça sorgulanmaktadır. Ancak görüşme, birçok çalışmada temel bir veri toplama aracı olarak kullanılmaktadır (Koro vd., 2018; Polat, 2022).

Bu çalışmada, katılımcılarla yapılan yarı yapılandırılmış mülakatlarda kullanılan görüşme formu aracılığıyla elde edilen veriler, MAXQDA 2024 yazılımı kullanılarak analiz edilmiştir. Bu çalışmanın analiz sürecinde, toplanan verilerin anlamlandırılması, kavramsallaştırılması, soyut kavramlar altında gruplandırılması ve mantıksal bir düzen içerisinde anlamlı bir şekilde organize edilmesi hedeflenmiştir. Bu süreçte, tekrarlayan temaların, örüntülerin ve anlamların belirlenmesi, verilerde gizli olan bağlantıların ortaya çıkarılması ve önemli bilgilerin saptanması amaçlanmıştır. Tüm bu hedefler doğrultusunda, verilerin içeriğini anlamak ve yorumlamak için güçlü bir araç olan tematik analizin uygulanması uygun görülmüştür (Braun & Clarke, 2019; Kaldırım & Tavşanlı, 2020; Özmen, 2021). Tematik analiz metodolojisi, bu çalışmadaki araştırma sorusunu yanıtlamak ve katılımcıların BT felaket kurtarma planları oluşturma konusundaki deneyimlerini, algılarını ve görüşlerini incelemek için de uygun bir yöntem olarak tercih edilmiştir.

Bu çalışmada kullanılan tematik analiz yönteminde, verilerin analiz edilmesi için altı adımlı bir yaklaşım kullanılmıştır. Şekil 3.1'de çalışmada kullanılan tematik analizde izlenen aşamalar ayrıntılı bir biçimde sunulmuştur.



Şekil 3.1. Nitel Veri Analizinde İzlenen Aşamalar.

3.1.5. Araştırmanın Sınırlılıkları

Bir çalışmada sınırlılıklar, olası zayıflıkları ele alarak bulguları doğrudan veya dolaylı olarak etkileyebilecek unsurları ifade etmektedir (Theofanidis & Fountouki, 2018). Bu çalışmanın sınırlılıklarından ilki, metodolojisine dayanmaktadır. Nitel araştırmaların doğası gereği, elde edilen verilerin anlam bakımından zengin ve derin olması çalışmanın güçlü yanlarından biri olsa da, deneyim sahibi küçük bir grupla çalışılma zorunluluğu, bulguların genelleme yeteneğini sınırlayabilir (Blundell, 2015). Katılımcıların deneyim sahibi olmaları, elde edilen verilerin doğruluğunu ve çalışmanın güvenilirliğini artırmakla birlikte, görüşme sürecinde katılımcıların belirli sorulara karşı önyargılı davranma olasılığı, çalışmanın kısıtlarından biri olarak değerlendirilmektedir. Bu kısıtın etkisini azaltmak amacıyla, katılımcıların yanıtlarını anonim olarak iletmeleri önerilmiş ve bu uygulamanın önyargı olasılığını düşürmede etkili olabileceği vurgulanmıştır (Braun vd., 2021).

Nitel çalışmalarda genellemeler, elde edilen bulguların farklı koşullarda veya farklı durumlarda aynı sonuçları sağlayıp sağlamayacağına ilişkin bir değerlendirme yapmayı amaçlamaktadır (Büyüköztürk vd., 2014). Bu tür çalışmalarda katılımcılardan elde edilen veriler, araştırma bulgularını genelleme yeteneğinden yoksun olabilir ve bu durum çalışmanın kalitesini düşürebilmektedir (Fisher vd., 2018). Bu bağlamda, bu araştırmanın kısıtlarından biri olan genellenebilirliği sağlamak adına, araştırma evrenini temsil edebilecek bir örneklem oluşturmak amacıyla katılımcılar, bu konuda deneyim sahibi kişiler arasından titizlikle seçilmiştir. Nitel çalışmaların doğası gereği, elde edilen sonuçların nicel çalışmalardaki gibi matematiksel doğrulamalara tabi tutulamaması, bu tür çalışmaların kısıtlarından biri olarak değerlendirilmektedir (Büyüköztürk vd., 2014). Fenomenolojik desenle yürütülen bu çalışmada, nihai bulgular sübjektif olup, görüş ve yargılara dayalıdır. Bu nedenle, elde edilen bulgular, bu çalışmada matematiksel doğrulamanın neredeyse imkânsız hale gelmesine neden olmaktadır. Buna ek olarak, katılımcıların duygu durumları, düşünceleri ve deneyimlerinin farklılık göstermesi, çalışmanın tekrarlanabilir sonuçlar üretmesini güçleştirmektedir. Bu durum, bu çalışmanın önemli kısıtlarından biri olarak görülmektedir.

Felaket kurtarma planı geliştirme, maliyet açısından birçok kamu üniversitesi için ağır bir yükümlülük olarak değerlendirilebilir. Kamu kurumlarının farklı mali kaynaklara sahip olması, bu ve benzeri çalışmaların çıktılarında yer alan bulgular doğrultusunda felaket kurtarma planlarının geliştirilmesini olumsuz etkileyebilmektedir. Bu durum, çalışmanın nihai hedeflerine ulaşmasında, kullanılan sübjektif görüşlerin ifade edilmesi sırasında örtük bir manipülasyon riski oluşturabilir ve bu da çalışmanın sınırlılıkları arasında yer almaktadır.

3.1.6. Araştırmanın Varsayımları

Bilimsel araştırmalarda, bir araştırmacı tarafından kanıtlar olmadan bile doğru olduğunu varsaydığı, incelenmemiş inançlarına varsayım denilmektedir (Gurbetoğlu, 2018). Bu çalışmada, çalışmanın geçerliliği ve güvenirliliğini sağlamak için çeşitli varsayımlar vardır. Araştırmacıların, çalışmalarında araştırma problemlerini çözmelerine kolaylık sağlamaları amacıyla varsayımlarda bulunmaları gerekmektedir (McKoy, 2021). Bu bağlamda, sosyal bilimler alanındaki çalışmalarda, araştırmacılar, olaylara ilişkin bazı ön değerlendirmeler yapabilir veya belirli varsayımlarda bulunma gerekliliği hissedebilirler (Baloğlu, 2005).

Bu çalışmada benimsenen ilk varsayım, katılımcıların özelliklerine yöneliktir. Çalışmaya dahil edilen katılımcılar titizlikle seçilmiş olmakla birlikte, bu kişilerin BT felaket kurtarma planlaması ve süreçlerine aşina oldukları ve bu konuda yeterli deneyime sahip oldukları varsayılmıştır. Çalışmadaki ikinci varsayım, katılımcıların verdikleri yanıtların tarafsız ve samimi olduğu yönündedir. Çalışma süresince, katılımcıların kimliklerini, çalıştıkları kurumları ve kullandıkları çözümleri ifşa etmemeleri için anonimlik ilkesi gözetilmiştir. Bu yaklaşım, veri toplama sürecinde hassas sorulardan kaçınılmasını sağlamış, aynı zamanda kişisel, tanımlanabilir veya manipüle edilmiş verilerin toplanmasını engellemiştir. Bu yöntem sayesinde, katılımcıların sorulara samimi, tarafsız ve doğru yanıt verme olasılıklarının artırıldığı değerlendirilmektedir.

3.2. ARAŞTIRMANIN BULGULARI

Araştırma kapsamında toplanan verilerin analizi sonucunda elde edilen bulgular, ilgili konulara açıklık getirecek şekilde alt başlıklar halinde sunulmuştur.

3.2.1. Katılımcılara İlişkin Demografik Bulgular

Katılımcılardan görüşme başlangıcında yaş, eğitim düzeyleri ve çalıştıkları kurumlardaki görevleri hakkında demografik bilgiler toplanmış ve bu verilere betimleyici istatistikler uygulanmıştır. Sonuçlar, Tablo 3.1'de sunulmuştur.

Tablo 3.1. Katılımcı Demografik Bilgileri.

Demografik Bilgi	Gruplar	N	%
Yaş	30-39	3	30.0
	40-49	5	50.0
	50 ve üzeri	2	20.0
Eğitim Seviyesi	Lise	1	10.0
	Ön Lisans	1	10.0
	Lisans	6	60.0
	Lisansüstü	2	20.0
Kurumdaki Görev Tanımı	Ağ ve/veya Sistem Uzmanı	3	30.0
	Grup veya Birim Sorumlusu	3	30.0
	Memur veya Çözümleyici	2	20.0
	Daire Başkanı	1	10.0
	Diğer	1	10.0

Tablo 3.1 incelendiğinde, katılımcıların yaş dağılımında çoğunluğun 40-49 yaş aralığında olduğu (N=5) görülmektedir. Eğitim seviyesi açısından, katılımcıların çoğunluğunu Lisans mezunları oluştururken (N=6), en az katılımın Ön Lisans ve Lise mezunları arasında olduğu (N=1) tespit edilmiştir. Kurumdaki görev tanımları açısından ise Ağ ve/veya Sistem Uzmanları (N=3) ile Grup veya Birim Sorumlularının (N=3) çoğunlukta olduğu belirlenmiştir.

Demografik bilgilerin yanı sıra, katılımcılara felaket kurtarma planlamasında kaç yıllık tecrübeye sahip oldukları sorulmuş ve analiz sonuçları Tablo 3.2'de sunulmuştur.

Tablo 3.2. Katılımcıların Felaket Kurtarma Planlaması Hakkında Tecrübe Yılları.

Felaket kurtarma planlamasında tecrübe yılı	N	%
3-5	3	30.0
6-8	3	30.0
9-11	2	20.0
12 yıl ve üzeri	2	20.0

Tablo 3.2 incelendiğinde, katılımcıların %60'ının 9 yıldan az felaket kurtarma planı geliştirme tecrübesine sahip oldukları görülmektedir.

3.2.2. Güncel Bir BT Felaket Kurtarma Planına Sahip Olunmasına Yönelik Bulgular

Katılımcılara görüşme sürecinde yöneltilen *"Kurumunuzda BT felaket kurtarma planı var mı? Varsa sıklıkla güncellenmekte midir?"* sorusuna verilen cevaplar Tablo 3.3'te sunulmuştur. Bu cevaplara göre, katılımcıların tamamının bir BT felaket kurtarma planına sahip olduğu belirlenmiştir. Aynı soruya verilen yanıtlar doğrultusunda, katılımcıların güncel bir plana sahip olup olmadıklarına ilişkin analiz sonuçları ise Tablo 3.4'te yer almaktadır.

Tablo 3.3. Katılımcı Güncel BT Felaket Kurtarma Planına Sahiplik Sonuçları.

Katılımcı	Cevabı	Plana Sahiplik
K1	*"Kurumumuzda BT felaket kurtarma planı var. Yaklaşık 2 yılda bir güncellenmekte, yenilenmekte."*	Plan var
K2	*"Kurumumuzda bilgi teknolojileri, felaket kurtarma planımız mevcuttur. Planın genel hatları sabit kalmakla birlikte 3 ayda bir toplantı yapmaktayız…"*	Plan var
K3	*"Daire Başkanlığımıza ait bir plan var. Hastane hizmeti verdiğimiz için yıl içerisinde çeşitli denetlemelerimiz oluyor. Denetlemeler öncesi planlar gözden geçiriliyor varsa eksiklikler ya da güncellemeler yapılıyor."*	Plan var

Tablo 3.3. (Devamı)

Katılımcı	Cevabı	Plana Sahiplik
K4	*Kurumumuzda bir felaket kurtarma planı var ama öyle özel bir felaketten kurtarma planı olmayıp; anasistem odasının küçük bir versiyonu … FKM'nin dolayısıyla planın güncellemeleri her yıl yapılmaktadır.*	Plan var
K5	*"BT Felaket kurtarma planımız var, planın tamamı değil ama yedekleme planı gibi alt başlıkları sık sık güncellenmektedir."*	Plan var
K6	*"Halihazırda kullandığımız bir kurtarma planımız var. Daha geçen sene yaptık yani güncel, kapasitemizin artmasına göre planı güncelleyeceğiz."*	Plan var
K7	*"Evet, kurumumuzda bir BT felaket kurtarma planı bulunmakta. Plan sürekli güncellenmekte…"*	Plan var
K8	*"Kurumumuzda felaket kurtarma planı var fakat sürekli güncellenmiyor."*	Plan var
K9	*"Evet, kurumumuzda bir BT felaket kurtarma planı mevcuttur. Ancak, son birkaç yıldır planın kapsamı ve içeriği güncellenmemiştir."*	Plan var
K10	*"Planımız var, 4 yılda bir defa güncellendi."*	Plan var

Tablo 3.4. Kurumların BT Felaket Kurtarma Planı Güncelleme Sıklığı.

BT Felaket kurtarma planı güncelleme sıklığı	N	%
1 yıl ve 1 yıldan daha az sürede güncelleme yapanlar	6	60.0
1 yıldan daha fazla sürede güncelleme yapanlar	4	40.0

Tablo 3.4 incelendiğinde, katılımcıların %60'ının 1 yıl veya daha az süre içerisinde felaket kurtarma planlarını güncelledikleri görülmektedir.

3.2.3. Görüşme Analizi Bulguları

Katılımcılarla, BT felaket kurtarma planlarını oluştururken edindikleri deneyimleri ve planı etkileyen faktörleri ortaya çıkartmak için yapılan 7 soruluk yarı yapılandırılmış görüşme yapılmıştır. Sonrasında, toplanan katılımcı cevapları tematik analiz yapılarak

incelenmiş ve 6 adet tema ve 40 adet alt tema oluşturulmuştur. Bu çalışmadaki alt temalar aynı zamanda alt kodlar olarak değerlendirilmektedir. Tema ve alt kodlara yönelik oluşturulan kod ilişkileri ve katılımcı görüşleri sırasıyla bu başlık altında sunulacaktır. Temalara ilişkin kısaltmalar ve tema isimleri Tablo 3.5'de sunulmuştur. Katılımcıların BT felaket kurtarma planı oluştururken etkilendikleri başlıca faktörlere bakıldığında ekonomik faktörler, eğitim faktörleri, çevresel faktörler, teknolojik faktörler, sosyal faktörler ve idari faktörlerin olduğu görülmektedir.

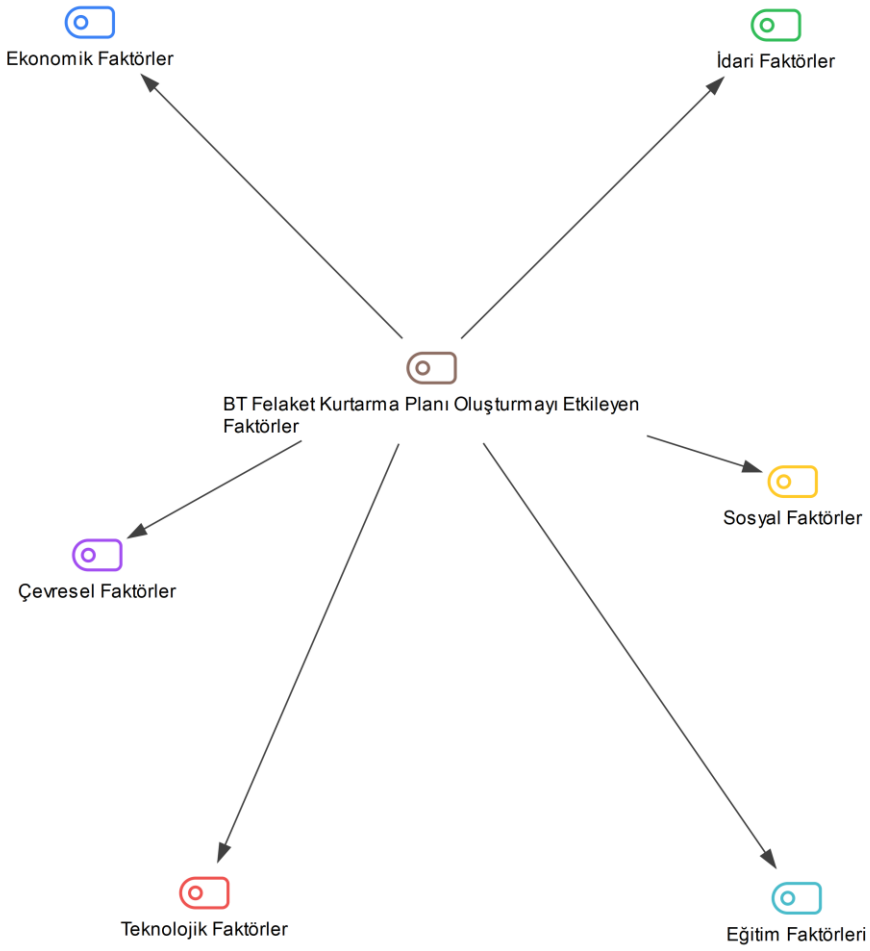
Tablo 3.5. Temalara İlişkin Kısaltmalar ve Tema İsimleri.

Kısaltma		Temanın Adı
T1		**Ekonomik Faktörler**
	T1K1	Hedef maliyetin tahsis edilen maliyetlerden yüksekliği
	T1K2	Yeterli bütçe temininin yapılamaması
	T1K3	Plan için yüksek bütçeye sahip olabilmek
	T1K4	Öngörülemez maliyetlerin karşılanabilir olamaması
	T1K5	Öngörülemez maliyetlerin karşılanabilir olması
	T1K6	Yasal gerekçelerle bütçe kısıtlamaları
	T1K7	Kriz durumunda ekonomik zorluklar
T2		**Eğitim Faktörleri**
	T2K1	Plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin sağlanması
	T2K2	Yöneticilerin plan hakkında bilgi eksikliği
	T2K3	Deneyimli ekip üyelerine sahip olma
	T2K4	Felaket psikolojisinin üstesinden gelebilecek eğitime sahip olmak
	T2K5	Çalışanların eğitim eksiklikleri
	T2K6	Plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin eksikliği
T3		**Çevresel Faktörler**
	T3K1	Yasal zorunluluklara uyma gerekliliği
	T3K2	Doğal afetlere karşı ön hazırlık
	T3K3	Kriz durumlarında ürün tedariği sorunları
	T3K4	Dış kaynaklı hizmetlere sahip olmak
T4		**Teknolojik Faktörler**
	T4K1	Güncel ve teknolojik yeterlilikte bir plana sahip olmak
	T4K2	Mevcut altyapının esneksizliği

Tablo 3.5. (Devamı)

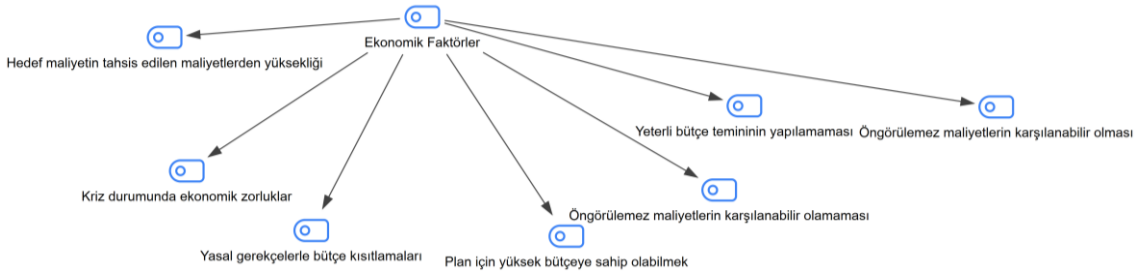
Kısaltma		Temanın Adı
	T4K3	Eski ve zayıf altyapının getirdiği zorluklar
	T4K4	Siber güvenlik önlemlerine sahip olmak
	T4K5	Güncel ve teknolojik yeterlilikteki bir plana sahip olamamak
	T4K6	Beklenmedik teknolojik zorluklar
	T4K7	Siber güvenlik önlemleri eksiklikleri
	T4K8	Kesintisiz iletişim altyapısına sahip olmak
	T4K9	Yeni ve yeterli altyapıya sahip olmak
T5		**Sosyal Faktörler**
	T5K1	İş birliği
	T5K2	Kritik kamu hizmeti sunmak
	T5K3	Farkındalık ve kültürel hazırlık eksiklikleri
	T5K4	Yeniliğe karşı direnç
	T5K5	Diğer üniversite personellerinden takdir beklentisi
	T5K6	İtibar beklentilerinin karşılanması
T6		**İdari Faktörler**
	T6K1	Yönetim desteği ve taahhüdü
	T6K2	Öngörü sahibi olma avantajı
	T6K3	Sürekli ve kesintisiz hizmet altyapısına sahip olmak isteği
	T6K4	Nitelikli personel eksikliği
	T6K5	Bürokrasi ve karar alma zorlukları
	T6K6	Belirsizlik ve öngörü eksiklikleri
	T6K7	Personel değişiklikleri sorunları
	T6K8	Kurumsal direnç ve değişim yönetimi sorunları

10 adet katılımcıya ait BT felaket kurtarma planı oluşturma ve hayata geçirme süreci ile ilgili görüşme formları ayrıntılı bir şekilde okunmuş ve uzmanların fikir birliği sonucunda oluşturulan temalar Şekil 3.2'de sunulmuştur. Ayrıca ek 2'de ayrıntılı tema şeması yer almaktadır.



