



TÜRKİYE BİLİŞİM DERNEĞİ
Kamu Bilişim Merkezi Yöneticileri Birliği
Kamu Bilişim Platformu XVI

ULUSAL VERİ MERKEZİ VE
KAMUDA GELECEK ÖNGÖRÜLERİ

Sürüm 1.0

1. ÇALIŞMA GRUBU

<http://www.tbd.org.tr>

Eylül 2014



TBD Kamu-BİB
Kamu Bilişim Platformu XVI

ULUSAL VERİ MERKEZİ ve
KAMUDA GELECEK ÖNGÖRÜLERİ

Sürüm 1.0

1. ÇALIŞMA GRUBU

Bu rapor, TBD Kamu Bilişim Merkezi Yöneticileri Birliği (TBD Kamu-BİB)'nin *onaltıncı dönem* çalışmaları kapsamında, 1. Çalışma Grubu (ÇG1) tarafından hazırlanmıştır. Çalışma, Bilgi toplumu sürecinde ülkelerin vermekte oldukları e-Devlet hizmetlerine ve teknolojideki gelişmelere istinaden sayıları ve kapasiteleri artan veri merkezlerinin, uygun bir model ve senaryo çerçevesinde Ulusal Veri Merkezi halinde konsolide edilmesine ilişkin mevcut durum, küresel yaklaşımlar ve Türkiye için en uygun model önerilerini içermektedir.

Hedef Kitle

Hükümet, üst düzey yöneticiler, öncelikle kamu bilişim merkezi yöneticileri olmak üzere Ulusal Veri Merkezi konusunda aktif rol alanlar ve bu konuda politika ve strateji belirleyicilerdir.

Belge No : TBD/Kamu-BİB/2014-ÇG1

Tarihi : 27 Eylül 2014

Durumu : Rapor – S 1.0

Yayını Hazırlayanlar

Başkan

Mustafa AFYONLUOĞLU

TÜBİTAK BİLGEM YTE

Başkan Yardımcısı

Sare Gül SEVİL

TÜBİTAK BİLGEM YTE

Grup Başkanları

Atilla AYDIN

TÜBİTAK BİLGEM YTE

Aydın DEMİRCİ

T.P. Petrol Dağıtım A.Ş

Nejdet KARAKELLE

Başbakanlık

Sare Gül SEVİL

TÜBİTAK BİLGEM YTE

Yazman

Sare Gül SEVİL

TÜBİTAK BİLGEM YTE

Grup Üyeleri

Cem KARACA

Veri Teknik Telekom

Ender YILDIZEL

GENMAK

Erol HAMURCU

Adalet Bakanlığı

F. Hidayet HALİLBEYOĞLU

SGK

Hakan SARIKAYA

Labris Teknoloji

Hanife BULUT

Başbakanlık

Kenan ÇAKMAK

İçişleri Bakanlığı

Nuran GÖRGÜN

Adalet Bakanlığı

TEŞEKKÜR

Bu çalışmanın ortaya çıkması, hazırlanması ve sonuçlandırılmasında yorumlarıyla ve önerileriyle bizleri yalnız bırakmayan TBD Yönetim Kurulu üyeleri ve On Altıncı Dönem TBD Kamu-BİB Yönetim Kurulu üyelerine; Ulusal Veri Merkezi konusunda öneriler sunarak eksiklerimizi tamamlamamızı kolaylaştıran değerlendirme toplantılarının katılımcılarına, saha araştırmalarımızda ve pilot çalışmalarımızda değerli zamanlarını ayırıp, bize tecrübeleri ile katkı sağlayan Adalet Bakanlığı, Sağlık Bakanlığı, İçişleri Bakanlığı ve Başbakanlık Bilgi İşlem Daire Başkanlığı'nın değerli yöneticilerine; ulusal ve uluslararası deneyim ve birikimlerini paylaşan özel sektörün kıymetli temsilcilerine (özellikle paylaştığı deneyim ve materyaller için EMC, IBM, Microsoft, HP, Fujitsu ve Oracle markalarının Türkiye yetkililerine); kamuda ulusal veri merkezine yönelik mevcut durumun tespiti için araştırmalarımıza vakit ayırıp, değerli görüş ve bilgilerini bizimle paylaşan kamu kurum ve kuruluşlarımızın Bilgi İşlem Daire Başkanlıkları'ndaki değerli anket katılımcılarına ve çalışmadaki hukuki değerlendirmeleri için TBD Ankara Bilişim Hukuku Çalışma Grubu'na en içten teşekkürlerimizi sunarız.

İÇİNDEKİLER

TEŞEKKÜR	3
İÇİNDEKİLER	4
TANIMLAR VE KISALTMALAR.....	6
ŞEKİLLER	11
TABLolar	13
1. GİRİŞ.....	14
1.1. Amaç ve Kapsam	14
1.2. Çalışma Yaklaşımı.....	15
2. GENEL ÇERÇEVE.....	17
2.1. Veri Merkezi	17
2.1.1. Veri Merkezi Bileşenleri ve Maliyetler.....	17
2.1.2. Veri Merkezlerinde Kaynak Yönetimi ve Maliyetler.....	18
2.2. Veri Merkezlerinin Birleştirilmesi (Konsolidasyonu)	25
2.3. Ulusal Veri Merkezi Kavramı	26
3. MEVCUT DURUM ÇALIŞMALARI	28
3.1. Türkiye’de Ulusal Veri Merkezi Kavramı ve Gelişimi	28
3.2. Kamu Kurumlarında Veri Merkezlerinin Mevcut Durumu	33
3.3. Kamu Kurumları Bilgi İşlem Yöneticilerinin Ulusal Veri Merkezi İle İlgili Değerlendirmeleri.....	40
4. ULUSLARARASI ÖRNEKLER	42
4.1. Uluslararası Eğilimler.....	42
4.1.1. EMC Veri Merkezlerinde Değişim	42
4.1.2. Intel’in Veri Merkezi Stratejisi	46
4.2. Ülke Değerlendirmeleri	48

4.2.1. Güney Kore.....	49
4.2.2. Amerika Birleşik Devletleri.....	62
4.2.3. Malezya	64
4.2.4. Estonya	67
4.2.5. Hong Kong	68
5 ULUSAL VERİ MERKEZİ AŞAMALARI VE KAMUDA GELECEK ÖNGÖRÜLERİ.....	69
5.1. Ulusal Veri Merkezi: Kamuyu Ne Bekliyor?.....	70
5.2. Ön Hazırlıklar.....	71
5.3. Kamu Kurumlarının Ön Hazırlıkları.....	71
5.4. UVM Sorumlularının Görevleri.....	72
5.5. Aşamalı Geçiş Süreci Önerileri.....	73
5.5.1. Aşama-1	78
5.5.2. Aşama -2.....	81
5.5.3. Aşama -3.....	82
5.6. Ulusal Veri Merkezinde Güvenlik Kurgusu.....	82
5.6.1. Fiziki Güvenlik	82
5.6.2. Siber Güvenlik.....	85
5.6.3. Güvenlik Denetimleri	88
5.6.4. Devlet Siber Güvenlik Hedefleri ve Regülasyonlar İle Etkileşim.....	88
6. SONUÇ	90
EK A: ANKET ÇALIŞMASINDA UYGULANAN YÖNTEM	91
EK B: ANKET SORULARI	92
EK C: ANKET NİTEL SORU CEVAPLARI	101
EK-D: İLGİLİ MEVZUAT ÖRNEKLERİ	111
KAYNAKÇA	131

TANIMLAR VE KISALTMALAR

AB	Avrupa Birliđi
ABD	Amerika Birleşik Devletleri
ADSL	Asymmetric Digital Subscriber Line (Asimetrik Dijital Abone Hattı)
ANSIS	Gelişmiş Ulusal Güvenlik Altyapı Sistemi
APT	Advanced Persistent Threat (Gelişmiş Kalıcı Tehdit)
AR-GE	Araştırma-Geliştirme
ASBİS	Araç ve Sürücü Bilgi Sistemi
ASHARE	American Society of Heating, Refrigerating and Air-Conditioning Engineers (Isıtma, Soğutma ve İklimlendirme Mühendisleri Amerika Topluluđu)
BİDB	Bilgi İşlem Daire Başkanlığı
BGYS	Bilgi Güvenliđi Yönetim Sistemi
BOME	Bilgisayar Olaylarına Müdahale Ekibi (CERT)
BPR	Business Process Reengineering (İş Süreçlerinin Yeniden Yapılandırılması)
BTYK	Bilim ve Teknolojileri Yüksek Kurulu
BT	Bilgi Teknolojileri
BTYK	Bilim ve Teknoloji Yüksek Kurulu
CCC	Central Computer Campus (Hong Kong - Merkezi Bilgisayar Yerleşkesi)
CCTV	Closed Circuit Television (Kapalı Devre Televizyon)

CERT	Computer Emergency Response Team (BOME)
CIO	Chief Information Officer
CRM	Customer Relations Management (Müşteri İlişkileri yönetimi)
DDoS	“Distributed Denial-of-Service”. İnternet üzerinden çok sayıda istemci bilgisayarın aynı anda tek bir yere istek yapması ile gerçekleştirilen bir saldırı çeşididir.
DEA	Gürcistan - Data Exchange Agency (Veri Değişim Ajansı)
DPT	Devlet Planlama Teşkilatı
EKAP	Elektronik Kamu Alımları Platformu
ERP	Enterprise Resource Planning (Kurumsal Kaynak Planlama)
FKM	Felaket Kurtarma Merkezi
FMC	Fixed-Mobile Convergence (Sabit-Mobil Yakınsaması)
GAP	Güneydoğu Anadolu Projesi
GIDC	Government Integrated Data Center (Kamu Entegre Veri Merkezi)
GITN	Government Integrated Telecommunication Network (Hükümet Entegre Telekomünikasyon Ağı)
GCN	Government Communication Network (Hong-Kong: Kamu İletişim Ağı)
IaaS	Infrastructure as a Service (Servis olarak Altyapı)
IDC	International Data Corporation (www.idc.com)
IDN	İnternet Değişim Noktası
IPTV	IP iletişim protokolü ile internet hattı üzerinden televizyon / görüntü yayını yapılmasına ilişkin yeni nesil yayın teknolojisi

İSS	İnternet Servis Sağlayıcı
İSYS	İş Sürekliliği Yönetim Sistemi
IT	Information Technologies (Bilgi Teknolojileri)
ITaaS	IT as a Service (Hizmet olarak BT)
ITIL	IT Infrastructure Library (BT Altyapı Kütüphanesi)
KİK	Kamu İhale Kanunu
KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
KOSGEB	Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı
LAN	Local Area Network (Yerel Ağ)
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit (Malezya İdari Modernizasyonu ve Yönetimi Planlama Birimi)
MERNİS	Merkezi Nüfus İdare Sistemi
MERSİS	Merkezi Sicil Kayıt Sistemi
MOSPA	Ministry of Security and Public Administration (Güney Kore Güvenlik ve Kamu Yönetimi Bakanlığı)
MTBF	Mean Time Between Failure (İki hata arası ortalama süre)
NCIA	National Computing Information Agency (Güney Kore Ulusal Bilişim ve Bilgi Ajansı)
NICE	Korean National Integrated Computing Environment
nTOPS	National Total Operation Platform System (Ulusal Toplam Operasyon Platform Sistemi)
OECD	Organization for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)
P2P	Peer to Peer
PaaS	Platform as a Service (Servis olarak Platform)

PCN	Putrajaya Campus Network (Putrajaya Kampüs Ağı)
PSB	Singapur - Public Services Broker (Kamu Servisleri Aracısı)
PUE	Power Usage Effectiveness (Güç Kullanım Etkinliği)
RIA	Estonian Information System Authority (Estonya Bilgi Sistemleri Kurulu)
ROI	Return on Invest (Yatırımların Geri Dönüşü)
SaaS	Software as a Service (Servis olarak Yazılım)
SLA	Service Level Agreement (Servis Seviyesi Anlaşması)
SRDF	Symmetrix (EMC's Enterprise Storage Array) Remote Data Facility (Symmetrix Uzak Veri Tesisi)
SSM	Savunma Sanayii Müsteşarlığı
STK	Sivil Toplum Kuruluşu
TAEK	Türkiye Atom Enerjisi Kurumu
TAKBİS	Tapu ve Kadastro Bilgi Sistemi
TCO	Total Cost of Ownership (Toplam Sahipolma Maliyeti)
TIA	Telecommunications Industry Association (Telekominikasyon Endüstrisi Birliği)
TPE	Türk Patent Enstitüsü
TTGV	Türkiye Teknoloji Geliştirme Vakfı
TUENA	Türkiye Ulusal Enformasyon Altyapısı Anaplanı
TÜBA	Türkiye Bilimler Akademisi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜRKSAT	Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş.
UBcN	Ultra Broadband Convergence Network (Ultra Genişbant Yakınsama Ağı)

UNIDO	United Nations Industrial Development Organization (Birleşmiş Milletler Sınai Kalkınma Örgütü)
UVM	Ulusal Veri Merkezi
UYAP	Ulusal Yargı Ağı Sistemi
VM	Veri Merkezi
WAN	Wide Area Network (Geniş Alan Ağı)
XML	Extensible Markup Language (Genişletilebilir İşaretleme Dili)

ŞEKİLLER

Şekil 1. Veri Merkezi Bileşenleri	18
Şekil 2. BİT Enerji Dağılımı.....	19
Şekil 3. 1989 – 2011 Yılları Arası Microsoft Örnek Veri Merkezi Nesilleri [4]21	
Şekil 4. Veri Merkezlerinde Etkin Soğutma Gelişmeleri [4]	23
Şekil 5. Belirtilen VM Seviyelerine Göre Verimlilik Karşılaştırmaları [10].....	25
Şekil 6. 2014 Yılı BT Harcamaları Öncelikleri [7]	27
Şekil 7 Anket Sonuçları: "Kurumunuz Bünyesinde Kaç Adet Veri Merkezi Mevcuttur ?".....	33
Şekil 8 Anket Sonuçları: "Kurumunuz Veri Merkezinin TIA Seviyesi"	34
Şekil 9 Anket Sonuçları: "Kurumunuzun Veri merkezi bileşenlerinden hangileri yedeklidir?"	35
Şekil 10 Anket Sonuçları: "Kurumların Hizmet Anlaşmaları"	36
Şekil 11 Anket Sonuçları: "Bilgi Güvenliği Yönetim sistemi var mıdır?"	37
Şekil 12 Anket Sonuçları: "İş Sürekliliği Yönetim Sisteminiz mevcut mudur?"	38
Şekil 13 Anket Sonuçları: "Veri Merkezi Konsolidasyonuna Bakış"	39
Şekil 14. EMC'nin 3 Aşamalı Dönüşüm Serüveni	42
Şekil 15 EMC Veri Merkezi Süreklilik Modeli	45
Şekil 16. Sayılarla EMC'nin Veri Merkezi Kapsamında Gelişimi	46
Şekil 17. Intel'in VM Stratejisi ile Sürekli İyileştirme Süreci	46
Şekil 18. 2003-2013 Intel Toplam VM Alanı ve VM Sayısı	47
Şekil 19. Yıllara göre Intel'in Ofis ve Kurumsal İşlem ve Depolama İhtiyacı	48
Şekil 20 NCIA Kurumunun G.Kore e-Devlet Üst Yapısındaki Yeri.....	50
Şekil 21 NCIA İdari Yapısı	51

Şekil 22. Güney Kore Kamu Entegre Veri Merkezi Planlaması	52
Şekil 23. NCIA Yerleşkeleri ve Merkezlerde Bulunan Sistemlerin Listesi	52
Şekil 24. Gelişmiş Ulusal Güvenlik Altyapı Sistemi (ANSIS)	57
Şekil 25. Felaket Önleme Sistemleri	58
Şekil 26 Güney Kore e-Devlet Standart Çerçeve Yaklaşımı	60
Şekil 27 Güney Kore e-Devlet Standart Çerçevesi ve Kazanımlar	60
Şekil 28. Standart Çerçeve Kullanım - Kazanımlar	61
Şekil 29. Standart Çerçeve – Yıllara Göre Mali Tasarruf	62
Şekil 30. ABD Kamu Kurumları'nda ve IBM'de 15 yıllık Veri Merkezi Konsolidasyon Süreçleri	63
Şekil 31 Kamu Kurumları Arası Bağlantı - Gürcistan Örneği (DEA Öncesi ve Sonrasının Temsili Gösterimi)	77
Şekil 32 Kurumlar ve UVM Bağlantı Alternatifleri - 1	77
Şekil 33 Kurumlar ve UVM Bağlantı Alternatifleri - 2	78
Şekil 34. Örnek Replikasyon Topolojileri (G.Kore ve Özel Sektör Uygulamaları)	81

TABLÖLAR

Tablo 1 G.Kore Kamu Entegre Veri Merkezi ile Sağlanan Kazanımlar.....	56
Tablo 2: Ulusal Veri Merkezi Tasarım Adımları.....	74
Tablo 3: Geçiş Seviyelerine Göre Kurum ve Veri Merkezi Sorumluluk Dağılımı	76

1. GİRİŞ

1.1. Amaç ve Kapsam

Neredeyse yarım asırdır büyümekte ve gelişmekte olan bilişim sektörü, hayatına oda büyüklüğünde cihazlarla başlamış, daha sonra bunların kişisel kullanıma uygun masaüstü versiyonlarından, avuç içine sığacak kadar küçük ebatlardaki cihazlara küçültmüş, diğer yandan ise benzer bir hızda bu cihazların kapasitelerini artırmıştır. Her geçen gün, kişisel, kurumsal ve küresel boyutlarda artan veri ve işlem hacmi ile bu cihazların kullanımındaki yöntemler ve bunların verimliliği, önemini hızla artırmaktadır.

Sektörün bu hızlı gelişimi pek çok yeni kavram ve yapının doğmasına sebep olmaktadır. Benzer veya ilintili amaçlar doğrultusunda kullanılmak üzere, telekomünikasyon, depolama, işlem kapasitesi gibi farklı bileşenlerden oluşan cihazların bir arada tutulduğu yerler olarak bilinen veri merkezleri buna örnek olarak gösterilebilir. Odalar büyüklüğünde cihazların var olduğu dönemden, bulut bilişim gibi kavramların ortaya çıktığı günümüze kadar veri merkezleri, farklı yapılarda var olmuş ve halen gelişimlerini devam ettirmektedir.

Yaşam döngüsünün başlarında, daha yönetilebilir ve güvenilir bulunduğu için veri merkezleri farklı farklı ihtiyaçlar için ayrıca kurulmuştur. Bu durum, seneler içerisinde her düzeyden birçok kurum ve kuruluşta, yönetilmesi güç, çoklu veri merkezi yapısının oluşmasına sebep olmuştur.

Bu kapsamda, dünyada, gerek özel sektörde, gerekse kamuda maliyetleri düşürmek, yönetilebilirliği ve güvenlik seviyelerini artırmak gibi çeşitli nedenlerden ötürü, çoklu veri merkezi yaklaşımından, veri merkezlerinin ortaklaştırılması yaklaşımına bir geçiş gözlenmiştir. Özellikle 2000'li yılların başlarından itibaren ortaya çıkan bu yaklaşım ile, gerek kurum/kuruluş düzeyinde, gerekse ulusal düzeylerde, verimli kapasite kullanımı, artırılmış güvenlik, yönetilebilirlik, süreklilik ve yedeklilik gibi birçok ciddi kazanım elde edilebildiği, ölçümleme sonuçları ile gösterilmektedir.

Bu deęerlendirme raporunun amacı, Türkiye’de kamu sektöründe çoklu veri merkezi yerine ulusal veri merkezi yaklaşımının benimsenmesi durumunda, Türkiye’de kamunun mevcut durumunun incelenmesi, uluslararası başarılı örneklerin de dikkate alınarak Türkiye’ye uygun geiş senaryolarının ortaya konmasıdır. Çalışma kapsamında ulusal veri merkezine geiş senaryoları, bunların günün şartlarına uygunluğu, avantajları ve dezavantajları ile kamuya etkilerine yönelik deęerlendirmeler ve öngörüler sunulacaktır.

1.2. Çalışma Yaklaşımı

Bilgi Toplumu sürecinde, sunduęu hizmetlerde teknolojiden maksimum ölçüde faydalanmayı ve bu hizmetleri etkin ve verimli olarak sunmayı hedefleyen ülkelerin gündemine giren “Ulusal Veri Merkezi” (UVM) ve “konsolidasyon” (ortaklaştırma) kavramlarının ortak tanımlar çerçevesinde ele alınmasını sağlamak amacı ile hazırlanan genel çerçeve bölümü, sağlıklı başlangı için üzerinde durulması gereken ilk bölüm olarak görölmektedir.

Konsolidasyon öncesi en önemli gereksinim, mevcut durumdaki varlıkların ortaya konulmasıdır. Teknolojik açıdan günümüzde yaşanan gelişmeler ve geleceęe yönelik eğilimler, UVM amacı doğrultusunda ülkemizde bu güne kadar yapılan atılımlar, alınan kararlar ve giden aşamalar, kamu kurumlarında veri merkezi açısından mevcut envanterin tespiti; böyle bir ulusal girişim öncesi mevcut durumu ortaya koyan önemli bileşenlerden bazılarıdır. Çalışmanın mevcut durum analizi bölümünde, literatür taraması, birebir görüşmeler, teknolojideki mevcut imkanlar ve geleceęe yönelik öngörüler için sektör ile işbirlięi ve anket çalışması gerçekleştirilmiştir. Özel sektör ile çalışmalar çerçevesinde gerçekleştirilen çalıştay ve toplantılarda; EMC, IBM Türk, Microsoft ve Oracle başta olmak üzere, Vodafone, Grid Telekom, Ko Sistem, Türkcell Superonline ve TURKSAT katılımları ile sektördeki deneyimlere ilişkin önemli katkılar sağlanmıştır.

Ayrıca UVM kapsamında çalışmalarda bulunan ve belirli bir deneyime sahip olan ülkelerin yapısal ve yaklaşımsal olarak incelenmesi ile, örnek modellerin kazanımları da, küresel mevcut durumu gözler önüne serebilmek adına genel hatları ile ele alınmıştır.

Raporun son bölümünde, bu bilgiler ışığında, kamu veya özel sektör için, veri merkezi konsolidasyonunda ele alınabilecek olası senaryolar deęerlendirilmiş ve yapılan anketler çerçevesinde kamu kurumlarındaki bilişim merkezi yöneticilerinin

paylaştığı deęerlendirmeler ile, lkemiz iin nerilebilecek UVM modelleri ortaya konulmaya alıřılmıştır.

Bu srece daha nceki yıllarda bařlayan lkelerin halen uzun yıllardır bu srecin olgunlařmasına ynelik adımları atmaya devam ettięi dikkate alındığında, bu bařlığın hayata gemesi ve olgunlařmasının uzun soluklu olarak lke gndeminde nemini koruyacaęı grlmektedir. Dolayısıyla her bir bileřeni detaylı analiz gerektiren ve bnyesinde teknolojik, hukuki, idari ve operasyonel detayları barındıran UVM iin, bu alıřma vesilesi ile ncelikle bir envanter alıřması, akabinde bařarılı lke rnekleri incelemesi ve sonu olarak olası senaryolar ve Trkiye iin nerilecek seeneklerin ortaya konulması ile bařlangıca katkı saęlanması hedeflenmiştir.

2. GENEL ÇERÇEVE

2.1. Veri Merkezi

Veri merkezi, bir kurum veya kuruluşun Bilgi Teknolojileri (BT) altyapısının tutulduğu ve bakımının sağlandığı fiziki yer olarak bilinmektedir. Geçmişte bu altyapılar tek bir fiziki yerde tutulduğu için isim “veri merkezi” olarak belirlenmiş olmakla birlikte, günümüz ihtiyaçları ile dağıtık yapıların ortaya çıkması, kapasite ihtiyacının ve kullanımının artması sebebi ile veri merkezleri sadece tek bir fiziki ortamda bulunmayabilmektedir. Bu durumda fiziken ne kadar dağınık olursa olsun, kuruluşun verilerinin tutulduğu “yer-ler-in” tamamı veri merkezi olarak adlandırılmaktadır.¹

Veri merkezleri boyutlarına ve alt yapı kapasitelerine göre de tanımlanabilmektedir. Örneğin IDC, veri merkezi boyut sınıflandırmasına göre “veri merkezleri”, sunucu ve altyapı bileşenlerinin bulunduğu, 30,5 m² (100 sq ft) üzerindeki odalar olarak tanımlanmıştır. [1]

2.1.1. Veri Merkezi Bileşenleri ve Maliyetler

Bir veri merkezinin temel bileşenleri Şekil 1’de verilmiştir. Bileşenler incelendiğinde kaynakların çok büyük bir kısmının mevcut BİT alt yapısını ayakta tutmak için kullanıldığı görülmektedir.

¹ <http://www.gartner.com/it-glossary/data-center/>

 <p>Sunucular</p>	 <p>Depolama</p>	 <p>Ağ Altyapısı</p>	 <p>Temel Güç</p>
 <p>Soğutma Sistemleri</p>	 <p>Kesintisiz Güç Kaynağı ve Aküler</p>	 <p>Jeneratör</p>	 <p>Felaket Kurtarma⁸</p>
 <p>İzleme /Yönetim</p>	 <p>Siber Güvenlik¹⁰</p>		

Şekil 1. Veri Merkezi Bileşenleri

2.1.2. Veri Merkezlerinde Kaynak Yönetimi ve Maliyetler

Yapılan bir araştırmaya göre, donanım, yazılım ve BT hizmetlerine senede 1,5 trilyon dolarlık harcama gerçekleştirilmektedir. Bu harcamaların yaklaşık %75'i ise sadece bir veri merkezi sisteminin ayakta tutulması için harcadığı görülmektedir

² <http://www.lenovo.com/images/OneWebImages/Brand/460x368/lenovo-rack-server-thinkserver-rd340-rd440-td340.png>

³ http://blog.architecting.it/wp-content/uploads/2011/10/offline_storage.png

⁴ <http://www.dantor.com/images/servers/servers2.jpg>

⁵ http://media.lehighvalleylive.com/breaking-news_impact/photo/power-lines-df23d88b81bb29b6.jpg

⁶ <http://donar.messe.de/exhibitor/cebit/2014/D289187/gallery-868x0-100404.jpg>

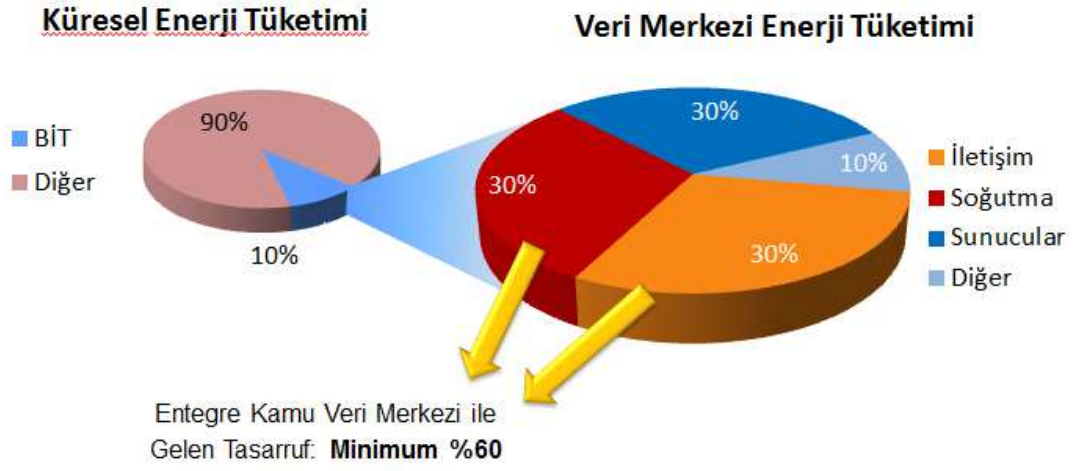
⁷ http://assets.bizjournals.com/sacramento/print-edition/RagingWire-generator2-020312DM*304.jpg?v=1

⁸ <http://2.bp.blogspot.com/-oq6QiTmFwj/T5VRtNmDwzI/AAAAAAAAAEzc/F9AvLFJYp20/s1600/disaster+recovery+plan.png>

⁹ <http://www.constanttech.com/images/v2/design/7.jpg>

¹⁰ http://1.bp.blogspot.com/_J6GQj5YL8v4/TScYVcQK-el/AAAAAAAAATs/s0B1UCDOIs/s1600/Smart-Meter-Security.jpg

[2]. Bir diğer araştırma ise, BİT tarafından dünyada tüketilen toplam enerjinin 1.500 Terawatt/saat olduğunu ve toplam tüketimin %10'una yaklaştığını belirtmektedir [3]. BİT tarafındaki tüketim incelendiğinde, yaklaşık %30'unun soğutma, %30'unun iletişim altyapısı ve %30'unun sunucular için harcadığı (Şekil 2), veri merkezlerinin konsolidasyonu gündeme geldiğinde, yaklaşık %60'lık bir tasarruf öngörüldüğü, bu modeli hayata geçiren ülkelerde de yaklaşık %60'lık bir tasarruf ölçümlendiği görülmüştür.



Şekil 2. BİT Enerji Dağılımı

Bir veri merkezinin ortaya çıkardığı masraflar, özetle aşağıda listelenmiş ana başlıklarda gruplanabilir.

- Cihaz, sistem temin maliyetleri
- Cihaz, sistem ve yazılımların bakım / işletme maliyetleri
- Enerji maliyetleri
 - Temel güç
 - Kesintisiz Güç Kaynağı
 - Jeneratör
- İklimlendirme / Soğutma Altyapıları
- Doğal Kaynaklara verilen zararın oluşturduğu maliyetler
- Doğal Kaynaklara zararın azaltılmasına yönelik maliyetler
- Yönetim masrafları

- Siber güvenlięin saęlanması
- Fiziki güvenlięin saęlanması
- Sürdürülebilirlik
- İletişim Altyapısı
- Sistem yönetimi için gereken insan kaynaęı

Bu kadar çok maliyet kalemi karşısında etkinlik ve verimlilik, (harcama büyüklükleri göze alındığında) dünya genelinde önem arz etmektedir. Veri merkezlerinin verimlilięinin belirlenmesi amacıyla birçok farklı ölçümleme yöntemi kullanılmaktadır. Bunlardan en öne çıkanı, en çok harcamanın olduęu güç maliyet bileşeninin etkinlięini ölçen Güç Kullanım Etkinlięi (Power Usage Effectiveness) – PUE ölçenidir.

PUE, veri merkezi için harcanan toplam güç miktarının sadece BİT bileşenleri için kullanılan güç kaynaęına oranı olarak tanımlanmıştır.

$$PUE = \frac{\text{Veri Merkezi için Harcanan toplam Güç Miktarı}}{\text{BİT Bileşenleri için Veri Merkezinde Harcanan Güç Miktarı}}$$

Örneęin, veri merkezindeki sunucu ve dięer aktif cihazlara harcanan enerji 1 birim iken bu sistemlerin süreklilięi için harcanan dięer çevresel cihazlara harcanan enerji 06 birim ise bu ortamdaki PUE deęeri 1,6 olmaktadır.

$$PUE = \frac{1 + 0,6}{1} = 1,6$$

Buna göre en verimli deęer sayılan PUE = 1 durumu, veri merkezinin BİT bileşenleri için harcanan gücünün harcanan toplam güce eşit olduęu ideal durum olarak tariflenmektedir. Bu ideal durumda BİT bileşenlerini ayakta tutmak için ilave gücün harcanmadıęı öngörülmektedir.

Dünya çapında büyük veri merkezlerine sahip özel sektörün PUE deęerini düşürmek için ciddi bir efor sarf ettięi ve farkı modeller oluşturuđu görülmektedir. Bu çalışmalar sayesinde veri merkezleri “nesiller” atlamakta, çıkarılan yeni

tasarımlar ile daha etkin ve verimli hale getirilmektedir. Şekil 3'te bu gelişime bir örnek sunulmuştur. Şekilde görüldüğü üzere, 2005 yılından itibaren yapılan veri merkezi tasarımı geliştirme çalışmaları ile 2 PUE değeri 2011 yılında 1.05 -1,2 PUE aralığına kadar düşürülmüştür.



Şekil 3. 1989 – 2011 Yılları Arası Microsoft Örnek Veri Merkezi Nesilleri [4]

Farklı veri merkezleri nesilleri arasındaki farklara bakıldığında, yapılan güncellemeler ile;

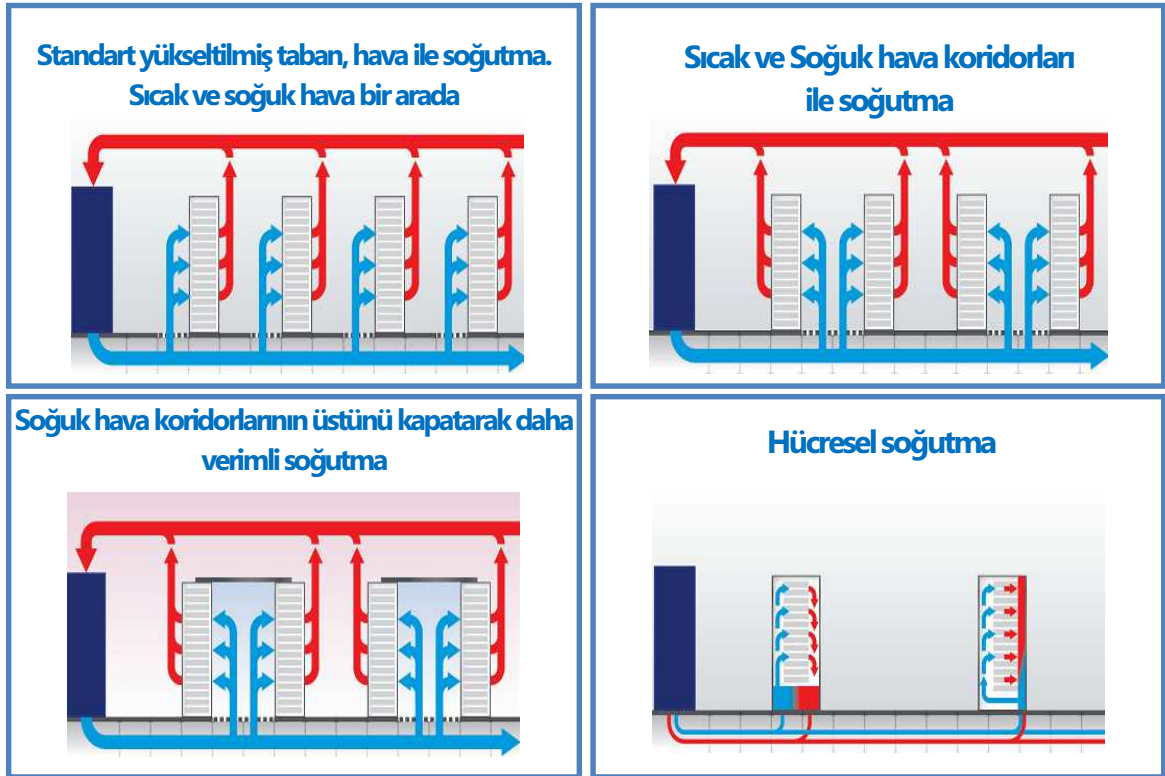
- Kabinlerde gereksiz yer kullanımının minimize edildiği,
- Ortamı değil ısınan cihazları soğutmaya yönelik kademeli geçişler ile, fiziki yapılanmanın modüler şekle dönüştüğü,
- Soğutma için mümkün olduğunca minimum enerji harcaması ile doğal kaynakların (soğuk hava, su kaynaklarından doğrudan alınan su vb.) kullanılarak, ve soğutma sürecinde ortaya çıkan atıkların (sıcak hava vb) doğaya zarar vermeyecek şekilde yeniden kullanılmasının öngörülerek ilave soğutma ihtiyacının azaltılmaya çalışıldığı ve
- Son jenerasyonlarda ise veri merkezi bileşenlerinin tek başına çalışabilir, taşınabilir, modüler kabin ve yapılara doğru taşındığı görülmüştür.

Dünyadaki büyük veri merkezlerinin kurulma yer tercihlerine baktığımızda genelde iklim açısından daha soğuk, teknoloji merkezi olan, ekonomik enerji altyapılarına yakın, alternatifli iletişim altyapılarının üzerinde yer alan ve güvenli bölgeler tercih edilmektedir. Bu sebeple, Avrupa ve Kuzey Amerika bölgelerinde veri merkezlerinin daha yoğun olarak yer aldığı görülmektedir.

Şekil 2’de görüldüğü üzere, veri merkezlerindeki en büyük maliyetlerin başında iklimlendirme / soğutma kalemi gelmektedir. Bu sebeple veri merkezleri için doğru ve ekonomik iklimlendirme açısından doğru bölge analizi yapılması ve buna uygun yer seçilmesi çok önem taşımakta, iklim açısından daha soğuk yerler tercih edilerek bu maliyet minimuma düşürülmeye çalışılmaktadır. ASHARE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) tarafından 2012 yılında veri merkezleri için tavsiye edilen sıcaklık aralığı 18-27 derece arasında, nem ise %30-%55 arasındadır.

Örnek bir yaklaşım olarak Facebook ele alınabilir. Prineville’de yer alan Facebook veri merkezi yaklaşık 30 km² alana yayılmış olup 800 milyondan fazla kullanıcıya hizmet vermektedir. Bu bölgenin ortalama sıcaklığı yılın 6 ayı boyunca 10 derecenin altında olup kalan dönemde de 20 dereceyi geçmeyen bir iklime sahiptir.

Veri merkezlerinin en büyük elektrik tüketiminden birini oluşturan soğutma sistemleri ile ilgili verimlilik çalışmaları önem teşkil etmektedir. Seneler içerisinde soğutma tasarımı ile ilgili önemli gelişmeler kat edilmiştir. Şekil 4’te soğutma sistemlerindeki tasarımsal gelişim gösterilmektedir. İlk veri merkezi tasarımlarında soğuk hava ve sıcak hava aynı ortamda bulunduğu tasarımlar kullanılırken, zaman içerisinde mümkün olduğunca sıcak/soğuk hava izolasyonu sağlanmış, ve soğutma sistemleri doğrudan soğutulmak istenen cihaza yaklaştırılarak performans artışı sağlanmaya odaklanılmıştır.



Şekil 4. Veri Merkezlerinde Etkin Soğutma Gelişmeleri [4]

Verimliliği artırmak için belirlenen modelden biri de Operasyonel Verimlilik modelidir [5]. Bu modelde veri merkezleri 4 seviyede tanımlanmıştır.

- **Temel:** Genel olarak stabil bir yapı kısa dönemli hedeflerle idame ettirilmektedir. Bu seviye veri merkezlerinde kendi başına çalışan (stand alone) altyapı kullanılmaktadır. Bu yapıda sunucu sanallaştırma avantajlarından yararlanmakta ancak sistemlerin sürekliliği konusunda araçlar kullanılmamaktadır.
- **Konsolide Edilmiş:** Sunucu sanallaştırma ve fiziki yerlerin birleştirilmesi (konsolidasyonu) ile yönetilebilir büyüklükler sağlanmaya çalışılarak, kaynak maliyetlerinin düşürülmesi hedeflenmiştir. Sunucu ve depolama yapıları daha verimli kullanılmaya, sanallaştırma ile hareketlilik (mobility) sağlanmaya başlanmıştır.
- **Hazır:** Bu veri merkezi seviyesinde BT alt yapısı genel bir kaynak havuzu olarak görülmekte, ihtiyaç bazlı olarak ölçeklenebilir şekilde değişen ihtiyaçları karşılamak için kullanılmaktadır. Bu yapıda iş yükü

dengelenmekte, süreklilik sağlanmakta, yüksek kullanım oranları ile performans artırılmaktadır. Bu yapılarda odak hizmet seviyesinde ölçümleme ve gelişim sağlanırken, oluşturulan yeni yönetim prosedürleri ile iş ihtiyaçları karşılanmaktadır.

- **Stratejik:** Bu seviyede, politika temelli otomasyon araçlarının yaygın kullanımı ile veri merkezinin karmaşıklığı düşürülmüş, süreklilik ihtiyaçları karşılanarak veri ve uygulamaların dinamik yer değişikliği sağlanmıştır. Çeşitli enstrüman ve ölçümleme kriterlerinin daimi kullanımı ile yönetim politikaları ile uyumun doğrulanması temin edilmiştir.

Belirlenen bu farklı seviyelerde, stratejik seviyeye yaklaşan veri merkezlerinde öne çıkan 4 temel özellik olduğu tespit edilmiştir [5].

- Sunucu, depolama, ağ kullanımı ve yerleşke varlıklarının kullanımının optimize edilmesi ile kapasite ve sürekliliğin en üst seviyeye taşınması
- Değişen iş gereksinimlerini karşılamak amacıyla daha esnek tasarımların kullanılması
- Hizmet seviyelerinin artırılması ve sürekliliğin sağlanması için daha fazla otomatik araçların kullanılması
- Kurumun iş hedefleri ile uyumlu bir veri merkez(ler)i planı oluşturulması ve bu planın güncel tutulması

Bu tespitler doğrultusunda, [5]'te yapılan araştırma sonuçlarına bakıldığında, tanımlanan 4 farklı seviye için oluşturulan verimlilik kıyaslaması Şekil 5'te verilmiştir.

	Temel	Konsolide	Hazır	Stratejik
İşlemler	11+ yıl	Veri tabanı yaşı		< 3 yıl
	2,5+	Güç Kullanımı Etkinliği (PUE)		< 1,5
Tesisler	Yok	Mekanik/Güç Yedekliliği		Tamamı
	Yüksek	Mekanik/Güç Güncellenmelerinde Bozulma		Hiç Yok
Sunucular	< %10	Sanallaştırma Oranı		%60+
	0-4	Fiziki Sunucu Başına Sanal Makine		8+
Depolama	%10-20	Depolamada Sanallaştırma Oranı		%80-90
	Arşiv olarak yedeklilik	Arşivleme		Veri Haritalaması
Ağ	Günler	Felaket Kurtarma Süresi		Saniyeler
Uygulamalar ve Araçlar	Kişiler Yönetiyor	Uygulama Portföy Kararları		Merkezi Yaklaşım
Yönetim	Yavaş ve Zor	Karar Alma Kolaylığı		Hızlı ve Kolay
Personel	0-10	Adam Başına Düşen Sunucu Sayısı		100'den Fazla
	< %30	Personelin Yeni Projelere Ayırdığı Vakit		%60+
Verimsiz ← → Çok Verimli				

Şekil 5. Belirtilen VM Seviyelerine Göre Verimlilik Karşılaştırmaları [10]

Veri merkezi verimliliği için kullanılan bir başka örnek ölçüm ise, bir firmanın kendi veri merkezi stratejisinde kullandığı Birim Hizmet Maliyeti ölçenidir. [1] Bu ölçen ise veri merkezinin toplam maliyetinin (sunucu, ağ, insan kaynağı, ortam işletme, işletim sistemi ve işletim yönetimi, yedeklilik ve kurtarma dahil) kurumun kendi işletme maliyetlerine (tasarım, ofis, üretim, girişim ve hizmet) oranı olarak tanımlanmıştır.

BİT ve veri merkezi harcamalarının bu şekilde kurum ve kuruluşların bütün harcamaları ile ilişkilendirilmesi sadece belirli örnekler tarafından da desteklenmemektedir. 2012 yılında farklı sektörlerden 308 bilişim yöneticisi ile yapılan bir çalışmada, yöneticilerin son yıllarda BİT harcamalarını, operasyonel harcamaları düşürmek için kullandıkları yönündeki eğilimin altı çizilmektedir. Çalışmada buna ek olarak, artık daha çok kurumun bu bakış açısı ile BİT harcamalarını, yatırımların geri dönüşü (ROI) bakış açısı ile gerekçelendirerek toplam kurumsal harcamalarda hafifletmeyi hedefledikleri ifade edilmiştir [1].

2.2. Veri Merkezlerinin Birleştirilmesi (Konsolidasyonu)

Bugün birçok veri merkezinin, karmaşık kaynak yığınları olduğu, verimli bir şekilde mevcut yapıları ayakta tutarak yeni ihtiyaçları karşılamada zorluk yaşandığı

ve bunun çok yüksek maliyetler ile yapılabildiği ifade edilmektedir ([6]). Bu duruma bir gerekçe olarak ise, gün geçtikçe artan ihtiyaçlar, gelişen teknoloji ve buna bağlı olarak oluşan yeni beklentiler gösterilmektedir. Bunlara ek olarak, kurumların vermekte olduğu hizmetlerin giderek tamamen elektronik ortama geçmesi sebebiyle, veri merkezlerinin beklenen performansta ve kesintisiz hizmet vermesi artık bir gereklilik halini almıştır. Bu yüzden veri merkezi sahibi olmak artık bir ayrıcalık veya prestij göstergesi olmaktan çıkmış, daha çok kurumlara ciddi bir işletme ve maliyet yükü olarak yansımaya başlamıştır. Birden fazla veri merkezi olan kurumlarda ise bu yük katlanarak artmakta ve yönetilemez bir hale gelmektedir.

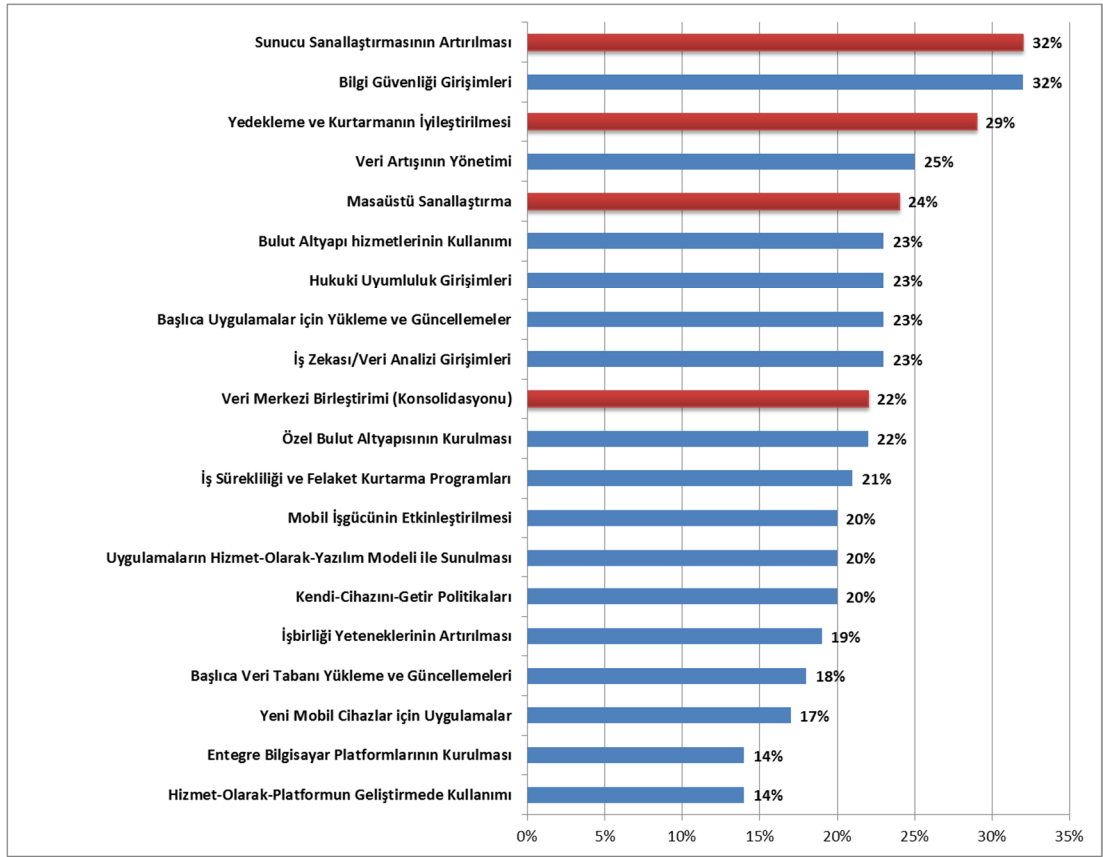
Yapılan bir kestirime göre 2015 yılına kadar mevcut ağ kapasitesinin 8, depolama kapasitesinin 16, işlem gücü kapasitesinin ise 20 kat artması beklenmektedir [6]. Artan bu ihtiyaçlar ve buna bağlı hızlı gelişim, veri merkezlerinin büyük veri merkezi yöneticilerini tasarruf yöntemlerine itmiş, veri merkezleri optimizasyon ile bir fabrika gibi hizmet veren yerler olarak tasarlanmaya başlanmıştır. Bu yaklaşımla değişikliklerin disiplinli olarak yönetilebilir bir hale getirilmesi hedeflenerek, hem ihtiyaçlar daha etkili bir şekilde karşılanmakta, hem de yeni teknolojilerin adaptasyon süreci iyi yönetilebilmektedir [1].

2014 yılı için yapılan BİT harcama araştırmasında bu değişimi destekleyen bulgular paylaşılmıştır [7]. 562 BİT yöneticisi ile gerçekleştirilen çalışmada, 2014 yılı için en önemli BİT öncelikleri olarak sayılan konuların bazıları Şekil 6'da gösterilmiştir. Bu çalışmada da görüldüğü üzere, "Sanallaştırma" ve "Veri Merkezi Konsolidasyonu" öne çıkan hedefler arasında yer almaktadır.

2.3. Ulusal Veri Merkezi Kavramı

Ulusal Veri Merkezi, bir ülkenin belirlenmiş bir alanı için var olan tüm ulusal verilerin ve bu verileri taşıyan BT alt yapısının bulunduğu yer veya yerlerin tamamını ifade eder. Ulusal Veri Merkezilerine örnek olarak aşağıdaki alanlar verilebilir.¹¹

¹¹ <http://en.wikipedia.org/w/index.php?search=national+data+center&title=Special%3ASearch&go=Go>



Şekil 6. 2014 Yılı BT Harcamaları Öncelikleri [7]

- Kamu Kurum ve Kuruluşlarının paydaşlarına (vatandaşa, özel sektöre, Sivil Toplum Kuruluşları'na (STK) vb.) yönelik hizmetlerini içeren Ulusal Veri Merkezi
- Ulusal jeofiziksel verilerin ve bu verilere ait hizmetlerin altyapısını içeren Ulusal Veri Merkezi
- Ulusal astronomik verilerin ve bu verilere ait hizmetlerin altyapısını içeren Ulusal Veri Merkezi
- Ulusal çevre verilerinin ve bu verilere ait hizmetlerin altyapısını içeren Ulusal Veri Merkezi

Bu çalışmada ele alınan UVM kavramı, ilk maddede belirtilen tarifi içermektedir. Yani kamu kurum ve kuruluşlarında halihazırda mevcut bulunan veri merkezlerinin ulusal politikalar çerçevesinde belirlenenlerinin, bir ya da birden fazla fiziki alanda konsolide edilerek bu fiziki merkezden hizmet vermesine yönelik yapılar UVM olarak bu çalışmada ele alınmıştır.

3. MEVCUT DURUM ÇALIŞMALARI

Bir Veri Merkezinin hangi ihtiyaçları karşılamak adına, nasıl bir model ile gerçekleştirilmesi gerektiği, teknik incelemeler ve fizibilite çalışması sonucu ortaya konulabilecek bir husustur. Ancak bu veri merkezinin ulusal boyutta ele alınması durumunda konu teknik bir sorun olmaktan çıkıp, çok eksenli bir başlık haline gelmektedir. Bu bağlamda, Türkiye için olası bir Ulusal Veri Merkezi modelinin tartışılabilmesi için ülkenin mevcutta bu anlamda elinde neler olduğunun tespiti ve iyi analiz edilmesi önem taşımaktadır.

Bu bölümde, Ulusal Veri Merkezi bakış açısı ile sırasıyla, şu ana kadar yapılmış çalışmalara, Merkezi Kamu İdarelerinin mevcut veri merkezi durumlarına ve kurumlardaki Bilgi İşlem Dairelerinin olası bir ulusal veri merkezine yönelik değerlendirmelerinin analizine yer verilmiştir.

3.1. Türkiye’de Ulusal Veri Merkezi Kavramı ve Gelişimi

Her ne kadar, ülke gündemine 15 Ocak 2013 tarihli 25. BTYK toplantısının 104 sayılı kararı ile girmiş gibi görünse de, Ulusal Veri Merkezi kavramının Türkiye’deki gelişimi, kamunun elektronik dönüşümü sürecinin başlarına dayanmaktadır.

1993 yılında, Türkiye ve Dünya Bankası iş birliği ile hazırlanan ve öneri eylem planı özelliği taşıyan “Bilişim ve Ekonomik Modernizasyon Raporu”, bu sürecin ilk adımlarından sayılmaktadır. Her ne kadar günün şartlarında “veri merkezi” kavramı henüz tam anlamıyla ortaya çıkmamış olsa da, belirtilen rapor içerisinde bir “ulusal veri tabanının” oluşturulması önerilmiştir, Böyle bir veri tabanından; kurumlar arası veri paylaşımını kolaylaştırma, mükerrer yatırımları önleme, kamu verisine özel sektör erişimini artırma, veri dağıtım kanallarının dağıtık bir yapıya ulaşması gibi faydaların sağlanabileceği ifade edilmiştir [10].

Dünya Bankası tarafından sunulan bu çalışma, o dönemde ilgili taraf ile yaşanan kredi anlaşması sorunlarından ötürü, rapor halinde kalmış ve uygulamaya konulamamıştır. [11]

Dünya Bankası ile gerçekleştirilen çalışmadan yaklaşık 6 yıl sonra, 1999’da, Türkiye Ulusal Enformasyon Altyapısı Ana Planı (TUENA), Ulaştırma Denizcilik ve

Haberleşme Bakanlığı ile TÜBİTAK tarafından hazırlanmıştır. TUENA ile Türkiye'nin enformasyon politikalarının belirlenmesi amacıyla enformasyon teknolojileri altyapı ve kullanımına yönelik olarak vizyon, hedefler ve kurumsal yapılanma önerileri ortaya konulmuştur.

Bu çalışmada, Merkez Bankası tarafından oluşturulması planlanan "Ulusal Veri tabanları Projesi'ne atıfta bulunulmuş, ancak detayları hakkında bilgi sağlanmamıştır [12].

1998 yılında yayınlanan Başbakanlık genelgesi ile kurulan ve 1998-2002 yılları arasında faaliyet gösteren KamuNET Teknik Kurulu, 2002 yılında çalışmalarına dair bir rapor yayınlamıştır.[11] Bu raporda, kurumlar arası bilgi ve veri paylaşımı konusunda olumlu katkıları olabilecek (ortak) platformlar ön görülmüştür. Ancak yine ulusal veri tabanları ve ulusal veri merkezi kavramlarından bahsedilmemiştir,

Başbakanlığın 2001/352 sayılı genelgesi ile bilgi toplumuna dönüşümün hedeflendiği e-Türkiye girişimi başlatılmıştır. Ancak 2002 yılı sonunda e-Türkiye girişimi, e-Dönüşüm Türkiye projesinin ilanı ile son bulmuştur.

e-Türkiye Girişimi Eylem Planında da, bu kez Çevre odaklı bir Ulusal Çevre Veritabanının oluşturulması önerilmiştir [14]. Ancak bu çalışmanın da sonuçları hakkında ilerleme raporlarına ulaşılammıştır.

58. Hükümet tarafından hazırlanan Acil Eylem planında e-Dönüşüm Türkiye Projesi'nin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile ilgili olarak DPT Müsteşarlığı görevlendirilmiştir. 2003 yılında yayımlanan 2003/12 sayılı Başbakanlık Genelgesi ile e-Dönüşüm Türkiye projesinin amaçları, kurumsal yapısı ve uygulama esasları belirlenmiştir. [11]

Türkiye'de Bilgi toplumuna dönüşüm kapsamında yapılan çalışmalarla e-devlet projelerinde önemli aşamalar kaydedilmiştir. E-vergi, e-ihale, e-sağlık, e-eğitim, e-adalet, e-ticaret, e-imza, e-sözleşme gibi birçok e-hizmet uygulamaya sokulmuştur. Bu kapsamda MERNİS, MERSİS, ASBİS, TAKBİS, UYAP, EKAP projeleri e-devlet uygulamalarının en önemlileri arasında yer alan örneklerdir. Ayrıca tüm kimlik doğrulama ve kamu hizmetlerine tek bir noktadan erişim imkanı sağlayan e-devlet kapısı¹² internet sitesi önemli uygulamalardan birisidir.

¹² www.turkiye.gov.tr

E-devlet hizmetlerinin temel girdisi, kurumların iç otomasyonu ve verdikleri hizmetlere ilişkin kendilerinde var olan verilerdir. Bu veriler kurumların kendi veri merkezlerinde tutulmakta ve işlenmektedir. Dolayısıyla kurumların veri merkezleri arasında önemli bir veri akışı meydana gelmektedir. Daha etkin ve verimli çalışan e-devlet uygulamalarında, Kamu Kurumları arasında birlikte çalışabilirlik ve veri paylaşımı konularında önemli ilerlemeler kaydedildiği dikkati çekmektedir.