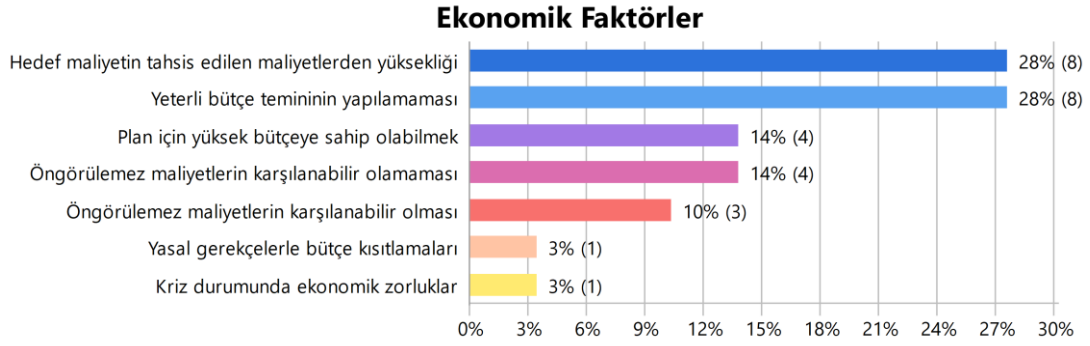
Şekil 3.2. Katılımcı Görüşmeleri Sonucunda Oluşturulan Temalar.

Katılımcıların verdiği cevaplar doğrultusunda BT felaket kurtarma planı oluşturmayı etkileyen faktörler içerisinden oluşturulan ekonomik faktörler temasına ait oluşturulan alt temalar Şekil 3.3'de sunulmuştur.



Şekil 3.3. Ekonomik Faktörler Temasına Ait Oluşturulan Alt Temalar.

Ekonomik faktörler teması için yapılan analizler sonucunda katılımcıların; Hedef maliyetin tahsis edilen maliyetlerden yüksekliği, Yeterli bütçe temininin yapılamaması, Plan için yüksek bütçeye sahip olabilmek, Öngörülemez maliyetlerin karşılanabilir olamaması, Öngörülemez maliyetlerin karşılanabilir olması, Yasal gerekçelerle bütçe kısıtlamaları, Kriz durumunda ekonomik zorluklar gibi alt temalarda toplamda 28 adet görüşlerini bildirdikleri görülmüştür. Şekil 3.4'de bu temaya ait katılımcı durumları gösterilmiştir.



Şekil 3.4. Ekonomik Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı.

Tablo 3.6'da katılımcı görüşlerinden çıkarılan ekonomik faktörler temasına ait ortak kod yorumları ve katılımcı bilgileri sunulmuştur.

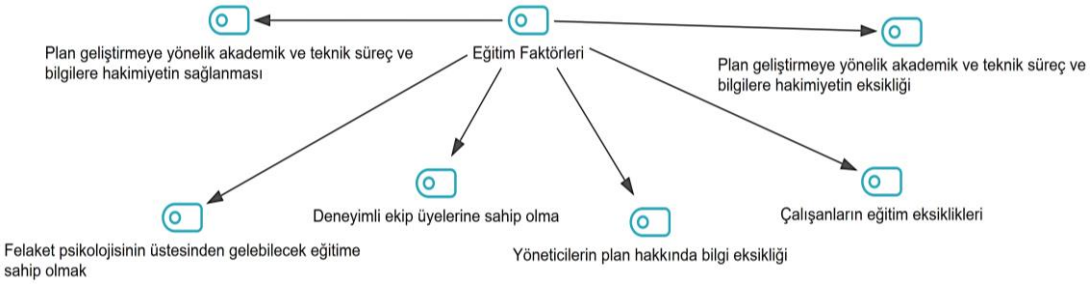
Tablo 3.6. Ekonomik Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri.

Katılımcı	Kod	Görüş
K1	T1K5	*"Bilgi işlem kanalından gelen. İstekleri çok fazla maliyet içermiyorsa genelde kabul ediyorlar…"*
K1	T1K1	*"Çünkü yüksek maliyetli projeler genelde kabul görmüyor…", "Maliyeti yüksek olduğu için bu işi yaptıramadık…"*
K2	T1K2	*"Beklentilerin karşılanması çoğu zaman daha fazla personel ve daha maliyetli çözümler gerektirdiğinden hedeflerin karşılanması mümkün olamamaktır…", "Bir başka zorlaştıran sebep ise doğal olarak mali sebepler ve personel yetersizliği gösterilebilir…", "Bu durumun sebebi ise en başta planın getirdiği mali külfet ve bilgi teknoloji süreçleri konusunda yeterli bilgi verilmeyen üst yönetimdir…"*
K3	T1K5	*"Bir de bu işin maddi kısmı var. Eğer gerekli miktarda bütçe bu iş için ayrılırsa zaten gerisi gelir…"*
K3	T1K2	*"Zorlaştıran kısımlar biraz önce de belirttiğim gibi aslında bütçenin yetersiz olması olabilir…"*
K4	T1K1	*"Olumsuz yanı ise sunucu ve storage değişim zamanlarında maliyetlerin artması (her iki sistem odasına yatırım yapılması) …"*
K5	T1K1	*"Aktif aktif bir mimari olsun istedik ama ekonomik açıdan ilk olarak aktif pasif çalışacak bir mimari oluşturmaya dikkat ettik..."*
K5	T1K3	*"Ekonomik açıdan harcama sınırının yüksek tutulması etkilidir…"*
K5	T1K2	*"Ekonomik açıdan dolar biriminden teknolojik cihazlarının satılması nedeniyle pahalı olmalarını sayabilirim…"*
K6	T1K1	*"Paramız olsa tüm sistemin birebir aynısını yaparız o zaman daha içimiz rahat eder…"*
K6	T1K5	*"Fakat planın olması gerekenleri için para gerekiyor bu konuda biraz kaynak bulmakta zorlanıyoruz…"*
K6	T1K3	*"Planı yaparken de uygularken de para, personel ve zamana ihtiyaç oluyor bular varsa plan kolay yazılıyor…"*
K6	T1K2	*"Para olarak bize sunucu-storage switch almazlarsa olmaz…"*
K6	T1K7	*"Şimdi plan yaparken her şeyi hesaba katsak bile bizim plan yaptığımız zamanki olanaklar ile felaketin olduğu zamanki olanaklar aynı olmazsa planında bir anlamı açıkçası kalmaz…"*
K7	T1K1	*"Olumsuz sonuçları ise, felaket kurtarma planını devreye alabilmek için mevcut sistem odasının tamamen kullanılmaz hale gelmesi gerektiği gibi bir gereklilik olabilir. Çünkü gerek ekonomik nedenlerden gerek diğer sorunlardan dolayı birebir canlı sistemin aynısı yedek veri merkezinde olamıyor. Öyle her yıl bütçede yüklü kalemleri yedeklemek içinde harcamakta olmuyor maalesef…", "Ayrıca, başlangıçta belirlenen bütçe dolar kurundaki değişimden dolayı yeterli olmayınca, bazı prosedürlerin uygulanmasında gecikmeler yaşandı…"*

Tablo 3.6. (Devamı)

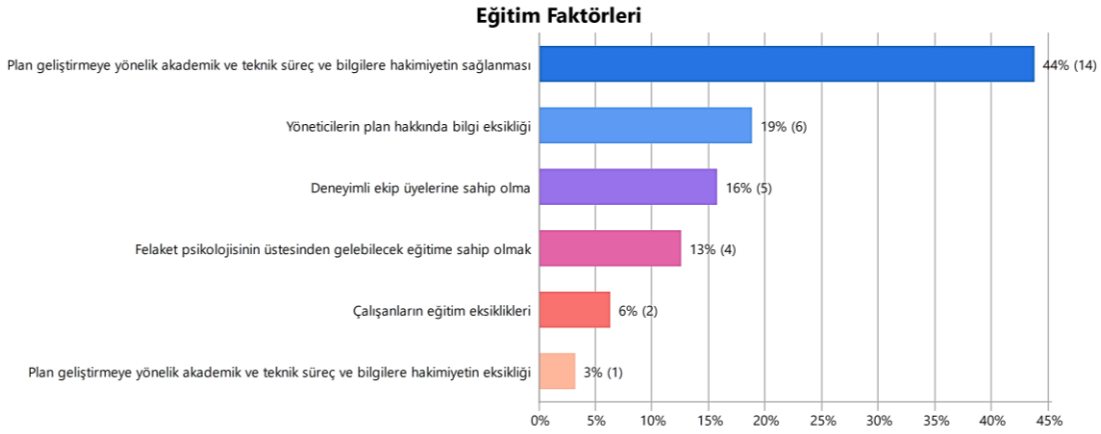
Katılımcı	Kod	Görüş
K7	T1K2	*"BT felaket kurtarma planı geliştirmeyi zorlaştıran birkaç önemli faktör bulunuyor. İlk olarak, maddi kaynak yetersizlikleri diyebilirim bunlar ciddi bir engel oluşturabiliyor…"*
K7	T1K4	*"Ayrıca, başlangıçta belirlenen bütçe dolar kurundaki değişimden dolayı yeterli olmayınca, bazı prosedürlerin uygulanmasında gecikmeler yaşandı…"*
K8	T1K6	*"Ama tasarruf tedbirleri teknik cihaz almamızı kısıtlıyor bu nedenle her şeyin daha düşük maliyetli halini araştırmak bizi yoruyor…"*
K8	T1K3	*"Planı kolaylaştıran faktörler maddi olanaklardır. Ne kadar bütçe yüksek olursa planda o kadar kolay hazırlanır…"*
K8	T1K4	*"Ufak farklılıklar oldu planı geliştirirken ekonomi güzeldi şimdi biraz dolar bazlı cihazlar pahalandı FKM'ye birebir plandakinin aynısını yapamadık…"*
K9	T1K4	*"Birde Vmware lisans politikasını değişti bizde mali açıdan kaynakları daha efektif kullanmak için bazı önem seviyesi düşük olan sanal sunucularımızın platformunu değiştik…", "Son olarak geliştirmeyi zorlaştıran başlıca faktörlerden biride her felaket tahmin edemezsiniz, öngöremediğiniz sorunlar için felaket senaryoları ve riskleri yazmak epey zor bir iş…"*
K9	T1K1	*"Ancak bu süreçlerin otomatiğe bağlanması gerektiği görüşündeyiz ama aktif-aktif çalışacak storage maliyeti epey yüksek…"*
K9	T1K2	*"BT felaket kurtarma planı geliştirmeyi zorlaştıran bazı temel faktörler vardır. Bunlardan ilki, para ve zamandır…"*
K10	T1K3	*"Finansal olanaklar planı oluşturmayı kolaylaştırır…*

Katılımcıların verdiği cevaplar doğrultusunda BT felaket kurtarma planı oluşturmayı etkileyen faktörler içerisinden oluşturulan eğitim faktörleri temasına ait oluşturulan alt temalar Şekil 3.5'de sunulmuştur.



Şekil 3.5. Eğitim Faktörleri Temasına Ait Oluşturulan Alt Temalar.

Eğitim faktörleri teması için yapılan analizler sonucunda katılımcıların; Plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin sağlanması, yöneticilerin plan hakkında bilgi eksikliği, deneyimli ekip üyelerine sahip olma, felaket psikolojisinin üstesinden gelebilecek eğitime sahip olmak, çalışanların eğitim eksiklikleri, Plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin eksikliği gibi alt temalarda toplam 32 adet görüşlerini bildirdikleri görülmüştür. Şekil 3.6'da bu temaya ait katılımcı durumları gösterilmiştir.



Şekil 3.6. Eğitim Faktörleri Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı.

Tablo 3.7'de katılımcı görüşlerinden çıkarılan eğitim faktörleri temasına ait ortak kod yorumları ve katılımcı bilgileri sunulmuştur.

Tablo 3.7. Eğitim Faktörleri Teması İçin Alt Kodlar ve Katılımcı Görüşleri.

Katılımcı	Kod	Görüş
K1	T2K2	*"BT kurtarma planı konusunda üst yöneticilerin fazlaca bir bilgiye sahip olduğunu düşünmüyorum…"*
K2	T2K4	*"Felaket anları panik havası, bilinmezlik ve öngörülemezlik durumların yaşandığı anılardır. Haliyle böyle anılarda sorumlu personellerin yetkinliği ne olursa olsun ne yapacaklarını bilememe durumları ortaya çıkabilir…"*
K2	T2K2	*"Burada önemli olan kurum bilgi teknolojileri yöneticilerinin ve bilgi teknolojilerinin sorumlu üst yönetimi, tam yedeklilik yüksek erişilebilirlik, hata toleransı gibi kavramların farkındalığını sağlaması ve beklentilerin gerçeklerle uyuşmasını sağlamasıdır...", "Bu durumun sebebi ise en başta planın getirdiği mali külfet ve bilgi teknoloji süreçleri konusunda yeterli bilgi verilmeyen üst yönetimdir…"*
K2	T2K5	*Burada önemli olan kurum bilgi teknolojileri yöneticilerinin ve bilgi teknolojilerinin sorumlu üst yönetimi, tam yeleklilik yüksek erişilebilirlik, hata toleransı gibi kavramların farkındalığını sağlaması ve beklentilerin gerçeklerle uyuşmasını sağlamasıdır.*

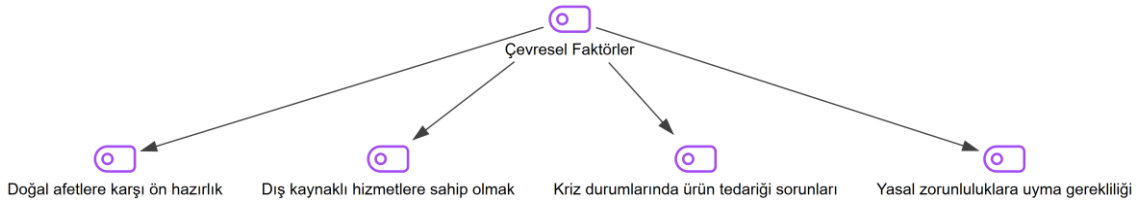
Tablo 3.7. (Devamı)

Katılımcı	Kod	Görüş
K2	T2K1	*"Birincisi, mevcut sistem ve iş süreçleri analizi, ikincisi kesintisizlik ve veri kaybı toleransı ve üçüncüsü Recovery süreçlerin belirlenmesi RPO ve RTO değerlerinin belirlenmesi. Planın geliştirilmesinde tüm paydaşlar ile birlikte hareket etme en önde gelen faktör olarak karşıma çıkmıştır. Bunun yanında ilgi teknolojileri, felaket kurtarma planını bir proje yönetimi gibi düşünmek ve proje yönetimi süreçlerini uygulamak plan oluştururken işimizi kolaylaştıran etkenlerden birisiydi. Proje yönetimi süreçlerini uygulamaktan kastım analizi planlaması uygulaması değerlendirmesi ve yeniden analiz şeklinde bir döngü oluşturmasıdır…"*
K2	T2K6	*"Bence bu süreci zorlaştıran en büyük faktör, sistem analizi ve iş süreçlerinin belirlenememesidir…"*
K3	T2K1	*"Planı geliştirirken ulusal veya uluslararası dokümanlara baktık…"*
K4	T2K3	*"Olası problemlerde minimum düzeyde veri kaybı planlanmaktadır bu yüzden FKM odası yapılırken Standby yöntemi tercih edilmiştir çünkü aktif aktif yapılarda Database bozulmaların da yedek tarafında bit bazında bozacaktır fakat kurumumuzda SQL cümleleri ile ekle, sil ya da edit mantığı ile yedek sistemlere veriler senkronize edilmektedir…"*
K5	T2K3	*"Personelin yetenekli ve sayıca çok olması etkilidir…"*
K5	T2K1	*"Çok farklı ana başlıkta çok farklı alt nedenler sayılabilir…"*
K6	T2K1	*"Bu sayede iş sürekliliğini de sağlamış oluruz…", "Planı yaparken de uygularken de para, personel ve zamana ihtiyaç oluyor bular varsa plan kolay yazılıyor…"*
K6	T2K2	*"Planı oluştururken zaman kısıtlaması olursa hemen yarına beklerseler olmaz…",*
K7	T2K1	*"Bir BT felaket kurtarma planına sahip olmanın olumlu sonuçları, olası sistem arızalarında veri kaybının yaşanmayacak olması ve sistemlerin hızlıca devreye alınmasıdır…", "Ayrıca, riskler açısından veri kaybı, sistem arızaları ve dış kaynaklı güvenlik açıkları da sürekli olarak izlenmekte ve bu risklerin olabildiği kadar en aza düşürülmesi bizden beklenmektedir. İş sürekliliği konusunda ise, herhangi bir aksaklık durumunda sistemlerin hızlı bir şekilde toparlanması, verilerin düzenli olarak yedeklenmesi ve gerektiğinde hızlıca kurtarılması beklenmekte, genellikle sorun olmadan önce sorun yapacak şeyleri bulup çözmemiz isteniyor…", "Felaket kurtarma planları, iş sürekliliği ve veri güvenliği gibi kritik alanlarda riskleri minimize etmek için yöneticiler, bu planların oluşturulmasına genellikle belirtiğim gibi tam destek vermektedirler…", "BT felaket kurtarma planını geliştirirken, en çok dikkat ettiğimiz unsurların başında kritik sistemler ve verilerin belirlenmesi geldi. Hangi sistemin ve içindeki hangi verilerin en önemli olduğunun net bir şekilde tanımlanması, planın odak noktasıydı. Ayrıca, yedekleme stratejilerini etkili bir şekilde uygulayarak verilerin düzenli yedeklenmesi ve güvenli depolanması sağlandı. Erişim ve yetki yönetimi konusuna da büyük özen gösterdik…"*

Tablo 3.7. (Devamı)