Kamu Kurumları veri merkezlerindeki önemli unsurlardan birisi de, hizmet sürekliliğidir. Hizmet sürekliliği ise enerji, iletişim, iklimlendirme, sunucu, güvenlik altyapısı, depolama v.b. her alanda yedeklilik oluşturma ve kaliteli işletme ihtiyacı gerektirmektedir. Bunları sağlamak kurumlarda yüksek giderler oluşturduğundan veri merkezleri için önemli bir maliyet kalemi meydana getirmiştir.

Veri merkezlerindeki bir diğer önemli husus elektronik ortamdaki veri güvenliğidir. Kurumların gündem önceliği, bu konuda nitelikli personel bulundurulması, ayrılmış olan bütçe, veri güvenliğine verilen önem ve gerekliliklerin yerine getiriliş seviyesi farklılıklar göstermektedir. Bu farklılıklar bazı kurumları siber saldırılara karşı alınan güvenlik önlemleri açısından yetersiz bırakmaktadır.

Kamu kurumlarına karşı artan siber tehditler karşısında güvenli kamu iletişimi ve siber güvenliği sağlama, bilgi toplumu sürecinde kamu veri merkezlerinin etkin ve verimli olarak hizmet vermesi, hizmet sürekliliğinin sağlanması amacıyla altyapılarda her türlü yedekliliğin oluşturulması, kurumlar arası birlikte çalışabilirlik ve veri paylaşımının daha etkin ve verimli yapılabilmesi ve bunlar yapılırken maliyetlerde önemli ölçüde tasarruf sağlanması için kamu veri merkezlerinin bir ya da birkaç merkezde birleştirilmesi düşünülmüştür.

Bilim ve Teknoloji Yüksek Kurulu'nun (BTYK) 15 Ocak 2013 tarihli 25. Toplantısı'nda alınan 2013/104 sayılı kararda;

“Kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulmasına ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılmasına karar verilmiştir.”

Bu karara ilişkin belirlenmiş sorumlu kuruluşlar :

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

İlgili Kuruluşlar :

Başbakanlık

Kalkınma Bakanlığı

TÜBİTAK

TÜRKSAT

şeklindedir.

Öte yandan, 20 Haziran 2013 tarihli 2013/4890 sayılı Bakanlar Kurulu Kararı ile “Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı” kabul edilmiştir.

Bu Eylem planıyla;

- a) Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanması,
- b) Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanması,
- c) Siber Güvenlik olaylarının etkilerinin en düşük düzeyde kalması, olayların ardından sistemlerin en kısa sürede normal çalışmasına yönelik stratejik siber güvenlik eylemlerinin belirlenmesi ve oluşan suçun adli makam ve kollukça daha etkin araştırılması ve soruşturulması

amaçlanmıştır.

Ayrıca 15 no’lu eylem;

“Eylem No : 15

Eylem : Kamu Kurum ve Kuruluşlarının İnternet Sayfalarının Yerli Veri Merkezlerine Taşınması

Alt Eylem-1 : Kamu kurumlarının internet sitelerinin yerli ve güvenilir bir veri merkezinde tutulmasını teminen veri merkezi hizmeti sunacak kuruluşun veya kuruluşların belirlenmesi.

Bitirilme Tarihi : Ekim 2013

Sorumlu Kuruluş : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

İlgili Kuruluş : Bilgi Teknolojileri ve İletişim Kurumu, TÜBİTAK

Alt Eylem-2 : İnternet sayfasını kendi bünyesinde barındıramayan belediyeler, hastaneler, İl/ilçe kamu birimleri gibi kamu kurumlarının internet sitelerini belirlenen veri merkezine/merkezlerine taşınması.

Bitirilme Tarihi : Aralık 2013

Sorumlu Kuruluş: Tüm Kamu Kurum ve Kuruluşları”

olarak belirlenmiştir.[16]

Günümüz itibarı ile, kamu kurum ve kuruluşlarının, Ulusal Veri Merkezi yapısına taşınmasına ve bu yapının kullanılmasına ilişkin hukuki değerlendirme gündeme geldiğinde, çok genel hatları yapılan mevzuat incelemesinde aşağıda özet olarak listelenen bazı hususlar dikkati çekmektedir.

- Bazı kamu kurumların mevzuatında, veri tabanının Bakanlık ve/veya genel müdürlükte tutulmasına ilişkin maddeler yer aldığı,
- Bazı kurumların mevzuatlarında, Bilgi işlem sistemlerinin ve/veya elektronik hizmetlerin kendi bünyelerinde düzenlenen ortak veri tabanlarında tutulması gerektiği,
- Bazı kamu kurumlarına, merkezi veri tabanının yedeğinin farklı bir yerde tutulması üzerine görev verildiği,
- Bazı kurumların verilerini paylaşma açısından önemli kısıtlara sahip olduğu,
- Kamu kurumlarının veri paylaşımına ilişkin esasların belirlendiği bir mevzuatın bulunmadığı,
- Bazı kamu kurumlarına, ortak haberleşme ve bilgi sistemleri standardını belirleme yetkisinin verildiği, bu konuda ulusal bir planlamanın ele alınmadığı,
- Bazı kamu kurumlarına, ulusal bilgi alt yapısının tek merkezden geliştirilmesine, yönetilmesine ve kullanıma sunulmasına ilişkin yetki verildiği,
- Kişisel verilere ilişkin “Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı’nın halen yasalaşmadığı,

Bu hususlara ilişkin örnek mevzuatlar Ek-D’de yer almaktadır.

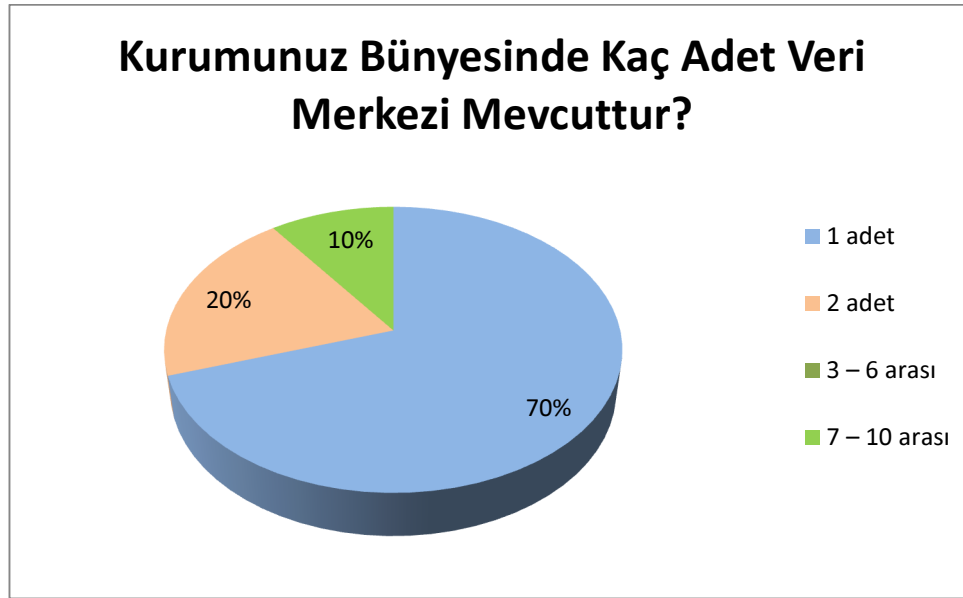
Ulusal Veri Merkezine ilişkin kurumsal yapılanma açısından bakıldığında, halen bu konuda kanunen görevlendirilmiş bir kurum olmadığı görülmektedir.

3.2. Kamu Kurumlarında Veri Merkezlerinin Mevcut Durumu

Bu çalışma çerçevesinde, mevcut durumu gözlemek amacı ile, Bakanlıklar, bağlı, ilgili ve ilişkili kamu kurum ve kuruluşlarının merkez ve taşra teşkilatları baz alınarak 27 sorudan oluşan anket gerçekleştirilmiştir. Anket çalışmasında uygulanan yöntem EK-A'da, anketin soruları EK-B'de, ankete ilişkin cevaplar Ek-C'de yer almaktadır.

Veri merkezlerinin durumu ile ilgili olarak, 4 Bakanlığın veri merkezi yöneticileri ile görüşmeler yapılmıştır. Görüşmeler sonucunda anket soruları hazırlanmış ve kamu Kurumlarından bu anketi doldurmaları istenmiş 10 kamu kurumu anketi doldurmuştur. Anket cevapları aşağıdaki değerlendirmelerde kullanılmıştır.

Kamu kurumlarının %70'inde 1 adet veri merkezi bulunduğu, %30 unda ise 1'den fazla veri merkezi olduğu görülmektedir.



Şekil 7 Anket Sonuçları: "Kurumunuz Bünyesinde Kaç Adet Veri Merkezi Mevcuttur ?"

Veri merkezlerinin fiziki alan büyüklüğü, Kurumların %60'ında 0-100 metrekare arasında, %30'unda 100-250 metrekare arasında, %10'unda 500-1000 metrekare arasında bulunmaktadır.

Birden fazla veri merkezi bulunan kurumlarda; veri merkezleri arasındaki sunucu, veri depolama ürünleri, kişisel bilgisayar, internet bant genişliği kapasitesi v.b. bilişim ihtiyaçlarının ve kapasite kullanımının tek merkezden koordine edilmesi, konsolidasyonu, ihtiyaç fazlası bilişim ürünlerinin ve kapasitenin diğer veri

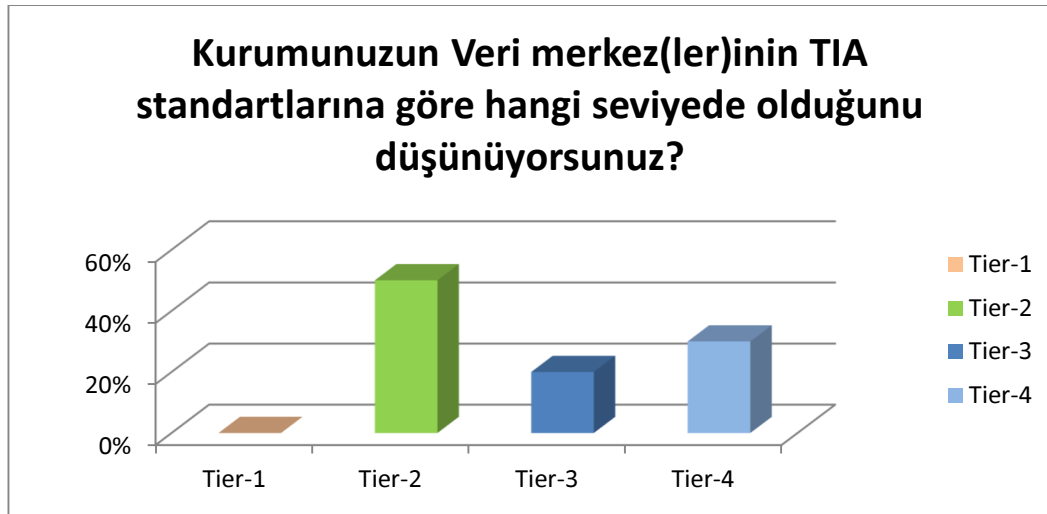
merkezleriyle paylaşımı konularında bir takım mesafeler alınmış ise de yeterli olmadığı gözlemlenmektedir.

Kurumların veri merkezlerinin %50'sine ait Felaket Kurtarma Merkezi (FKM) yapılanması olmadığı, %20'sinde veri merkezlerinin tamamının, %20'sinde veri merkezlerinin çoğunun, %10'unda ise veri merkezlerinin bazılarının Felaket Kurtarma Merkezi yapılanması olduğu görülmektedir.

Kurumlarda diğer kurumlara ve vatandaşa hizmete yönelik portaller mevcuttur. Bu konuda e-devlet kapsamındaki çalışmalarla önemli ilerlemeler kaydedilmiştir. Kurumlarda minimum 2 portal, maksimum 100 portal, ortalama olarak ise 40 portal bulunmaktadır.

Aylık ortalama olarak kurumların %40'ı 101-1.000 kişiye, %30'u 101.000-500.000 kişiye, %30'u ise 500.000'den fazla kişiye hizmet vermektedir. Bu da, kurumların elektronik olarak verdiği hizmetlerin önemli kitlelere ulaştığını göstermektedir.

Kurumların veri merkezlerinin TIA standartlarına göre %50'si Tier-2, %20'si Tier3 ve %30'u Tier-4 seviyesindedir.



Şekil 8 Anket Sonuçları: "Kurumunuz Veri Merkezinin TIA Seviyesi"

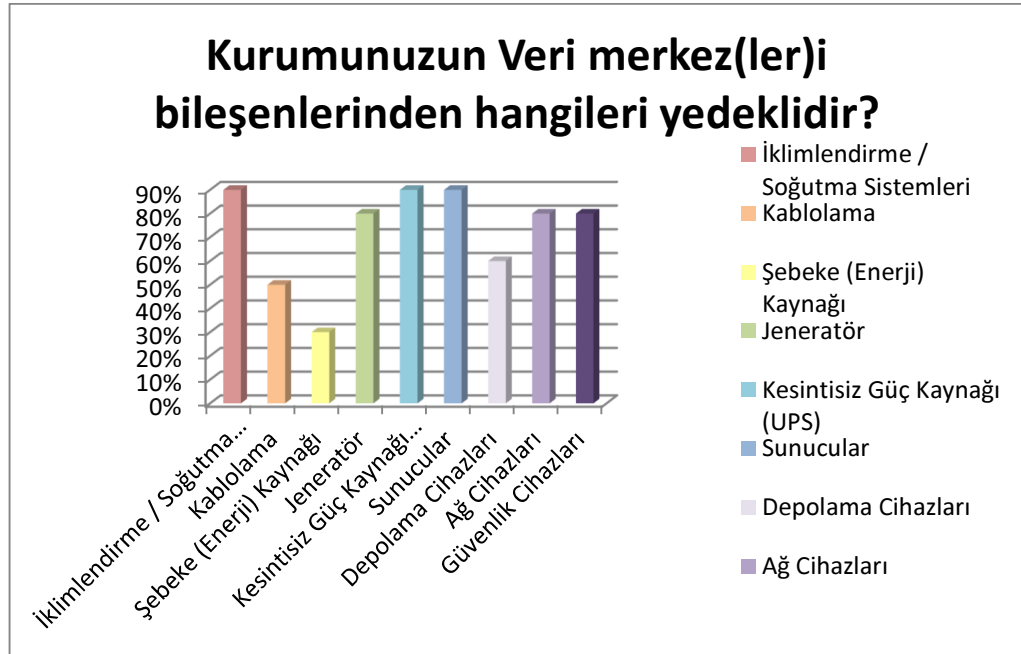
Veri merkezlerinin enerji altyapısı, soğutma sistemleri, su basması v.b. ile ilgili kurumların %80'inin izleme sistemi mevcuttur, %20'sinde ise böyle bir izleme sistemi yoktur.

Veri merkezlerindeki alt yapı bileşenleri açısından; kurumların %90'ında iklimlendirme/soğutma sistemleri, %50'sinde kablolama altyapısı, %30'unda şebeke

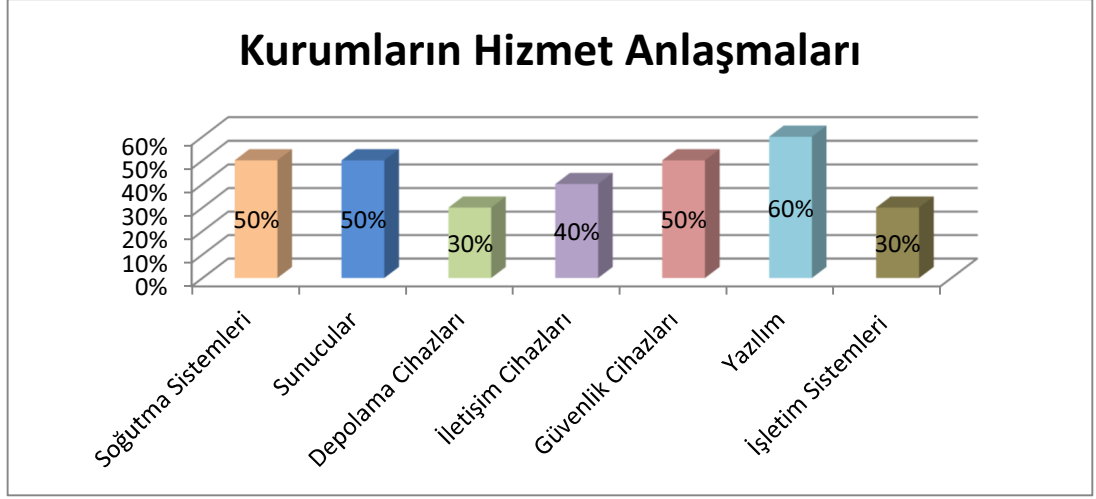
(enerji) kaynağı, %80'inde jeneratör, %90'ında Kesintisiz Güç kaynağı (UPS), %90'ında sunucular, %60'ında depolama cihazları, %80'inde ağ cihazları ve %80'inde güvenlik cihazları yedeklidir.

Kurumlar veri merkezlerinin hizmet sürekliliği ve işletilmesine ilişkin özel sektör ile hizmet anlaşmaları yapmaktadırlar. Kurumların %10'u hizmetlerin tamamı için, %70'i hizmetlerin bir kısmı için hizmet anlaşması yapmaktadır. %20'sinin ise hizmet anlaşması olmayıp bu hizmeti kendi iç imkanları ile sağlamaktadırlar.

Kurumların %50'si iklimlendirme/soğutma sistemleri, %50'si sunucular, %30'u depolama cihazları, %40'ı iletişim cihazları, %50'si güvenlik cihazları, %60'ı yazılım ve %30'u işletim sistemleri için hizmet satın almaktadır.



Şekil 9 Anket Sonuçları: "Kurumunuzun Veri merkezi bileşenlerinden hangileri yedeklidir?"



Şekil 10 Anket Sonuçları: "Kurumların Hizmet Anlaşmaları"

Kurumlar alt yapı bileşenlerini görüldüğü gibi çoğunlukla yedekli olarak bulundurmakta, hizmetin kesintisiz devam edebilmesi için bu alt yapı bileşenleri ile ilgili hizmet satın almakta ve bakım anlaşmaları yapmaktadır. Bu durum her kuruma ayrı ayrı büyük bir mali yük getirmektedir.

Veri merkezlerinde, kurumların %30'unda tek jeneratör mevcut olup, bunların %10'u 0-100 KVA arası, %10'u 251-500 KVA arası ve %10'u 1000 KVA ve daha büyük kapasiteye sahiptir. Kurumların %70'inde ise yedekli jeneratör mevcut olup, bunların %20'si 251-500 KVA arası ve %50'si 1000 KVA ve daha büyük kapasiteye sahiptir.

Kurumların %20'sinde tek kesintisiz güç kaynağı (UPS) mevcut olup, bunlar 0-100 KVA arası kapasiteye sahiptir. Kurumların %80'inde ise yedekli kesintisiz güç kaynağı (UPS) mevcut olup, bunların %20'si 251-500 KVA arası ve %40'si 500 KVA ve daha büyük kapasiteye sahiptir.

Kurumların veri merkezlerindeki enerji kullanımı maliyetlerinin de bir hayli yüksek olduğu gözlemlenmektedir.

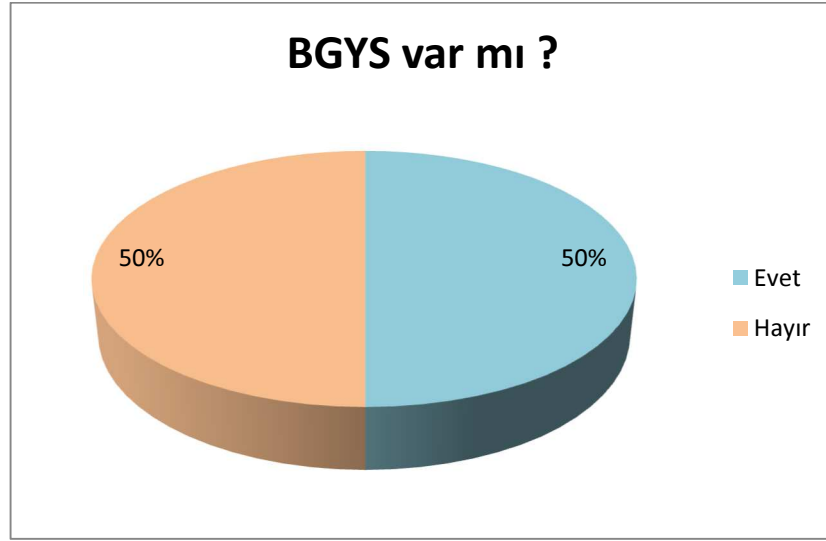
Veri merkezlerinde;

- Yangın riskine karşı Kurumların %20'sinde algılama sistemi, %90'ında uyarı alarm sistemi, %20'sinde ise kamera ile izleme sistemi mevcuttur.
- Su baskını riskine karşı Kurumların %10'unda algılama sistemi, %40'ında uyarı alarm sistemi, %20'sinde ise kamera ile izleme sistemi mevcuttur.
- Deprem riskine karşı Kurumların %10'unda uyarı alarm sistemi, %20'sinde ise kamera ile izleme sistemi mevcuttur.

Kurumların %90'ında veri merkezlerine uygun (FM200 gazlı) yangın söndürme sistemi mevcuttur.

Kurumların %50'sinde Bilgi Güvenliği Yönetim Sistemi (BGYS) mevcuttur. Ancak BGYS çalışmaları ile bilgi güvenliğine yönelik bir takım önlemler mevcuttur. Bununla birlikte, bu önlemlerin zaman zaman yetersiz kaldığı gözlemlenmektedir. Bu durum ise bilgi güvenliğini tehlikeye düşürmektedir.

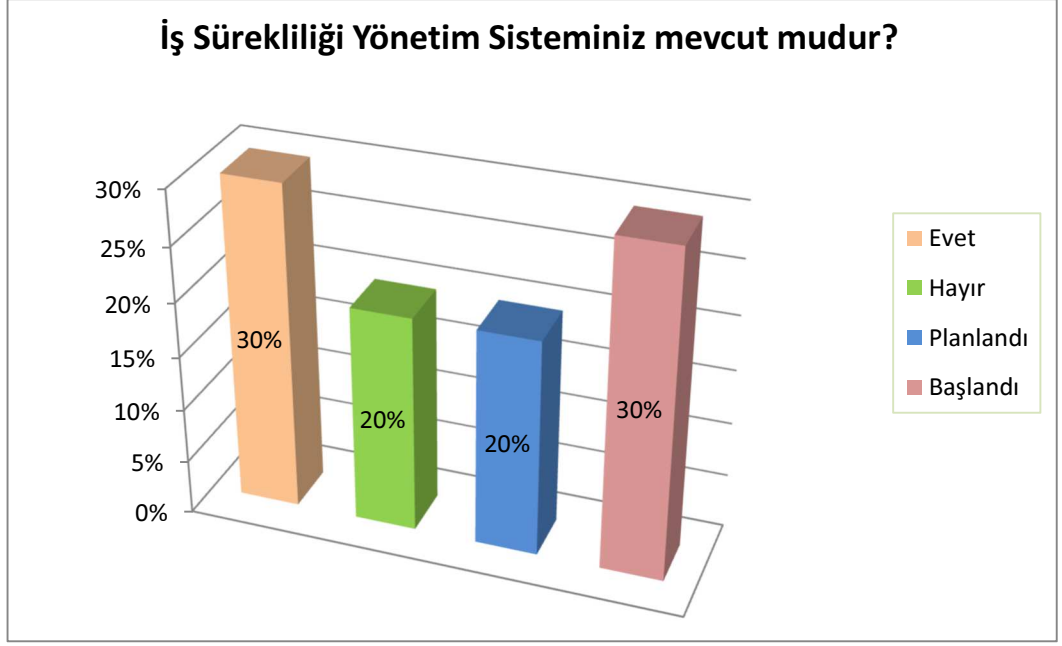
Kurumların %60'ında Bilgi Güvenliği Yönetim Sistemi ve buna bağlı kurum içi bilişim hizmetlerinin yürütülmesine dair yönerge, genelge, yönetmelik v.b. mevzuat bulunmaktadır.



Şekil 11 Anket Sonuçları: "Bilgi Güvenliği Yönetim sistemi var mıdır?"

Kurumların veri merkezlerinde siber saldırılar ya da teknik sebeplerle zaman zaman kısa süreli olarak hizmet kesintileri yaşanmaktadır. Bu kesintiler minimum 10 dakika, maksimum 30 dakika, ortalama olarak 24 dakika olarak gerçekleşmiştir. Son bir yıl içinde Kurumların %50'sinde bu kesintiler 1-5 dakika olarak gerçekleşmiş, %50'sinde ise hiç kesinti yaşanmıştır.

Kurumların %30'unda İş Sürekliliği Yönetim Sistemi (ISYS) mevcuttur, %70'inde ISYS mevcut değildir. Ancak iş sürekliliğini sağlamaya yönelik birtakım önlemler mevcuttur. Kurumların %20'sinde bu husus planlanmış, %30'unda çalışmalara başlanmıştır. %20'sinde ise ISYS hiç yoktur. Kurumların iş sürekliliğini sağlama konusunda çoğunlukla yetersiz kaldıkları görülmektedir.



Şekil 12 Anket Sonuçları: "İş Sürekliliği Yönetim Sisteminiz mevcut mudur?"

Kurumların %80'inde veri yedekleme stratejisi olduğu, %10'unun veri yedekleme stratejisini planladığı, %10'unun ise veri yedekleme stratejisi çalışmalarına başladığı belirlenmiştir. Kurumların veri yedekleme konusunda iyi bir durumda olduğu görülmekle birlikte bu stratejilerin kabul gören standartlara uyumluluğu hususunda bir bilgi bulunmamaktadır.

Veri merkezi hizmetleri sunulurken karşılaşılan problemlerin çözümünde,

- İdari açıdan: Kurumların %10'u sıkıntı yaşandığını, %90'ı sıkıntı olmadığını,
- Teknik açıdan: Kurumların %20'si sıkıntı yaşandığını, %80'i sıkıntı olmadığını,
- Mali açıdan: Kurumların %20'si sıkıntı yaşandığını, %80'i sıkıntı olmadığını

belirtmişlerdir. Yaşanan sıkıntılar ise kurumlar tarafından:

- Yeterli kalifiye personel bulunmaması,
- Zaman, zaman mali açıdan sıkıntı yaşanması,
- Resmi prosedürlerden kaynaklanan gecikmeler,
- Bilişim projelerine zaman zaman yeterli idari desteğin olmaması,
- KİK kaynaklı sıkıntılar

olarak belirtilmiştir.

Kurumların 2013 yılı BİM yatırım bütçelerine bakıldığında minimum 250.000 TL, maksimum 500.000.000 TL, ortalama olarak ise 76.268.750 TL olduğu görülmektedir.

“Mevcut veri merkezinizin bir başka kamu kurumunun fiziki çatısı altında yer alıp, sistem ve verilerin sorumluluğunun yine şu anda olduğu gibi sizin kontrolünüzde olması gibi bir durum karşınıza çıksa idi, böyle bir çalışma modelini tercih eder miydiniz?” sorusuna Kurumlar %50 “evet”, %50 “hayır” cevabını vermişlerdir.



Şekil 13 Anket Sonuçları: "Veri Merkezi Konsolidasyonuna Bakış"

Kurumlar böyle bir modelin avantajlarını :

- Maliyet,
- Fiziki Güvenlik,
- Kullanım kolaylığı,
- Entegrasyon,
- Bilgi güvenliği,
- İş sürekliliğinin sağlanması,

- Alt yapı yatırımlarının tek elden yapılması ve teknolojik olarak güncellenmesi,
- Alt yapı İşletim kolaylığı

dezavantajlarını:

- Hukuki,
- Veri güvenliği,
- Fiziki müdahale zorluğu,
- Bilgi güvenliğinin tek noktadan sağlanması

olarak belirtmişlerdir.

3.3. Kamu Kurumları Bilgi İşlem Yöneticilerinin Ulusal Veri Merkezi İle İlgili Değerlendirmeleri

Anket sonuçlarına göre mevcuttaki “Kamu Veri Merkezlerinin” analizi yapıldığında; hizmet verilen portföyün sunucu merkezi kaynakları ile birlikte ölçülmesi durumunda, kamu varlıklarındaki israflar göze çarpmaktadır.

Ortalama bin kişiye hizmet veren bir veri merkezinin, 1.000 KVA'dan daha yüksek jeneratöre sahip olduğu ve bu veri merkezlerinin de FKM'leri olduğu görülmektedir.

Yapılan ankette; idari, teknik ve mali açıdan sıkıntıların olmadığı görülmesine rağmen, tahsis edilen kaynakların ihtiyacın üstünde olması bir çelişki yaratmaktadır. Kamu veri merkezlerinin oluşturulması üzerine henüz bir devlet politikası ya da regülasyonu olmamasının, veri merkezi kurulumunda ve idaresinde tasarruf yapılamamasına neden olduğu görülmektedir.

Olumlu bir tespit, anket değerlendirmesini yapanların yarısının, uygulanabilir UVM geçiş senaryolarından birinci faza sıcak bakması yönündeki görüşleridir. Diğer yarısının belirttiği olumsuz görüşlerinin de, daha detaylı şekilde araştırılıp incelenmesi ve buna göre politikalar üretilmesinde yarar vardır.

UVM'ye geçiş ile birlikte kurulum ve yönetim maliyetlerinde büyük tasarrufa gidileceği aşıkardır. Anket sonuçlarının da gösterdiği gibi, UVM sadece bir binadan ibaret olmamalı, regülasyonları, teknik kriterleri ve mevzuatları ile birlikte tam bir

sistemi ifade etmelidir. Bir yandan mühendislik çalışmaları yapılırken, diğer yandan da verimlilik temelli mevzuat çalışmalarına odaklanılmalıdır.

4. ULUSLARARASI ÖRNEKLER

Ulusal Veri Merkezi modelinin oluşturulabilmesi öncesinde, bir veri merkezi kurulumu için teknik altyapı bilgisi ve ülkenin mevcut durumu bilgilerinin yanı sıra, uluslararası arenada belirli büyüklüğün üstünde veri merkezlerine sahip özel sektör ile ulusal veri merkezi oluşturulmasında başarılı olmuş ülke örneklerinin kullandıkları yöntemler, karşılaştıkları sorunlar ve tecrübelerinin incelenmesi de kritik öneme sahiptir.

Bu bölümde, öncelikle önde gelen özel sektör firmalarının, veri merkezi konsolidasyonu tecrübeleri ve bu alandaki uluslararası eğilimlere, akabinde ise e-Devlet çalışmalarında ön plana çıkıp, ulusal veri merkezi çalışmalarında önemli yol kat etmiş olan ülke örneklerinin çalışmalarına yer verilmiştir.

4.1. Uluslararası Eğilimler

Bilişim sektörüne yön veren büyük firmalara ait veri merkezlerinde seneler içerisinde gerçekleşen değişim, veri merkezi teknolojilerindeki eğilimlerin tespiti için önemli referans kaynağı olmaktadır.

Bu bölümde, öne çıkan firmalardan, EMC ve Intel örneklerine yer verilmiştir.

4.1.1. EMC Veri Merkezlerinde Değişim

EMC'nin 2004 yılından günümüze yaşadığı değişim, 3 aşamalı bir geçiş süreci ile gerçekleştirilmiştir. Aşamaların özeti Şekil 14'te verilmiştir.



Şekil 14. EMC'nin 3 Aşamalı Dönüşüm Serüveni

2004-2008 yılları arasında sürdüğü belirtilen 1. aşamada EMC, kendisine 2 temel hedef belirlemiştir. Bunlar; BT alt yapısının birleştirilmesi (konsolide edilmesi) ve test, geliştirme ve uygulama sunucularının sanallaştırılmasıdır. Bu hedefler ışığında 4 sene boyunca süren çalışmalarla en büyük sorunlardan biri olarak tariflenen verimsiz kaynak kullanımı ortadan kaldırılmaya çalışılmıştır. Çalışma öncesinde;

- 3 aydan daha uzun süreler boyunca depolama kapasitesinde %30 kullanım oranı,
- Senelik %60 fiziki depolama büyümesi,
- %10'dan daha düşük oranlarda işlemci kullanımı,
- Buna rağmen sunucularda senelik %20 büyüme,
- Veri merkezi fiziki alanında verimsiz kullanım ve
- BT personelinin üzerindeki fazla iş yükü

gibi temel ve kronik sorunların gözlendiği belirtilmektedir. Yapılan çalışmalarda bu sorunları gidermek için atılan en önemli adımlardan bir tanesinin, çalışmaların başı sayılabilecek erken bir noktada tüm mimarinin standartlaştırılması ve sanallaştırmaya geçilmesi kararları olduğu vurgulanmıştır.

Değişimin ikinci aşaması, 2009-2010 yılları arasında gerçekleştirilmiş, bu aşamada kritik misyon uygulamalarının sanallaştırmasına odaklanılmıştır. Bu uygulamalar arasında, Microsoft Exchange, Active Directory, Oracle 11i E-Business Suite gibi uygulamaların yanı sıra, iş zekası, kurumsal raporlama gibi bir çok farklı uygulamanın da bulunduğu belirtilmektedir. 2 sene süren bu süreç sonunda EMC'nin sunucularında %70lik sanallaştırma oranına ulaştığı ölçülmüştür.

Bu yaklaşım ile %60-90 arasında üretkenlik artışı, 10 katı daha iyi performans ve 7 Milyon Dolarlık yerleşke, lisanslama bakım ve idame tasarrufu sağlandığı tespit edilmiştir.

2011 yılından günümüze uzanan ve 3. aşama olarak isimlendirilen son aşamada ise, hizmet-olarak-BT (ITaaS) yaklaşımı ile kurumda çeviklik hedeflenmiştir. Bu şekilde, hizmet sunum modellerinin değiştirilmekte olduğu, artık teknoloji yerine insan ve süreçlere odaklanıldığı ifade edilmektedir.

Bu süreç içerisinde, EMC'nin veri merkezleri için otomatize edilmiş araçlar kullanmasının özellikle BT insan kaynağını daha verimli kullanmasına sebep olduğu

raporlanmaktadır. Konsolidasyon ile enerji verimliliğinde %34 oranında artış görüldüğü, CO₂ salınımında ise 45 Milyon kg'lık bir düşüş olduğu ifade edilmiştir. Felaket anlarında güvenlik analiz araçlarının tepki süresi ise 26 saatten 10 dakikaya kadar düşürülmüştür.

Veri merkezi yerleşkesinde çevre duyarlı yaklaşımların izlendiği de kaydedilmiştir. Yağmur suyu birikimi yapılarak, şehir suyu kullanımı %40 azaltıldığı, bu oranın doğal hava soğukluğu kullanılarak soğutma yapıldığında %57'lere kadar ulaştığı ölçümlenmektedir.

Yedeklemede de verimlilik sağlayan EMC, canlı arşivleme ile 1 Petabyte'lık verinin veri tabanı yedekleme takviminden çıkması sağlamıştır. Deduplication¹³ kullanımı ile verimlilik daha da artırılmış, yedekleme süreleri %75 azaltılmıştır. Yedekleme hataları %99 oranında azaltılmıştır.

Tüm bu çalışmalar ile aynı zamanda finansal şeffaflık ve hesap verebilirlik sağlayan EMC, gerçek kullanım değerlerine göre BT masrafı çıkartabilir seviyeye ulaşmıştır. Sağlanan şeffaflık ile hem operasyonel hem de BT birimlerinin gereksiz kaynak tahsisi yapmalarının önüne geçilmiş, talep ve gerçekleşen BT kullanımı arasındaki farkın kapatıldığı gözlenmiştir. Hizmetlerin %54 ile %89 oranında daha az masraf çıkardığı, oluşan bu ilave kaynakların yenilikçi yaklaşımlarda kullanılabildiği kayıtlara geçmiştir. Bu şekilde birim seviyesinde değil kurumsal seviyesinde kazanımların elde edilebildiği gözlenmiştir.

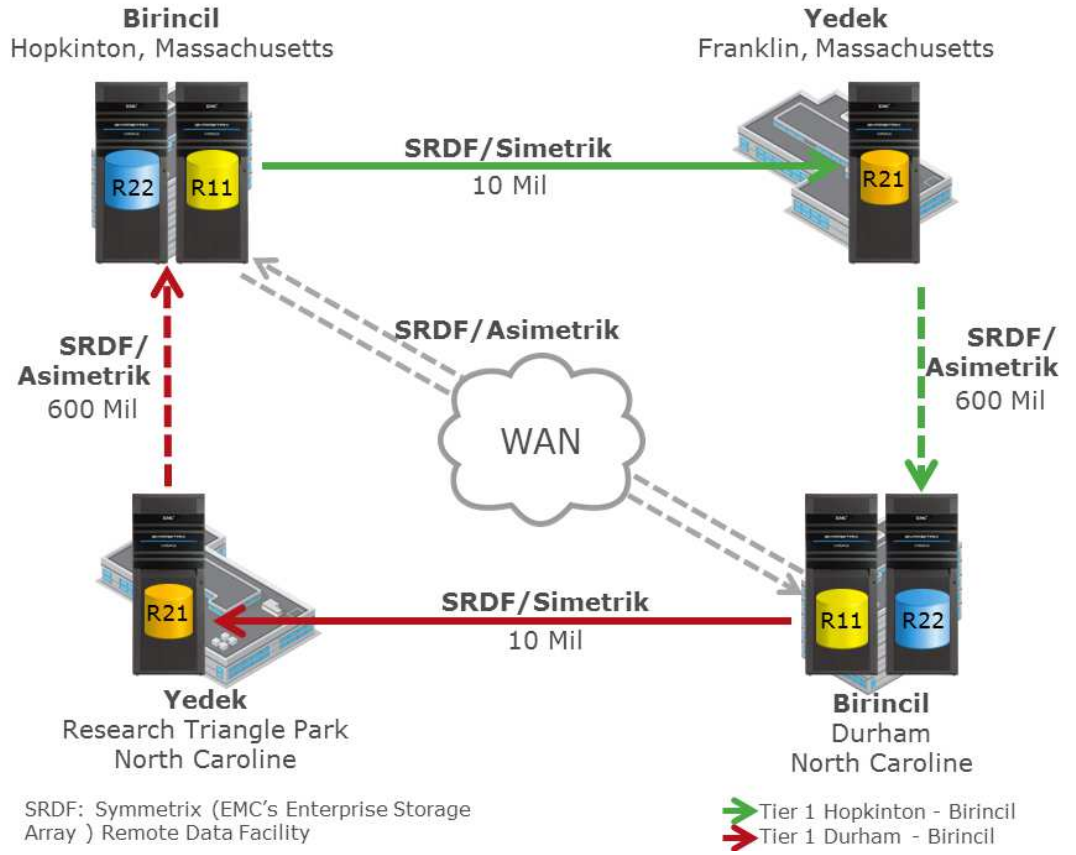
EMC Veri merkezlerinde konsolidasyon sürecine girerken ayrıca bir süreklilik modeli de öngörmüştür. İki veri merkezi için süreklilik modeli Şekil 15'te görülmektedir. Günümüz teknik imkanları ve fiziksel kısıtlamaları dahilinde, simetrik yedekleme için teknik olarak iki veri merkezi arasında en fazla 300 km mesafe bulunmak zorundadır¹⁴. EMC'nin modeli incelendiğinde, mesafelere ilişkin teknik kısıtlar da göz önünde bulundurularak hem simetrik hem de asimetrik yedekleme yaklaşımının kullanıldığı dikkati çekmektedir. Bu yapıda, her birincil veri merkezinin fiziki olarak yakınında (16,1 km) kurulan yedek veri merkezleri sayesinde simetrik yedekleme mümkün kılınmıştır.

Bu süreklilik yaklaşımında veriler 3 seviyede korunmaktadır:

¹³ Deduplication: Veritabanında tekrarlı verilerin kaldırılmasıdır. Özellikle bir veya daha fazla veritabanı bir listede birleştirildiğinde kullanılır. (www.adobe.com/products/vdp/glossary.html)

¹⁴ Oracle, "The Art of Data Replication", Eylül 2011, <http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-080-art-data-replication-487868.pdf>

- Kritik Görev Verileri: En önemli veri grubudur. Bu veri grubu için sıfır veri kaybı, modeldeki “yıldız konfigürasyonlu EMC SRDF Senkron ve asenkron” yapı sayesinde sağlanmaktadır.
- Kritik İş Verileri: İkincil önemli veri grubu olup, asenkron yedeklilik ile en fazla 15 dakikalık veri kaybı riskine sahiptir.
- Önemli İş Verileri: Üçüncü önemli veri grubu olup, asenkron yedeklilik ile en fazla 24 saatlik veri kaybı riskine sahiptir.



Şekil 15 EMC Veri Merkezi Süreklilik Modeli

EMC'nin 2004-2013 yılları arası gerçekleştirdiği bu dönüşümün sonucu olarak elde edilen kazanımların özeti Şekil 16'da verilmiştir.

	2004	2013
İÇ KULLANICI SAYISI	24,000	60,000
BT ALANI	5 VERİ MERKEZİ, 960 TB DEPOLAMA ALANI	5 VERİ MERKEZİ, ~13 PB DEPOLAMA ALANI
İŞ UYGULAMASI	~400	~500
SANALLAŞTIRMA	2,000 FİZİKSEL SUNUCU	~10,000 İŞLETİM SİSTEMİ GÖRÜNTÜSÜ 93% SANALLAŞTIRMA ORANI

Şekil 16. Sayılarla EMC'nin Veri Merkezi Kapsamında Gelişimi

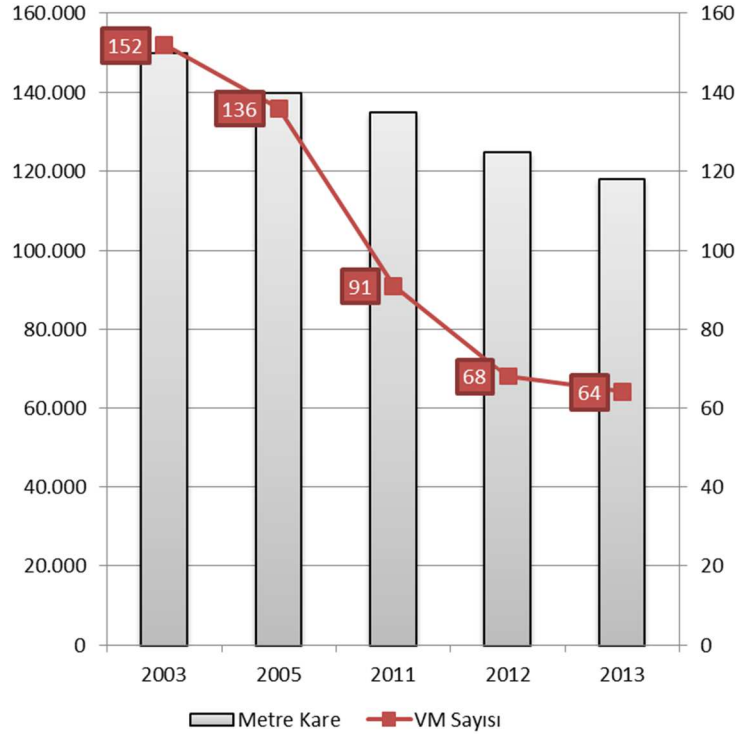
4.1.2. Intel'in Veri Merkezi Stratejisi

Intel, 2000 yılı başında veri merkezi konusuna planlı olarak eğilme kararı almış, son 14 yıl içerisinde, izlediği strateji ile ciddi ilerlemeler kaydetmiştir. Intel'in Sürekli İyileştirme olarak adlandırdığı bu süreç Şekil 17'de özetlenmiştir.



Şekil 17. Intel'in VM Stratejisi ile Sürekli İyileştirme Süreci

Intel Veri Merkezi birleştirme yaklaşımı ile, artan ihtiyaçlara rağmen, 10 sene içerisinde 152 veri merkezi sayısını 64'e düşürerek tasarruf sağlamıştır. Şekil 18'de de görüldüğü üzere, Intel 2003-2013 yılları arasında %24'lük yerleşke küçülmesine gitmiştir. Kaynakları verimli kullanmaya odaklanan Intel, %45 kaynak kullanımı oranını %50'lerin üzerine çıkararak 5,9 milyon dolarlık tasarruf sağlamıştır.



Şekil 18. 2003-2013 Intel Toplam VM Alanı ve VM Sayısı

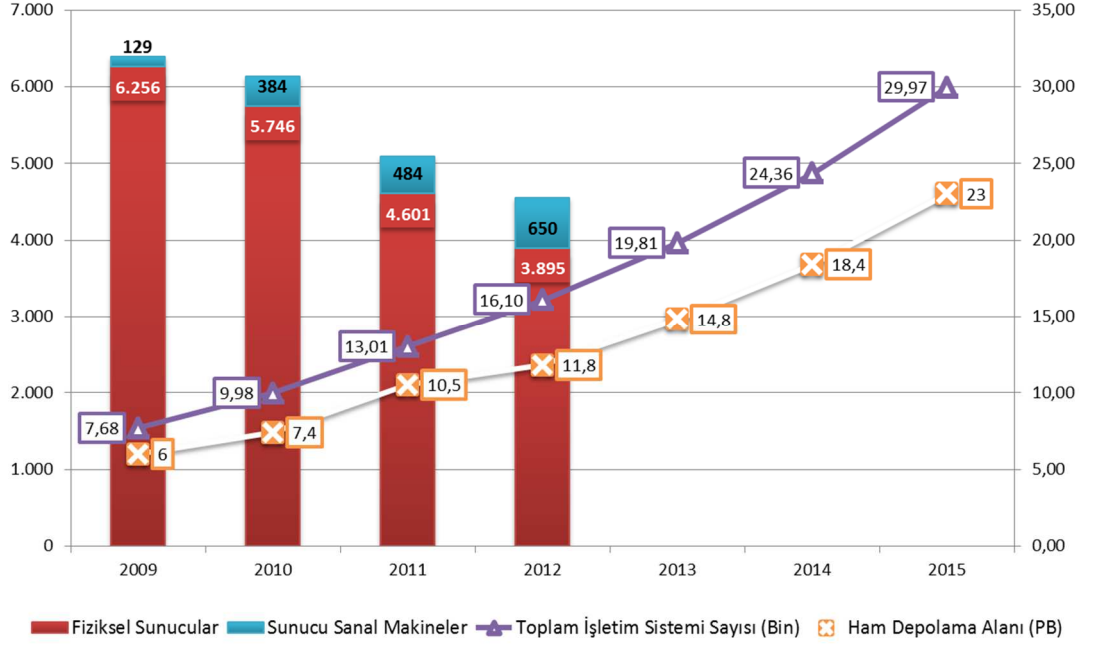
Verimsiz çalışan ve etkin olmayan 32 veri merkezinin kapatılmasını hedefleyerek yola çıkan Intel, yaklaşık 18.830 metre karelik yerleşke alanını yaklaşık 7.200 metre kareye kadar küçültmüştür. Yaklaşık %35 oranındaki bu veri merkezi küçülmesi Intel'e senelik olarak 24,54 milyon dolarlık bir tasarruf sağlamıştır.

Belirtilen oranlardaki bu küçülme için kullanıldığı belirtilen bazı uygulamalar aşağıdaki gibidir.

- Kapalı, özel tasarım içeren ve yeniden sınıflandırılmış veri merkezleri
- Verimliliğin artırılması
- Yerel alt yapı yerleşkelerinin uzaktan yönetilmesi
- Stratejik yatırımlar ile yerleşke güç kullanımının verimliliğinin artırılması

Veri merkezi yerleşkelerindeki küçülmenin yanı sıra, Intel'in sadece ofis ve kurumsal ihtiyaçları için gereken kaynak miktarının bile hızla büyüdüğü görülmektedir. Ancak sanallaştırmaya verilen önem ile, 2009-2012 yılları arasında %60 oranında fiziksel sunucu sayısı azaltılmış, sanal makinelerin sayısı ise

aynı sürede 5 katından fazla artış sağlamıştır. Intel'in bu ihtiyaçları, ve karşılığında değişen bileşen sayıları Şekil 19'da gösterilmektedir.



Şekil 19. Yıllara göre Intel'in Ofis ve Kurumsal İşlem ve Depolama İhtiyacı

Fiziki yer küçültmesinin yanı sıra, enerji verimliliği için Intel'de cihazların yenilenme döngüleri 4 yıla indirilmiştir. Buna göre, daha iyi performans ve enerji verimliliği sağlayan cihazlarla hem cihaz sayıları, hem de enerji maliyetleri düşürülmüştür.

4.2. Ülke Değerlendirmeleri

e-Devlet alanında belli bir ivme almış ülkelerde veri merkezlerinin konsolide edilmesi ve e-Devlet uygulamalarında daha sağlıklı bir veri paylaşım ortamı yaratılması amacıyla farklı senaryolarda entegre veri merkezlerinin hayata geçirildiği görülmektedir.

Diğer ülkelerdeki ulusal veri merkezleri örneklerinde sürecin belirli bir geçiş senaryosuyla yürütüldüğü görülmüştür.

Bu kapsamda internet taraması yapmak suretiyle ve e-Devlet alanında başarılı olarak gösterilen ülkeler arasından belirlenen ülkeler olarak ABD, G.Kore, Malezya, Estonya, Filipinler ve HongKong bu raporda ele alınmıştır.

4.2.1. Güney Kore

Birleşmiş Milletler e-Devlet Gelişmişlik Raporunda 2010 yılından bu yana iki dönemdir birincilik sırasında yer alan Güney Kore, ayrıca NCIA isimli kamu kurumu tarafından işletilen ve dünyada ilk kurulan kamu entegre veri merkezinde (GIDC) de yaklaşık 8 yıllık bir deneyim çerçevesinde başarı hikayesine sahiptir.

Bu veri merkezi, Eylül 2010'da "Veri Merkezi Mükemmeliyet Ödülü", Temmuz 2011'de "Akıllı BT Servis Yönetim Sistemleri ile En İyi Kamu Servis Merkezi Ödülü" kazanmıştır¹⁵. ITIL¹⁶ standartlarına dayalı operasyonel yönetimi, 8 katmanlı siber güvenlik altyapısı, siber saldırılara karşı 4 seviyeli analiz sistemi ve verilen hizmetlerde SLA uygulaması ile dikkati çeken NCIA, entegre yönetimini nTOPS (National Total Operation Platform System – Ulusal Toplam Operasyon Platform Sistemi) ile gerçekleştirmektedir.

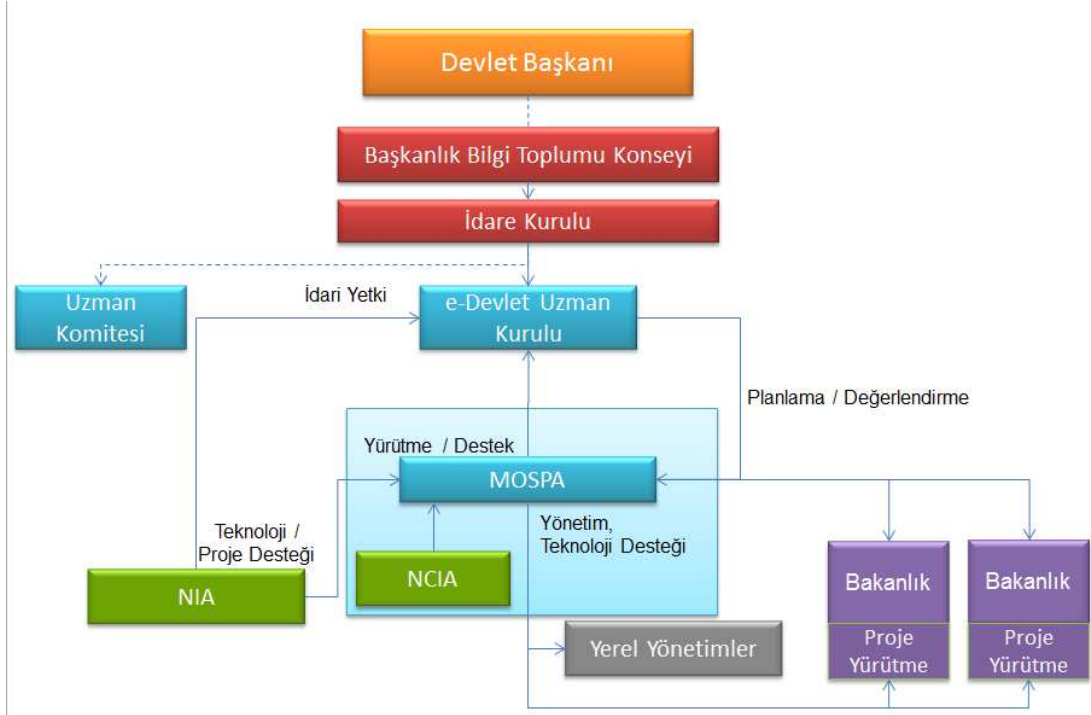
Bir başka ilgi çekici yapı ise, kamu kurumlarının BİT alanındaki donanım ve yazılım alımlarının toplu olarak bu merkez tarafından yapılmasıdır. Bu kaynakların hayat döngülerinin kontrol ve takibi de NCIA tarafından yapılmaktadır.

NCIA, K-Net adı verilen ve sadece kamu kurumları için hazırlanmış kapalı iletişim altyapısı ile tüm kamu kurumlarının merkezi iletişimini de sağlamaktadır. İş ağı ile kamu ağı tamamen izole edilerek güvenlik sağlanmış olup bu hatlar bilgi güvenliği açısından 7/24 izlenmektedir. Bu merkezi altyapı sayesinde IPv6, IPTV, FMC ve UBcN (Ultra Broadband Convergence Network) gibi teknolojiler kolaylıkla tüm kamu iletişimine uygulanabilmektedir.

Gerek uygulanan model, gerekse yapılanma ve yaklaşımlar açısından Güney Kore'deki oluşumun bu alanda belirli alanlarda örnek alınabileceği değerlendirilmektedir.