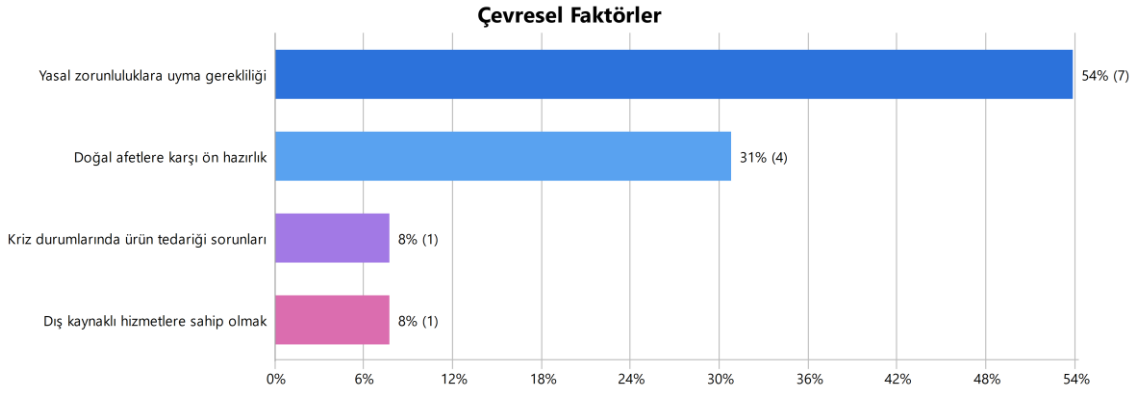
Katılımcı	Kod	Görüş
K7	T2K3	*"Ayrıca, ekibimizin deneyimi, her aşamada bize has hızlı çözüm üretmemize olanak tanıdı…"*
K7	T2K2	*"Bir diğer engel ise, sizin ne yaptığınızı fark etmeyen idari personeller olabilir…"*
K7	T2K5	*"…planın etkili olabilmesi için tüm personelin eğitim alması şart…"*
K8	T2K2	*"Çünkü yöneticilerimiz planın sadece maddi olanaklarla güncellenebileceğini düşünüyorlar…"*
K8	T2K4	*"Felaket olduğunda insan bir şoka girer, sonra şoku atlatınca ne yapacağını bilemez. Eğer elinde bir plan olursa en azından ona göre hareket eder..."*
K9	T2K1	*"Mesela plana sahip olunursa veri kaybı, kesintiler veya öğrenci kimlik verilerinin güvenli saklanması gibi konularda önleyici tedbirler alınarak büyük zararların önüne geçilebilir…"*
K9	T2K4	*"…çünkü tüm çalışanlar felaket durumunda hangi adımları atacakları konusunda bilgilendirilmiş olurlar.", "Ayrıca, planın düzgün bir şekilde uygulanabilmesi için tüm çalışanların eğitilmesi gerekir, bu da ek kaynak ve eğitim gereksinimleri doğurabilir. Felaket durumunda planın işe yaramaması olursa eğer bu da ciddi bir güven kaybına neden olabilir…"*
K9	T2K1	*"Ayrıca, planın düzgün bir şekilde uygulanabilmesi için tüm çalışanların eğitilmesi gerekir, bu da ek kaynak ve eğitim gereksinimleri doğurabilir. Felaket durumunda planın işe yaramaması olursa eğer bu da ciddi bir güven kaybına neden olabilir…", "…özellikle son yıllarda artan siber güvenlik tehditleri ve doğal afetler gibi riskler, yöneticilerimizin bu tür planları onaylamalarını kolaylaştırdı diye düşünmekteyim..."*
K10	T2K1	*"Planımız var, 4 yılda bir defa güncellendi…"*
K10	T2K3	*"Plan varsa personel nasıl hareket edeceğini bilir. Önceden hazır olmayı sağlar…", "Tecrübeli olmak planı oluşturmayı kolaylaştırır…"*
K10	T2K1	*"Planı geliştirirken ilk önce neler lazım, bizim için önemli olanlar neler onları listeledik. Sonra alternatifleri, yedekleri nasıl kurulur bunlara baktık. Sonra hazır planları internetten araştırdık. Tecrübeli olmak planı oluşturmayı kolaylaştırır…"*

Katılımcıların verdiği cevaplar doğrultusunda BT felaket kurtarma planı oluşturmayı etkileyen faktörler içerisinden oluşturulan çevresel faktörler temasına ait oluşturulan temalar Şekil 3.7'de sunulmuştur.



Şekil 3.7. Çevresel Faktörler Temasına Ait Oluşturulan Alt Temalar.

Çevresel faktörler teması için yapılan analizler sonucunda katılımcıların; Yasal zorunluluklara uyma gerekliliği, doğal afetlere karşı ön hazırlık, kriz durumlarında ürün tedariği sorunları, dış kaynaklı hizmetlere sahip olmak gibi alt temalarda toplam 13 adet görüşlerini bildirdikleri görülmüştür. Şekil 3.8'de bu temaya ait katılımcı durumları gösterilmiştir.



Şekil 3.8. Çevresel Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı.

Tablo 3.8'de katılımcı görüşlerinden çıkarılan çevresel faktörler temasına ait ortak kod yorumları ve katılımcı bilgileri sunulmuştur.

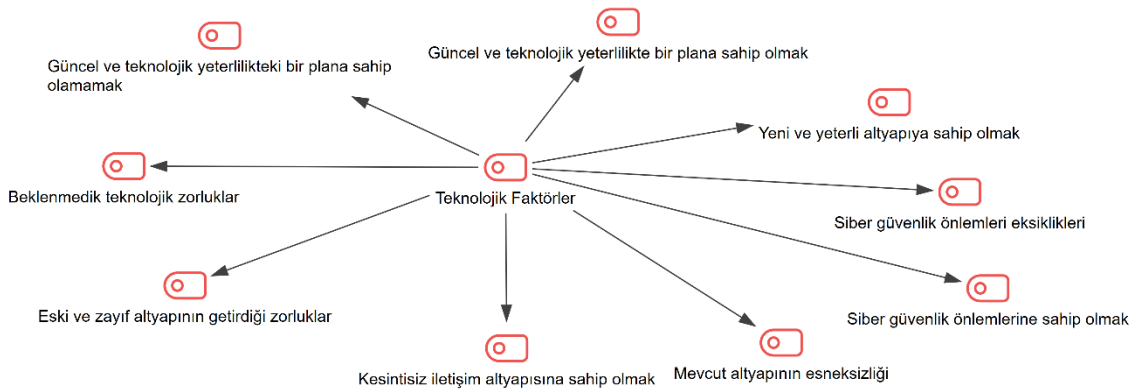
Tablo 3.8. Çevresel Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri.

Katılımcı	Kod	Görüş
K3	T3K1	*"Plana sahip olmanın olumlu yönleri denetimlerde kolaylık sağlıyor…"*
K3	T3K2	*"…deprem, sel, yangın gibi felaketlere karşı hazır olmamızı sağlıyor…"*
K3	T3K1	*"İş sürekliliğini sağlamak ISO belgesi almak içinde gerekli bir durum…"*
K5	T3K1	*"Bulut merkezli olabilse çok alternatif var ama gerek yasalar gerek buluta olan güven dolayısıyla kendimize ait bir veri merkezinde verilerimizi tutmak zorundaydık buna dikkat ettik…"*
K6	T3K2	*"Plana göre şimdi şu sistem odasını su bassa yedek veri merkezinden en azından duyuru yapacak kadar sistemi çalıştırırız…"*

Tablo 3.8. (Devamı)

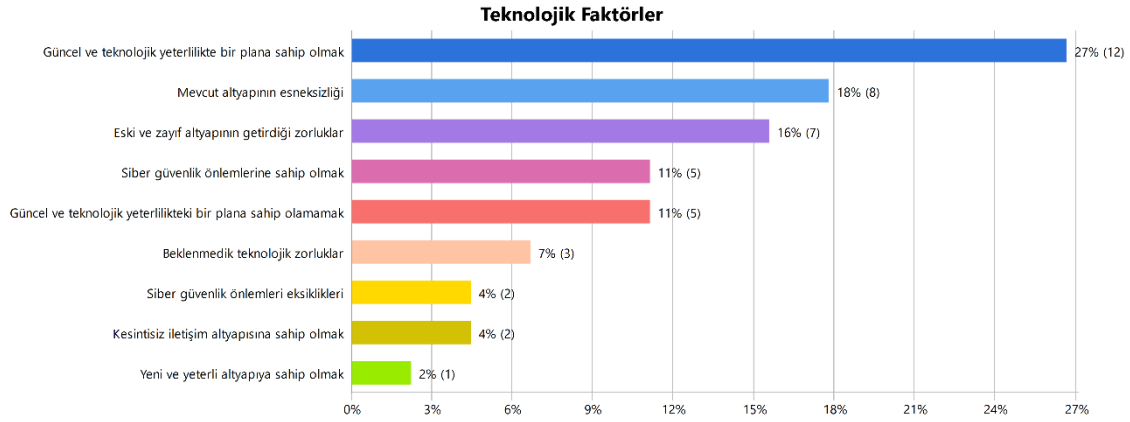
Katılımcı	Kod	Görüş
K6	T3K2	*"Şimdi plan yaparken her şeyi hesaba katsak bile bizim plan yaptığımız zamanki olanaklar ile felaketin olduğu zamanki olanaklar aynı olmazsa planında bir anlamı açıkçası kalmaz…"*
K7	T3K2	*"Evet, kurumumuzda bir BT felaket kurtarma planı bulunmakta. Plan sürekli güncellenmekte çünkü bilgi işlem altyapısının sürekliliğini sağlamak ve saldırılarda falan verilerin kaybını engellemek ve verdiğimiz hizmetlerin en kısa sürede tekrar verilmesi için güncellememiz gerekiyor…"*
K7	T3K1	*"Bazı durumlarda mesela tasarruf tedbirleri gibi durumlarda onlarda destek konusunda zorlanıyorlar…"*
K8	T3K1	*"Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin yönergelerine baktık…"*
K9	T3K4	*"…özellikle yemekhane otomasyonu sisteminde bulut tabanlı bir çözüme geçiş yaptık…"*
K9	T3K1	*"Cumhurbaşkanlığı dijital dönüşüm ofisi bilgi ve iletişim güvenliği rehberine hazırlık süreci yer almaktadır…"*
K10	T3K1	*"Üst yönetim yasal zorunluklar kapsamında planın olmasını istiyor. Bizden desteklerini esirgemiyorlar…"*
K10	T3K3	*"Bir fark olmadı ama ürünleri tedarik ederken zorlandık pandemi vardı o zaman. Yurtdışından ürün getirirken epey beklemek zorunda kaldık…"*

Katılımcıların verdiği cevaplar doğrultusunda BT felaket kurtarma planı oluşturmayı etkileyen faktörler içerisinden bulunan teknolojik faktörleri temasına ait oluşturulan alt temalar Şekil 3.9'da sunulmuştur.



Şekil 3.9. Teknolojik Faktörler Temasına Ait Oluşturulan Alt Temalar.

Teknolojik faktörler teması için yapılan analizler sonucunda katılımcıların; güncel ve teknolojik yeterlilikte bir plana sahip olmak, mevcut altyapının esneksizliği, eski ve zayıf altyapının getirdiği zorluklar, siber güvenlik önlemlerine sahip olmak, güncel ve teknolojik yeterlilikteki bir plana sahip olamamak, beklenmedik teknolojik zorluklar, siber güvenlik önlemleri eksiklikleri, kesintisiz iletişim altyapısına sahip olmak, yeni ve yeterli altyapıya sahip olmak gibi alt temalarda toplam 45 görüşlerini bildirdikleri görülmüştür. Şekil 3.10'da bu temaya ait katılımcı durumları gösterilmiştir.



Şekil 3.10. Teknolojik Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı.

Tablo 3.9'da katılımcı görüşlerinden çıkarılan teknolojik faktörler temasına ait ortak kod yorumları ve katılımcı bilgileri sunulmuştur.

Tablo 3.9. Teknolojik Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri.

Katılımcı	Kod	Görüş
K1	T4K5	*"Yaklaşık 2 yılda bir güncellenmekte, yenilenmekte…"*
K1	T4K8	*"İşin sürekliliği, kesilmemesi çok önemli. Beklenti de hiç kesintiye uğramadan 7/24 çalışması…"*
K1	T4K9	*"Bu konuda bize en fazla kolaylık sağlayan farklı bir lokasyondaki ikinci sistem odamızı oluşturmamız…"*
K1	T4K2	*"2 farklı lokasyonda 2 farklı omurga çalıştırma işinde olması gereken bütün kenar Switch'lere fiber 2 noktadan fiber çektirmek…"*
K2	T4K1	*"Planın genel hatları sabit kalmakla birlikte 3 ayda bir toplantı yapmaktayız. Toplantılar ile varsa eksiklikler görüşülerek giderilmesi veya planda güncelleme yapılması amaçlanmaktadır…"*
K2	T4K8	*"Aslında bu soru tüm kurumlar için aynı cevabı içeriyor. Mümkünse hiç güvenlik açığı olmasın. 365 gün 7-24 sistem çalışsın…"*

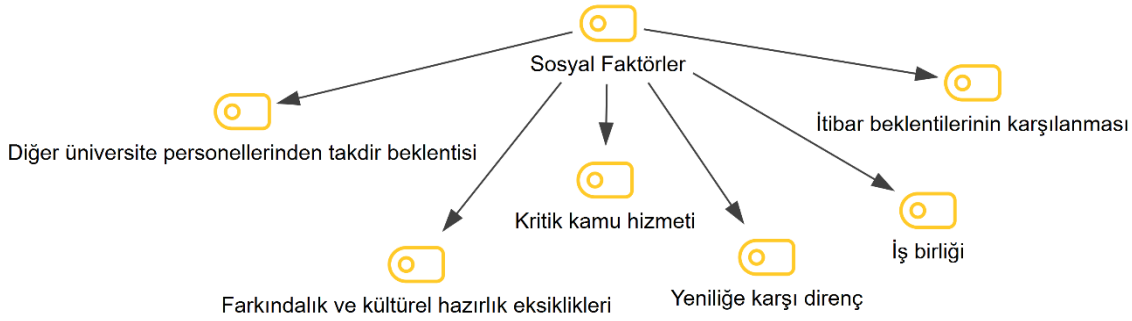
Tablo 3.9. (Devamı)

Katılımcı	Kod	Görüş
K2	T4K4	*"Aslında bu soru tüm kurumlar için aynı cevabı içeriyor. Mümkünse hiç güvenlik açığı olmasın. 365 gün 7-24 sistem çalışsın…"*
K3	T4K1	*"Denetlemeler öncesi planlar gözden geçiriliyor varsa eksiklikler ya da güncellemeler yapılıyor…", "Olumsuz bir yön göremiyorum plana sahip olunca ama plan olmazsa felaket durumunda karmaşa yaşanır ve muhtemelen sağlıklı bir çalışma ortamı olmaz ve sağladığımız hizmetleri çok geç eski haline getiririz…"*
K4	T4K5	*"Kurumumuzda bir felaket kurtarma planı var ama öyle özel bir felaketten kurtarma planı olmayıp; anasistem odasının küçük bir versiyonu (storage ler bire bir aynı, sunucular daha düşük kapasitede olmak üzere) başka bir blokta bulunmaktadır. Bu sistem odası Standby olarak çalışmaktadır…"*
K4	T4K3	*"Kurumumuzda olası bir sunucu arızası veritabanı problemi olduğu durumlarda fkm tarafından sistem devreye alınmamakta olup mevcut sistem odasındaki problemin çözülmesi beklenmektedir…"*
K4	T4K2	*"FKM tarafını devreye almak için mevcut kullanmakta olduğumuz sistem odasının tamamen kullanılamaz olması gerekmektedir…", "Olası problemlerde minimum düzeyde veri kaybı planlanmaktadır bu yüzden FKM odası yapılırken Standby yöntemi tercih edilmiştir çünkü aktif aktif yapılarda Database bozulmaların da yedek tarafında bit bazında bozacaktır fakat kurumumuzda SQL cümleleri ile ekle, sil ya da edit mantığı ile yedek sistemlere veriler senkronize edilmektedir…", "Mevcut sistem odasında kalıcı bir şekilde çalışamaz duruma geldiğinde; yedek sistem odası çalışır fakat..", "...çünkü ana sistem odası tüm lokasyonlardan network erişimi bulunmakta ama yedek sistem odasından erişim bulunmamaktadır. Biraz önce belirttiğim sıkıntılardan dolayı gerekli altyapı çalışması yapılamamaktadır…"*
K5	T4K1	*"BT Felaket kurtarma planımız var, planın tamamı değil ama yedekleme planı gibi alt başlıkları sık sık güncellenmektedir…", "Kolaylaştırıcı unsurlar olarak Sanallaştırma sisteminin olması, kurtarma süresi ve sanal makinelerin geri yüklenmesi için gereken süreyi kısaltma konusunda planda etkilidir…"*
K5	T4K7	*"Keşke hiç güvenlik açığı olmasa ama neredeyse her gün bir güvenlik açığı haberi geliyor bunun için ilk olarak kurumda güvenlik açıklıkları ele alınıyor sonra yedeklemenin önemi bizim kurumda öncelikli konulardandır…"*
K5	T4K3	*"Depolama alanının kısıtlı olması nedeniyle sadece ilk etapta en kritik sistemlerin birebir yedeğini uzak lokasyona almaya dikkat ettik..."*
K5	T4K3	*"Bunlardan teknolojik olarak Sanallaştırma platformunda olmayan sunucuların kurtarılması ve yedeklenmesi konusunda eksiklik ve zorlukların var olmasını sayabilirim…"*
K6	T4K1	*"Halihazırda kullandığımız bir kurtarma planımız var. Daha geçen sene yaptık yani güncel, kapasitemizin artmasına göre planı güncelleyeceğiz…", "Kurum ilk olarak Hacklenmeyelim, elektrik gidince hemen sistem kapanmasın gibi basit beklentilerde ama uzun vadede bire bir felaket anında yaptığımız işlerin aynen devam etmesini düşünmekte…"*

Tablo 3.9. (Devamı)

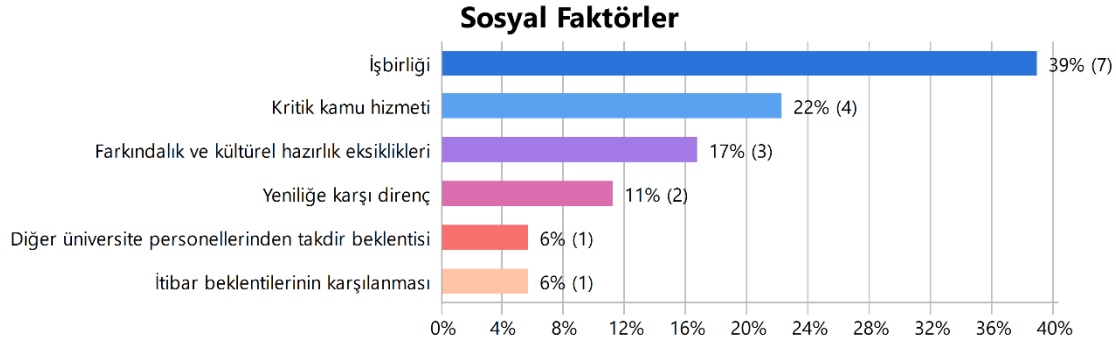
Katılımcı	Kod	Görüş
K7	T4K1	*"Evet, kurumumuzda bir BT felaket kurtarma planı bulunmakta. Plan sürekli güncellenmekte çünkü bilgi işlem altyapısının sürekliliğini sağlamak ve saldırılarda falan verilerin kaybını engellemek ve verdiğimiz hizmetlerin en kısa sürede tekrar verilmesi için güncellememiz gerekiyor…", "Ayrıca, riskler açısından veri kaybı, sistem arızaları ve dış kaynaklı güvenlik açıkları da sürekli olarak izlenmekte ve bu risklerin olabildiği kadar en aza düşürülmesi bizden beklenmektedir. İş sürekliliği konusunda ise, herhangi bir aksaklık durumunda sistemlerin hızlı bir şekilde toparlanması, verilerin düzenli olarak yedeklenmesi ve gerektiğinde hızlıca kurtarılması beklenmekte, genellikle sorun olmadan önce sorun yapacak şeyleri bulup çözmemiz isteniyor…", "BT felaket kurtarma planını geliştirirken, en çok dikkat ettiğimiz unsurların başında kritik sistemler ve verilerin belirlenmesi geldi. Hangi sistemin ve içindeki hangi verilerin en önemli olduğunun net bir şekilde tanımlanması, planın odak noktasıydı. Ayrıca, yedekleme stratejilerini etkili bir şekilde uygulayarak verilerin düzenli yedeklenmesi ve güvenli depolanması sağlandı. Erişim ve yetki yönetimi konusuna da büyük özen gösterdik…", "…planın, herkes için ayrı ayrı görevleri içermesi ve yetkilerin seviyeleri güvenliği artırdı."*
K7	T4K3	*"Ayrıca, karmaşık bir altyapı varsa da sorun olur…"*
K7	T4K4	*"Kurumumuz, BT güvenlik açıkları konusunda özellikle siber saldırılara karşı korunma, ağ güvenliği ve erişim kontrolüne büyük önem vermekte..."*
K7	T4K2	*"Ayrıca, karmaşık bir altyapı varsa da sorun olur…", "Bu farklılıklar, genellikle yedek veri merkezine canlı sistemle aynı cihazı koyamadığımız için kaynaklandı…"*
K8	T4K5	*"Kurumumuzda felaket kurtarma planı var fakat sürekli güncellenmiyor…"*
K8	T4K4	*"Güvenlik açığı anlamında yatırımlar, beklentiler çok yüksek. Veri sızıntısından çok korkuyoruz. Bir veri merkezimizde veri tabanları durursa hemen FKM'den devam etmesi için plan yaptık ama test edemedik daha…"*
K8	T4K6	*"Bir veri merkezimizde veri tabanları durursa hemen FKM'den devam etmesi için plan yaptık ama test edemedik daha…"*
K8	T4K3	*"…eskiden kalan karmaşık ama çalışması gereken sistemlerin test edilememesi planı zorlaştırıyor…"*
K8	T4K2	*"…eskiden kalan karmaşık ama çalışması gereken sistemlerin test edilememesi planı zorlaştırıyor…"*
K9	T4K5	*"Evet, kurumumuzda bir BT felaket kurtarma planı mevcuttur. Ancak, son birkaç yıldır planın kapsamı ve içeriği güncellenmemiştir. Planın güncellenmesi gerektiğini düşünüyoruz…"*
K9	T4K3	*"Bir de şu an felaket durumlarında veri yedekleme ve kurtarma işlemleri manuel olarak yapılmakta…", "…özellikle eski yazılım ve donanımların korunması konusunda riskler mevcut…"*
K9	T4K4	*"Felaket kurtarma planının olumlu sonuçları olarak hem güvenliğin artığının hem de kurumun itibarının korunduğunu söyleyebilirim…", "Ayrıca, iç ve dış tehditlere karşı savunmasız olmamak adına güvenlik duvarları, antivirüs ve sızma testi gibi önlemlerle her zaman etkin olamaya çalışıyoruz…"*

Katılımcıların verdiği cevaplar doğrultusunda BT felaket kurtarma planı oluşturmayı etkileyen faktörler içerisinden oluşturulan sosyal faktörler temasına ait oluşturulan alt temalar Şekil 3.11'de sunulmuştur.