¹⁵ http://www.ncia.go.kr/eng/awards/awards_01.jsp

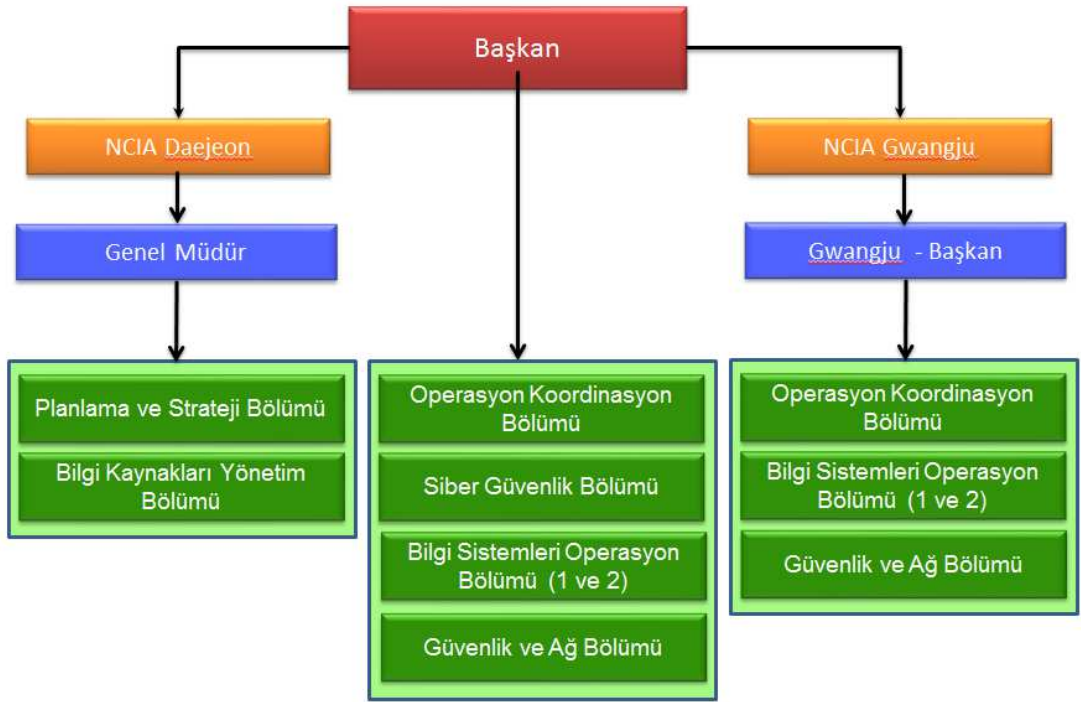
¹⁶ ITIL: IT Infrastructure Library



Şekil 20 NCIA Kurumunun G.Kore e-Devlet Üst Yapısındaki Yeri

4.2.1.1 Ulusal Bilişim ve Bilgi Ajansı (NCIA) Hakkında Kurumsal Bilgiler

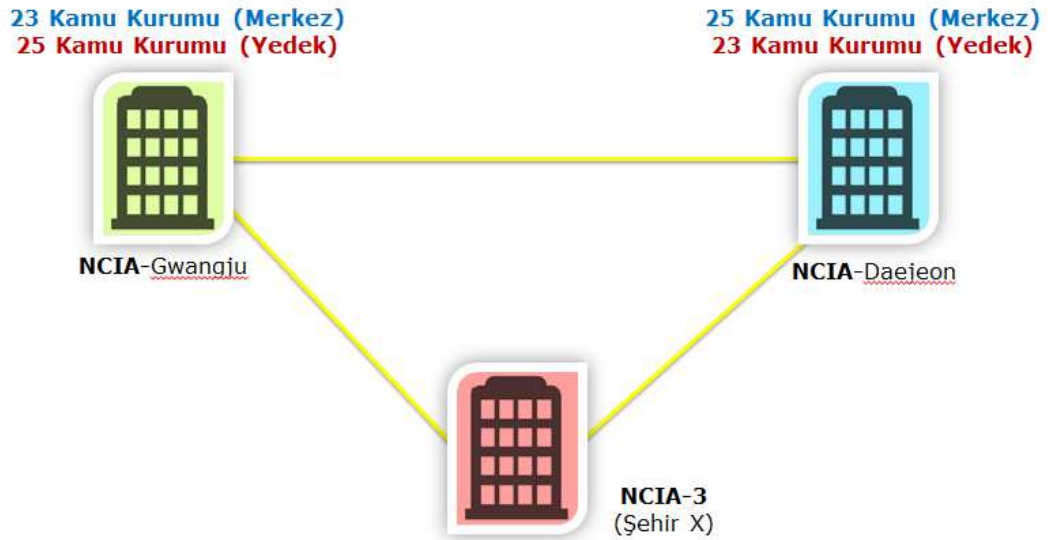
Ulusal Bilişim ve Bilgi Ajansı (NCIA), 2005 yılında e-Devlet çalışmaları kapsamında, Güney Kore Güvenlik ve Kamu Yönetimi Bakanlığı (MOSPA) altında kurulan bir kamu kuruluşudur. NCIA'nın Güney Kore e-Devlet üstyapısındaki yeri Şekil 20'de, idari yapısı Şekil 21'de gösterilmektedir. Kurumun temel faaliyet alanları, Güney Kore'nin 48 merkezi kamu idaresinin bilgi sistemlerine ev sahipliği yapmak, bu sistemlerin güvenliği ve sürekliliği için gerekli alt yapıyı sağlamak ve idarelerin BT ihtiyaçlarını idareler adına tedarik etmektir.



Şekil 21 NCIA İdari Yapısı¹⁷

NCIA'nın Daejeon ve Gwangju illerinde iki adet merkezi bulunmaktadır. 2012 yılı itibariyle var olan 48 kamu idaresinin 25'inin sistemleri NCIA Daejeon, 23'ünün sistemleri ise NCIA Gwangju merkezinde bulunmaktadır. Sistemlerin sürekliliğini sağlamak ve olası veri kayıplarını önlemek amacıyla bu iki merkez arasında ağ bağlantısı kurulmuştur ve her merkezde diğer merkezin verilerinin yedekleri tutulmaktadır. 2015 yılında 3. merkezin açılmasının hedeflendiği, bu merkezin sadece yedekleme amaçlı kullanılacağı belirtilmektedir.

¹⁷ http://www.ncia.go.kr/eng/about/about_04.jsp#



Şekil 23'te NCIA Yerleşkeleri ve merkezde bulunan sistemlerin listesi ile ilgili şema verilmiştir.

Şekil 23. NCIA Yerleşkeleri ve Merkezlerde Bulunan Sistemlerin Listesi

4.2.1.2 Mevcut Entegre Kamu Merkezi Hakkında Bilgiler

NCIA öncesinde, 2004 yılı Aralık ayında yapılan bir ankette, sunucularının sadece %18.1 'inin tam yüke yakın çalıştığı görülmüştür. Sunucu

kapasitesinin %76.4'ünün küçük ebatlı olduğu, sadece %3'ünün büyük ebatlı sunucu altyapısı olduğu ve bu durumun sıkça servis kesintileri yaşanmasına sebep olduğu, bu sebeple önemli iyileştirmeler yapılmasına gereksinim gösterdiği görülmüştür. Yine bir çok kurumun yeterli bilgi güvenliği sistemlerine ve bu konuda uzman personele sahip olmadığı için muhtelif saldırılara hedef olduğu tespit edilmiştir.

Güney Kore'de öncelikli olarak entegre operasyonel altyapı kurulduktan sonra her kurumun bilgi kaynaklarının transfer edilmesi sağlanmıştır. Güney Kore'de de NCIA tesislerine geçiş öncesinde hangi kurumların bu sürece dahil olacağına yönelik yoğun tartışma yaşanmıştır. Öncelik hali hazırda bir e-Devlet projesi hayata geçirme sürecinde olan kurumların Daejon'daki bir numaralı merkeze taşınması yönünde olmuştur. Başta söz konusu olan tartışmalardan bir diğeri de tüm kurumların sıfır-aksama süresi (zero-downtime) ile geçişi üzerine olmuştur. Ancak bütçe tasarrufu gerekçesiyle gruplama yapılmıştır. Buna göre servisin durması yasal sorun yaratacak ve kamuya hizmet sunan başlıklar için sıfır-aksamalı geçiş planlanmıştır.¹⁸

NCIA kurulumu 4 faz olarak kurgulanmıştır:

- 2002-2004 planlama fazı
- 2004-2006 kurulum fazı
- 2005-2007 yeniden konumlandırma fazı
- 2008 – günümüze operasyonel geliştirme fazı

Tarihi süreçte kamu veri merkezinin kurulması ile ilgili şu başlıklar öne çıkmıştır:

- 2002: Ulusal e-Devlet Özel Komitesi'nin 11 temel projesinden birisi olarak İş süreçlerinin yeniden yapılandırılması (NICE BPR Projesi) başlatılmıştır.
- 2003: e-Devlet inisiyatifleri içerisinde en önemlilerinden biri olarak, kamu idareleri arası veri merkezinin kurulması için yasa çıkarılmıştır,
- Ağustos 2003: Kore için 31 e-Devlet Yol Haritası projesi seçilmiştir. Bu projelerin ortak hedefi olarak “dünyada lider bir elektronik devlet olma” belirlenmiştir.

¹⁸ Korea - NCIA - Development, 2010 Report, <http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN042708.pdf>

- 2004: İdareler arası veri merkezinin kurulması için Bilgi Stratejisi Planı (hazırlanmıştır,
- 2005: NCIA 6 takım ve 165 personel ile kurulmuştur, (4 Kasım 2005)
- 2006: 19 merkezi idarenin bilgi sistemleri NCIA Daejeon merkezinde eş konumlu olarak işletilmeye başlanmıştır,
- 2007: NCIA Gwangju merkezi kurulmuştur,
- 2008: Ulusal Bilgi Kanunu ile merkezi veri yönetimi ve paylaşımı zorunlu hale gelmiştir,
- 2008: Merkezi idarelerin bilgi sistemleri yönetimi NCIA bünyesinde bütünleştirilmeye başlanmıştır,
- 2011: 48 kamu kurumunun hizmetlerinin NCIA üzerinden geçmesi sağlanmıştır,
- 2011: Kamu bulut platformu hizmete girmiştir,
- 2011: e-ANSI isimli kapsamlı e-devlet güvenlik izleme sistemi kurulmuştur,
- 2012: Mobil e-Devlet hizmetleri destek merkezi açılmıştır.

4.2.1.3 Mevcut Entegre Kamu Merkezinin Faydaları

Güney Kore'deki bu çalışma çerçevesinde, tüm merkezi kamu kurumlarının veri merkezlerinin tek noktaya toplanmasının gerekçeleri şu şekilde belirtilmektedir.

- Veri merkezinin önemi, sürekliliği, gereksinimleri, bilgi güvenliğinin sağlanması gibi başlıklarda idari farkındalık, sahiplenme ve ayrıca yeterli bütçe temini, Bakanlıktan Bakanlığa farklılık göstermekte, ayrıca her bakanlıkta nitelikli insan kaynağı açısından istenilen seviyede bir yapı oluşturmak mümkün olamamaktadır.
- Kurumlar arası bütçe farklılıklarından dolayı, dağınık yapıda tüm kurumların ihtiyaçlarını yeterli ölçüde karşılayamadığı durumlar söz konusudur. Kaynakların tek bir yere taşınması ve alımların tek yerden yönetilmesi ile bütçe farklılıklarından kaynaklanan bu sorunlar çözülmüştür.
- Dağınık sistemlerde ihtiyaç fazlası alım gerçekleşebilmektedir. Benzer ihtiyaçların ortaklaştırılarak kaynak havuzu oluşturulması ve bu kaynaklarda sanallaştırmak kullanımı ile var olan kaynakların daha verimli kullanılması sağlanmıştır.
- Kaynakların tek noktada yönetilmesi ile eskimiş altyapı cihazlarının tespiti ve yenilenmesi daha kolay sağlanmıştır.

- Kurumların güvenlik, sistem bakımı gibi sorumluluklar için ayrı ayrı personel istihdam etmesi kaynak israfına sebep olduğu için, merkezi yapıda daha az kişinin istihdamı ile daha iyi hizmet verilebilmektedir.
- Kurumlar kendi kendilerine gerekli tüm güvenliği sağlayamadıkları için, merkezi yaklaşım ile daha etkin ve güvenli servis sağlanmaktadır.

Tablo 1'de, NCIA'nın veri merkezlerinin kurulması ile elde edilen kazanımların bir kısmı listelenmiştir.

	NCIA Öncesinde	Bugün (2012 Verileri)¹⁹
Sistem Sürekliliği	% 99.9908	% 99.9999
Uluslararası Sertifikasyon	Yok	4 (ISO-20000, ISO-9010, BS-25999, GISMS)
Ortalama Devre Dışı Kalma Süresi (makine/ay)	67 Dakika	4.8 Saniye
Siber Güvenlik Altyapısı: Kural Sayısı	7.000	13.300
DDoS Saldırıların Tespiti	Yok	0-10 Dakika
Satınalma, İşletme ve Bakım Masraflarında Tasarruf	-	% 30
Sunucu Sayısı Azaltılması	1994 Sunucu	315 Sunucu
Gerçekleştirim Maliyetleri	496 M \$ (Müstakil Gerçekleştirim)	350 M \$ (Entegre Gerçekleştirim)
Müşteri Memnuniyeti	% 64	% 90.4

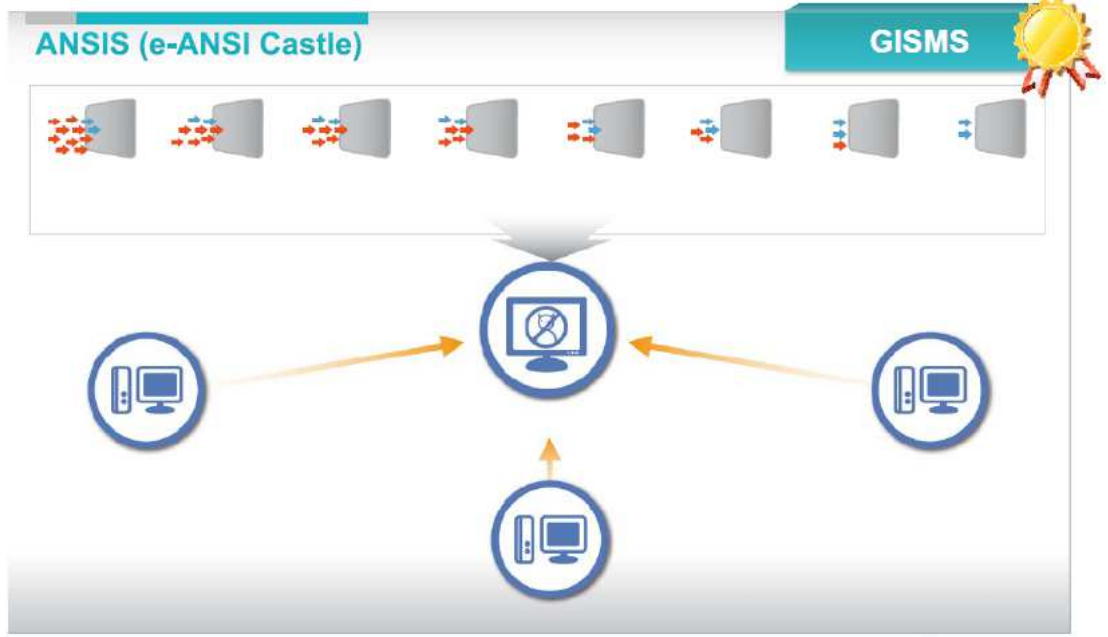
¹⁹ <http://korea.ncia.go.kr/index2.html>

	NCIA Öncesinde	Bugün (2012 Verileri)¹⁹
Sağlanan Platformlar	-	Ortak Yönetim Servisleri Kamu Bulutu Büyük Veri Platformu Mobil Platform
KOBİ Katılımı	% 26,8	% 55,7
Okyanus Ötesi Ziyaretler	4 ülkeden 43 ziyaretçi	51 ülkeden 450 ziyaretçi
Enerji Tasarrufu (Yıllık Elektrik ve Co2)	-	% 30
Felaket Kurtarma Merkezi	% 45	% 59 (2010)

Tablo 1 G.Kore Kamu Entegre Veri Merkezi ile Sağlanan Kazanımlar

NCIA'nın devreye girmesi ile 2012 yılı itibariyle toplam BT sistemleri işletme ve geliştirme maliyetinde de, toplam enerji tüketiminde de yıllık %30 civarında tasarruf sağlanmıştır. Merkezi idare sistemlerinin NCIA'ya taşınmasından önce sistem başına ortalama devre dışı kalma süresi aylık 67 dakika iken NCIA veri merkezlerinin kullanıma açılması ile bu süre 4,8 saniyeye düşürülmüştür.

Sunulan hizmetlerin kullanıcılar tarafından kullanımını engelleyen Hizmet Reddi (Distributed Denial of Service - DDoS) saldırılarına karşı önlem alma süresinde de NCIA'nın kurulması ile ciddi bir iyileşme yaşanmıştır. NCIA, Şekil 24'te şeması verilen Gelişmiş Ulusal Güvenlik Altyapı Sistemi ile tek noktadan tüm merkezi kurum hizmetlerini etkin bir şekilde korumaktadır. NCIA öncesinde DDoS saldırılarına tepki süresi ölçülemezken, 2012 yılı itibarıyla tüm hizmetlerde 0 - 10 dakikada saldırı tespit gerçekleştiği ölçülmüştür.



Şekil 24. Gelişmiş Ulusal Güvenlik Altyapı Sistemi (ANSIS)

NCIA tarafından yürütülmekte olan Felaket Önleme Sistemleri ile NCIA öncesi sistem başına düşen kurtarma yüzdesi %45 iken 2010 yılında bu yüzde %59'a yükseltilmiştir. Şekil 25'te Felaket Önleme Sistemleri arasında;

- Verilerin tek bir nokta yerine dağıtık olarak yedeklenmesi,
- Yedekleme merkezlerinin kullanımı,
- Felaket Kurtarma Sistemi,
- Düzenli tatbikatlar düzenlenmesi

yer almaktadır.

Bu kazanımlara ek olarak 2010 yılından bu yana NCIA sayesinde hiçbir kamu hizmeti elektrik kesintisiyle karşı karşıya kalmamıştır.



Şekil 25. Felaket Önleme Sistemleri

NCIA'nın 2011 yılı bütçesi yaklaşık 300 Milyon ABD Doları olarak verilmiştir. Kurumda yaklaşık 1.000 çalışan görev yapmaktadır. Bu çalışanların 300'ü kamu görevlisi olup, 700'e yakını özel sektörden alınan sözleşmeli personeldir. Burada önemli bir kamu-özel sektör işbirliği göze çarpmaktadır. Güney Kore'de kamu kurumlarında çalışan personelin maaşları ile özel sektörde verilmekte olan maaşların arasında uçurum olmadığı, yakın miktarlarda maaşlar bulunduğu görülmektedir. Bu nedenle kuruma özel sektörden sözleşmeli personel alımında sıkıntı yaşanmamaktadır.

NCIA veri merkezinde bulunan donanımlar, merkezi kurumlardan getirilen mevcut donanımlardır. Merkezin kurulmasında herhangi bir yeni donanım alınmamıştır. Bu vesile ile kurumların ellerinde bulunan ve çok verimli bir şekilde çalışmayan donanımlar NCIA'nın denetimi altında daha etkin kullanılmaya başlanmıştır. Böylelikle BT yatırım planları birbirleriyle uyumlu hale getirilmiştir, altyapı işletme maliyetleri düşürülmüştür. Bu sayede kaynak kullanımı konusunda tasarruf sağlanmış. Aynı zamanda, NCIA veri merkezinde bulut bilişim konusunda çalışmaların olduğu görülmüştür.

Kamu hizmeti ile ilgili verilerin tek merkez üzerinden kontrolü ile ulusal güvenlik ve bilgi güvenliği ihtiyaçlarına daha üst standartta cevap verebilmektedirler.

20

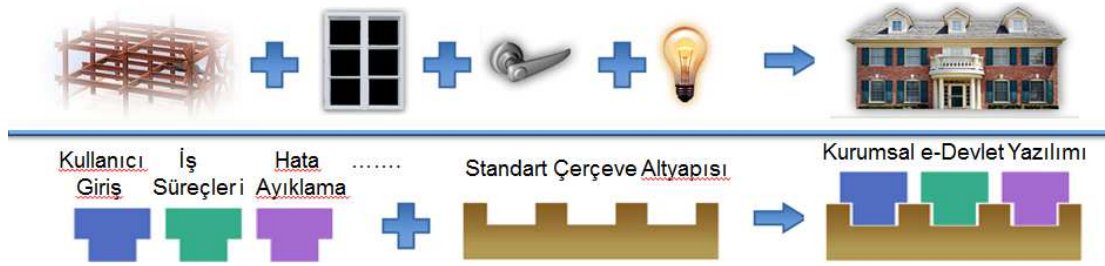
4.2.1.4 Entegre Kamu Merkezi ve e-Devlet Standart Çerçevesi

Kamu kurumlarının, veri merkezlerinde e-Devlet yazılımları aracılığıyla dış paydaşlara hizmet vermektedir. Bu yazılımların geliştirilmesinde kamu kurumları zaman zaman kendi insan kaynaklarını, bazen özel sektör dış kaynak kullanımı yöntemini, bazen de bu iki modelin birleşimi olan proje yönetim modellerini kullanılmaktadır. E-Devlet alanında ihtiyaç duyulan yazılım hangi modelle geliştirilmiş olursa olsun, projenin doğası gereği:

- Diğer kamu kurumları, özel sektör ve STK'lar ile veri alışverişine ihtiyaç duymaktadır.
- Belirli güvenlik standartlarına uymak durumundadır.
- Bilgi güvenliği, kişisel veriler, ulusal güvenlik, veri standardı vb. konularda yayınlanmış olan mevzuata uymak durumundadır.

Bu ve benzeri diğer ortak şartlardan dolayı, e-Devlet alanında yazılım geliştiren kamu kurumları ve özel sektörün, müstakil geliştirmelerden dolayı mükerrer olan süreçleri bulunmaktadır. Örneğin bir standarda (veya mevzuata) uyumluluğu yerine getirmek için bir bakanlıkta belli kütüphaneler geliştirilirken, aynı uyumluluk ihtiyacı sebebiyle diğer e-Devlet projelerinde de benzer kütüphaneler her kurumda her proje için genelde yeniden geliştirmektedir. Bu yaklaşım ciddi boyutta zaman, insan kaynağı ve maliyet kaybına yol açmaktadır. Üstelik her kütüphanenin yeniden test edilmesi, benzer güvenlik zaafiyetlerine karşı güçlendirilme ihtiyacı olması ve iyileştirmeler için de ilerleyen süreçte yine aynı mükerrerliklerin devam etmesi kaçınılmaz olmaktadır.

²⁰ NCIA Kurumsal Tanıtım Broşürü. [Çevrimiçi]. Erişim: http://korea.ncia.go.kr/admin/board/dev/board/download.jsp?id=engbo_105&idx=49&aidx=603 [Erişim tarihi: 27 Şubat 2012].
M. K. Kwon, "The Heart of Korean e-Gov.", NCIA Daejeon Merkezinde yapılan sunum, 8 Şubat 2012.

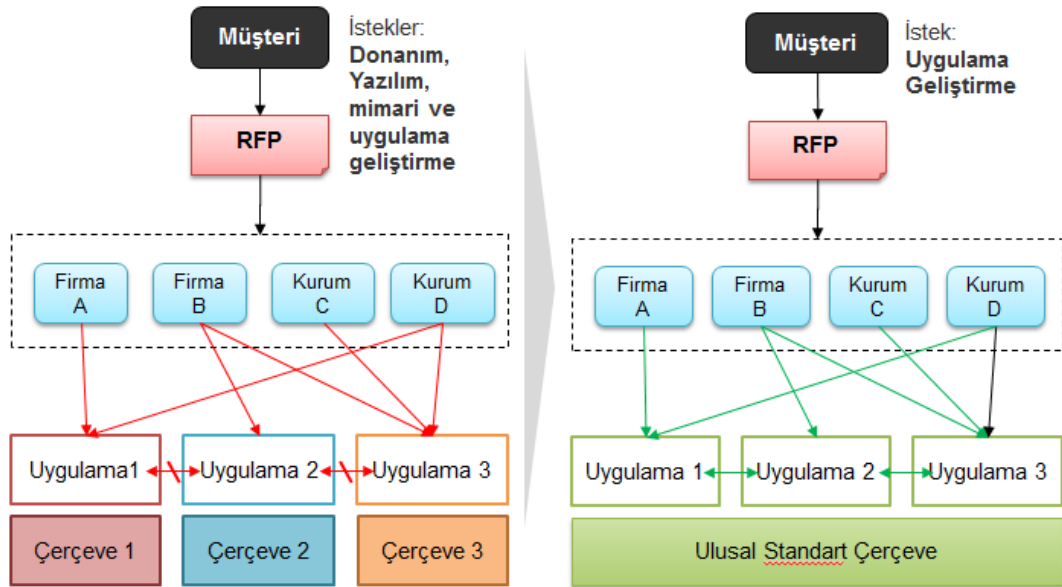


Şekil 26 Güney Kore e-Devlet Standart Çerçeve Yaklaşımı

İşte bu tablodan yola çıkan Güney Kore, her e-Devlet projesinde tekrar eden kütüphanelerin ortaklaştırıldığı bir “e-Devlet Standart Çerçevesi” oluşturmuş ve kamu ile özel sektörün yazılım geliştirme sürecine bunu sunmuştur. Bu çerçeve ayrıca beklenen minimum standartların otomatik olarak desteklenmesi, tüm kurumlar tarafından uyulması zorunlu mevzuatın uygulanması, güncel teknolojilerin hızlı adaptasyonu gibi imkanları otomatik olarak destekleyen ve bu konularda yazılım geliştirme süreçlerine hiçbir yük bindirmeyen bir mimariye sahiptir.

< Firma/kurum çerçeveleri ile yazılım geliştirme>

< Standart çerçeve ile yazılım geliştirme>



Şekil 27 Güney Kore e-Devlet Standart Çerçevesi ve Kazanımlar²¹

Başlangıcı 1987’de ulusal veri tabanı oluşturmaya dayanan bu inisiyatif, 2001-2002 yıllarında e-Devlet Altyapısı’nın oluşturulması ve gerekli mevzuatın

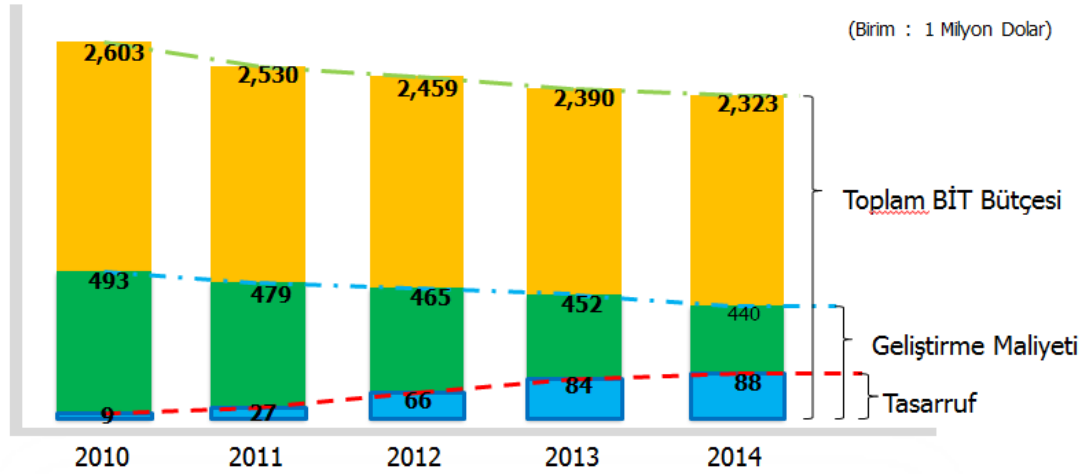
²¹ http://www.egovframe.go.kr/EgovIntro_Eng.jsp?menu=1&submenu=1

düzenlenmesi ile önemli ilerlemeler kaydedilmiştir. E-Devlet projeleri geliştirilirken belirli markaların sektöre baskın olması, her kurum ve firmanın, kendi kütüphanesini müstakilen geliştirmek zorunda kalması ve bunların birbirleri ile haberleşememesi, bu tür kütüphaneleri müstakilen ve mükerrer geliştirmenin yüksek maliyeti, yazılım geliştiricilerin süreçten çok standartlar, uyumlandırmalar, mevzuat, veri alışveriş vb. hususlara önemli zaman harcaması gibi sorunların yaşanması sebebi ile bu çalışma hazırlanmıştır. Çerçeve sayesinde toplam sahip olma maliyeti (TCO) ve yatırımların geri dönüşünde (ROI) önemli kazanımlar olması planlanmıştır.

Güney Kore tarafından oluşturulan bu çerçeve, <http://www.egovframe.go.kr/> adresinden kamu kurumlarına ve özel sektörün kullanımına sunulmaktadır. Bu güne kadarki geliştirmeler ile 270'den fazla ortak bileşen ve fonksiyon bu çerçeve ile kullanıma açılmış, yazılım geliştirmede hem kamu hem de özel sektör için yazılım geliştirme süreçlerinde %30 seviyesinde bir tasarruf olduğu ölçümlenmiştir. 2010 yılında kullanıma açılan bu yapı kapsamında, 2014 itibarı ile bu yapı sayesinde e-Devlet projelerinde toplam 274 milyon dolarlık bir tasarruf gerçekleşmiştir. Ayrıca bu yapıyı kullanan KOBİ'lerdeki kazanım %64 olarak ölçümlenmiştir.



Şekil 28. Standart Çerçeve Kullanım - Kazanımlar



Şekil 29. Standart Çerçeve – Yıllara Göre Mali Tasarruf

e-Devlet standart çerçevesinin en önemli kazanımlarından birisi de, yazılımların çalıştığı donanım altyapısından bağımsız ve oradaki değişimlere tam uyumlu bir ara katman sunmasıdır. Böylece, UVM'nin ilerleyen aşamalarında gündeme gelecek altyapı standardizasyonu sürecine, kamu kurumları tarafından hiçbir yazılım güncelleme yükü getirmeden otomatik uyumu sağlamaktadır. Ayrıca yazılımların standartlaşmış bir şekilde yönetim ve takibini de sağlaması açısından UVM ile bütünlük ortak hedeflere hizmet etmektedir. Bu sebeple çerçeve çalışması, UVM'ye ilişkin ulusal yol haritasının geleceğinde önemli bir yer teşkil etmektedir.

4.2.2. Amerika Birleşik Devletleri

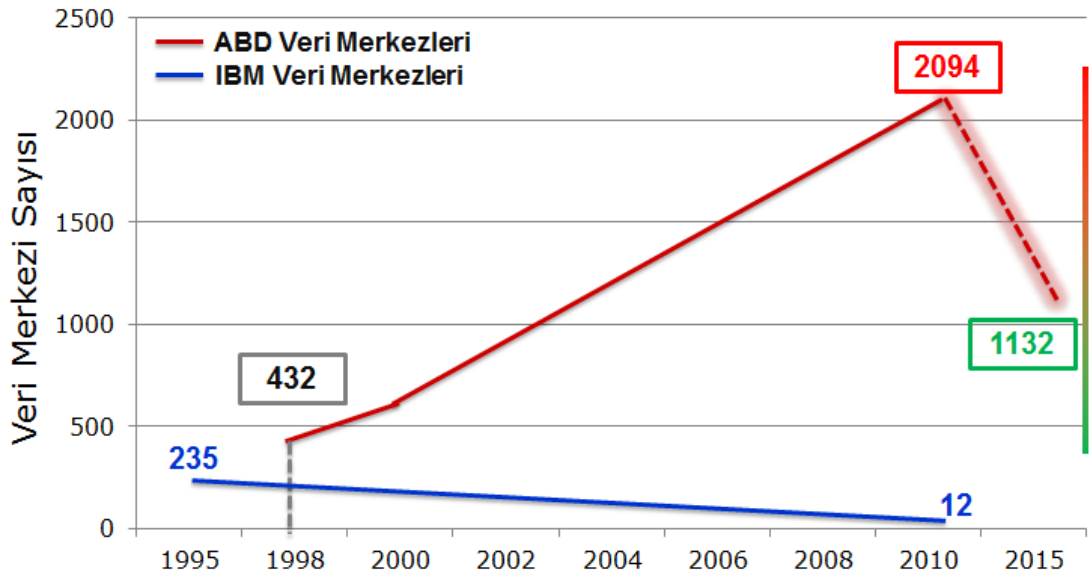
ABD'de yürütülen çalışmalar merkezi bir kurumdan ziyade yerel federal kurumun kendi içerisinde bir bütünlük sağlaması ve Federal CIO tarafından ortaya konan iyi uygulamaları takip etmesi prensibine dayanmaktadır. Gerçekleştirilen çalışmalarda oluşturulan görev gücü (Task Force) kılavuzlar ve stratejiler belirlemek yönünde kurumlara katkı sağlamaktadır. Kurumlar özel sektör tercihlerine göre konsolidasyon çalışmalarını operasyonel düzeyde yürütmektedirler.

ABD'de planlamanın iyi olması ile birlikte hacmin büyüklüğünden ve kurumlarda oluşan dirençten dolayı takvimde gecikmeler olduğu görülmektedir. İlk yapılan çalışmalarda federal hükümete bağlı 2094 veri merkezi olduğu değerlendirilmiştir. Ancak 1 yıl sonrasında sayı 3133 olarak güncellenmiştir. Kamu Muhasebeleri Ofisi tarafından yakın zamanda bu sayı 6836 olarak düzeltilmiştir.

Savunma Departmanının da eklenmesiyle 7000 civarında olduğu ifade edilmektedir.²²

Bütçe ve Yönetim Ofisi ve Federal CIO tarafından 2010 yılında başlatılan Federal Veri Merkezi Konsolidasyonu İnisiyatifi doğrultusunda, bulut bilişim ve ortak veri merkezi yaklaşımlarıyla 2015 yılına kadar 1130'dan fazla veri merkezini kapatmayı planlamıştır. Bu kapsamda 2015 yılı sonunda 3 Milyar ABD Doları tasarruf edilmesi öngörülmektedir. Şubat 2014 itibarı ile, 640 veri merkezi konsolide edilerek kapatılmış, 30.09.2014 tarihine kadar aynı yöntem ile 471 veri merkezinin kapatılması planlanmıştır²³.

Süreçteki gelişmelerin izlenmesine yönelik olarak; açık veri ve şeffaflık çalışmaları kapsamında oluşturulan data.gov internet sitesi altında oluşturulmuş bir sayfadan konsolidasyon çalışmalarının takip edilmesi mümkün olmaktadır.²⁴



Şekil 30. ABD Kamu Kurumları'nda ve IBM'de 15 yıllık Veri Merkezi Konsolidasyon Süreçleri

²² <http://oversight.house.gov/wp-content/uploads/2013/07/Powner-Final.pdf>

²³ <http://www.whitehouse.gov/blog/2011/07/20/shutting-down-duplicative-data-centers>

²⁴ <https://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37>

ABD'de yürütülen çalışmaların sayısı azaltmakla birlikte 3 milyar ABD Dolarlık tasarruf hedefini tutturma ve bunu ölçümleme konusunda zayıf olduğu gözlemlenmiştir.²⁵

4.2.3. Malezya

4.2.3.1 MAMPU Hakkında Kurumsal Bilgiler

Malezya Kamuya özel ağ altyapısına geçiş yapan ilk ülkelerin başında gelmektedir.

Malezya'da başkent olarak iki şehir söz konusudur. Birincisi resmi başkent Kuala Lumpur, ikincisi ise başkentteki yoğunluktan dolayı devlet birimlerinin taşındığı idari başkent Putrajaya'dır.

Başbakanlığa bağlı bir birim olan MAMPU (Malaysian Administrative Modernisation and Management Planning Unit) genel olarak veri merkezleri ile diğer altyapı ve e-dönüşüm çalışmalarını koordine etmektedir. Verilecek her bir hizmeti satış kalemi gibi ayırmış durumdadır. Kurum geçiş için hizmet başvurusu yapmakta ve profesyonel destek olarak süreç başlatılmaktadır²⁶.

Kurumları bu veri merkezine taşıma konusunda katı bir politikadan ziyade özel bir veri merkezi gibi hizmet sunarak, opsiyonel olarak hizmetler de sunabilmektedir.

Kurumlar katı bir emirle veya kanunla, ulusal veri merkezine geçişe zorlanmamaktadır. Ancak amaç olarak kamunun tümleşik bir ağ içine toplanması hedeflendiğinden, kurumlar eskiyen yapılarının yeni yatırımlarını bu merkezde ayağa kaldıracak şekilde yapılandırmaktadırlar.

4.2.3.2 Mevcut Entegre Kamu Merkezi Hakkında Bilgiler

KamuNet Putraya'da kurulmuş bir kampüs ağı olarak tasarlanmıştır. İlk başlarda adı ElectronicGovernmentNet iken, zamanla bant genişliği artırımı ve kurumlar arası iletişimle beraber veri merkezinin de kurulumu ile ismi 1GovNet adını almıştır.

²⁵ <http://www.forbes.com/sites/oracle/2013/08/13/the-surprising-truth-about-federal-data-center-consolidation/>

²⁶ <http://www.mampu.gov.my/web/en/mampu>

1GovNet tek bir tümleşik ağ içine kamu BİT ağlarını dönüştürmeyi amaçlayan bir hükümet girişimidir. Amacı, devlet hizmet sunumunun etkinliğini ve kalitesini artırmak için konsolidasyon yoluyla kaynaklarını optimize etmektir.

1GovNet devlet kurumları için yüksek kapasiteli bant bağlantısının sağlanması ile geçerli EGNNet hizmetinin yeni adı olmuştur.

1GovNet MAMPU tarafından merkezi olarak yönetilen, güvenilir ve güvenli Hükümet Entegre Telekomünikasyon Ağı (GITN) 'dir. Bu veri, ses ve video iletişim hizmetleri (birleşik iletişim) sağlar.

Malezya'da Kamu Entegre Veri Merkezi çalışmaları ulusal stratejiye dayanmaktadır. Vizyon 2020 Master Plan çerçevesinde yürütülen alt stratejik girişimlerden biri Ulusal Anahtar Ekonomik Alanlar (National Key Economic Area) strateji ve eylem planıdır. Bu kapsamda 2010 yılında tanımlanmış olan e-Devlet çalışmaları neticesinde 2020 yılına kadar devlet tarafından verilen tüm hizmetlerin %90 seviyesinde internet üzerinden yürütülmesi hedeflenmiştir. Bu üst hedefler doğrultusunda belirlenen öncül projelerden (Entry Point Project) bir tanesi de kamu için ortak hizmetler merkezinin kurulmasıdır.

BİT envanterinin çıkarılması da bu başlık altında başlatılan çalışmalardan bir tanesi olmuştur. Gerçekleştirilen çalışmalar neticesinde 2011 yılı itibarıyla;

- Kurumların %22'sinde veri merkezi olduğu (toplam 393 adet),
- %4'ünde felaket kurtarma merkezi olduğu,
- 19 kurumun birden fazla veri merkezine sahip olduğu,
- kurumların %87'sinin 2Mbps'nin altında bant genişliği olduğu
- veri merkezlerinin %11'inde tier seviyelerinin olduğu tespit edilmiştir.

Malezya'da entegre veri merkezi konsepti 2011 yılı sonrasında hayata geçmeye başlamıştır. Yıllara göre planlama yapılmıştır:

- 2011 yılı içerisinde envanter çalışması yapılarak mevcut durum anlaşılmıştır.
- Aynı yıl içerisinde kritik olmayan ortak servisler için entegrasyon çalışmaları başlatılmıştır.

- 2012 yılı IaaS, PaaS ve SaaS olmak üzere kamu bulut hizmetleri verilmeye başlanmıştır. Bu kapsamda 1GovUC (birleştirilmiş kamu iletişim altyapısı) hizmeti verilmeye başlanılmıştır.
- Aynı yıl içerisinde IaaS olarak kamu belge yönetim sistemleri için altyapı sağlanmaya başlanılmıştır.
- 2013 ve 2014 yıllarında kamu bulutu servis kataloğunun genişletilmesi hedeflenmektedir.
- 2015 yılında kamu bulutu hizmetlerine tam geçiş hedeflenmektedir.

Malezya'da kamu entegre veri merkezi 1GovCloud çerçevesi altında bir unsur olarak değerlendirilerek çalışmalar şekillendirilmiştir. Bu kapsamda 2 farklı entegre veri merkezi hizmet vermektedir. Putrajaya'da hizmet veren GIDC-1, 20 kamu kurumuna IaaS kapsamında altyapı ve ev sahipliği hizmetini vermektedir. PaaS olarak MyGovXchange platformu ile 28 kurumun ödeme hizmetlerini entegre etmiştir. MyGovernment Portal platformu ile 60 kurum web hizmetlerine platform sağlamaktadır.

i-CITY Shah Alam ve Petaling Jaya'da kurulu veri merkezi ve felaket kurtarma merkezleri ile GIDC-1'e felaket kurtarma desteği sağlamaktadır. Tier-3 standardını sağlamaktadır.

Kamu Sektörü Veri Merkezi tarafından sağlanan hizmetler şu şekilde sıralanabilir:²⁷

1. **Fiziksel ve Sanal Sunucu Barındırma:** sunucular, güvenlik ekipmanları, ağ entegrasyonu ve iletişimi için sunucu barındırma hizmetlerini yönetmekte ve alan sağlamaktadır.
2. **E-posta Barındırma:** MAMPU Ortak Posta hizmetlerinden yararlanmak suretiyle e-posta hizmetlerini sağlamakta, işletmekte ve izlemektedir.
3. **Ağ Geçidi VirusWall:** Ağ Geçidi VirusWall hizmetlerini işletmekte ve izlemektedir.
4. **Groupware VirusWall:** Groupware VirusWall hizmetlerini işletmekte ve izlemektedir.

²⁷ <http://www.mampu.gov.my/web/en/data-centre>

5. **Putrajaya Kampüs Ağı (PCN) için Internet erişimi:** PCN'nin içerisindeki kurumlar için internet erişim hizmetlerini yönetmekte, izlemekte ve güvenliğini sağlamaktadır
6. **Destek hizmetleri:** veri merkezi altyapısı ile ilgili destek ekipmanlarını operasyonel olarak yönetmekte ve izlemektedir.

4.2.4. Estonya²⁸

Estonya küçük bir Baltık ülkesi olması sebebiyle yaygınlaştırma çalışmaları daha kolay olmakla birlikte planlı bir yaklaşım sonucunda e-Devlet çözümleri açısından örnek gösterilen ülkeler arasında girmeyi başarmıştır.

Estonya özellikle 2007 yılında yaşanan yoğun siber saldırılar sonrasında, eDevlet alanında önemli güvenlik yatırımları yapmış ve hem siber hem de fiziki güvenlik açısından güçlendirici önlemler almıştır.

Ulusal ölçekli çalışmalar Estonya Bilgi Sistemleri Kurulu (RIA) tarafından yürütülmektedir.

Sunulan Hizmetler

Veri sahibi kurumun talebi üzerine RIA ihtiyaç ve önceliğe göre farklı lokasyonda veri yedeklemesi yapmaktadır.

Sunucu ve diğer ekipmanlar için farklı lokasyonda fiziki mekan sağlamaktadır. Belirlenen standartları sağlama konusunda önemli çaba sarf etmektedir.

Başlangıç fazında olan hizmetlere koordinasyon ihtiyacını en aza indirmek ve başlangıç risklerini azaltmak için depolama ve işlem gücü tahsis edebilmektedir.

Destekleyici Altyapılar

Kamu Ağı

Estonya'da PeaTee isimli kamu ağı mevcuttur. Bu ağ üzerinden merkezi ve yerel kamu kurumları arası iletişim sağlanmaktadır.

Güvenlik hizmetleri amaçlı olarak 1993 yılında oluşturulmuş ASONet omurgası üzerine inşa edilmiştir.

²⁸ <https://www.ria.ee/about-it-infrastructure/>

Omurga ağ RIA tarafından işletilmektedir ve tüm masraflar merkezi hükümet tarafından karşılanmaktadır. Ağa dahil olmak isteyen kurumlar omurga ağı erişim yöntemini belirlerler. Kurumlar sadece bu erişim için gerekli ücreti ödemek durumundadırlar.

Veri Takas Katmanı X-Road

Kamu bilgi sistemleri arasında internet tabanlı olarak veri takas yapılmasını sağlamak üzere teknik ve organizasyonel çevre oluşturulmuştur. 2001 yılından bu yana faal olan sistem “Kamusal Bilgi Kanunu” ile düzenlenmiştir. Buna göre tüm kamu kurumları bu sistem üzerinden veri paylaşımlarını gerçekleştirmektedir. Özel sektör ve diğer kuruluşlar da bilgi sistemlerini bu sisteme dahil ederek e-Hizmet sunabilmektedirler.

Bilgi Sistemleri Kataloğu²⁹

RIA tarafından sunulan bir hizmettir. Bu kapsamda aşağıdaki bilgiler sunulmaktadır:

- Veri tabanları ve bilgi sistemleri,
- Hangi bilgi sisteminde hangi veri toplanmakta ve işlenmekte,
- Sunulan hizmetler nelerdir ve kim tarafından kullanılmakta,
- Bilgi sistemleri ve veri tabanları için yetkili kişi iletişim bilgileri,
- Veri sahipliği ile ilgili yasal dayanaklar,
- Bilgi sistemlerinin birlikte çalışabilmesi için tekrar kullanılabilen bileşenler (XML varlıklar, sınıflandırmalar, ontolojiler),

4.2.5. Hong Kong^{30 31}

Bilişim sektörünün güçlü olduğu Hong Kong’da CIO Ofisi tarafından işletilmekte olan Merkezi Bilgisayar Yerleşkesi (CCC³²) kamunun kritik altyapılarında

²⁹ <https://www.ria.ee/administration-system-of-the-state-information-system/>

³⁰ http://www.ogcio.gov.hk/en/infrastructure/e_government/

³¹ http://www.ogcio.gov.hk/en/infrastructure/e_government/ccc/index.htm

³² Central Computer Centre

iş sürekliliği sağlamaktadır. 3 farklı lokasyonda yer alan veri merkezi mevcuttur. Ev sahipliği hizmeti yanında öncelikli bölümler için felaket kurtarma altyapısı sunmaktadır.

Kritik altyapıları ve kamu ağın yönetimini sağlayan merkez, aynı zamanda yardım masası ile kurumlara destek hizmeti vermektedir. Aşağıdaki altyapılara destek olmaktadır;

- Kamu Omurga Ağı (GNET)
- Merkezi İnternet Kapısı
- Merkezi Siber Devlet Ofisi (Kamu çalışanların erişimi ve hizmet almaları için intranet portalidir)
- Kamu İletişim Ağı (GCN) (kamu çalışanları arasında haberleşme, e-posta altyapısı sunmaktadır)
- Birçok e-Hizmet için altyapı sunulmaktadır.

5 ULUSAL VERİ MERKEZİ AŞAMALARI VE KAMUDA GELECEK ÖNGÖRÜLERİ

Veri Merkezlerinin gelişimi ve mevcut eğilimlere bakıldığında, yönetilebilirlik, süreklilik, maliyet ve güvenlik kapsamında sağladığı dezavantajlardan ötürü kamu kurumların kendi veri merkezlerini işletmeleri etkin ve verimli bir yöntem değildir. Bu kapsamda belirlenen kamu kurumlarının veri merkezlerinin konsolidasyonu, diğer bir adıyla ulusal veri merkezi artık açık bir ihtiyaç olarak kendini göstermektedir.

Gerek uluslararası başarılı ülke örnekleri, gerekse özel sektördeki büyük veri merkezi örnekleri incelendiğinde, bu tarz büyük veri merkezi konsolidasyonu çalışmasının tek seferde gerçekleştirilemeyeceği, kademeli olarak hayata geçirilecek, 10 yılı bulabilen uzun olgunlaşma süreçleri sonucu tamamlandığı görülmektedir.

Bu bölümde, yapılan mevcut durum incelemelerindeki tespitler göz önünde bulundurularak, oluşturulan UVM geçiş önerileri yer almaktadır. Bu öneriler tüm süreci tariflemeyip, genel kurgu hakkında bir ön rehber niteliğinde hazırlanmıştır. Burada belirtilen her bir aşamanın müstakil fizibiliteye ihtiyaç olduğu aşikar olduğu okuyucu tarafından göz önünde bulundurulmalıdır.

5.1. Ulusal Veri Merkezi: Kamuyu Ne Bekliyor?

Tam entegre bir UVM ile beklenen kazanımlar kısaca şu şekilde özetlenebilir.

- Yeşil BT ile çevresel tasarruflar
- Altyapı konsolidasyonundan kaynaklı tasarruflar
 - o Enerji, soğutma, yangın koruma, fiziki güvenlik, ekipman,
 - o İnsan kaynağı ile işletme maliyeti tasarrufları
- Bulut Bilişim ile kaynak etkinliği ve verimliliği
- Sanallaştırma ile kaynak etkinliği ve verimliliği
 - o Lisans,
- Toplu alımlardan kaynaklı satın alma verimliliği
- Standartlaşmadan kaynaklı kazanımlar
- Güvenlik kazanımları
 - o Siber Güvenlik
 - o Fiziki Güvenlik
 - o Uygulama Güvenliği
- Yüksek erişilebilirlik kazanımları
- FKM yatırımlarının (bir anlamda) kalkmasından kaynaklı kazanımlar
- Hizmet kalitesi sebebi ile artan güven ve itibar kazanımları
- Kamu bulutu ve veri alışverişi için en etkin ortamın oluşmasından kaynaklı tasarruflar
- Ortak platform olmasından kaynaklı kazanımlar
 - o Yeni teknolojilerin hızlı ve bütüncül adaptasyonu
 - o Regülasyonlara uygunlukta kolay adaptasyon
- E-Devlet Standart çerçevesinin³³ uygulanmasından kaynaklı kazanımlar
- Ulusal Gösterge ve Karar Destek Sistemleri'ni oluşturabilmenin getireceği kazanımlar

³³ Kore e-Devlet Standart Çerçevesi (eGov Standard Framework)
http://www.egovframe.go.kr/EgovIntro_Eng.jsp?menu=1&submenu=1

Bu kazanımlara en üst seviyede sahip olmak, orantısal olarak en radikal ve büyük değişiklikleri yapmayı gerektirecektir. Bu değişiklikler sadece teknik platformdaki yenilikçi yaklaşımlardan ve gelişen trendlerin dikkate alınmasından ibaret değildir. UVM işletilmesine ve veri güvenliğine ilişkin idari yapılanmaları, UVM geçişine engel teşkil eden mevzuatın yeniden düzenlenmesi ve UVM işletilmesine ilişkin mevzuat hazırlanması gibi birçok hususun, bu ekosistemin unsurları olarak ele alınması gerekecektir. Ayrıca bu sürecin benimsenerek kurumlar tarafından sahiplenilmesi başarının ilk temel şartıdır. Bu sebeple teknik, idari ve hukuki açıdan belirli olgunluk seviyelerini sağlamak, bu geçişin başarısı için çok önemlidir.

İşte bu sebeple, UVM'ye geçecek ülkenin kamu işleyiş kültürü, konsolidasyon ve veri merkezlerine yönelik mevzuatın olgunluk düzeyi, konuya ilişkin farkındalık ve benimsenme düzeyi gibi kriterler, UVM'ye geçişin hangi aşamalarda ve hangi adımlarla olacağını belirlemesi açısından, önemlidir.

5.2. Ön Hazırlıklar

Ulusal Veri Merkezine kademeli geçiş planlanırken, gerek UVM'ye taşınacak olan kamu kurumlarının, gerekse UVM'nin kurulması ve yönetiminden sorumlu olacak olan kurumun yapması gereken bazı ön hazırlıklar bulunmaktadır. Bu bölümde, bu ön hazırlıklara yönelik bazı önerilere ve dikkate alınması faydalı olacak hususlara yer verilmiştir.

5.3. Kamu Kurumlarının Ön Hazırlıkları

UVM'ye geçiş öncesi, burada veri merkezlerini barındıracak olan kurum ve kuruluşların da bazı ön hazırlıklar yapması elzemdir. Bu hususlar genel bir analiz çalışması gerektirmekle birlikte, fikir vermesi açısından ilk aşamada genel olarak sayılabilecek temel başlıklar aşağıda listelenmiştir:

- Öncelikle, kurumun mevcut veri merkezinde hangi hizmet ve servislerin verilmekte olduğuna dair bir envantere ihtiyaç vardır.
- Hazırlanan envanter çerçevesinde hangi hizmet ve servislerin UVM'ye aktarılacağına karar verilmelidir. Tüm hizmetlerin aktarımı, kurum içi ERP, CRM vb. uygulamaların muaf tutulması veya kurumun tamamen UVM geçişinden muafiyeti gibi hususlar, kurumun görev alanı, etkinlik, verimlilik veya ulusal stratejiler açısından ele alınmalıdır.

- Geçiş konu olacak alan belirlendiğinde, bu alandaki donanım, yazılım ve iletişim altyapısına ilişkin envanter hazırlanmalıdır.
- Geçiş konu olacak alanlara ilişkin kurum mevzuatında geçiş engel teşkil eden hususlar mevcut ise, buna ilişkin mevzuat düzenlemesi yapılmalıdır.
- Bilgi güvenliği çerçevesinde, kurumun verdiği hizmet çerçevesinde ihtiyaç duyulacak fiziki güvenlik seviyeleri (tamper-proof fiziki elektromanyetik izolasyon ortamı, buna uygun kablolama altyapısı, bakım ve işletme süreçlerinde buna ilişkin kural ve yönergeler vb.) var ise, bunlar belirlenmeli ve UVM'ye bildirilmelidir. Aynı şekilde geçiş sürecinde uygulanacak güvenlik kuralları da hazırlanmalıdır.
- Raporda belirtilen ülke örneklerinde, UVM'nin en az 2 lokasyonda ve aktif olarak hizmet vermekte olduğu dikkati çekmektedir. Genel olarak bir şehirdeki UVM, diğerine istinaden bir anlamda FKM görevinde olduğundan, aktif-aktif (her iki lokasyondaki hizmetlerin de canlı olarak hizmet verdiği) modellerin ön plana çıktığı görülmüştür. Bu durumda, çıkartılan yazılım envanteri göz önüne alınarak, her bir yazılımın bu tür bir çalışma şekline uyumu, eğer uyumlu değil ise, uyumlandırma çözümleri, geçiş aşamasından önce sağlanmalıdır.
- UVM'ye geçiş sürecinde, verilen hizmetlerin kesintiye ne kadar tahammülü olduğu, geçiş süreci dikkate alınarak değerlendirilmeli ve kabul edilen maksimum hizmet kesintisi göz önüne alınarak gerekli tedbirler alınmalı, geçiş modelleri buna göre kurgulanmalıdır.

5.4. UVM Sorumlularının Görevleri

UVM kurgusunda, “4.1.1 EMC Veri Merkezlerinde Değişim” bölümünde ele alınan süreklilik modelinde olduğu gibi 4 merkezli veya G.Kore için kurgulanan ve “4.2.1.1 Ulusal Bilişim ve Bilgi Ajansı (NCIA) Hakkında Kurumsal Bilgiler” bölümünde tariflenen 3 bölgesi süreklilik yaklaşımına benzer süreklilik modelleri yer almalıdır.

Farklı ülke örneklerinde de görüldüğü üzere, bir ülkedeki kurumların tamamını UVM kapsamına almak yerine, kurumun görev alanı ve stratejik yaklaşımlar çerçevesinde, hangi kurumların UVM kapsamında yer alacağını belirlenmesi de, UVM kurgusu içerisinde ele alınması gereken bir diğer husustur.

5.5. Aşamalı Geçiş Süreci Önerileri

Önceki bölümlerde, UVM kurmuş olan başarılı ülkelerin deneyimleri incelenmiş ve geçiş evresinin belli adımlar neticesinde tamamlanmasına ilişkin bir çerçeve oluşturulmasının faydalı bulunduğu gözlenmiştir. Bu örneklerde de dikkati çektiği gibi, ilk etapta sadece fiziki olarak ortak alanı kullanan ortak altyapı tasarruflarını başlangıç hedefi olarak görmek daha gerçekleştirilebilir bir yaklaşımdır. Bu durumda, sanallaştırmadan ve ortak donanım kullanımından kaynaklı tasarrufları daha ileride gündeme almak UVM'ye geçişte ilk aşamada gerekli olan idari ve hukuki gereksinimleri azaltacaktır.

Elbette bu tarz kademeli geçişte, sanallaştırma, ortak donanım kullanımı gibi teknolojilerin sağlayacağı kazanımlardan bir süreliğine feragat edilmektedir. Ancak bu teknolojilere doğrudan geçişte yaşanabilecek olası bir başarısızlığın kamuya maliyeti çok daha fazladır.

Veri merkezi entegrasyonu yaklaşımında, öncelikle UVM tasarım adımlarının netleştirilmesi gerekmektedir. Bu adımlar “Altyapısal” ve “Yönetimsel” başlıkları altında toplanarak Tablo 2’deki şekilde özetlenebilir.

7	Yönetimsel	Uygulama	Tekilleştirmiş Uygulamalar Veri Bütünlüğü
6		Entegrasyon	Kurumlar arası güvenlik, iletişim ve veri paylaşım standartlarının oluşturulması
5		Güvenlik ve Yetkilendirme	Yetkilendirme seviyeleri ve güvenlik yönergeleri
4	Altyapısal	Sanallaştırma	Sanallaştırma
3		Yönlendirme	Kurumlar arası iletişim
2		Bağlantılar	Kurumlar ile iletişim altyapısı, Internet Değişim Noktası (Potansiyel Operatörler vb)

1		Fiziki	Arazi, yükseklik, iklim, boyut, fiziki güvenlik, güvenli hava sahası vb
---	--	--------	---

Tablo 2: Ulusal Veri Merkezi Tasarım Adımları

Bunların öncelikle teknik içerikteki kısmının hayata geçirilmesi için geniş kapsamlı bir çalışma yapılması gerekmektedir. Teknik altyapı açısından dikkat edilmesi gereken konular aşağıdaki şekilde ele alınabilir.

1- Fiziki Katman

- a. Veri Merkezi için seçilecek arazinin boyutu
- b. VM coğrafik lokasyonu
- c. Arazi iklimi (Nem, ortalama sıcaklık, toz, yükseklik)
- d. Arazinin stratejik güvenliği (hava sahası güvenliği, fiziki saldırıya ilişkin tedbirler, ...)
- e. UVM bünyesinde genel güvenlik (Depreme karşı dayanıklılık, yüksek ağırlığa dayanıklı mimari, CCTV, Yangın Koruma altyapısı, akıllı bina sistemi, biyometrik ve kartlı erişim kontrol sistemleri, çift duvar koruma, giriş kısıtlı alanların tanımı, sabit disk imha cihazları vd.)