Şekil 3.11. Sosyal Faktörler Temasına Ait Oluşturulan Alt Temalar

Sosyal faktörler teması için yapılan analizler sonucunda katılımcıların; iş birliği, kritik kamu hizmeti, farkındalık ve kültürel hazırlık eksiklikleri, yeniliğe karşı direnç, diğer üniversite personellerinden takdir beklentisi, itibar beklentilerinin karşılanması gibi alt temalarda toplam 18 adet görüşlerini bildirdikleri görülmüştür. Şekil 3.12'de bu temaya ait katılımcı durumları gösterilmiştir.



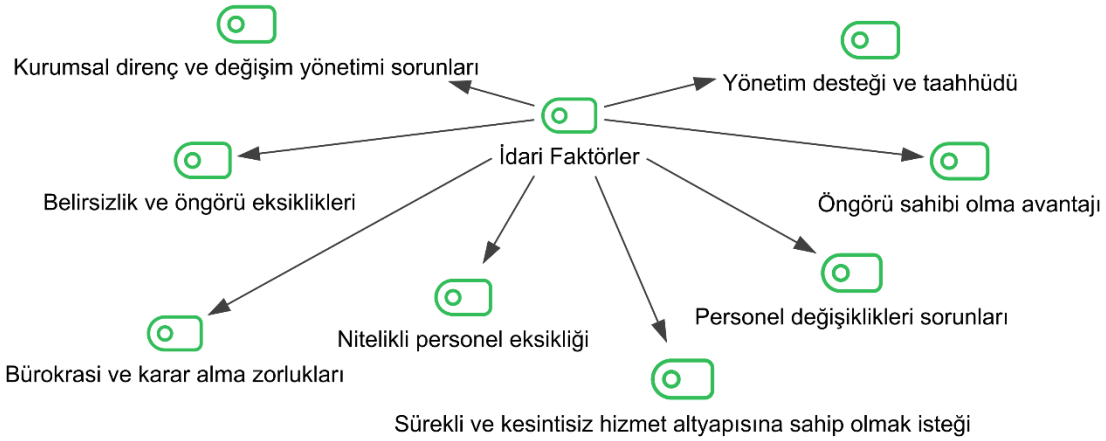
Şekil 3.12. Sosyal Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı.

Tablo 3.10'da katılımcı görüşlerinden çıkarılan Sosyal faktörler temasına ait ortak kod yorumları ve katılımcı bilgileri sunulmuştur.

Tablo 3.10. Sosyal Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri.

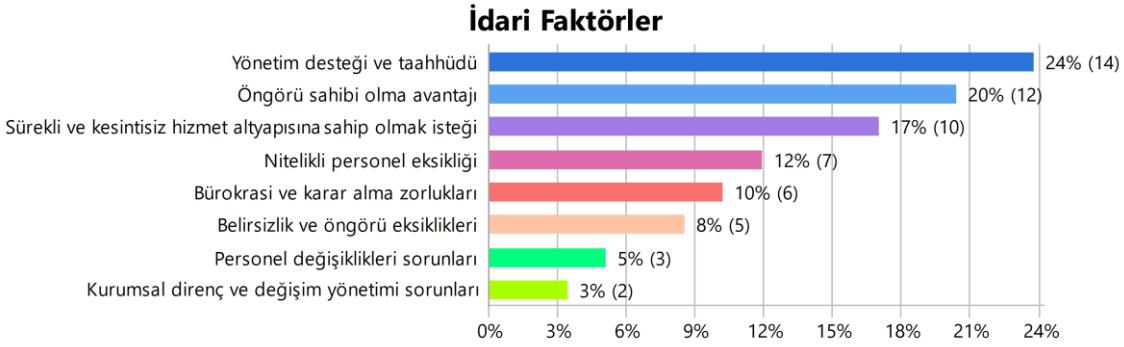
Katılımcı	Kod	Görüş
K1	T5K2	*"Sağlık hizmeti de veren bir kurum olduğumuz için…"*
K2	T5K3	*"Burada önemli olan kurum bilgi teknolojileri yöneticilerinin ve bilgi teknolojilerinin sorumlu üst yönetimi, tam yeleklilik yüksek erişilebilirlik, hata toleransı gibi kavramların farkındalığını sağlaması ve beklentilerin gerçeklerle uyuşmasını sağlamasıdır…"*
K2	T5K1	*"Planın geliştirilmesinde tüm paydaşlar ile birlikte hareket etme en önde gelen faktör olarak karşıma çıkmıştır…"*
K3	T5K2	*"Hastane hizmeti verdiğimiz için yıl içerisinde çeşitli denetlemelerimiz oluyor..."*
K3	T5K1	*"Bize teknolojik cihazlar sağlayan tedarikçi firmalardan destek aldık. İşi kolaylaştıran kısım bilen birilerinden destek almaktan geçiyor…"*
K4	T5K3	*"İsteklerin akademik kanaldan gelmesi ile güvenlik açığı olup olmadığına bakılmaksızın yaptırmaya çalışmaları zafiyet oluşturmaktadır…"*
K4	T5K2	*"…hastanenin tüm lokasyonlarında sistem devreye alınamaz…"*
K6	T5K1	*"Planı oluştururken geçmiş tecrübelerimiz etkili oldu ayrıca ULAKNET'ten tanıdığımız hocalara sorduk ne yapabiliriz diye…"*
K7	T5K2	*"Bir BT felaket kurtarma planına sahip olmanın olumlu ve olumsuz sonuçları hem kısa vadeli hem de uzun vadeli açılardan değerlendirirsem özellikle üniversiteler gibi büyük ve kompleks altyapılara sahip kurumlar kamu için öneme sahip olduğundan dolayı aynı zamanda kritiktirler…"*
K7	T5K5	*"Bu belki kullanıcılar tarafından hissedilmez bile…"*
K7	T5K3	*"Bir diğer engel ise, sizin ne yaptığınızı fark etmeyen idari personeller olabilir…"*
K8	T5K4	*"Çünkü yöneticilerimiz planın sadece maddi olanaklarla güncellenebileceğini düşünüyorlar…*
K8	T5K1	*"Bize ürün satan firmalara sorduk…"*
K9	T5K6	*"Felaket kurtarma planının olumlu sonuçları olarak hem güvenliğin artığının hem de kurumun itibarının korunduğunu söyleyebilirim…"*
K9	T5K1	*"Ayrıca, planın uygulanması kurum içindeki ekiplerin daha iyi bir işbirliği yapmasını sağlar…", "Özellikle, Planlamada, her felaket için tek tek çözüm üretirken araştırdığımız, bu işin olması gerekeniyle bize uyan çözüm yolları ve prosedürler teknolojik açıdan beklenmedik bazı zorluklar yaptı, mesela bazı kritik yazılım ve sistemlerin yedekten dönme süreleri planlandığı gibi çalışmadı..."*
K9	T5K4	*"…diğeri kurum personellerinin özellikle teknik olmayan personelleri değişime karşı direnç göstermeleridir…"*
K10	T5K1	*"Planı geliştirirken ilk önce neler lazım, bizim için önemli olanlar neler onları listeledik. Sonra alternatifleri, yedekleri nasıl kurulur bunlara baktık. Sonra hazır planları internetten araştırdık. Tecrübeli olmak planı oluşturmayı kolaylaştırır. Finansal olanaklar planı oluşturmayı kolaylaştırır…"*

Katılımcıların verdiği cevaplar doğrultusunda BT felaket kurtarma planı oluşturmayı etkileyen faktörler içerisinden oluşturulan idari faktörler temasına ait geliştirilmiş alt temalar Şekil 3.13'de sunulmuştur.



Şekil 3.13. İdari Faktörler Temasına Ait Oluşturulan Alt Temalar.

İdari faktörler teması için yapılan analizler sonucunda katılımcıların; yönetim desteği ve taahhüdü, öngörü sahibi olma avantajı, sürekli ve kesintisiz hizmet altyapısına sahip olmak isteği, nitelikli personel eksikliği, bürokrasi ve karar alma zorlukları, belirsizlik ve öngörü eksiklikleri, personel değişiklikleri sorunları, kurumsal direnç ve değişim yönetimi sorunları gibi alt temalarda, toplamda 59 adet görüşlerini bildirdikleri görülmüştür. Şekil 3.14'de bu temaya ait katılımcı durumları gösterilmiştir



Şekil 3.14. İdari Faktörler Teması İçin Alt Temalar ve Katılımcı Görüşleri Dağılımı.

Tablo 3.11'de katılımcı görüşlerinden çıkarılan idari faktörler temasına ait ortak kod yorumları ve katılımcı bilgileri sunulmuştur.

Tablo 3.11. İdari Faktörler Teması İçin Alt Kodlar ve Katılımcı Görüşleri.

Katılımcı	Kod	Görüş
K1	T6K2	*"BT felaket planına sahip olmak. Oluşabilecek problemler için önceden fikir sahibi olmaya yarıyor…"," Bu sayede sunucu ve ağ cihazlarını, omurga cihazlarımızı 2 farklı lokasyonda çalıştırabiliyoruz…"*
K1	T6K3	*"E tabii iki sistem odası işletmenin zorlukları da var. Yani 2 taraftaki güç kaynakları. işte soğutma sistemleri, ortam izleme sistemleri, yangın söndürme sistemlerini çalışır durumda tutmak da zorluklarından diyebiliriz…"*
K1	T6K5	*"BT felaket kurtarma planını zorlaştıran en büyük engelin gereken yatırımı yönetime kabul ettirmek olduğunu düşünüyorum…"*
K2	T6K3	*"Bu noktada en kritik olan felaket anında ve hemen sonunda muhakkak hizmet vermesi gereken servislerin belirlenmesi ve kaynakların ve eforların bu yönde tahsis edilmesidir…"*
K2	T6K2	*"Bu noktada en kritik olan felaket anında ve hemen sonunda muhakkak hizmet vermesi gereken servislerin belirlenmesi ve kaynakların ve eforların bu yönde tahsis edilmesidir…", "Bir BT felaket planı bu tarz durumlar için önceden hazırlanmış, test edilmiş ve inisiyatif gerek kalmadan yapılacakların belirlendiği bir kılavuz niteliğinde olduğundan böyle bir plana sahip olmak oldukça olumlu sonuçlar doğurmaktadır…"*
K2	T6K1	*"Bir plana sahip olmamanın getirdiği olumsuz bir sonuç düşünemiyorum. Zira en kötü plan bile plansızlıktan iyidir…", "Kurumumuzdaki üst yönetim her zaman için bu tarz planları olumlu karşılama eğilimindedir. Düzgün yapılandırılmış kurumun ihtiyaçlarıyla örtüşen ve hakkında detaylı bilgi verilmiş bir plana. Üst yönetimin soğuk baktığını görmedim…"*
K2	T6K4	*"Beklentilerin karşılanması çoğu zaman daha fazla personel ve daha maliyetli çözümler gerektirdiğinden hedeflerin karşılanması mümkün olamamaktır…", "Bir başka zorlaştıran sebep ise doğal olarak mali sebepler ve personel yetersizliği gösterilebilir…"*
K2	T6K3	*"Sahip olunan bilgi teknolojisi kaynaklarının ve iş akışlarının belirlenememesi, iş kritik tanımlarının yapılamamasına ve felaket anında recovery edilmesi ya da hazırda bekletilmesi gereken sistemin belirlenememesine sebebiyet verir…"*
K2	T6K6	*"Bundan dolayı planlar hazırlanırken amaca en uygun ve en uygulanabilir şekilde hazırlanmaya özen gösterilmelidir…"*
K3	T6K3	*"Olumsuz bir yön göremiyorum plana sahip olunca ama plan olmazsa felaket durumunda karmaşa yaşanır ve muhtemelen sağlıklı bir çalışma ortamı olmaz ve sağladığımız hizmetleri çok geç eski haline getiririz…"*

Tablo 3.11. (Devamı)

Katılımcı	Kod	Görüş
K3	T6K1	*"Başkanımızın bizden isteği de zaten hep bu yönde hazır olmamızdır…", "Yöneticilerimiz teknik tabanları olan insanlar olduğu için felaket kurtarma planı açısından hep bizim yanımızda oluyorlar…"*
K3	T6K4	*"Başka, kalifiye personelin olmaması olabilir…"*
K3	T6K2	*"Bizim planımız aslında adım adım gitti. Kervan yolda düzülür dedik. Onun için zaten plan hayata geçirildiğinde plan oldu…"*
K4	T6K2	*"Bu sistemin olumlu yanı olası problemlerde veri kaybınızın olmadığını bilmeniz olacaktır…"*
K4	T6K8	*"Kurumumuzda IT ekibinin Memur ve işçi kadrosundan oluşması buna parelel olarak hizmet verdiğimiz kitlenin akademik personel ya da onları arkasına almış olan diğer personellerin bitmek bilmeyen istekleri…", "Kurumumuzda üst yöneticilerimiz sistem çalıştığı sürece IT birimini ve ekibini bir eksiğiniz ihtiyacınız var mı diye sormamaktadır…"*
K4	T6K5	*"IT personellerinin arkasında duran idari ya da akademik bir kadronun olması ile işlerin içinden çıkılamaz hale gelmesi iş sürekliliğini sekteye uğratmaktadır…", "Fakat herhangi bir problem olduğunda hemen suçlu aramaktadırlar…", "Konu hususunda bilgili bir yöneticinin olmaması ya da birimin müdürlük kadrosunda olmaması sebebi ile tüm birimler IT birimini kendileri ile eşit görmekte ve verdiğiniz kararları umursamamaktadırlar…"*
K4	T6K4	*"Konu hususunda bilgili bir yöneticinin olmaması ya da birimin müdürlük kadrosunda olmaması sebebi ile tüm birimler IT birimini kendileri ile eşit görmekte ve verdiğiniz kararları umursamamaktadırlar…"*
K5	T6K3	*"Plan olmadan dijital varlıklarımız yani sunucu ve depolama ünitelerimiz risk altında olur mesela Öğrenci Bilgi Sisteminden tutun E-posta Sistemine kadar verdiğimiz hizmetler risk altında olur…"*
K5	T6K2	*"Plan bizi ve yöneticileri risklere karşı bilinçlendirme konusunda gereklidir…", "Üst yöneticilerimize gerekli açıklamaları yaptığımız için bu konuda bilgileri bulunmakta, konunun önemini bilmektedirler…"*
K5	T6K1	*"Ekonomik olarak onların verecekleri kararları kolaylaştırdığımız sürece genellikle planı onaylamaktadırlar…"*
K5	T6K7	*"Yetişen, plana hakim olan personelin emekli olması, işten ayrılması gibi nedenleri sayabilirim..."*
K5	T6K3	*"Her şeyi test ettik çalıştığından emin olduk mimari olarak bizim tasarladığımızla birebir aynısı oldu ama bu sistemde yetersiz biz aktif pasif bir mimari tercih ettik bire bir aktif aktif çalışacak bir mimaride planı yeniden güncellememiz gerekecek…"*

Tablo 3.11. (Devamı)

Katılımcı	Kod	Görüş
K6	T6K2	*"Halihazırda kullandığımız bir kurtarma planımız var. Daha geçen sene yaptık yani güncel, kapasitemizin artmasına göre planı güncelleyeceğiz…", "Şimdiye kadar planı uygulama bir ihtiyacımız olmadı çok şükür. Fakat planın olması hem idari hem de mali açıdan bize avantaj sağlayacağını düşünüyorum…", "Plan olmazsa idareye felaketten sonra hesap veremezsiniz. Neden yapmadınız derler en basit anlamda planın olumsuz tarafı bu…"*
K6	T6K1	*"Şimdiye kadar planı uygulama bir ihtiyacımız olmadı çok şükür. Fakat planın olması hem idari hem de mali açıdan bize avantaj sağlayacağını düşünüyorum…", "Yöneticiler plan olmasını istiyor. Plana katkıda da bulunuyorlar…"*
K7	T6K3	*"Evet, kurumumuzda bir BT felaket kurtarma planı bulunmakta. Plan sürekli güncellenmekte çünkü bilgi işlem altyapısının sürekliliğini sağlamak ve saldırılarda falan verilerin kaybını engellemek ve verdiğimiz hizmetlerin en kısa sürede tekrar verilmesi için güncellememiz gerekiyor…", "Ayrıca, riskler açısından veri kaybı, sistem arızaları ve dış kaynaklı güvenlik açıkları da sürekli olarak izlenmekte ve bu risklerin olabildiği kadar en aza düşürülmesi bizden beklenmektedir. İş sürekliliği konusunda ise, herhangi bir aksaklık durumunda sistemlerin hızlı bir şekilde toparlanması, verilerin düzenli olarak yedeklenmesi ve gerektiğinde hızlıca kurtarılması beklenmekte, genellikle sorun olmadan önce sorun yapacak şeyleri bulup çözmemiz isteniyor…"*
K7	T6K2	*"Evet, kurumumuzda bir BT felaket kurtarma planı bulunmakta. Plan sürekli güncellenmekte çünkü bilgi işlem altyapısının sürekliliğini sağlamak ve saldırılarda falan verilerin kaybını engellemek ve verdiğimiz hizmetlerin en kısa sürede tekrar verilmesi için güncellememiz gerekiyor…"*
K7	T6K1	*"Kurumumuzda, rektörlük ve kurum kültürü olarak tüm yöneticiler planın önemini kavrayarak bize her zaman destek oluyorlar…", "Felaket kurtarma planları, iş sürekliliği ve veri güvenliği gibi kritik alanlarda riskleri minimize etmek için yöneticiler, bu planların oluşturulmasına genellikle belirtiğim gibi tam destek vermektedirler…", "Planı geliştirmeyi kolaylaştıran faktörler arasında ise yönetimin destekleyici yaklaşımının çok önemli olduğunu söyleyebilirim…"*
K7	T6K4	*"…planın uygulanabilmesi için gerekli olan teknik altyapı ve insan kaynağı da bazen yeterli olmuyor. Bizde olmadı ama olsa işimiz epey zorlaşırdı…"*
K7	T6K6	*"Evet, BT felaket kurtarma planımız ile hayata geçirilen plan arasında bazı farklılıklar oldu…"*

Tablo 3.11. (Devamı)

Katılımcı	Kod	Görüş
K7	T6K7	*"Son olarak planlama sırasındaki personellerin istifa etmeleri ya da özel sektöre gitmeleri rol dağılımını değiştirmemizi gerektirdi ama plan son haliyle devreye alındı…"*
K8	T6K5	*"Çünkü yöneticilerimiz planın sadece maddi olanaklarla güncellenebileceğini düşünüyorlar…"*
K8	T6K1	*"Plan geliştirme konusunda yöneticilerimiz bizleri destekliyor…"*
K8	T6K4	*"Personel yetersizliği…"*
K9	T6K4	*"Olumsuz sonuçlar olarak, plana hazırlık süreçlerinde harcanan zamanda personel yetersizliği duyan birimlerde farklı iş süreçleri geliştirilebilir…"*
K9	T6K7	*"Olumsuz sonuçlar olarak, plana hazırlık süreçlerinde harcanan zamanda personel yetersizliği duyan birimlerde farklı iş süreçleri geliştirilebilir…"*
K9	T6K1	*"Kurumumuzda üst yöneticiler, BT felaket kurtarma planlarının önemini kabul etmekte ve bu planların oluşturulmasına büyük bir destek vermektedir. Planı onaylıyorlar…", "Planın geliştirilmesini kolaylaştıran faktörler arasında, üst yönetimden alınan tam destek…"*
K9	T6K3	*"Planların etkili olabilmesi için yöneticilerimiz, bizden düzenli raporlar almakta ve planların güncel tutulmasına önem vermektedir…"*
K9	T6K6	*"Son olarak geliştirmeyi zorlaştıran başlıca faktörlerden biride her felaket tahmin edemezsiniz, öngöremediğiniz sorunlar için felaket senaryoları ve riskleri yazmak epey zor bir iş…", "Evet, planlanan ile hayata geçirilen felaket kurtarma planımız arasında bazı farklılıklar yaşandı…"*
K9	T6K3	*"Son olarak, planın sürekli güncellenmemesi de bir sorun oluşturdu. Planı yaptığımız ilk zamanlar sunucular, sistemler, cihazlar yeni ve günceldi sonra teknoloji değiştikçe planın içeriğini değiştirmek bizi zorladı…"*
K10	T6K6	*"Kurum riskleri en aza indirmek için önceden önlem almayı istiyor. Her şeyi yedekleyerek iş sürekliliğinin sağlanabileceği düşünülmekte…"*
K10	T6K1	*"Üst yönetim yasal zorunluklar kapsamında planın olmasını istiyor. Bizden desteklerini esirgemiyorlar…"*
K10	T6K5	*"Üst yönetim izin vermezse, destek olmazsa, finansal olanak tanımazsa, kimse planı uygulamak istemezse plan oluşturulamaz…"*

Katılımcılarla yapılan görüşme formlarının tamamı tematik bir biçimde analiz edildiğinde oluşturulan tüm temalara ait frekans ve yüzde değerleri Tablo 3.12'de sunulmuştur.

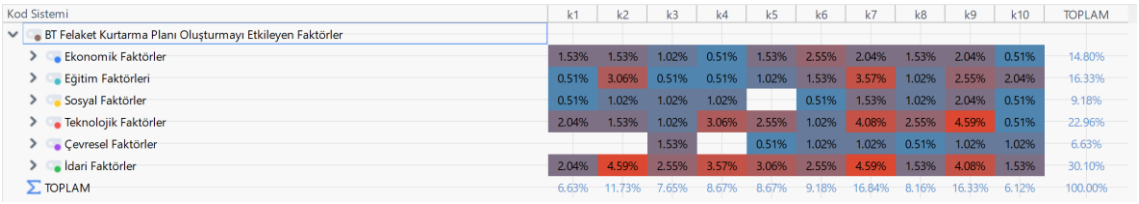
Tablo 3.12. Tüm Temalara Ait Frekans ve Yüzde Değerleri.

Temalar	**Frekans**	**Yüzde**
Plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin sağlanması	14	7.14
Yönetim desteği ve taahhüdü	14	7.14
Öngörü sahibi olma avantajı	12	6.12
Güncel ve teknolojik yeterlilikte bir plana sahip olmak	12	6.12
Sürekli ve kesintisiz hizmet altyapısına sahip olmak isteği	10	5.10
Yeterli bütçe temininin yapılamaması	8	4.08
Mevcut altyapının esneksizliği	8	4.08
Hedef -maliyetin tahsis edilen maliyetlerden yüksekliği	8	4.08
Yasal zorunluluklara uyma gerekliliği	7	3.57
Nitelikli personel eksikliği	7	3.57
İş birliği	7	3.57
Eski ve zayıf altyapının getirdiği zorluklar	7	3.57
Yöneticilerin plan hakkında bilgi eksikliği	6	3.06
Bürokrasi ve karar alma zorlukları	6	3.06
Deneyimli ekip üyelerine sahip olma	5	2.55
Güncel ve teknolojik yeterlilikteki bir plana sahip olamamak	5	2.55
Siber güvenlik önlemlerine sahip olmak	5	2.55
Belirsizlik ve öngörü eksiklikleri	5	2.55
Plan için yüksek bütçeye sahip olabilmek	4	2.04
Öngörülemez maliyetlerin karşılanabilir olamaması	4	2.04
Felaket psikolojisinin üstesinden gelebilecek eğitime sahip olmak	4	2.04
Kritik kamu hizmeti	4	2.04
Doğal afetlere karşı ön hazırlık	4	2.04
Öngörülemez maliyetlerin karşılanabilir olması	3	1.53
Farkındalık ve kültürel hazırlık eksiklikleri	3	1.53
Beklenmedik teknolojik zorluklar	3	1.53

Tablo 3.11. (Devamı)

Temalar	Frekans	Yüzde
Personel değişiklikleri sorunları	3	1.53
Çalışanların eğitim eksiklikleri	2	1.02
Yeniliğe karşı direnç	2	1.02
Kesintisiz iletişim altyapısına sahip olmak	2	1.02
Siber güvenlik önlemleri eksiklikleri	2	1.02
Kurumsal direnç ve değişim yönetimi sorunları	2	1.02
Kriz durumunda ekonomik zorluklar	1	0.51
Yasal gerekçelerle bütçe kısıtlamaları	1	0.51
Plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin eksikliği	1	0.51
Diğer üniversite personellerinden takdir beklentisi	1	0.51
Yeni ve yeterli altyapıya sahip olmak	1	0.51
Dış kaynaklı hizmetlere sahip olmak	1	0.51
Kriz durumlarında ürün tedariki sorunları	1	0.51
İtibar beklentilerinin karşılanması	1	0.51
TOPLAM	**196**	**100.00**

Son olarak analiz sonuçlarında katılımcıların hangi temalarda daha fazla görüş bildirdiklerini gösteren ısı matrisi Şekil 3.15'de sunulmuştur.



Şekil 3.15. Katılımcıların Tema Görüş Sıklıkları.

Şekil 3.15'e göre idari faktörler teması %30,10 oranında en sık kullanılan temadır. En az sıklıkta geçen temanın %6,63 oranında çevresel faktörler olduğu analiz edilmiştir.

SONUÇ VE TARTIŞMA

Çalışmanın bu bölümünde literatür ve bulgulardan elde edilen bilgiler doğrultusunda sonuçlara ve önerilere yer verilmiştir.

Bu çalışmada, BT felaket kurtarma planının kamu üniversiteleri için çok sayıda fayda sağladığı, BT felaket planlamasının BT tabanlı tüm süreçlerde ve sistemlerde, başta verilerin korunması olmak üzere, sistemin esnekliğini artırma ve iş sürekliliğini sağlama açısından hayati önem taşıdığı görülmüş, BT felaket kurtarma planı oluşturulurken birçok farklı faktörün etkili olduğu sonucuna varılmıştır. Bir BT felaket kurtarma planının geliştirilmesi, zorlu bir süreç olmasına rağmen, genel olarak hem yasal zorunlulukların yerine getirilmesinde hem de pratik BT yönetiminde plana sahip olmanın, planın zorlukları ve dezavantajlarına kıyasla daha ağır basan bir avantaj sağladığı görülmektedir. Kamu üniversitelerindeki BT felaket kurtarma planlarının stratejik biçimde etkilendiği faktörler, bu planların gerekliliklerini değerlendirmek amacıyla 10 katılımcı ile yapılan görüşmelerin sonuçlarıyla ortaya konmuştur. Bu veriler, fenomenolojik bir yaklaşımla analiz edilerek katılımcıların deneyimlerine odaklanılmıştır. Çalışmada, 6 adet tema ve 40 adet alt tema içeren bulgulara ulaşılmıştır. Ayrıca, bu alt temalar, çalışmada alt kodlar olarak değerlendirilmiştir.

Bu çalışmada, elde edilen bulgular, özellikle sosyal faktörler alt temasında yer alan kritik kamu hizmeti alt temasını incelendiğinde, üniversitelerin sunduğu kamu hizmetlerinin önemini vurgulamaktadır. Fenomenoloji kuramı, bireylerin yaşantılarının öznel anlamlarını derinlemesine anlamayı hedefleyen bir yaklaşımdır. Bu doğrultuda, katılımcı ifadeleri incelendiğinde, üniversite altyapılarının sosyal bağlamda ne derecede kritik olduğu ve bireysel deneyimlerin bu kritikliği nasıl algıladığına dair anlamlı ipuçları ortaya çıkmaktadır. Bu bağlamda, katılımcı 7'nin (K7) *"Bir BT felaket kurtarma planına sahip olmanın olumlu ve olumsuz sonuçlarını hem kısa vadeli hem de uzun vadeli açılardan değerlendirirsem, özellikle üniversiteler gibi büyük ve kompleks altyapılara sahip kurumlar, kamu için öneme sahip olduğundan dolayı aynı zamanda kritiktirler."* ifadesi, BT felaket kurtarma planlarına ilişkin bireysel algıların hem kısa vadeli hem de uzun vadeli etkiler üzerinden şekillendiğini ortaya koymaktadır. Bu ifade, üniversitelerin karmaşık ve geniş ölçekli BT altyapılarının yalnızca teknik bir olgu olarak değil, aynı zamanda sosyal bir gereklilik olarak değerlendirilmesi gerektiğini göstermektedir.

Fenomenoloji kuramına göre, bireylerin deneyimleri ve bu deneyimlerin bağlam içerisindeki anlamları, sadece bireylerin kişisel yaşantılarını değil, aynı zamanda o bireylerin içinde bulundukları sosyal sistemlerin dinamiklerini de yansıtır. Bu bağlamda, K7'nin kamuya hizmet sunan üniversiteleri kritik bir yapı olarak tanımlaması, onun sosyal bağlamdaki "kritiklik" kavramını nasıl deneyimlediğine dair ipuçları sunmaktadır. Benzer şekilde, katılımcı 4'ün (K4) *"Mevcut sistem odasında kalıcı bir şekilde çalışamaz duruma geldiğinde; yedek sistem odası çalışır fakat hastanenin tüm lokasyonlarında sistem devreye alınamaz çünkü ana sistem odasından tüm lokasyonlara network erişimi bulunmakta ama yedek sistem odasından erişim bulunmamaktadır. Biraz önce belirttiğim sıkıntılardan dolayı gerekli altyapı çalışması yapılamamaktadır."* ifadesi, BT sistemlerinin kesintisiz işlevselliğinin kamu hizmetleri açısından vazgeçilmez olduğunu vurgulamaktadır. Bu, katılımcının, sistemlerin başarısızlığı durumunda ortaya çıkabilecek sosyal ve operasyonel sonuçları nasıl algıladığını göstermektedir. Fenomenolojik açıdan bakıldığında, bu ifade, bireyin deneyimlerinin sosyal yapıların kırılganlığına dair farkındalıkla harmanlandığını ortaya koymaktadır.

Jamali ve diğerlerinin çalışması ile bu bulgular arasındaki uyum, fenomenolojik analiz açısından dikkate değer bir bulgu olarak öne çıkmaktadır (Jamali vd., 2019). Literatürdeki bu bulgular, bireylerin BT sistemlerine yönelik deneyimlerinin ve algılarının, yalnızca teknik detaylardan ibaret olmadığını, aynı zamanda sosyal bağlamın önemli bir parçası olduğunu desteklemektedir. Sonuç olarak, fenomenoloji kuramı perspektifinden, BT felaket kurtarma planlarının sosyal ve bireysel algılar üzerinden değerlendirilmesi, bu planların başarısı açısından kritik bir öneme sahiptir. Üniversiteler gibi kamuya hizmet sunan büyük ölçekli kurumlarda, bireylerin bu hizmetleri "kritik" olarak algılaması, sistemlerin yalnızca teknik değil, aynı zamanda sosyal yönlerinin de göz önünde bulundurulması gerektiğini işaret etmektedir. Sadece felaket anında ya da felaket geçirildikten sonra değil, BT sistemlerinde yaşanabilecek herhangi bir olumsuz olay sonrasında, üst yönetim, üniversitenin bir BT felaket kurtarma planına sahip olup olmadığını sorgulayabilir ve bu planın oluşturulmasına yönelik baskı yapabilir. Eckhardt ve arkadaşlarına göre, üst düzey yöneticiler yalnızca büyük felaketler sonucunda kurumlarının savunmasız kalmasından değil, bazen elektrik kesintisi gibi karmaşık olmayan küçük olayların bile BT hizmetlerini uzun süreli kesintilere neden olabileceğinin farkında olduklarını vurgulamıştır (Eckhardt vd., 2019). Bu çalışmada elde edilen

bulgulardan, idari faktörler teması altında ele alınan ön görü sahibi olma ve kesintisiz hizmet altyapısına sahip olma isteği alt temaları, literatürdeki bu çalışmanın sonucuyla paralellik göstermektedir. Ayrıca, Katılımcı-2 (K2)'nin *"...Bir plana sahip olmamanın getirdiği olumsuz bir sonuç düşünemiyorum. Zira en kötü plan bile plansızlıktan iyidir..., kurumumuzdaki üst yönetim her zaman bu tür planları olumlu karşılama eğilimindedir. Düzgün yapılandırılmış ve kurumun ihtiyaçlarıyla örtüşen, hakkında detaylı bilgi verilmiş bir plana. Üst yönetimin soğuk baktığını görmedim."* şeklindeki görüşü ve Katılımcı-7 (K7)'nin *"Felaket kurtarma planları, iş sürekliliği ve veri güvenliği gibi kritik alanlarda riskleri minimize etmek için yöneticiler, bu planların oluşturulmasına genellikle belirttiğim gibi tam destek vermektedirler..., Planı geliştirmeyi kolaylaştıran faktörler arasında yönetimin destekleyici yaklaşımının çok önemli olduğunu söyleyebilirim..."* İfadeleri, yönetim desteği ve taahhüdü temasının önemini ortaya koymaktadır. Bu bulgular, BT felaket kurtarma planı geliştirilmesinde yönetici desteğinin, idari faktörler arasında önemli bir etken olduğunu göstermektedir. Çalışmanın dayandığı Planlı Davranış Teorisi'ne göre, katılımcıların yönetici desteğiyle felaket kurtarma planlarının önemini kavramaları ve bu planların üniversitenin sürdürülebilirliği için gerekli olduğunu benimsemeleri, olumlu bir tutum sergilemelerine katkı sağlayacaktır. Ayrıca, sosyal normlar bağlamında, üniversite içindeki liderlerin ve üst düzey yöneticilerin felaket kurtarma planlarına verdikleri önem, çalışanların bu planlara yönelik sosyal normlarının şekillenmesinde belirleyici bir rol oynar. Yöneticilerin bu planların uygulanmasını desteklemeleri durumunda, diğer çalışanların da bu desteği örnek alarak benzer bir tutum sergileme eğiliminde olmaları beklenebilir.

Kamu üniversitelerinin ve diğer kuruluşların BT envanterleri, hizmet verdikleri alanlara göre mimari açıdan farklılıklar göstermekle birlikte, temel hizmetler açısından benzerlikler taşımaktadır. Felaket anlarında olduğu kadar felaket öncesinde de BT varlık envanterinin doğru bir şekilde bilinmesi, yapılacak yatırımların planlanması ve değerlendirilmesi açısından kritik bir öneme sahiptir. Ayrıca, BT altyapılarının esnekliği, felaket sonrasında sistemlerin hızla yeniden aktif hale getirilmesini ve hizmetlerin kesintisiz bir şekilde sürdürülmesini sağlamada önemli bir avantaj sunmaktadır (Sarker vd., 2020). Sarker ve arkadaşlarının elde ettiği sonuçlar, bu çalışmada elde edilen bulgulardan biri olan "teknolojik faktörler" teması altındaki eski ve zayıf altyapının getirdiği zorluklar alt teması ile paralellik göstermektedir. Bu bulgular, katılımcıların BT

felaket kurtarma planı geliştirirken karşılaştıkları zorluklara işaret etmektedir. Bununla birlikte, bazı katılımcıların yeni ve yeterli altyapıya sahip olmaları sayesinde plan geliştirme sürecinde teknolojik faktörler açısından kolaylık yaşadıkları gözlemlenmiştir. Aynı tema altında yer alan bir diğer alt tema olan mevcut altyapının esneksizliği ise katılımcı 8'in (K8) şu ifadesiyle vurgulanmaktadır: *"...eskiden kalan karmaşık ama çalışması gereken sistemlerin test edilememesi planı zorlaştırıyor..."*. Bu bulgu, mevcut altyapının esneksizliğinin BT felaket kurtarma planlarının geliştirilmesinde kritik bir faktör olduğunu açıkça ortaya koymaktadır. Planlı Davranış Teorisi çerçevesinde değerlendirildiğinde, bireylerin felaket kurtarma planlarına katılım niyetlerinin, algıladıkları davranışsal kontrol düzeyleriyle yakından ilişkili olduğu görülmektedir. Katılımcılar, felaket kurtarma faaliyetlerine katılmak için yeterli bilgi, beceri ve kaynağa sahip olduklarına inandıkları takdirde, bu faaliyetlere katılım ihtimalleri artmaktadır. Bununla birlikte, felaket anında karşılaşılan lojistik zorluklar, eğitim eksiklikleri ve kaynak yetersizlikleri, katılımı olumsuz yönde etkileyebilmektedir. Bu doğrultuda, afet hazırlık eğitimlerinin güçlendirilmesi ve kaynakların artırılması, bireylerin davranışsal kontrol algılarını iyileştirerek felaket kurtarma planlarına katılım düzeyini artırabilir.

Yedeklilik, BT felaket kurtarma planlarının temel unsurlarından biridir ve bu kavram, hem sistemlerin güvenilirliğini artırma hem de operasyonel sürekliliği sağlama adına kritik bir rol oynamaktadır. Ancak, modern veri merkezlerinin bulut bilişim olanaklarından faydalanmasına rağmen, geleneksel felaket kurtarma yaklaşımlarının hâlâ birçok avantaja sahip olduğu bilinmektedir. Bu durum, felaket kurtarma stratejilerinin çeşitli alt yapı seçenekleriyle desteklenmesi gerektiğini ortaya koymaktadır (Arief & Putra, 2020). Arief ve Putra tarafından vurgulanan bu görüş, bireylerin ve kurumların farklı ekonomik ve operasyonel koşullara göre tercihlerde bulunmalarını açıklayan bir bağlam sunmaktadır. Bu bağlamda, fenomenoloji ve planlı davranış teorisi kuramları, katılımcıların yedeklilik ve ekonomik kısıtlamalarla ilgili deneyimlerini daha derinlemesine anlamak için faydalı bir yaklaşım sunmaktadır.