2- Bağlantılar

- a. IDN (İnternet Değişim noktası) bağlantısı
- b. Kamu Veri Merkezleri arasında uçtan uca bağlantı (LAN)
- c. Diğer kamu kurumlarına olan uçtan uca bağlantılar (VPN)
- d. Operatörlere olan bağlantılar

3- Yönlendirme

- a. Veri Merkezi içerisinde kurumlara göre yapılacak bölmeleme (oda, kabin vs)
- b. Kurumlar arası hızlı veri iletişimi için LAN kurulumu ve güvenliği
- c. WAN çıkış güvenliği (ortak, münferit)

4- Sanallaştırma

- a. Ölçeklendirilebilirlik ve yüksek erişilebilirlik için sanallaştırma
- b. Verimlilik için sanallaştırma
- c. Yönetilebilirlik açısından sanallaştırma

Bu bağlamda Tablo 3 ile geçiş evreleri birinci, ikinci ve üçüncü adım şeklinde sınıflandırılmış ve her evrede kurumlar ve UVM için önerilen görev ve sorumluluklar belirtilmiştir. Her tablo kalemi için ortaya çıkacak teknik, idari ve hukuki ön şartlar, uygulama evresi başında ilgili tarafça (UVM/Kamu Kurumu) tarafından hayta geçirilmelidir.

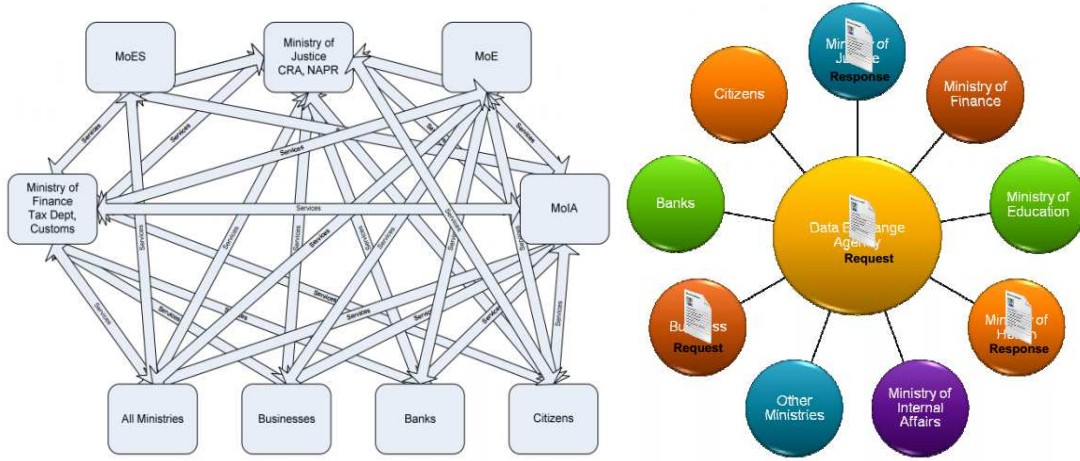
Aşamalar	1.Aşama		2. Aşama		3. Aşama	
Sorumluluklar	Kurum	UVM	Kurum	UVM	Kurum	UVM
Ön Hazırlıklar	✓	✓				
Sunucuların Taşınması	✓					
Fiziksel Güvenliğin Sağlanması		✓		✓		✓
Ortak Servis ve Uygulamalar (Seviye-1) (E-posta, Ofis Uygulamaları vb.)				✓		
Ortak Servis ve Uygulamalar (Seviye-2) (ERP, CRM vb.)						✓
İnternet Erişimi		✓				
Güvenlik (Siber)	✓	✓		✓		
Sistem Yönetimi	✓		✓	✓		
Donanım Temin	✓	✓		✓		✓
Sanallaştırma	✓		✓	✓		
Yüksek Erişilebilirlik				✓ ½		✓
Kayıt (Loglama)	✓			✓		

Aşamalar	1.Aşama		2. Aşama		3. Aşama	
Sorumluluklar	Kurum	UVM	Kurum	UVM	Kurum	UVM
Verimlilik (Utilizasyon)				✓½		✓
Ölçeklendirilebilirlik				✓½		✓
Yetkilendirme						✓
Entegrasyon						✓

Tablo 3: Geçiş Seviyelerine Göre Kurum ve Veri Merkezi Sorumluluk Dağılımı

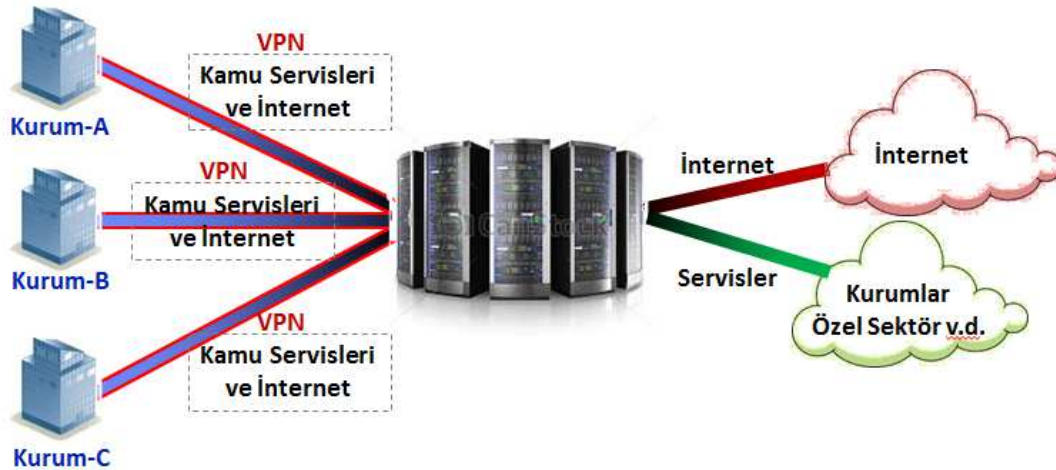
Sistemin omurgası olarak kurumlar ile UVM arasında kurulacak olan iletişim altyapısı için muhtelif senaryolar ele alınabilir. Ülke örnekleri incelendiğinde, farklı uygulamalar olduğu görülmektedir. Kamu kurumlarının birbirleri ile iletişimde bir merkezi kullanmak üzere kurdukları yıldız şeklindeki yapı: Bu yapıda tüm kurumlar merkez ile VPN benzeri güvenlik mekanizmaları ile bağlıdır. Hem kendi aralarındaki veri akışı, hem de özel sektör ve vatandaşlara verilen hizmetler bu merkezi bağlantı üzerinden gerçekleştirilir. (Gürcistan Adalet Bakanlığı yönetimindeki Data Exchange Agency (DEA), Singapur Public Services Broker (PSB) ve benzeri yapılar) [Şekil 31]

Bu model, kurumların aynı hat (merkez) üzerinden internete çıkması [Şekil 32] veya kurumdaki ikincil bir hat üzerinden ayrık internet bağlantısı yapması [Şekil 33] gibi alt alternatifleri de içermektedir. Bu şekilde modellenen altyapı, ayrıca “**Ulusal Kamu Kapalı Ağı**” kavramı olarak bilinen yapının da oluşması anlamına gelmektedir.



Şekil 31 Kamu Kurumları Arası Bağlantı - Gürcistan Örneği (DEA Öncesi ve Sonrasının Temsili Gösterimi)³⁴

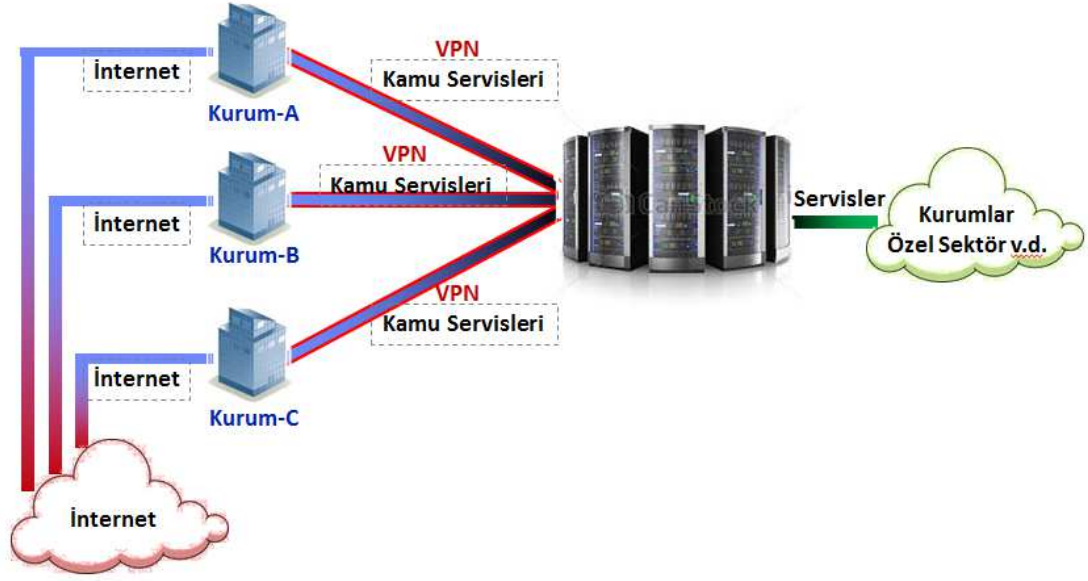
Kurum ile UVM arasındaki bağlantının VPN vb. güvenlik altyapısı içermesi sebebiyle, internetin de aynı bu hatta dahil edilmesi, internet trafiğinin de merkeze kadarki kısmının aynı güvenlik altyapısını kullanması ve buna bağlı olarak yönetim/işletim maliyetini beraberinde getirmekte [Şekil 32], ancak 2 ayrı hattın sürekliliğini ve işletmesini sağlamaktan kaynaklanan maliyet ve zorluğu da ortadan kaldırmaktadır. Bakanlıkların bulunduğu lokasyonlarda fiber altyapısının sıkıntılı olmaması halinde, internet trafiğinin bu yapının dışında tutulması (ikinci alternatif, Şekil 33) tercih edilebilir.



Şekil 32 Kurumlar ve UVM Bağlantı Alternatifleri - 1

³⁴

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/presentations/Regional%20Ws%20on%20Cybercrime_13May10/2215_Data%20Exchange%20Agency%20Georgia_Illomidze.pdf



Şekil 33 Kurumlar ve UVM Bağlantı Alternatifleri - 2

Enerji gereksinimini karşılamak için, UVM modeli kurulur ve projelendirilirken, bu veri merkezinin ihtiyaç duyacağı miktarda enerjiyi (gelecek dönemlerdeki genişleme tahminlerini de içerebilecek şekilde) sağlayabilecek uygun kapasitede yeşil enerji üretim altyapısının da değerlendirilmesi önerilmektedir.

UVM'deki iklimlendirmenin enerji tüketimindeki önemli rolü düşünüldüğünde, UVM için seçilecek coğrafi lokasyonun önemi de daha çok öne çıkmaktadır. Bu açıdan Türkiye incelendiğinde ülkemizdeki iklimin veri merkezleri açısından yeterli düşük sıcaklığı bulamadığı görülmektedir. Yurtdışı örnekler ile kıyaslandığında daha çok ülkemizin kuzey ve/veya yüksek bölgelerinin iklim açısından daha düşük ortalama sıcaklıklara sahip olduğu görülmektedir. UVM'(ler)in lokasyon seçim kriterleri arasında bu hususunda değerlendirilmesinin önemli olduğu düşünülmektedir.

5.5.1. Aşama-1

5.5.1.1 Kazanımlar

Günümüzde tipik TIER3 ve üzeri standartta tasarlanan bir veri merkezinin birim metrekare maliyeti yaklaşık 5.000 Amerikan Doları tutmaktadır. Her bir

kamusal kurumun ve bu kurumlara bağı kamu iktisadi teşebbüsün günümüzde her boyutta veri merkezi bulunmaktadır.

Kurum sunucularının UVM'ye taşınması ile başlayacak süreçte, kurumlar kendi bünyelerinde veri merkezi oluşturmayı terk edecek ve kamunun çok önemli miktarda paraları yeni veri merkezleri yapımı için harcamasının önüne geçilmiş olacaktır.

Veri merkezi kurma maliyetlerinin yanı sıra, işletme ve enerji maliyetleri de önemli ölçüde azalacaktır.

Bir sunucu merkezindeki verimliliği ölçmek için hesaplarımızın içerisine kurulum maliyetleri, işletme maliyetleri ve enerji maliyetlerini katmamız gerekir.

Şu andaki durumda veri merkezlerimizin verimlilik analizini yapmamız ne yazık ki mümkün gözükmemektedir. Veri merkezleri, üzerlerinde barındırdıkları sunucuların sayısından bağımsız olarak verdikleri hizmetlerin, bu hizmetler verilirken yapılan harcamalara oranı doğrultusunda verimlilik hesaplarının yapılması gerekmektedir. Bilimsel çalışma gerektiren bu hesapların yapılabilmesi de ortak veri merkezi sayesinde mümkün olabilecekti. Bilimsel açıdan verimliliği hesaplamamız kolay olmasa da, ilk kurulum maliyeti, personel tasarrufu ve enerji tasarrufu konusunda açık bir tasarrufa gidileceği aşikârdır.

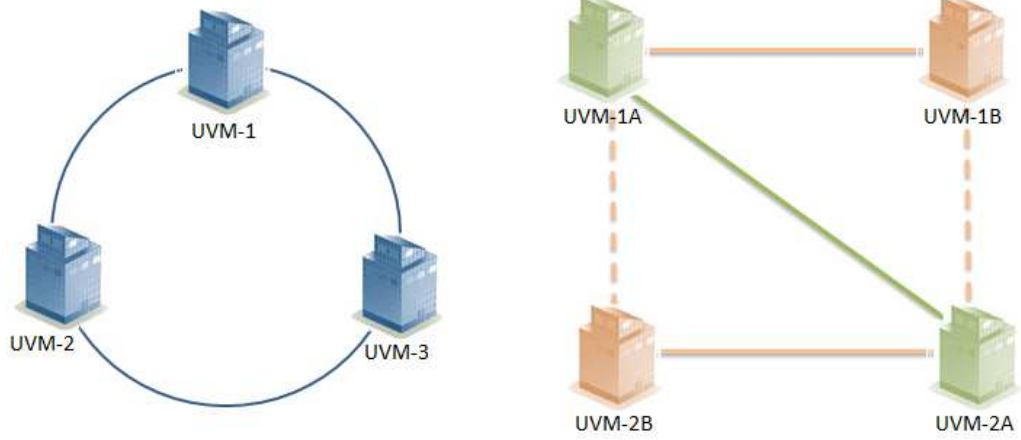
Dağıtık yapıdaki kamusal veri merkezlerinde, her bir veri merkezi bağımsız İnternet erişimi almakta, satın alınan İnternet erişimleri küçük değerlerde olsa bile, maliyetleri yüksek olmaktadır. Tüm dünyada olduğu gibi, Türkiye'de de İnternet hat kapasitesi yükseldikçe birim maliyetler astronomik şekilde düşmektedir. Örneğin günümüzde 50 Mbps kurumsal erişim ortalama 3.500 TL iken, asimetrik Veri Merkezi tarifesinde 1.000 Mbps kapasiteli hattın fiyatı 11.000 TL'dir, yani 20 kat fazla bant genişliği için ödenen miktar yaklaşık 3 kattır. Başka bir deyişle birim maliyet 70 TL'den 11 TL'ye düşmektedir.

İnternet Erişimi için kamu kurumları, kendi bünyesindeki TURKSAT ile erişim sağlayıp, diğer İSS'lerin veri merkezine bağlanmasını da tercihe bırakırsa, özel sektör İSS'leri de bir ücret talep etmeden bağlantı kurmayı gündemlerine alabileceklerdir. Eğer uygun strateji ile yol alınırsa, özel İSS'ler daha önceden bağlantı için ücret talep ederken, kamu ücret talep eder duruma geçebilir. Şöyle ki, kamu içerik sağlayıcıdır, kamunun sağladığı içerik, TTNET ve benzeri İSS'ler için müşterilerine ADSL gibi hizmetleri satabilmelerindeki nedenlerden biridir. Bu İSS'ler zaten son kullanıcılarından ücret talep edip, kamunun ve diğer veri merkezlerinin içeriğini müşterilerine sunmaktadırlar. Şu andaki dağıtık yapıda, İSS'ler hem son

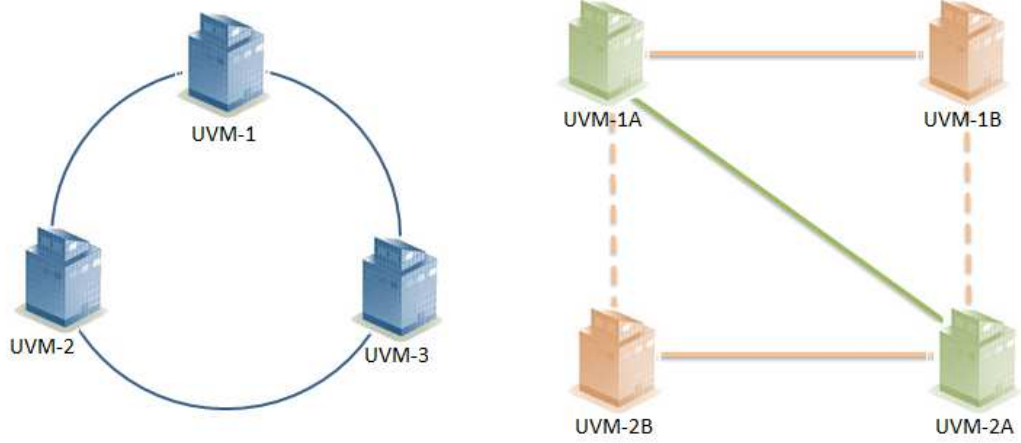
kullanıcılardan hem de kamudan erişim için ücret talep etmektedir. İSS'lere sunulan içerik için kamunun ücret ödemesi kamu yararına olmadığı gibi, büyük kayıplara neden olan bu verimsiz durum UVM oluşumu ile sona erecektir, ancak UVM altyapısı planlanırken, bu UVM'lerin aynı zamanda İnternet Değişim Noktası (IDN) olarak da görev yapması, ülkede İnternetin gelişmesine ve ucuzlamasına muazzam şekilde fayda sağlayacaktır.

5.5.1.2 Riskler

UVM, yapısı itibarıyla stratejik hedef olarak değerlendirilebilecek yapıdır. Bütünlüğü nedeniyle potansiyel sabotajların ve saldırıların hedefi olabilecektir. Bu nedenle UVM tasarlanırken, tasarım birden çok fiziksel lokasyonu içermeli, bu veri merkezleri arasındaki replikasyon anlık değişiklikleri kapsayacak şekilde tasarlanmalıdır. Örnek replikasyon topolojisi



Şekil 34'de temsil edilmiştir. Burada, İnternet ortamından DDoS türü saldırıların da hedefi olabilecek UVM'lerin İnternet erişim kapasitesi, meydana gelebilecek en büyük DDoS saldırı kapasitesinden en az iki kat büyük olmalıdır.



Şekil 34. Örnek Replikasyon Topolojileri (G.Kore ve Özel Sektör Uygulamaları)

5.5.2. Aşama -2

5.5.2.1 Kazanımlar

Sistem Yönetiminin tek elden yapılması, uzman kadroların oluşmasına, personel tasarrufuna ve arızalara müdahalede deneyimden dolayı daha hızlı çözümlerin sağlanmasına olanak verecektir.

Aynı şekilde Donanım temini UVM tarafından yapıldığında, rekabetçi fiyatlar oluşacaktır, yedek parça stoku tutmak kolaylaşacaktır. Ürün çeşitliliği nispeten azalacağından, donanıma hâkim teknik personel yetişmesi kolaylaşacak, konusunda uzman teknik birimlerin oluşmasına katkı sağlayacaktır.

Sanallaştırmanın UVM tarafından yapılmaya başlanması ile kritik önemdeki verilerin yüksek erişilebilirlik ile korunması ve her daim erişilebilir olması sağlanacaktır. Sanallaştırma, Yüksek Erişilebilirlik, yönetim ve ölçeklendirilebilirlik gibi konularda çok büyük kolaylıklar sağlamakla birlikte önemli ölçüde ilk maliyet düşüşü ve enerji tüketiminde azalma gibi faydalar sağlamaktadır.

Kayıt tutmanın UVM tarafından yapılması ile kütük yönetimi kolaylaşacak, mükerrer kütüklerin elimine edilmesi sayesinde depolama kapasitesinde tasarrufa gidilecektir.

5.5.2.2 Riskler

Sanallaştırma ile birlikte, büyük verinin yönetimi sorunu ortaya çıkacaktır. Depolama birimlerinde çıkabilecek arızalarda veri taşıma işlemleri uzun zaman alabilecek, içeriğe erişimde sıkıntılar olabilecektir.

Yüksek erişilebilirlik ve ölçeklendirme uzmanlık gerektiren konulardır, yüksek maliyetli teknik personelin istihdamı gerekmektedir.

Verimlilik, ancak çok iyi tasarlanmış standartlar, yönergeler ve yönetmeliklerle sağlanabilir, sadece sanallaştırma yapmak yeterli değildir. UVM içerisindeki sunucuların tek tek takip edilmesi, işlemci yoğunluğu düşük olan sistemlerin raporlanması gerekmektedir. Bu tarz bir çalışmanın hayata geçirilmesi belirli bir olgunluk süreci gerektirecektir.

5.5.3. Aşama -3

Yetkilendirme, entegrasyon ve UVM Portalı gibi başlıklar üçüncü evrenin konularıdır. Tamamen hukuki çerçevede tamamlanacak olan bu konular tüm kurumların ortak mutabakatı altında tasarlanması gereken ve konseptleri dahi temel yasalarda değişiklik gerektirecek ölçüde konulardır.

5.6. Ulusal Veri Merkezinde Güvenlik Kurgusu

Kamunun kritik veri ve cihazlarının barınacağı tüm ortamlar gibi Ulusal Veri Merkezi için de güvenlik, başlı başına ele alınması gereken, yüksek öncelikli ve titizlikle yaklaşılması gereken bir başlıktır. Bu kapsamda yüksek güvenlik önlemlerinde endüstri standartlarını gözetken, güvenli sistem pratikleri ve öğrenilmiş derslerin dikkate alınmasında fayda görülmektedir. Bu bölümde, bir veri merkezi açısından güvenlik alanında alınabilecek önlemler ve dikkat edilmesi gereken bazı hususlara genel hatları ile yer verilmiştir.

5.6.1. Fiziki Güvenlik

Bir veri merkezinin risk yaratabilecek ilk zaafiyeti, fiziki yerleşkesinden kaynaklanabilmektedir. Bu açıdan olası güvenlik açığı teşkil edecek bileşenlere bakıldığında,

- Yerleşke Güvenliği
- Bina İç Güvenliği

- İletişim Hatları Güvenliği
- Enerji Altyapısı
- İklimlendirme Altyapısı

başlıkları sayılabilir.

Fiziki güvenlik için temel gerekliliğe bakıldığında, yedeklilik ve yetkilendirilmiş erişimin en önde gelen kriter olduğu değerlendirilebilir. Bu bölümde, sıralanmış olan bileşenler için önerilen güvenlik önlemlerine yer verilmiştir.

Yerleşke Güvenliği

Veri merkezinin yerleşke güvenliğinin sağlanabilmesi için hem yerleşkenin yerinin seçimi önem teşkil etmekte, hem de tercih edilen yerleşkenin güvenliği ile ilgili dikkat edilmesi gereken bazı hususlar bulunmaktadır. Yerleşke yeri seçilirken, deprem, su basması, heyelan ve sel gibi doğal afetlerin olabileceği yerler tercih edilmemelidir.

Yerleşke güvenliğinin sağlanması için, bina(lar)ın çevresinin her şartta görünebilir olması gerekmektedir. Yerleşkenin kamera ve izleme sistemi ile izlenirken, dış çevrede ağaçlandırma yapılmaması, kamera görüntülerini engelleyecek objelerden uzak durulması gerekmekte, tercihen ısıya duyarlı kameraların kullanımı ile ısı değişikliği algılandığında uyarı sistemlerinin olası tehditleri tespitine ilişkin altyapı sağlanmalıdır.

Bina İç Güvenliği

Binanın güvenliğini sağlayabilmek için, cam ve pencere gibi kontrolsüz giriş noktalarının bulunmaması önemlidir. Bina iç güvenliğini sağlamak için kullanılacak kamera ve izleme sistemleri için ilave bir güvenlik kademesi olarak kameraların kafesler içerisinde, müdahaleye karşı korumalı tutulması önerilmektedir. En az 6 ay süre ile kamera kayıtları güvenli bir alanda tutulmalıdır.

Erişim hatlarına ve diğer yükseltici cihazlara izinsiz erişim olmaması, sunucu odalarının giriş ve çıkışlarının parmak izi, yüz, retina veya iris algılama sistemleri ile denetlenmesi, sunucuların yetkisiz müdahaleye karşı erişim kontrollü çelik kafeslerde barındırılması cihazların fiziki güvenliğini artıracaktır.

Bunların yanı sıra, sunucular isimlendirilirken anlaşılabilir isimler yerine kodlamaların kullanılması önemlidir.

İletişim Hatları Güvenliği

Fiber iletişim hatlarının yüzeyden uzakta ve yüksek güvenli kanallar içerisinde gitmesi gerekecektir. Kullanılan güvenli kanalların, olası deformasyonlar hakkında uyarıda bulunabilecek alt yapılarının bulunması, kontrol noktaları içermeleri ile olası sorunların tespitinin kolaylıkla gerçekleştirilebilmeleri hedeflenmelidir. Bunlara ek olarak, olası sorunlarda en az kesinti ile durumu atlatabilmek için kullanılan her alt yapı türünün (fiber, uydu, kablosuz gibi) en az iki adet olacak şekilde yedekli olarak kurgulanması önem teşkil etmektedir.

Enerji Altyapısı

Enerji alt yapısında yedeklilik, farklı trafolar ve besleme şebekeleri üzerinden temin edilecek şekilde en az iki farklı sağlayıcıdan destek alınarak sağlanabilir. Özellikle yeşil bilişimi desteklemek ve enerji sağlayıcılarına bağımlılığı düşürmek adına kendi enerjisini yenilenebilir enerji kaynaklarının kullanımını üretebilecek bir veri merkezi kurgusu ciddi kazanımlar sağlayacaktır. Bu kapsamda raporun ilk kısımlarında belirtilen envanter çalışmasının, veri merkezi bileşenlerine ait enerji gereksinim bilgilerini de içermesi halinde, fizibilite neticesinde elde edilen genişleme kapasiteleri de dikkate alınarak, yurtdışı örneklerde uygulandığı üzere, UVM enerji gereksinimini üreten ve yeşil enerji odaklı bir enerji santrali / altyapısının ana projeye dahil edilmesi, bu büyüklükteki bir ulusal veri merkezi için de mutlaka tavsiye edilmektedir. Böyle bir enerji üretim modeline ilişkin muhtelif modeller ve teşvikler, 6446 sayılı Elektrik Piyasası Kanunu'nda yer almaktadır.³⁵

Jeneratör altyapısında, en az iki adet ile yedekliliğin sağlanması, sistemi her türlü kesintide 72 saat ayakta tutabilir şekilde ek mazot depolarının bulundurulması da önemli bir husustur. Kesintisiz güç kaynaklarının, ada başına en az iki adet olacak şekilde sağlanmaları önerilmektedir. Kesintisiz güç kaynağının işlevini, motor-rotor bağı ile otomatik olarak yapan yüksek kapasiteli jeneratör sistemlerini yedekli olmak kaydı ile de kullanmak bir başka alternatif çözüm önerisidir.

Enerji altyapısında tam yedeklilik sağlayabilmek için enerji nakil hatlarından jeneratör ve kesintisiz güç kaynağına, buradan enerji panolarına, enerji ölçüm ve yönetim sistemine ve akabinde veri merkezindeki cihazlardaki güç kaynağında

³⁵ Elektrik Piyasası Kanunu, 30.03.2013 tarih 28603 sayılı Resmi Gazete, Erişim Tarihi: 26.09.2014, <http://www.resmigazete.gov.tr/eskiler/2013/03/20130330-14.htm>

kadarki yolun tamamının, kablolama altyapısı da dahil olmak üzere yedekli olması ve kablolama açısından farklı yollardan ilerleyecek şekilde konumlandırılmaları da önem arz etmektedir.

İklimlendirme Altyapısı

Uçtan uca yedekliliği sağlamak için, diğer başlıklardakine benzer şekilde, iklimlendirme için de yedekliliğin oluşturulması önemlidir. Bu kapsamda kullanılacak cihazların en az ikili gruplar halinde tasarlanmaları, verimlilik için “Free Cooling”, “evaporasyon” gibi yeni nesil teknolojilere yatırım yapılması fayda sağlayacaktır. Olası yangın durumlarına karşı sistem oksijen alımını engelleyecek şekilde otomatik havalandırma kesiciler ile yapının desteklenmesi felaket durumlarında koruyucu etken olacaktır.