Kuramsal olarak fenomenoloji perspektifinden, katılımcıların BT felaket kurtarma planlarıyla ilgili deneyimleri, yalnızca teknik gereksinimler değil, aynı zamanda sosyal, ekonomik ve psikolojik faktörlerle şekillenmektedir. Katılımcı 6'nın (K6) *"Paramız olsa tüm sistemin birebir aynısını yaparız, o zaman daha içimiz rahat ederiz..."* ifadesi, bireylerin yedeklilik ve güvenlik konusundaki kaygılarını ve arzu ettikleri ideal durumu

yansıtmaktadır. Bu görüş, fenomenolojik açıdan, katılımcının içsel dünyasında güvenlik ve yedekliliğe duyduğu ihtiyacı ortaya koymaktadır. Fenomenoloji kuramı, bireylerin bu tür sistemlere ilişkin deneyimlerinin öznel ve duygusal bağlamda nasıl şekillendiğine dikkat çeker ve bu tür ifadeler, katılımcıların risk algısını ve BT felaket senaryolarına karşı duyduğu endişeleri anlamamıza yardımcı olur. Katılımcıların, ekonomik sınırlamalar nedeniyle ideal yedeklilik çözümünü hayata geçirememe deneyimleri, bu tür kişisel ve sosyal algıları derinlemesine incelemeyi gerektirir. Benzer şekilde, planlı davranış teorisi kuramı da bu durumu anlamada önemli bir çerçeve sunmaktadır. Planlı davranış teorisi, bireylerin davranışlarını, tutumlar, öznel normlar ve algılanan davranışsal kontrol gibi faktörlerin şekillendirdiğini öne sürer. Katılımcı 5'in (K5) *"Aktif aktif bir mimari olsun istedik ama ekonomik açıdan ilk olarak aktif pasif çalışacak bir mimari oluşturmaya dikkat ettik…"* ifadesi, bir yandan arzu edilen hedefe ulaşmak için gösterilen niyeti (aktif aktif mimari), diğer yandan ekonomik kısıtlamaların yol açtığı davranışsal sınırları (aktif pasif mimari) ortaya koymaktadır. Bu tür ifadeler, planlı davranış teorisi perspektifinden, katılımcıların felaket kurtarma planlarına dair tutumlarının, ekonomik koşullar ve dışsal faktörler tarafından ne kadar şekillendiğini göstermektedir. Katılımcıların, ekonomik kısıtlamalara rağmen felaket kurtarma hedeflerine ulaşmak için uygun bir çözüm yolu bulma çabası, onların bu hedeflere yönelik planlama süreçlerinde ne derece kontrol sahibi olduklarını ve bu sürecin sonuçlarına ilişkin beklentilerini yansıtmaktadır.

Planlı davranış teorisi ve fenomenolojik bakış açıları, katılımcıların teknoloji ve felaket kurtarma planları konusundaki deneyimlerinin, sadece teknik gereksinimlerden değil, aynı zamanda ekonomik, sosyal ve bireysel faktörlerden de etkilendiğini ortaya koymaktadır. Bu bağlamda, yedekliliğin sağlanamaması, yalnızca bir tasarım hatası veya teknik bir eksiklik değil, aynı zamanda katılımcıların sınırlı kaynaklar ve ekonomik baskılar karşısında verdikleri stratejik bir tepki olarak değerlendirilebilir. Bu süreç, kurumların ve bireylerin belirli hedeflere ulaşmak için algıladıkları kontrol ve kaynak kısıtlamaları doğrultusunda şekillenir. Bu teorik yaklaşımlar, bireylerin ve organizasyonların BT altyapılarıyla ilgili kararlarını etkileyen çok boyutlu faktörleri anlamamıza yardımcı olarak, daha etkili ve sürdürülebilir felaket kurtarma stratejilerinin geliştirilmesine katkıda bulunabilir.

İyi hazırlanmış bir veri koruma planının, bir kuruluşun verilerini hırsızlık, kayıp ve yolsuzluğa karşı korunmasına yardımcı olduğu bilinmektedir (Atiku vd., 2021). Bu bağlamda, BT felaket kurtarma planı geliştirilirken veri koruma planlamasının, diğer bir ifadeyle yedekleme ve yedekten dönme süreçlerinin iyi ayarlanması gerekmektedir. İyi hazırlanmış bir plan, uyulması gereken yasal zorunluluklar konusunda da fayda sağlayabilmektedir. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı Bilgi ve İletişim Güvenliği Rehberi'ne uyum zorunluluğu taşıyan kamu kurumlarının yedekleme planlarının olması gerekmektedir. Bu bağlamda, bu çalışmanın çevresel faktörler teması içerisinde yer alan yasal zorunluluklara uyma gerekliliği temasına göre katılımcı 8'in (K8) planı oluştururken faydalandığı dış kaynaklar arasında bu belgenin yer aldığı *"…Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yönergelerine baktık…"* görüşü, plan geliştirirken yasal zorunlulukların planı geliştirmeye yönelik etkilerini göstermektedir. Fenomenolojik bir bakış açısıyla, katılımcı 8'in ifadesi, felaket kurtarma planlaması sürecinde dışsal faktörlerin, özellikle yasal gerekliliklerin, nasıl bir anlam taşıdığını ve bu gerekliliklerin katılımcıların kişisel deneyimleriyle nasıl etkileşime girdiğini göstermektedir. K8'in *"Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yönergelerine baktık"* şeklindeki açıklaması, çevresel faktörlerin bireylerin karar alma süreçlerine nasıl etki ettiğini, özellikle de yasal uyumluluğun oluşturulacak plan üzerindeki etkilerini vurgulamaktadır. Bu durum, katılımcının yalnızca teknik bir gereklilikten ziyade, yasal sorumluluklarını yerine getirme çabasıyla hareket ettiğini ve bu çabanın, kurumlar arasındaki standartları ve güvenliği sağlama amacını taşıdığını gösterir. Fenomenolojik açıdan, bireylerin dışsal zorunluluklar karşısındaki deneyimleri, onların planlama sürecine bakış açısını şekillendirir ve bu süreç, hem yasal hem de güvenliksel gereksinimleri dengede tutmayı amaçlayan bir "yaşantı" olarak değerlendirilir.

Felaket anlarında personelin bilinçli olması büyük önem taşımaktadır. Bilgi Teknolojileri ile ilgili kritik durumlarda, yalnızca belirli personelin değil, organizasyonun tüm yapısındaki herkesin gerekli eğitimi almış ve sorumluluk bilincine sahip olması gerekmektedir (Paredes vd., 2019). Yaşanacak felaket durumunda, kimsenin ne yapacağını bilmemesi gibi bir durumla karşılaşılabilir. Böyle bir durumda, felaket kurtarma planının etkisi düşecektir (Appleby-Arnold vd., 2021; Eser & Marangoz, 2023). Literatürde yer alan bu bilgilere paralel olarak, bu çalışmanın bulguları içerisinde yer alan eğitim faktörleri temasının alt temalarından biri olan felaket psikolojisinin üzerinden

gelebilecek eğitime sahip olmak ve plan geliştirmeye yönelik akademik ve teknik süreç ve bilgilere hakimiyetin sağlanması alt temaları için katılımcıların; *"...Ayrıca, planın düzgün bir şekilde uygulanabilmesi için tüm çalışanların eğitilmesi gerekir, bu da ek kaynak ve eğitim gereksinimleri doğurabilir. Felaket durumunda planın işe yaramaması olursa eğer bu da ciddi bir güven kaybına neden olabilir…(K9)*" ve *"…Felaket olduğunda insan bir şoka girer, sonra şoku atlatınca ne yapacağını bilemez. Eğer elinde bir plan olursa en azından ona göre hareket eder…(K8)"* görüşleri saptanmıştır.

Fenomenolojik bir bakış açısıyla, katılımcıların felaket anlarında yaşadıkları duygusal ve bilişsel süreçler, onların bu tür durumlarla nasıl başa çıkacaklarını anlamada kritik bir önem taşır. K9'un ifadesinde yer alan, *"Ayrıca, planın düzgün bir şekilde uygulanabilmesi için tüm çalışanların eğitilmesi gerekir, bu da ek kaynak ve eğitim gereksinimleri doğurabilir. Felaket durumunda planın işe yaramaması olursa eğer bu da ciddi bir güven kaybına neden olabilir…"* görüşü, felaket anında bireylerin karşılaştığı potansiyel şok ve belirsizlik karşısında nasıl bir duygu durumuna gireceklerini ve bu durumun, eğitim ve bilinçlenme gerekliliğini nasıl anlamlandırdıklarını gösterir. Fenomenoloji kuramına göre, bireyler bu tür felaket anlarında, sadece teknik bir aksaklık değil, aynı zamanda duygusal bir deneyimle karşı karşıya kalırlar. Bu da, felaket durumunun yalnızca işlevsel değil, aynı zamanda sosyal ve psikolojik bir boyut taşıdığı anlamına gelir. K9'un güven kaybına dair yaptığı vurgu, bireylerin bu tür duygusal ve sosyal kayıpların etkilerini nasıl deneyimleyeceklerini ve bunun kurum içindeki bağları nasıl etkileyebileceğini ortaya koymaktadır. Bir diğer katılımcı, K8, felaket anlarında *"Felaket olduğunda insan bir şoka girer, sonra şoku atlatınca ne yapacağını bilemez. Eğer elinde bir plan olursa en azından ona göre hareket eder…"* diyerek, felaket psikolojisinin bireylerin tepki verme biçimlerini nasıl etkilediğine dikkat çekmiştir. Fenomenolojik açıdan, bu ifade, bireylerin felaket sırasında yaşadıkları duygusal ve bilişsel karmaşıklığı anlamamıza olanak tanır. Şok ve belirsizlik, bir bireyin felaket anındaki en belirgin tepkilerindendir ve fenomenolojik bakış açısına göre, bu tepkiler, kişinin geçmiş deneyimlerine, değerlerine ve çevresindeki sosyal dinamiklere dayalı olarak şekillenir. K8'in, planın elinde bulunmasının bireyin tepki verme biçimini nasıl yönlendirebileceğine dair vurgusu, bu durumun sadece bir teknik çözüm değil, aynı zamanda bireyin yaşadığı korku ve belirsizlikle başa çıkma stratejisi olarak değerlendirilebileceğini gösterir.

Fenomenoloji kuramına göre, felaket kurtarma planları yalnızca bir organizasyonel araç değil, aynı zamanda bireylerin kriz anındaki duygusal ve psikolojik deneyimlerini organize etme biçimidir. Katılımcıların ifadeleri, felaket durumlarında eğitimli olmanın, bireylerin bu duygusal süreçleri daha iyi yönetmelerine yardımcı olacağına işaret etmektedir. Felaket planları, bireylerin duygusal durumlarına hitap ederek, onlara bir rehberlik ve kontrol duygusu sunar, bu da yaşadıkları felaket deneyiminin daha az travmatik ve daha yönetilebilir olmasına olanak tanır.

Son olarak ileride yapılacak çalışmalar için araştırmacılara aşsağıdaki maddelerde belirtilen öneriler sunulmuştur.

- Kriz durumlarında liderlik ve kriz yönetimi konuları ele alınabilir. Gelecekteki araştırmacıların, BT felaket kurtarma süreçlerinin liderlik boyutunu keşfetmeleri ve farklı liderlik tarzlarının BT felaket kurtarma planlarının gelişimini nasıl etkileyebileceği konusunda daha fazla bilgi edinmeleri faydalı olacaktır. Bu sayede, kriz anlarında liderlerin rolleri ve etkileri üzerine derinlemesine analizler yapılabilir ve daha etkili kriz yönetim stratejileri geliştirilebilir.
- Örneklem sayısı genişletilebilir veya evren daha dar bir çerçeveye düşürülerek spesifik sonuçlar elde edilebilir. Gelecek çalışmalarda Sadece Üniversite hastaneleri ve BT süreçleri ele alınılabilir.

KAYNAKÇA

Abualkishik, A. Z., A., A., & Gulzar, Y. (2020). "Disaster Recovery in Cloud Computing Systems: An Overview". *International Journal of Advanced Computer Science and Applications*, *11*(9). https://doi.org/10.14569/IJACSA.2020.0110984

Adeshiyan, T., Attanasio, C. R., Farr, E. M., Harper, R. E., Pelleg, D., Schulz, C., Spainhower, L. F., Ta-Shma, P., & Tomek, L. A. (2009). "Using Virtualization for High Availability and Disaster Recovery". *IBM Journal of Research and Development*, *53*(4), 1-8.

Aerts, J. C. J. H., Botzen, W. J. W., Botzen, W. J. W., Botzen, W. J. W., Clarke, K. C., Cutter, S. L., Hall, J. W., Merz, B., Michel-Kerjan, E. O., Mysiak, J., Surminski, S., & Kunreuther, H. (2018). "Integrating Human Behaviour Dynamics Into Flood Disaster Risk Assessment". *Nature Climate Change*, *8*, 193-199. https://api.semanticscholar.org/CorpusID:4568675

AFAD. (2024). *Afet Türleri*. https://www.afad.gov.tr/afet-turleri

Ajzen, I. (1991). "The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes", 50, 179–211. *De Young*, *50*(2), 509-526.

Ajzen, I. (2002). Constructing a TPB questionnaire: Conceptual and methodological considerations. *University of Massechusetts Amherst, Office of Information Technologies*.

Ajzen, I. (2005). *Attitudes, Personality and Behaviour*. UK: McGraw-hill education.

Akıllı, Y. (2016). *Sanal Sunucu Sistemlerinde Felaket Kurtarma Yönetimi ve Felaket Kurtarma Plan Önerisi*. (Yüksek Lisans Tezi). İstanbul: Aydın Üniversitesi Fen Bilimleri Enstitüsü.

Aksu, H. (2011). *BT Yöneticisinin El Kitabı: Kurumsal Bilişim Olgunluk Modeli* (C. 235). İstanbul: Pusula.

Alhazmi, O. H., & Malaiya, Y. K. (2013). "Evaluating Disaster Recovery Plans Using the Cloud". *2013 Proceedings Annual Reliability and Maintainability Symposium (Rams)*, 1-6.

Alkan, C. (1998). *Egitim Teknolojisi*. Ankara: Anı Yayıncılık.

Andrade, E., Nogueira, B., Matos, R., Callou, G., & Maciel, P. (2017). "Availability Modeling and Analysis of A Disaster-Recovery-as-a-service Solution". *Computing*, *99*, 929-954.

Appleby-Arnold, S., Brockdorff, N., & Callus, C. (2021). "Developing a "Culture of Disaster Preparedness": The Citizens' View". *International Journal of Disaster Risk Reduction*, *56*, 102133. https://doi.org/10.1016/j.ijdrr.2021.102133

Arief, R., & Putra, Y. H. (2020). *Design Business Continuity Plan of Data Center Using ISO 22301:2012*. https://doi.org/10.2991/aebmr.k.200108.013

Armitage, C. J., & Conner, M. (2001). "Efficacy of the Theory of Planned Behaviour: A Meta-analytic Review". *British Journal of Social Psychology*, *40*(4), 471-499.

Arno, B. R., Friedl, A., Gross, P., & Schuerger, R. (2010). "Reliability of Example Data Center Designs Selected by Tier Classification". *2010 IEEE Industrial and Commercial Power Systems Technical Conference - Conference Record*, 1-8. https://doi.org/10.1109/ICPS.2010.5489890

Arregoces, M., & Portolani, M. (2003). *Data Center Fundamentals*. Indianapolis: Cisco Press.

Ateş, V., & Güneş, B. (2016). "Üniversitelerde Bilişim Teknolojileri Risk Yönetimi Başarısını Etkileyen Faktörler Üzerine Nitel Bir Araştırma: Ankara İli Örneği". *Bilgi Dünyası*, *17*(1), 39-56.

Atiku, M., Garba, A. A., & Bade, A. M. (2021). A Brief Analysis on the Existing Disaster Recovery Phases and Activities Plans.

Bach, C., Gupta, A. K., Nair, S. S., & Birkmann, J. (2013). "Critical Infrastructures and Disaster Risk Reduction". *National Institute of Disaster Management and Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ), New Delhi*, *72*.

Badotra, S., Sundas, A., Ganguli, I., Verma, A., & Singh, G. (2023). "Intelligent Network Load Balancing System with Geographic Routing and SDN Multi-Controller Architecture". *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 83-86. https://doi.org/10.1109/SmartTechCon57526.2023.10391811

Bagozzi, R. P., Baumgartner, J., & Yi, Y. (1989). "An Investigation Into the Role of Intentions as Mediators of the Attitude-Behavior Relationship". *Journal of Economic psychology*, *10*(1), 35-62.

Bal, H. (2012). *Nitel Araştırma Yöntemleri.* Isparta: Fakülte Kitabevi.

Baloğlu, B. (2005). "Hipotez ve Varsayım Birbirlerinin Yerine Kullanılabilir Mi?". *Istanbul Journal of Sociological Studies*, *32*, 125-129.

Baz, F. Ç., & Uludağ, K. (2021). "Veri Merkezi Güvenliğinin Sağlanmasında IoT Sensörlerinin Kullanımı Üzerine Bir Uygulama". *Avrupa Bilim ve Teknoloji Dergisi*, *27*, 392-397. https://doi.org/10.31590/ejosat.939216

Bhardwaj, A., & Krishna, C. R. (2021). "Virtualization in Cloud Computing: Moving from Hypervisor to Containerization—A Survey". *Arabian Journal for Science and Engineering*, *46*(9), 8585-8601. https://doi.org/10.1007/s13369-021-05553-3

Blue, C. L. (1995). "The Predictive Capacity of the Theory of Reasoned Action and the Theory of Planned Behavior in Exercise Research: An Integrated Literature Review". *Research in Nursing & Health*, *18*(2), 105-121. https://doi.org/10.1002/nur.4770180205

Blundell, S. (2015). *A Descriptive Phenomenological Investigation of the Academic Information Search Process Experience of Remedial Undergraduate Students* [Ph.D. Dissertation, Kent State University, College of Communication and Information]. Içinde *ProQuest Dissertations and Theses*. https://www.proquest.com/dissertations-theses/descriptive-phenomenological-investigation/docview/1700193255/se-2?accountid=8319

Boyatzis, R. E. (1998). *Transforming Qualitative İnformation: Thematic Analysis and Code Development*. Sage.

Bradley, W. C. (2017). *Handbook of: Data Center Management* (L. C. Bradley, Ed.). Auerbach Publications. https://doi.org/10.1201/9780203712726

Braun, V., & Clarke, V. (2019). "Psikolojide Tematik Analizin Kullanımı". *Journal of Qualitative Research in Education*, *7*(2), 1-26. https://doi.org/10.14689/issn.2148-2624.1.7c.2s.17m

Braun, V., Clarke, V., Boulton, E., Davey, L., & McEvoy, C. (2021). "The Online Survey As A Qualitative Research Tool". *International Journal of Social Research Methodology*, *24*(6), 641-654. https://doi.org/10.1080/13645579.2020.1805550

Bruzzese, J. P. (2009). Virtualization and Disaster Recovery.

Büyüköztürk, Ş., Akgün, Ö. E., Demirel, F., Karadeniz, Ş., & Çakmak, E. K. (2014). *Bilimsel Araştırma Yöntemleri*. Ankara: Pegem Akademi.

Cervone, H. F. (2017). "Disaster Recovery Planning and Business Continuity for Informaticians". *Digital Library Perspectives*, *33*(2), 78-81.

Chang, V. (2015). "Towards a Big Data System Disaster Recovery in A Private Cloud". *Ad Hoc Networks*, *35*, 65-82.

Conner, M. (2020). "Theory of Planned Behavior". İçinde *Handbook of Sport Psychology* (ss. 1-18). Wiley. https://doi.org/10.1002/9781119568124.ch1

Crosby, C., & Curtis, C. (2021). "Hosting Or Colocation Data Centers". Içinde *Data Center Handbook* (ss. 65-75). Wiley. https://doi.org/10.1002/9781119597537.ch4

Crump, G. (2024). *The HCI Disaster Recovery Problem*. https://www.verge.io/blog/protection/the-hci-disaster-recovery-problem/

Curtis, P., Carey, M., & Committee of Sponsoring Organizations of the Treadway Commission. (2012). Risk assessment in practice.

Çakır, H., & Yaşar, H. (2015). "Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri". *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *3*(2), 488-507.

Das, D. (2023). *ISO 27031 - The Business Continuity Appendix to ISO 27001*. https://www.linkedin.com/pulse/iso-27031-business-continuity-appendix-27001-das-cisa-cissp?ysclid=lylx9189jx296513968

Demirel, Ö. (1993). *Eğitim Terimleri Sözlüğü: İngilizce-Türkçe, Türkçe-İngilizce*. Ankara: USEM Yayınları.

Demirkasımoğlu, M. (2018). "Tatbikat Planlaması ve Yönetimi". *Resilience*, *2*(2), 145-165.

Dhanujati, N., & Girsang, A. S. (2018). "Data Center-disaster Recovery Center (DC-DRC) for High Availability IT Service". *2018 International Conference on Information Management and Technology (ICIMTech)*, 55-60.

Dinçer, E. M., Yılmaz, P. K., & Ekşi, H. (2023). *Nitel Desenler: Fenomenoloji*. EDAM.

Doğan, A., Söylemez, İ., & Özcan, U. (2016). "Importance of Information Systems For Organizations in Terms of Disaster Recovery". *International Conference on Research in Education and Science (ICRES)*.

Drasgow, F., Luecht, R. M., & Bennett, R. E. (2006). "Technology and Testing". *Educational measurement*, *4*, 471-515.

Eagly, A. H., & Chaiken, S. (1993). "The psychology of attitudes. New York: Hartcourt Brace Janovich". *Psychol. Mark.*, *12*, 459-466.

Eckhardt, D., Leiras, A., & Thomé, A. M. T. (2019). "Systematic Literature Review of Methodologies for Assessing the Costs of Disasters". *International Journal of Disaster Risk Reduction*, *33*, 398-416. https://doi.org/10.1016/j.ijdrr.2018.10.010

Eren, C. (2013). "İş Süreklilik Planlarının Test Edilmesi: Örnek Vaka Çalışması". *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, *49*.

Ersöz, B., & Özmen, M. (2020). "Dijitalleşme ve Bilişim Teknolojilerinin Çalışanlar Üzerindeki Etkileri". *AJIT-e: Academic Journal of Information Technology*, *11*(42), 170-179.

Erten, S. (2002). "Planlanmış Davranış Teorisi İle Uygulamalı Öğretim Metodu". *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, *19*(2), 217-233.

Esen, S. (2015). *Edmund Husserlin fenomenolojisi ve Batı krizi*. (Yüksek Lisans Tezi). Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü.

Eser, N., & Marangoz, A. Y. (2023). "Kriz Dönemlerinde Risk Algısının Tüketici Davranışlarına Etkisi: Deprem Örneği". *Alanya Akademik Bakış*, *8*(1), 237-253.

Fallara, P. (2004). "Disaster Recovery Planning". *IEEE Potentials*, *23*(5), 42-44.

Fisher, A. J., Medaglia, J. D., & Jeronimus, B. F. (2018). "Lack of Group-to-individual Generalizability is A Threat to Human Subjects Research". *Proceedings of the*

National Academy of Sciences, *115*(27). https://doi.org/10.1073/pnas.1711978115

Fontana, R. E., Hetzler, S. R., & Decad, G. (2012). "Technology Roadmap Comparisons for TAPE, HDD, and NAND Flash: Implications for Data Storage Applications". *IEEE Transactions on Magnetics*, *48*(5), 1692-1696.

Frechette, J., Bitzas, V., Aubry, M., Kilpatrick, K., & Lavoie-Tremblay, M. (2020). "Capturing Lived Experience: Methodological Considerations for İnterpretive phenomenological inquiry". *International Journal of Qualitative Methods*, *19*, 1609406920907254.

Frisch, Æ. (2008). "System Backup: Methodologies, Algorithms and Efficiency Models". Içinde *Handbook of Network and System Administration* (ss. 205-239). Elsevier.

Gabriel, C. (2015). *Data Center Disaster Recovery and High Availability*. Hoboken, NJ, USA: Wiley & Sons.

Gallagher, S. (2022). *What Is Phenomenology?* (ss. 1-10). https://doi.org/10.1007/978-3-031-11586-8_1

Gang, M., Yan, B., & Hu, B. (2023). "Design and Implementation of Industrial Real-Time Ethernet Redundant Network Based on Parallel Redundancy Protocol". *2023 3rd International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology (CEI)*, 92-98. https://doi.org/10.1109/CEI60616.2023.10527882

Gazdağı, O., & Çetinyokuş, T. (2020). "Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme". *Journal of Humanities and Tourism Research*, *10*(2), 475-491.

Genco, A. (2020). "Türkiye'de Kritik Altyapi ve Kritik Altyapiya Yönelik Tehditler". *Kamu Yönetimi ve Teknoloji Dergisi*, *2*(2), 38-46.

Geng, H. (2014). *Data Center Handbook*. New Jersey: John Wiley & Sons.

Gilstrap, D. L. (2007). "Phenomenological Reduction and Emergent Design: Complementary Methods for Leadership Narrative Interpretation and

Metanarrative Development". *International Journal of Qualitative Methods*, *6*(1), 95-113.

Giorgi, A. (2009). *The Descriptive Phenomenological Method in Psychology: A Modified Husserlian Approach.* Pittsburgh: Duquesne university press.

Gonzales, S. A. (2010). Project management process for disaster recovery projects.

Gökmen, H. T., & Küçüksille, E. U. (2013). *Veri Merkezi Tasarımı*. Antalya: Akademik Bilişim, Akdeniz Üniversitesi.

Gregory, P. H. (2011). *IT Disaster Recovery Planning for Dummies*. New Jersey: John Wiley & Sons.

Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2019). "Exiting the Risk Assessment Maze". *ACM Computing Surveys*, *51*(1), 1-30. https://doi.org/10.1145/3145905

Groenendaal, J., & Helsloot, I. (2020). "Organisational Resilience: Shifting From Planning-Driven Business Continuity Management to Anticipated Improvisation". *Journal of Business Continuity & Emergency Planning*, *14*(2), 102-109.

Gurbetoğlu, A. (2018). Bilimsel Araştırma Yöntemleri. *Erişim Adresi: http://agurbetoglu. com/files/2% 20ARA% C5% 9ETIRMA*, *20*.

Günal, S., Kaleli, C., Bilge, A., & Hoşcan, Y. (2017). *Veri Merkezleri Üzerine Bir İnceleme*. https://ceur-ws.org/Vol-2045/21_Bilisim_2017_paper_18.pdf

Günay, D. (2017). "Teknoloji Nedir? Felsefi Bir Yaklaşım". *Yükseköğretim ve Bilim Dergisi*, *1*, 163-166.

Günel, A. (2014). *Üniversitelere Yönelik Yeni Bir Veri Merkezi Tasarımı ve Uygulaması* (Yüksek Lisans Tezi), Bilecik: Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü]. https://acikkaynak.bilecik.edu.tr/xmlui/bitstream/handle/11552/219/10038962.pdf?sequence=1&isAllowed=y

Hagger, M. S., Cheung, M. W.-L., Ajzen, I., & Hamilton, K. (2022). "Perceived Behavioral Control Moderating Effects in the Theory of Planned Behavior: A

Meta-Analysis". *Health Psychology, 41*(2), 155-167. https://doi.org/10.1037/hea0001153

Hançerlioğlu, O. (2000). *Felsefe Sözlüğü.* 12. Basım, İstanbul: Remzi Kitabevi.

Hartimo, M. H. (2008). "From Geometry to Phenomenology". *Synthese, 162*(2), 225-233.

Hash, J. (2002). *Risk Management Guidance for Information Technology Systems*. ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151253

Hatab, L. J. (2013). "Phainomenon and Logos in Aristotle's Ethics.". *Phenomenology and virtue ethics*, 9-28.

Hawkins, S. M., Yen, D. C., & Chou, D. C. (2000). "Disaster Recovery Planning: A Strategy For Data Security". *Information Management & Computer Security*, *8*(5), 222-230.

Ho, R. T. K., & Sae-Jong, H. (2017). Smoking behavior and its possible cessation among young smokers in Thailand: Evaluation of and comparison between the protection motivation theory and the theory of planned behavior. In A. H. Seyal & M. N. A. Rahman (Eds.), *Theory of planned behavior: New research* (pp. 133–164). Nova Science Publishers.

Hoban, C. F. (1965). "From Theory to Policy Decisions". *AV Communication Review*, 121-139.

Holmberg, J. M. B., & Bilmes, M. (2004). "The Phenomenology of Technology: A Theoretical Exploration of the Relationship Between Technological Medium and Experience". Içinde *ProQuest Dissertations and Theses*. https://www.proquest.com/dissertations-theses/phenomenology-technology-theoretical-exploration/docview/305052533/se-2?accountid=8319

Husserl, E. (1975). *Experience and Judgment*. Evanston: Northwestern University Press.

Husserl, E. (2020). *Kesin Bir Bilim Olarak Felsefe*. Ankara: Yapı Kredi Yayınları.

Husserl, E., Panzer, U., & Holenstein, E. (1968). *Logische Untersuchungen*. Tübingen: M. Niemeyer.

Ihde, D. (1995). *Postphenomenology: Essays in the Postmodern Context*. Evanston: Northwestern University Press.

İnce, K., İnce, C., Topal, A., Çiçekli, M., Adanur, K., & Kuzu, B. (2020). "Bilişim Altyapı Sistemi Yenileme Çalışması: İnönü Üniversitesi Örneği". *Computer Science*, *5*(1), 54-61.

Irmak, H., & Baz, F. Ç. (2019). "Kurumsal Bilgi Güvenliği, Tehditler ve Alınması Gereken Önlemler Üzerine Bir İnceleme". *2. Uluslararası Mardin Artuklu Bilimsel Araştırmalar Kongresi*.

ISACA. (2024). *Control Objectives for Information Technologies*. https://www.isaca.org/resources/cobit

İzmirli, A. (2023). *İş Sürekliliğinin Sağlanmasında Bilişim Teknolojilerinin Etkisi*. (Yüksek Lisans Tezi). Karaman: Karamanoğlu Mehmetbey Üniversitesi Sosyal Bilimler Enstitüsü.

Jackson, C., Vaughan, D. R., & Brown, L. (2018). "Discovering Lived Experiences Through Descriptive Phenomenology". *International Journal of Contemporary Hospitality Management, 30*(11), 3309-3325.

Jamali, M., Nejat, A., Ghosh, S., Jin, F., & Cao, G. (2019). "Social Media Data and Post-Disaster Recovery". *International Journal of Information Management, 44*, 25-37. https://doi.org/10.1016/j.ijinfomgt.2018.09.005

Kaldırım, A., & Tavşanlı, Ö. F. (2020). "Türkiye'de Süreç Temelli Yazma Yaklaşımı: Bir Tematik Analiz Çalışması". *Cumhuriyet Uluslararası Eğitim Dergisi*, *9*(1), 108-138. http://cije.cumhuriyet.edu.tr/tr/pub/cije/issue/53201/543600

Kasim, S. A. B. M., & bin Mohamed, I. (2018). "Level of Readiness in IT Disaster Recovery Plan". Içinde K. A. Z. Abidin, M. Mohd, & Z. Shukur (Ed.), *Proceedings Of The 2018 Cyber Resilience Conference (CRC).*

Kayrak, M. (2012). "Bilgi Kriterleri Çerçevesinde Bilişim Teknolojileri Denetimi". *Sayıştay Dergisi*, *87*, 143-167.

Kenan, İ., Cemile, İ., Topal, A., Çiçekli, M., Adanur, K., & Bünyamin, K. (2020). "Bilişim Altyapı Sistemi Yenileme Çalışması: İnönü Üniversitesi Örneği". *Computer Science, 5*(1), 54-61.

Khatavakhotan, A. S., & Ow, S. H. (2012). "Improving IT Risk Management Process by an Embedded Dynamic Verifier Core: Towards Reducing IT Projects Failure". *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, 684-687. https://doi.org/10.1109/ISMS.2012.47

Kılıç, E. A. (2019). *Firmalarda iş Sürekliliği Yönetiminin Öncülleri ve Ardılları Üzerine Bir Çalışma*. (Yüksek Lisans Tezi). Bursa: Uludağ Üniversitesi Sosyal Bilimler Enstitüsü.

Koçak, İ., & Akbel, M. (2023). "Edmund Husserl'in Fenomenolojik Yönteminde Yönelimsellik". *Kalemname, 8*(16), 503-513.

Koro-Ljungberg, M., MacLure, M., & Ulmer, J. (2018). "D… a… t… a…, data++, data, and Some Problematics". *The SAGE Handbook of Qualitative Research, 5*, 462-484.

Kulaklı, A., & Aslan, S. (2010). "İşletmelerde Bilgi Teknolojilerindeki Gelişmelerin İşletme ve Yönetim Fonksiyonları Üzerine Etkileri". *Beykent Üniversitesi Sosyal Bilimler Dergisi*, *4*(1), 1-16.

Kuyumcuoğlu, M., & Başoğlu, A. N. (2008). "Bilişim Sistemlerinde Risk Yönetimi Benimseme Modeli". *Yönetim*, *19*(61), 143-164.

Larkin, M., Shaw, R., & Flowers, P. (2019). "Multiperspectival Designs and Processes in Interpretative Phenomenological Analysis Research". *Qualitative research in psychology*, *16*(2), 182-198.

Larkin, M., & Thompson, A. R. (2011). "Interpretative Phenomenological Analysis in Mental Health and Psychotherapy Research". *Qualitative Research Methods in Mental Health and Psychotherapy: A Guide for Students and Practitioners*, 99-116.

Larsen, H. G., & Adu, P. (2021). *The Theoretical Framework in Phenomenological Research: Development and Application*. London: Routledge.

Lewis, T. G. (1995). “Where is Client/Server Software Headed?”. *Computer, 28*(4), 49-55.

Liduo, H., & Yan, C. (2010). “Design and implementation of Web Content Management System by J2EE-based Three-tier Architecture: Applying in Maritime and Shipping Business”. *2010 2nd IEEE International Conference on Information Management and Engineering*, 513-517. https://doi.org/10.1109/ICIME.2010.5477670

Lochmiller, C. (2021). “Conducting Thematic Analysis with Qualitative Data”. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2021.5008

McKoy, T. E. (2021). “The Second-Year Retention Effect of Early Enrollment in a First-Year Seminar”. *Teaching and Learning Excellence through Scholarship*, *1*(1). https://doi.org/10.52938/tales.v1i1.1368

Meechang, K., Leelawat, N., Tang, J., Kodaka, A., & Chintanapakdee, C. (2020). “The Acceptance of Using Information Technology for Disaster Risk Management: A Systematic Review”. *Engineering Journal*, *24*(4), 111-132. https://doi.org/10.4186/ej.2020.24.4.111

Meilani, D., Arief, I., & Habibitullah, M. (2019). “Designing Disaster Recovery Plan of Data System for University”. *IOP Conference Series: Materials Science and Engineering*, *697*(1), 012028.

Mendonça, J., Andrade, E., Endo, P. T., & Lima, R. (2019). “Disaster Recovery Solutions For IT Systems: A Systematic Mapping Study”. *Journal of Systems and Software*, *149*, 511-530. https://doi.org/10.1016/j.jss.2018.12.023

Microsoft (2023). *Disaster Recovery With Storage Spaces Direct*. https://azure.microsofts.workers.dev/en-us/windows-server/storage/storage-spaces/storage-spaces-direct-disaster-recovery

Mistry, C. D., Sweet, S. N., Latimer-Cheung, A. E., & Rhodes, R. E. (2015). “Predicting Changes in Planning Behaviour and Physical Activity Among Adults”. *Psychology of Sport and Exercise*, *17*, 1-6.

Mitts, J. S. (2005). “Business Continuity and Disaster Recovery Plans: How and When to Test Them”. *EDPACS, 33*(5), 8-24.

Moore, R. L., D'Aoust, J., McDonald, R. H., & Minor, D. (2007). "Disk and Tape Storage Cost Models". *Archiving Conference*, *4*, 29-32.

Moran, D. (2002). *Introduction to Phenomenology*. Routledge. https://doi.org/10.4324/9780203196632

Muparadzi, T., & Rodze, L. (2021). "Business Continuity Management in a Time of Crisis: Emerging Trends for Commercial Banks in Zimbabwe during and Post the Covid-19 Global Crisis". *Open Journal of Business and Management*, *09*(03), 1169-1197. https://doi.org/10.4236/ojbm.2021.93063

Najafi, M., Ardalan, A., Akbarisari, A., Noorbala, A. A., & Elmi, H. (2017). "The Theory of Planned Behavior And Disaster Preparedness". *PLoS Currents*, *9*.

Nakamura, S., Zhao, X., & Nakagawa, T. (2017). "Constant and Random Full Backup Models With İncremental and Differential Backup Schemes". *International Journal of Reliability, Quality and Safety Engineering*, *24*(03), 1750015.

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). "Business Continuity of Business Models: Evaluating the Resilience of Business Models for Contingencies". *International Journal of Information Management*, *49*, 208-216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

Nurhanudin, N. (2021). "Designing a Disaster Recovery Plan Using NIST 800-34 Framework on the Information System of The Directorate General of Hajj and Umrah". *Jurnal Sısfotek Global*, *11*(2), 75-81.

Okeagu, C. N., Reed, D. S., Sun, L., Colontonio, M. M., Rezayev, A., Ghaffar, Y. A., Kaye, R. J., Liu, H., Cornett, E. M., Fox, C. J., Urman, R. D., & Kaye, A. D. (2021). "Principles of Supply Chain Management in the Time of Crisis". *Best Practice & Research Clinical Anaesthesiology*, *35*(3), 369-376. https://doi.org/10.1016/j.bpa.2020.11.007

Oneal, B. (2020). *The Benefits of Hyperconverged Infrastructure for Disaster Recovery*. https://www.tierpoint.com/blog/the-benefits-of-hyperconverged-infrastructure-for-disaster-recovery/

Orhan, A., & Genç, S. Y. (2018). "Bilişim Teknolojisindeki Gelişimin Sosyoekonomik Etkileri". *Journal of Management and Economics Research*, *16*(1), 264-275.

Oxford University Press. (2024). *Phenomenology*. Oxford University Press. https://www.oxfordlearnersdictionaries.com/definition/english/phenomenology?q=phenomenology

Özbilgin, İ. G. (2012). "Risk ve Risk Çeşitleri". *Bilişim Dergisi, 7*, 86-93.

Özdemir, A., & Gökgöz, B. (2018). "Bulut Bilişimde Felaket Kurtarma Tekniklerinin İncelenmesi". *Internatıonal Symposium on İnnovative Approaches in Scientific Studies*, 3-202.

Özdemir, M. (2010). "Nitel Veri Analizi: Sosyal Bilimlerde Yöntembilim Sorunsalı Üzerine Bir Çalışma". *Eskişehir Osmangazi üniversitesi sosyal bilimler dergisi*, *11*(1), 323-343.

Özer, L., Kement, Ü., & Gültekin, B. (2015). "Genişletilmiş Planlanmış Davranış Teorisi Kapsamında Yeşil Yıldızlı Otelleri Tekrar Ziyaret Etme Niyeti". *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *33*(4), 59-85.

Özmen, E. (2021). *E-ticaret Sitelerinde Çok Kanallı Kullanılabilirlik ve Kullanıcı Deneyimi Çalışması*. (Doktora Tezi), Erzurum: Atatürk Üniversitesi Sosyal Bilimler Enstitüsü. https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=8tbPippmWV_b-Irrn9YEAm7enr-iiNpTufi8-33bl0jicLRCGZsaYO0tgncHeFlE

Paredes, L. A., Serrano, B. R., & Molina, M. G. (2019). "FACTS Technology to Improve the Operation of Resilient Microgrids". *2019 FISE-IEEE/CIGRE Conference - Living the energy Transition (FISE/CIGRE)*, 1-7. https://doi.org/10.1109/FISECIGRE48012.2019.8984960

Parry, J. (2010). *Art and Phenomenology*. New York: Routledge.

Pietkiewicz, I., & Smith, J. A. (2014). "A Practical Guide to Using İnterpretative Phenomenological Analysis in Qualitative Research Psychology". *Psychological journal*, *20*(1), 7-14.

Polat, A. (2022). "Nitel Araştırmalarda Yarı-Yapılandırılmış Görüşme Soruları: Soru Form ve Türleri, Nitelikler ve Sıralama". *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, *22*(Özel Sayı 2), 161-182. https://doi.org/10.18037/ausbd.1227335

Posey, B. (2019). *What is the Role of HCI in a Disaster Recovery Architecture?* https://www.techtarget.com/searchdisasterrecovery/answer/What-is-the-role-of-HCI-in-a-disaster-recovery-architecture

Prasetyo, H. N., Supriatna, N., Raharjo, A. P., & Wikusna, W. (2020). "Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia". *IJAIT (International Journal of Applied Information Technology), 3*(01), 34. https://doi.org/10.25124/ijait.v3i01.2317

Puspitaningrum, A. C. (2022). "Proposed Business Continuity Plan Information Technology using ISO 22301 And ISO 27031". *Sistemasi: Jurnal Sistem Informasi*, *11*(3), 601-613.

Qadriina, H. I., Herdiansyah, H., & Aryo, B. (2023). "The Role of Social Capital in the Response and Recovery Process of Post-Disaster Affected Communities". *International Journal of Science and Society*. https://api.semanticscholar.org/CorpusID:265015211

Rashid, A., & Chaturvedi, A. (2019). "Virtualization and its Role in Cloud Computing Environment". *International Journal of Computer Sciences and Engineering*, *7*(4), 1131-1136. https://doi.org/10.26438/ijcse/v7i4.11311136

Rebah, H. Ben, & Sta, H. Ben. (2016). "Disaster Recovery As A Service: A Disaster Recovery Plan in the Cloud For SMEs". *2016 Global Summit on Computer & Information Technology (GSCIT)*, 32-37.

Rothstein, P. J. (2007). *Disaster Recovery Testing: Exercising Your Contingency Plan*. Connecticut: Rothstein Associates Inc.

Rouhanizadeh, B., Kermanshachi, S., & Nipa, T. J. (2020). "Exploratory Analysis of Barriers to Effective Post-Disaster Recovery". *International Journal of Disaster Risk Reduction*, *50*, 101735. https://doi.org/10.1016/j.ijdrr.2020.101735

Saei, M. (2019). *Varlık Fenomenolojisinde Şiir ve Mekan*. https://acikbilim.yok.gov.tr/handle/20.500.12812/435954

Sarker, M. N. I., Peng, Y., Yiran, C., & Shouse, R. C. (2020). "Disaster Resilience Through Big Data: Way to Environmental Sustainability". *International Journal*

of Disaster Risk Reduction, *51*, 101769. https://doi.org/10.1016/j.ijdrr.2020.101769

Sartakov, V. A., & Kapitza, R. (2017). "Multi-site Synchronous VM Replication for Persistent Systems With Asymmetric Read/Write Latencies". *2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC)*, 195-204.

Savaş, R. N., Zaim, A. H., & Aydın, M. A. (2020). "KVKK ve GDPR Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme". *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, *19*(38), 208-223. https://dergipark.org.tr/en/pub/ticaretfbd/issue/58122/847247

Sawalha, I. H. (2020). "Business Continuity Management: Use and Approach's Effectiveness". *Continuity & Resilience Review*, *2*(2), 81-96. https://doi.org/10.1108/CRR-05-2020-0016

Schrag, C. O. (2006). "Heidegger Felsefesinde Fenomenoloji, Varlıkbilim ve Tarih". *Çağdaş Türkiye Tarihi Araştırmaları Dergisi*, *5*(13), 205-215.

Schulz, G. (2016). "Data Storage—Disk, Tape, Optical, and Memory". Içinde *The Green and Virtual Data Center* (ss. 225-268). Auerbach Publications.

Selvi, O., & Küçüksille, E. (2014). "Bulut Bilişimin Eğitim Alanında Uygulanması". *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *16*(3), 248-254. https://doi.org/10.19113/sdufbed.46976

Sengupta, S., & Annervaz, K. M. (2014). "Multi-site Data Distribution for Disaster Recovery—A Planning Framework". *Future Generation Computer Systems*, *41*, 53-64. https://doi.org/10.1016/j.future.2014.07.007

Seo, W., Kim, J., & Kang, Y. (2022). "Calculating the Cost İmpact in Loss of Productivity Claims". *Automation in Construction*, *140*, 104341. https://doi.org/10.1016/j.autcon.2022.104341

Shen, S., Chang, R. H., Kim, K., & Julian, M. (2022). "Challenges to Maintaining Disaster Relief Supply Chains in İsland Communities: Disaster Preparedness and Response in Honolulu, Hawai'i". *Natural Hazards*, *114*(2), 1829-1855. https://doi.org/10.1007/s11069-022-05449-x

Shropshire, J., & Kadlec, C. (2009). "Developing the IT Disaster Recovery Planning Construct". *Journal of Information Technology Management*, *20*(4), 37.

Shuvo, S. R. S., Islam, Md. N., & Islam, S. T. (2022). "Role of information and Communication Technologies in Build Back Better to Post Disaster Recovery Practices: İnsights From Bangladesh". *International Journal of Disaster Resilience in the Built Environment*, *13*(2), 233-247. https://doi.org/10.1108/IJDRBE-08-2021-0097

Singh, A. K., & Shanker, U. (2016). "Database Replication Techniques: A Review". *International Journal Of Research Review In Engineering Science & Technology*, *5*(4).

Smith, A. D. (2015). "The Idea of Phenomenology. *Central Works of Philosophy v4: Twentieth Century: Moore to Popper*, *4*, 38.

Smith, D. W. (2019). *Husserl*. Alfa Yayınları.

Smith, J. A., Flowers, P., & Larkin, M. (2021). *Interpretative Phenomenological Analysis: Theory, Method and Research*.

Smith, J. A., Jarman, M., & Osborn, M. (1999). "Doing Interpretative Phenomenological Analysis". *Qualitative Health Psychology: Theories and Methods*, *1*(1), 218-240.

Snedaker, S., & Rima, C. (2013). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Waltham: Syngress.

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). "NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems". *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Şahinaslan, E., Kandemir, R., & Şahinaslan, Ö. (2009). "Bilgi Güvenliği Farkındalık Eğitimi Örneği". *Akademik Bilişim*, *9*, 189-194.

Şahinaslan, Ö., Şahinaslan, E., & Küçükali, E. (2023). "Üçüncü Taraf Yazılım Bileşenlerinden Kaynaklanan Zayıflıkların Tespiti ve Yönetimine İlişkin Bir Uygulama". *Denetişim*, *28*, 53-74. https://doi.org/10.58348/denetisim.1225325

Şalcı, İ. (2021). *Dijital Dönüşüm (e-uygulamalar) ve Muhasebe Mesleğine Getirdiği Yenilikler*. (Yüksek Lisans Tezi). Işık Üniversitesi Lisansüstü Eğitim Enstitüsü.

Şaşmaz, Z., & Tengilimoğlu, E. (2024). "Planlı Davranış Teorisi Bağlamında Gerçekleştirilen Çalışmaların Sistematik Değerlendirmesi; Dergi Park Örneği". *Selçuk Turizm ve Bilişim Araştırmaları Dergisi*, *5*, 23-35. https://dergipark.org.tr/en/pub/stbad/issue/85393/1481692

Tan, C. B., Hijazi, M. H. A., Lim, Y., & Gani, A. (2018). "A Survey on Proof of Retrievability for Cloud Data Integrity and Availability: Cloud Storage State-of-the-art, Issues, Solutions and Future Trends". *Journal of Network and Computer Applications, 110,* 75-86. https://doi.org/10.1016/j.jnca.2018.03.017

TBD (2006). *Bilişim Teknolojilerinde Risk Yönetimi*. https://www.tbd.org.tr/eski/usr_img/cd/kamubib12/RaporlarPDF/RP2-2006.pdf

TBD (2009). *Felaketten Kurtarma ve Depolama*. https://eski.tbd.org.tr/usr_img/cd/kamubib12/RaporlarPDF/RP2-2009.pdf

Tekindal, M., & Arsu, Ş. U. (2020). "Nitel Araştırma Yöntemi Olarak Fenomenolojik Yaklaşımın Kapsamı ve Sürecine Yönelik Bir Derleme". *Ufkun Ötesi Bilim Dergisi*, *20*(1), 153-172.

Theofanidis, D., & Fountouki, A. (2018). "Limitations and Delimitations in the Research Process". *Perioperative Nursing-Quarterly Scientific, Online Official Journal of GORNA, 7*(3 September-December 2018), 155-163.

Timms, P. (2018). "Business Continuity and Disaster Recovery – Advice for Best Practice". *Network Security*, *2018*(11), 13-14. https://doi.org/10.1016/S1353-4858(18)30113-2

Turner IV, W. P., PE, J. H., Seader, P. E., & Brill, K. J. (2006). "Tier Classification Define site İnfrastructure Performance". *Uptime Institute, 17*.

TÜBİTAK (2017a). *Felaket Kurtarma Merkezi Hizmeti Rehberi*. https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TUBITAK-BILGEM-F.pdf

TÜBİTAK (2017b). *Felaket Kurtarma Merkezi Kurulumu Rehberi*. https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TUBITAK-BILGEM_YT.pdf

Uğuz Arsu, Ş., & Tekindal, M. (2020). "Nitel Araştırma Yöntemi Olarak Fenomenolojik Yaklaşımın Kapsamı ve Sürecine Yönelik Bir Derleme". *Ufkun Ötesi Bilim Dergisi*, *20*(1), 153-172. https://dergipark.org.tr/en/pub/uobild/issue/58856/813813

Uptime Institute. (2024). *Data Center Design Document Certification*. https://uptimeinstitute.com/tier-certification/design

Varol, N. (2007). "Doğal ve Teknolojik Afetler Konusunda Toplumun Bilinçlendirilmesi ve "AFEM" in Rolü". *TMMOB Afet Sempozyumu*, *5*(7).

Veiga, A. P. (2017). "Hyper Converged Infrastructures: Beyond Virtualization". *arXiv preprint arXiv:1711.09747*.

Volvach, I., & Globa, L. (2016). "Mobile Networks Disaster Recovery Using SDN-NFV". *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, 1-3. https://doi.org/10.1109/UkrMiCo.2016.7739648

Vural, Y., & Sağıroğlu, Ş. (2013). "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme". *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *23*(2), 0. https://dergipark.org.tr/en/pub/gazimmfd/issue/6676/88512

Walsh, R. D. (1988). "Husserl's Epoche as Method and Truth". *Auslegung: A Journal of Philosophy*, *14*(2), 211-223.

Wang, Y., & Li, S. (2006). "Research and Performance Evaluation of Data Replication Technology in Distributed Storage Systems". *Computers & Mathematics with Applications*, *51*(11), 1625-1632. https://doi.org/10.1016/j.camwa.2006.05.002

Wiboonratr, M., & Kosavisutte, K. (2009). "Optimal Strategic Decision for Disaster Recovery". *International Journal of Management Science and Engineering Management*, *4*(4), 260-269.

Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., Van der Merwe, J., & Venkataramani, A. (2010). "Disaster Recovery as a Cloud Service: Economic

Benefits & Deployment Challenges". *2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10).*

Yazır, S. (2018). *Türkiye'de Bulut Bilisimin Teknolojik Gelisimi ve Bulut Platformu Üzerinde Örnek Bir Kisisel Web Uygulamasinin Sunulması,* (Yüksek Lisans Tezi), Konya: Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü]. Içinde *PQDT - Global*. https://www.proquest.com/dissertations-theses/türkiyede-bulut-bilisimin-teknolojik-gelisimi-ve/docview/2600829369/se-2?accountid=8319

Yener, Ö. (2012). "Varoluşçu Felsefeden Varoluşçu Psikolojiye (Birbirlerini Sürekli Yanlış Anlayanların Ontolojik Bütünlüğü)". *Gümüşhane Üniversitesi Sosyal Bilimler Enstitüsü Elektronik Dergisi*, *3*(5), 266-286.

Yurt, İ., & Şentürk, B. N. (2022). "İş Sürekliliği Yönetim Sisteminin İşletmelerin Stratejik Çevikliğine Etkisi". *Journal of Humanities and Tourism Research*, *12*(3), 486-508.

Yüzgeç, U., & Günel, A. (2016). "Üniversitelere Yönelik Bir Veri Merkezinin İklimlendirme Planlaması". *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, *1*(2), 37-44.

Zack, N. (2019). *Adan Zye Felsefe: Antik Yunandan Postmodern Döneme Felsefe Tarihi*. İstanbul: Say Yayınları.

Zaman, U., Zahid, H., Habibullah, M. S., & Din, B. H. (2021). "Adoption of Big Data Analytics (BDA) Technologies in Disaster Management: A Decomposed Theory of Planned Behavior (DTPB) Approach". *Cogent Business & Management*, *8*(1). https://doi.org/10.1080/23311975.2021.1880253

Zgureanu, A. (2022). The role of RPO and RTO in disaster recovery planning. *30 Years of Economic Reforms in the Republic of Moldova: Economic Progress via Innovation and Competitiveness, Vol III*, 221-232. https://doi.org/10.53486/9789975155663.26

Zhang, H. (2013). Architecture of network and client-server model. *arXiv preprint arXiv:1307.6665*.

EKLER

EK 1. Araştırmada Kullanılan Ölçek

Sayın Yetkili,

Bu görüşme ile **"BİLGİ TEKNOLOJİSİ FELAKET KURTARMA PLANLAMASININ FENOMENOLOJİK YAKLAŞIMLA İNCELENMESİ: KAMU ÜNİVERSİTELERİ ÖRNEĞİ"** adlı yüksek lisans çalışmasına veri toplanması amaçlanmaktadır.

Görüşmede kişisel bilgilerini ortaya çıkarmaya yönelik herhangi bir bilgi toplanmamaktadır. Adınız soyadınız gibi bilgiler istenmemektedir.

Toplanan veriler sadece nicel ya da nitel olarak değerlendirilecek ve anonim olarak kullanılacaktır.

Vereceğiniz samimi cevaplar için şimdiden teşekkür ediyoruz.

GÖRÜŞME SORU FORMU

1-) Yaşınız □ 19-29 □ 30-39 □40-49 □50 ve üzeri

2-) Eğitim Durumunuz □ Lise □ Ön Lisans
□ Lisans □ Lisansüstü

3-) Felaket kurtarma planlamasında kaç yıllık bir tecrübeniz var

□ 3-5 yıl □ 6-8 yıl
□ 9-11 yıl □ 12 ve üzeri

4-) Kurumdaki görev tanımınız

□ Ağ ve/veya Sistem Uzmanı □ Grup Sorumlusu veya Birim Sorumlusu
□ Merkez Müdürü □ Memur veya Çözümleyici
□ Daire Başkanı □ Diğer (…….)

5-) Kurumunuzda BT felaket kurtarma planı var mı? Varsa sıklıkla güncellenmekte midir? Lütfen açıklayınız.

6-) Bir BT felaket kurtarma planına sahip olmanın olumlu ve olumsuz sonuçları nelerdir?

7-) Kurumunuzun BT güvenlik açıkları, riskler ve iş sürekliliği konusundaki beklentileri nelerdir? Lütfen açıklayabilir misiniz?

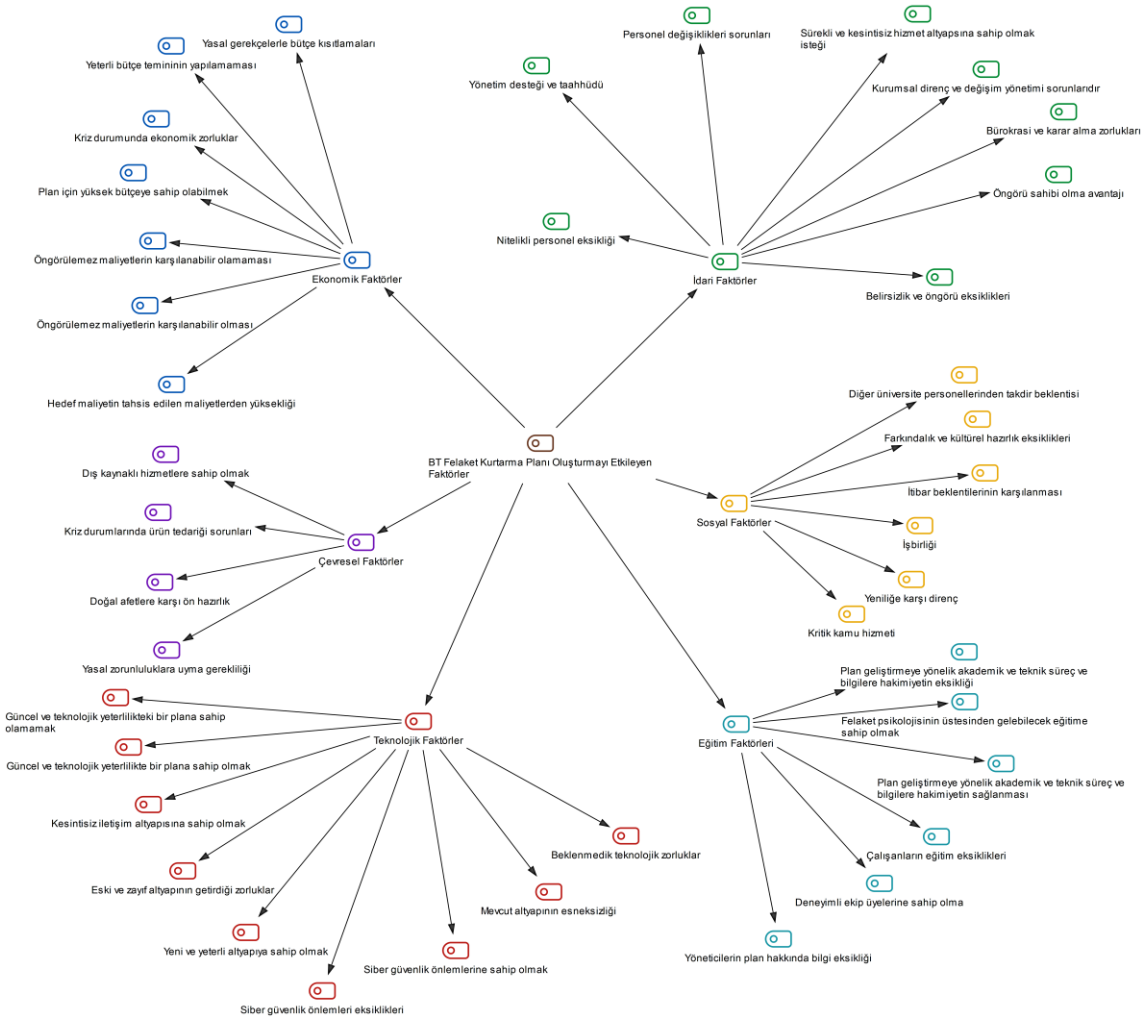
8-) Kurumunuzda üst yöneticileriniz veya kurumsal yönetim açısından bir BT felaket kurtarma planı geliştirme konusunda genel düşünceler nelerdir? Yöneticiler bu planları onaylıyorlar mı yoksa onaylamıyorlar mı?

9-) BT felaket kurtarma planı geliştirme aşamasında nelere dikkat ettiniz planı geliştirmeyi kolaylaştıran faktörler sizce nelerdir?

10-) Sizce BT felaket kurtarma planı geliştirmeyi zorlaştıran faktörler veya engelleyen faktörler nelerdir? Lütfen açıklayabilir misiniz?

11-) Sizin BT felaket kurtarma planınızda, planlanan ile hayata geçirilen arasında farklılıklar oldu mu? Olduysa bu duruma hangi nedenler sebep oldu? Lütfen açıklayınız.

EK 2. Ayrıntılı Tema Şeması



ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Oğuz ERDEN
Eğitim Durumu	
Lisans Öğrenimi	
Yüksek Lisans Öğrenimi	
Bildiği Yabancı Diller	
İş Deneyimi	
Çalıştığı Kurumlar	
İletişim	
E-posta Adresi	
Tarih	