5.6.2. Siber Güvenlik

5.6.2.1 Ağ Güvenliği

5.6.2.1.1 Veri Alanı Bölümleme ve Otomatik Güvenlik Önlemleri

Veri merkezlerinde her bir kurum bölümünün birbirinden ayrık olduğundan emin olunmalıdır. Bu, uygulanacak senaryoya bağlı olarak fiziken veya VLAN ve benzeri teknikleri ile yapılabilir. Genelde gözden kaçan bir nokta olarak; veri merkezleri içindeki farklı bölümlerin birbirleri arasındaki iletişiminin, veri merkezinin standart güvenlik önlemlerinden daha aşağıda bir güvenlik seviyesinde oluşmasına izin verilmemelidir. Dolayısıyla aynı veri merkezindeki 2 kurumun yan yana duran kabinlerinin dahi kendi aralarında erişimi veri merkezi güvenlik cihazları üzerinden yine kurumların talep ettikleri güvenlik politikaları dahilinde gerçekleşmesi sağlanmalıdır.

Bununla beraber veri merkezi ağı içerisindeki herhangi bir sistemden kaynaklı dışarı doğru anormal ve önemli trafik oluşumlarında, tamamen otomatik olarak, birinci aşamada sistem sahibinden izahat istenmesi, trafiğin diğer sistemleri etkiler hale gelmesi olasılığına karşı da bu dışarı trafik üreten sistemin yalıtılması gerçekleştirilebilmelidir. Veri merkezinin iç sağlığı ve temiz sistemlerden oluşması sağlanmadan kaliteli bir veri merkezi hizmeti ve güvenlik söz edilemez.

Veri merkezinde kurumlara statik bant genişliği limitleri (limitin üzerine çıkamayan) yerine ortalama trafik tabanlı bant genişliği ücretlendirme modelleri kullanılmalıdır. Bu sayede sistemlerin DDoS saldırılarına karşı dirayetini artıracaktır.

5.6.2.1.2 Temel Standart Güvenlik Servisleri

Veri merkezi kullanıcı kurumlarının tamamı için standart olarak bazı güvenlik servisleri verilmelidir. Hizmetlerin tamamının istendiği takdirde kurumlar tarafından bizzat yönetimi imkan dahilinde olmalıdır. Bu şekilde, bir güvenlik SLA anlaşması olmayan kurumlar güvenlik sistemlerine hakim olabilecektir. Bu servislerin bazıları aşağıdaki şekilde özetlenebilir.

- Ağ Güvenlik Duvarı
- DoS/DDoS Yatıştırma
- Saldırı Tespit ve Önleme
- Anlık veri trafiği izleme ve anormallik bildirimi
- L7 protokol detayında iletişim kaydı
- Ağ tabanlı zaman

5.6.2.1.3 Opsiyonel güvenlik servisleri

Veri merkezi kullanıcı kurumları, veri merkezi içerisinden paylaşımlı olarak opsiyonel güvenlik servisleri talep edebilmelidir. Bu konudaki bazı örnek servisler aşağıda verilmiştir.

- Web Uygulama Güvenlik Duvarı
- Veri Sızıntısı Tespiti ve Önleme
- Güvenlik Taraması
- Veri Bütünlüğünün korunması için Zaman Damgası Servisi

5.6.2.1.4 Temel Güvenlik Yönetim ve Test Hizmetleri

Veri merkezleri kendi içerisinde yeterli sayıda veya gerekli deneyimde personel barındıramayan kurumlar için sözleşme ile garanti edilir (SLA) güvenlik yönetim hizmetleri sunmalıdır. Bu sayede kurumlar ağlarındaki servislerin tamamına hâkim deneyimli personeller ile veri merkezi sistemlerinin güvenliğini yönetebilecektir.

Diğer yandan veri merkezindeki kurum sistemlerinin düzenli olarak güvenlik taramalarının yapılması ve ileri servis olarak da açık tespiti amaçlı profesyonel servisler sağlanabilmelidir.

5.6.2.1.5 DDoS Saldırı Önleme Hizmetleri

DoS/DDoS saldırılarına özel olarak olay anında müdahale ve bazı durumlarda saldırının yatıştırılması için profesyonel yatıştırma hizmeti sunulmalıdır. Opsiyonel olacak bu profesyonel hizmet sayesinde, özellikle APT niteliği kazanmış DDoS saldırılarında anında müdahale ile hizmetin tekrar sağlanması mümkün olabilecektir. Tercih edilen senaryoya göre bu özellik, UVM tarafından standart olarak da sağlanabilir.

5.6.2.2 Güvenlik Yönetimi

5.6.2.2.1 Ağ ve Güvenlik Görünürlüğü

Veri merkezi ağındaki tüm trafiğkte, kurumların sistemlerinin güvenlik durumlarının detaylı olarak izlenebilmesi için ağ görünürlük sistemleri işletilmelidir. Bu sistemlerle ağdaki herhangi bir yüksek trafiğin ya da beklenmedik trafiklerin kaynağı görsel olarak tespit edilebilmeli ve otomatik olarak sistem sahibi kurumlar ile iletişime geçilebilmelidir. Bunun yanında ağ içerisindeki trafiğin içerisinde güvenlik zaafiyetlerini istismar etmeye çalışan trafikler ayırt edilebilmeli ve alarm üretilebilmelidir.

5.6.2.2.2 Güvenlik Pratikleri ve Regülasyonlar

Veri merkezleri için konulmuş güvenlik regülasyon ve pratikleri incelenmeli ve veri merkezinin kurulması aşamasında hedef regülasyonlar seçilmelidir. Yine veri merkezi planlanması aşamasında veri merkezinde hedeflenen standartlar (fiziksel ve siber açıdan) saptanmalı, veri merkezi fiziksel ve siber güvenlik standartlarına uygun şekilde tesis edilmeli ve mutlaka ilgili belgeler için denetimler yaptırılarak belgeler alınmalıdır. İncelenmesi önerilen temel regülasyonlar/standartlar aşağıda listelenmiştir.

- ISO 27001: Bilgi Güvenliği Yönetimi
- ISO 27000: IT Servis Yönetimi
- ISO 9001: Kalite Yönetimi
- ISO 22301: İş Süreklilik Yönetimi
- PCI DSS: PCI Veri Güvenliği Standartları

- SOC 1/2/3: Hizmet Organizasyonlarında Raporlama

5.6.2.2.3 Güvenlik Operasyon Merkezi

Ulusal veri merkezinin, kurumlara verdiği güvenlik hizmetleri dışında, veri merkezinin kendisine ait siber güvenlik olaylarının yönetimi görevini üstelenecek, tesis edilmiş sistemler tarafından ve zamanlanmış görevlerle tetiklenen bir güvenlik operasyon merkezi ve güvenlik operasyon ekibi kurulmalıdır. Bu ekip kurumların günlük çağrılarına muhatap olmadan aşağıdaki görevleri en iyi şekilde yerine getirmelidir.

- Veri merkezine ihbar edilen güvenlik olayların analizi ve güvenliğin iyileştirilmesi
- Veri merkezi ağ güvenlik cihazlarından alarmlanan olayların analizi ve güvenliğin iyileştirilmesi
- Veri merkezi düzenli güvenlik denetimleri
- Veri merkezi ile ulusal ve uluslararası BOME (CERT) iletişimlerinin sağlanması

5.6.3. Güvenlik Denetimleri

Veri merkezi güvenlik denetimleri en az dahil olunmuş regülasyonların gerektirdiği ölçüde düzenli olarak gerçekleştirilmelidir.

5.6.4. Devlet Siber Güvenlik Hedefleri ve Regülasyonlar İle Etkileşim

5.6.4.1 Ulusal Siber Güvenlik Stratejisi Eylem Planı

Ulusal Siber Güvenlik Stratejisi Eylem Planları içerisinde belirtmiş olan veri merkezleri ile ilgili başlıklar, veri merkezi sahibi kurum tarafında hassasiyetle uygulanmalıdır. Bunların uygulanması esnasında her bir eylemin sahibi kurum ile iletişimde olunmalı ve eylem planına uygunluk garanti edilmelidir. Ulusal kamu veri merkezlerinde eylem planının bir parçası olarak yerli ürün ve hizmetlerin kullanımı sağlanmalıdır.

5.6.4.2 Stratejik Güvenlik

Günümüz, savaşların siber ortamda gerçekleşmeye başladığı bir dönemdir. Siber ortamda olan çatışmalar konvansiyonel çatışmalara yol açabildiği gibi,

konvansiyonel çatışmalar da siber çatışmalar doğrulanabilmektedir. Veri merkezlerinde barındırılan sistemler e-devlet ve ilişkili projeler kapsamında gün geçtikçe halkın tamamını doğrudan etkiler hale gelmiştir. Vatandaşlar devlet ve kurumları ile olan günlük iletişimlerinde günde birkaç kez bir veri merkezi ilişkili hizmete temas etmektedir. Bu göstermektedir ki, veri merkezlerinde verilen hizmetlerin aksaması ya da veri sızması durumlarında vatandaşlar ve sektör başta olmak üzere tüm paydaşlar bundan etkilenebilecektir. İşte bu ilişki, veri merkezlerindeki siber sistemleri birer psikolojik savaş aracı olarak da cazip hale getirmektedir.

Diğer yandan her yıl birkaç yabancı menşeli üründe bilinçli/bilinçsiz şekilde bırakılmış arka kapılar ve bu üreticilerin bazı devletler ile doğrudan ilişkilerin tespit edilmiş olması da, veri merkezlerinde kullanılacak ürün ve sistemlerin seçiminde önemle değerlendirilmelidir.

Bulut bilişimin yaygınlaşması ile beraber bulut üzerinden hizmetlerin sunumu da gittikçe artmıştır. Veri merkezlerinde kullanılan sistemlerin güvenlik ya da başka bir amacı sağlamak için herhangi bir veriyi kendi bulut sistemlerine iletmediğinden emin olunmalıdır. (Örnek: Bulut merkezli kötücül yazılım analizi, dosyaların başka bir ülkedeki bulut merkezlerinde incelenmesi şeklinde çalışmaktadır.)

5.6.4.3 Veri Merkezleri ve 5651 Sayılı Kanun

Veri merkezleri, kamuoyunda internet yasası olarak da bilinen 5651 sayılı “*İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*” ve ilişkili yönetmelik, tebliğ ve kanun değişikliklerinin tamamına hakim olmalıdır. Tüm kurumların bu kanunlarda yazılmış unsurları hassasiyetle uygulamaları konusunda aktif olarak yönlendirmelidir.

5.6.4.4 Veri mahremiyeti

Veri merkezleri ilişkili kurumlarla ilişkisini ve mevcut olan verilerin muhafaza ve kullanımını, hukuk kuralları içerisinde tesis etmelidir. Veri-bilgi paylaşımını kanunların emrettiği şekilde ve belirlenmiş iç prosedürlerine uygun olarak, tüm emir ve çıktılarını hassasiyetle saklayarak gerçekleştirmelidir.

6. SONUÇ

Kamu kurumlarının veri merkezlerinin etkinlik ve verimlilik açısından ortak fiziki alan(lar)da konsolide edilmesi prensibine dayanan Ulusal Veri Merkezi yaklaşımı, Bilgi Toplumu sürecinde giderek artan ihtiyaçların kamu kurumları tarafından yönetilebilir bir şekilde karşılanabilmesi için günümüzde giderek önem kazanan bir başlıktır.

UVM'nin başlatılması, kurulması ve işletilmesi sürecinde, bu yapıyı sahiplenecek kurumun idari yapılanması ve kurumsal kapasitesi ile bu konudaki hukuki konumu da, başarılı örneklerdeki yaklaşımlara benzerlik göstermelidir.

Bununla birlikte, gerek özel sektör gerekse başarılı ülke örneklerindeki deneyimlere bakıldığında, veri merkezi konsolidasyonunun uzun soluklu bir süreçte kademeli adımlarla nihai hale gelebildiği görülmektedir.

UVM'ye geçerken, kamu işleyiş kültürü, konsolidasyon ve veri merkezlerine yönelik mevzuatın olgunluk düzeyi, konuya ilişkin farkındalık ve benimsenme düzeyi gibi kriterler, geçişin hangi aşamalarda ve hangi adımlarla olacağının belirlenmesi açısından, önemlidir. Geçiş aşamalarında, teknik bir bütüncül yaklaşıma ilaveten, sürecin idari ve hukuki yanları da ele alınmalı, paydaşlar tarafından benimsenen bir çalışma modeli ortaya konulmalıdır.

Belirlenecek çalışma modelinde tüm kurumların UVM'ye geçmesi de bir zorunluluk değildir. Kurumların görev alanı ve stratejik yaklaşımlar çerçevesinde, hangi kurumların UVM kapsamında yer alacağının belirlenmesi de, UVM kurgusu içerisinde ele alınması gereken bir diğer husustur.

Ayrıca, kurulacak yapıda süreklilik modeli başta olmak üzere tüm aşamaları ele alan fizibilite süreci gerçekleştirilmeli, bu çalışmalar mutlaka paydaşlar ile birlikte yürütülmelidir.

UVM, Ülkelerin elektronik ortamda vermekte olduğu hizmetleri daha etkin ve verimli olarak sağlayabilmesi için önemli bir yapıtaşdır. Bu sebeple UVM konusunda ülkemizde atılacak adımlar, hem Bilgi Toplumunda ilerleme sürecine hem de ulusal e-Devlet hedeflerine önemli katkılar sağlayacaktır. Bu hedefe katkı sağlaması amacıyla, bu raporda UVM sürecindeki temel bilgileri, öngörüler ve önerileri içeren bir ön rehberin oluşturulması amaçlanmıştır.

EK A: ANKET ÇALIŞMASINDA UYGULANAN YÖNTEM

Kamu Kurum ve Kuruluşlarında bulunan veri merkezlerinin mevcut durumunun incelenmesi ve belirlenmesi amacıyla Kurumlara sorulacak sorular hazırlanmıştır. Bu kapsamda 21 soruluk bir anket oluşturulmuştur.

Daha sonra 4 kurumun Bilgi İşlem Dairesi Başkanlıklarının veri merkezleri ziyaret edilmesi planlanmıştır. Sırasıyla Adalet Bakanlığı, Sağlık Bakanlığı, SGK ve İçişleri Bakanlığı'nın ilgili yöneticileri ile yapılan görüşmelerde bu anket soruları sözel olarak sorulmuş, cevaplar alınırken ayrıca soruların anlaşılabilirliği ve cevaplayan kişilerin anketin kapsam ve yapısına ilişkin değerlendirmeleri alınmıştır.

Bu görüşmeler sonucunda anket soruları revize edilerek 27 soruluk bir soru seti hazırlanmış ve cevap seçenekleri belirlenmiştir. Ayrıca sorular ve cevaplar anket teknikleri açısından değerlendirilmiştir. Nihai versiyon ayrıca Çalışma Grubu 3-D (Anket Çalışma Grubu)'na iletilerek, anket tekniği açısından değerlendirmeleri alınarak son haline getirilmiştir.

Ankete katılımın artırılması, anket doldurulmasının kolaylaştırılması ve daha hızlı ve hatasız sonuca erişme amaçları ile, anketin ayrıca elektronik ortama da taşınmasına karar verilmiştir. Veri merkezi yöneticilerinin web sayfası üzerinden doldurabilecekleri anket sayfaları "Google Docs" ortamında oluşturulmuştur.

Ankete ilişkin duyuru, Bakanlıklar, ilgili, bağlı ve ilişkili kuruluşlara, resmi yazı ile gönderilerek, çalışmanın amaç ve kapsamında kısaca bahsedilmiş, elektronik ortamdaki anketin doldurulması talep edilmiştir.

Ayrıca resmi yazışmadan kaynaklı evrak sürecinin risklerini minimuma indirebilmek için, 5018 sayılı kanun ekinde faydalanılarak bir kurum listesi oluşturulmuş ve kurumlar ile birebir görüşülerek ilgili birimlerin yetkililerinin iletişim bilgilerine (ad soyad ve e-posta adresi) erişilmiş, elde edilen bu listeye e-posta ile de (ekine resmi yazıyı ilave etmek sureti ile) anket duyurusu gönderilmiştir.

25 Nisan 2014 tarihi itibarı ile 6 kamu kurum ve kuruluşundan elektronik ortamda geri dönüş gelmiş, 4 pilot kurum ile birlikte anket çalışması 10 kurum için değerlendirmeye alınmıştır.

Değerlendirme öncesi her sorunun hangi grafik modeli ile gösteriminin uygun olacağı çalışma grubu tarafından belirlenmiş ve grafik sonuçlar rapor ekine, değerlendirmeler ilgili bölümlere ilave edilmiştir.

EK B: ANKET SORULARI

ULUSAL VERİ MERKEZİ ANKETİ

Bu anket, Türkiye Bilişim Derneği (TBD) Kamu BİB Birinci Çalışma Grubu'nun hazırlanmakta olduğu "**Ulusal Veri Merkezi ve Kamuda Gelecek Öngörülleri**" çalışmasında ihtiyaç duyulmakta olan istatistiki bilgilerin temini amacı ile hazırlanmıştır.

Soruları cevaplarken Kurumunuzun merkez ve taşra teşkilatlarını dahil ederek cevaplayınız. Bağlı, ilgili ve ilişkili Kuruluşları dikkate almayınız.

Kurum Adı :

1. Bu ankette paylaşacağınız bilgilerin TBD KamuBİB ÇG-1 raporunda envanter olarak paylaşılmasını uygun görüyor musunuz?
 - a. Evet
 - b. Hayır, kurum isminin gizlenerek anonimleştirilmesini istiyorum.
2. Kurum bünyesinde kaç adet veri merkezi mevcuttur? :
 - a. 1 adet
 - b. 2 adet
 - c. 3 – 6 arası
 - d. 7 – 10 arası
 - e. 11 – 19 arası
 - f. 20'den fazla
3. Veri merkezlerinden kaç tanesine ait Felaket Kurtarma Merkezi (FKM) mevcuttur ?
 - a. Tamamına
 - b. Çoğuna
 - c. Yarısına
 - d. Bazılarına
 - e. Hiçbirine

4. Veri merkeziniz, aylık ortalama kaç kişiye hizmet vermektedir?
- a. Ortalama 100 kişi
 - b. 101 - 1.000 kişi arası
 - c. 1.001 - 100.000 kişi arası
 - d. 100.001 - 500.000 kişi arası
 - e. 500.000 Kişiden Fazla
5. Veri merkezinizin fiziki alan büyüklüğü (sadece sunucuların bulunduğu alan) kaç metrekaredir?
- a. 0 - 100 metrekare arasında
 - b. 100 - 250 metrekare arasında
 - c. 250 - 500 metre kare arasında
 - d. 500 – 1.000 metrekare arasında
 - e. 1.000 metrekareden büyük

Bu büyüklük sadece ana veri merkezimize ait değerdir.

Bu büyüklük, Bakanlık bünyesindeki tüm veri merkezlerinin toplamına ait yaklaşık değerdir.

6. Veri Merkezinizin TIA standartlarına göre hangi seviyede olduğunu düşünüyorsunuz?
- a. Tier-1: (Tek bir enerji ve soğutma sistemine sahip, yedeklilik mevcut değil. Yıllık maksimum kesinti süresi: 28.8 saat)
 - b. Tier-2: (Enerji ve soğutma altyapısında kısmi yedeklilik var, Yıllık maksimum kesinti süresi: 22 saat)
 - c. Tier-3: (Enerji, soğutma ve diğer donanımlarda yedeklilik var. Yıllık maksimum kesinti süresi: 1.6 saat)
 - d. Tier-4: (Enerji, soğutma, donanım ve hata tolerans sistemlerinde tam yedeklilik. Yıllık maksimum kesinti süresi: 26 dakika)

7. Veri merkezinin enerji alt yapısı, soğutma sistemleri, su basması v.b. ile ilgili izleme sisteminiz var mıdır?

- a. Evet
- b. Hayır

8. Veri Merkez(ler)i bileşenlerinden hangileri yedeklidir?

İklimlendirme / Soğutma Sistemleri

Kablolama

Şebeke (Enerji) Kaynağı

Jeneratör

Kesintisiz Güç Kaynağı (UPS)

Sunucular

Depolama Cihazları

Ağ Cihazları

Güvenlik Cihazları

Diğer:

9. Lütfen Veri Merkezinizin Jeneratör bilgilerini giriniz.

Jeneratör Yedekliliği ve Toplam Jeneratör Kapasitesi		0 - 100 KVA arası	101 - 250 KVA arası	251 - 500 KVA arası	1000 KVA veya daha büyük
<input type="checkbox"/>	Tek jeneratör mevcuttur.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Yedekli jeneratör mevcuttur	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Veri merkezine hizmet veren jeneratör bulunmamaktadır.				

Bu bilgiler sadece ana veri merkezimize ait değerlerdir.

Bu bilgiler, Bakanlık bünyesindeki tüm veri merkezlerinin toplamına ait yaklaşık değerdir.

10. Lütfen Veri Merkez(ler)inizin kesintisiz güç kaynağı (UPS) bilgilerini giriniz.

		0-100 KVA arası	101- 250 KVA arası	251- 500 KVA arası	500 KVA'dan Büyük
<input type="checkbox"/>	Tek UPS mevcuttur.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Yedekli UPS mevcuttur.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Jeneratör ile bütünleşik UPS sistemi mevcuttur.				
<input type="checkbox"/>	Veri merkezine tahsis edilmiş UPS bulunmamaktadır.				

Bu bilgiler sadece ana veri merkezimize ait değerdir.

Bu bilgiler, Bakanlık bünyesindeki tüm veri merkezlerinin toplamına ait yaklaşık değerdir.

11. Veri Merkez(ler)inde aşağıdaki risklere karşı hangi önlemler mevcuttur?

		Algılama Sistemi	Uyarı Alarm Sistemi	Kamera ile İzleme Sistemi
<input type="checkbox"/>	Yangın	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Su Baskını	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Deprem (temel izolasyon sistemi)			
<input type="checkbox"/>	Diğer:			

12. Veri merkez(ler)inin hizmet sürekliliği ve işletilmesine ilişkin özel sektör ile hizmet anlaşmanız mevcut mudur?

- a. Veri merkezindeki hizmetlerin tamamı için hizmet anlaşmamız bulunmaktadır.
- b. Veri merkezindeki hizmetlerin çoğu için hizmet anlaşmamız bulunmaktadır.
- c. Veri merkezindeki hizmetlerin bir kısmı için hizmet anlaşmamız bulunmakta.
- d. Hizmet anlaşmamız yoktur. İhtiyaçlarımızı kendi kaynaklarımız ile karşılıyoruz.

13. Veri merkez(ler)inin hizmet sürekliliği ve işletilmesine ilişkin hangi başlıklarda hizmet almaktasınız?

<input type="checkbox"/>	İklimlendirme / Soğutma Sistemleri
<input type="checkbox"/>	Sunucular
<input type="checkbox"/>	Depolama/Yedekleme Cihazları
<input type="checkbox"/>	İletişim Cihazları
<input type="checkbox"/>	Güvenlik Alt Yapısı
<input type="checkbox"/>	Güvenlik Cihazları
<input type="checkbox"/>	Yazılım
<input type="checkbox"/>	Ağ Cihazları
<input type="checkbox"/>	İşletim Sistemleri
<input type="checkbox"/>	Diğer:

14. Veri merkezinizde Bilgi Güvenliği konusunda Bilgi Güvenliği Yönetim Sistemi (BGYS) veya bu konuda alınmış bir sertifika mevcut mudur ?

		Sertifika Geçerlidir.	Sertifikanın Geçerlilik Tarihi
<input type="checkbox"/>	ISO 27001	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Bilgi Güvenliđi Yönetim sistemi ve buna bađlı kurum içi yönerge / yönetmeliklerimiz mevcuttur.

15. Veri Merkez(ler)ine uygun (FM200 gazlı) yangın söndürme sistemi var mı?

- ☐ Evet
- ☐ Hayır

16. Veri Merkez(ler)inizde (siber saldırı, teknik arıza vb) herhangi sebeple son bir yıl boyunca ortalama kaç kez hizmet kesintisi yaşandı ? Ortalama kesinti süresi nedir?

- a. Hiç kesinti yaşanmadı.
- b. 1-5 defa : Dakika
- c. 6-10 defa : Dakika
- d. 11-20 defa : Dakika
- e. 20'den fazla : Dakika

17. İş Sürekliliđi Yönetim Sisteminiz mevcut mudur?

- a. Evet
- b. Hayır
- c. Yok ancak planlandı
- d. Yok ancak çalışmalarına başlandı

18. Kurumun veri yedekleme stratejisi var mıdır?

- a. Evet
- b. Hayır
- c. Hayır ancak hazırlama çalışmaları mevcut

19. Veri Merkez(ler)inde kurum personeline ve dışarıya hizmet veren portal sayısı nedir?

20. Veri Merkez(ler)i hizmetleri sunulurken karşılaşılan sorunların çözümünde idari açıdan sıkıntı yaşıyor musunuz? Cevabınız Evet ise lütfen temel sebepleri ile birlikte açıklayınız.

- a. Hayır
- b. Evet

21. Veri Merkez(ler)i hizmetleri sunulurken karşılaşılan sorunların çözümünde teknik açıdan sıkıntı yaşıyor musunuz? Cevabınız Evet ise lütfen temel sebepleri ile birlikte açıklayınız.

- c. Hayır
- d. Evet

22. Veri Merkez(ler)i hizmetleri sunulurken karşılaşılan sorunların çözümünde mali açıdan sıkıntı yaşıyor musunuz? Cevabınız Evet ise lütfen temel sebepleri ile birlikte açıklayınız.

a. Hayır

b. Evet

23. Kurumda Veri Merkez(ler)i ile ilgili mevzuat var mıdır?

☐ Evet

☐ Hayır

24. Kurumunuzun 2013 yılı BİM yatırım bütçesi yaklaşık ne kadar idi?
..... TL

25. Mevcut veri merkez(ler)inizin bir başka kamu kurumunun fiziki çatısı altında yer alıp, sistem ve verilerin sorumluluğunun yine şu anda olduğu gibi sizin kontrolünüzde olması gibi bir durum karşınıza çıksa idi, böyle bir çalışma modelini tercih eder miydiniz?

a. Evet

b. Hayır

26. Sizce böyle bir modelin avantajları nelerdir ?

27. Sizce böyle bir modelin dezavantajları nelerdir?

Zaman ayırarak çalışmamıza katkı sağladığınız için çok teşekkür ederiz.

Türkiye Bilişim Derneği

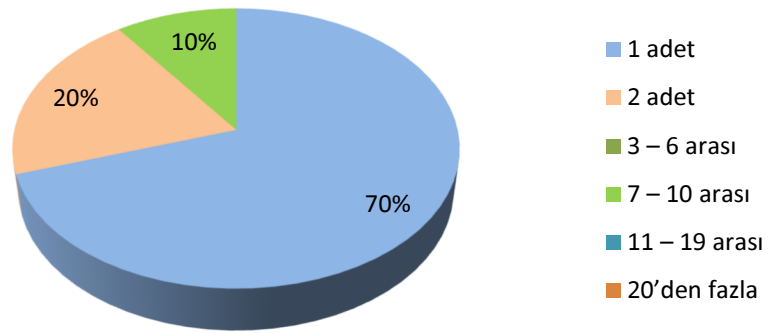
Kamu BİB

“Ulusal Veri Merkezi ve Kamuda Gelecek Öngörüler” Çalışma Grubu

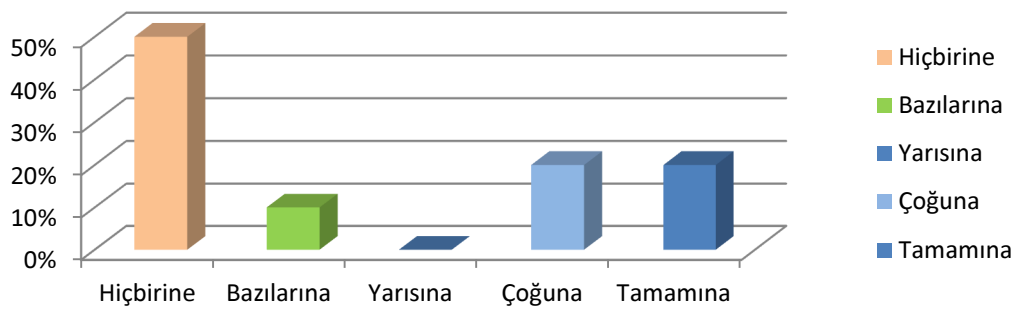
Şubat 2014

EK C: ANKET NİTEL SORU CEVAPLARI

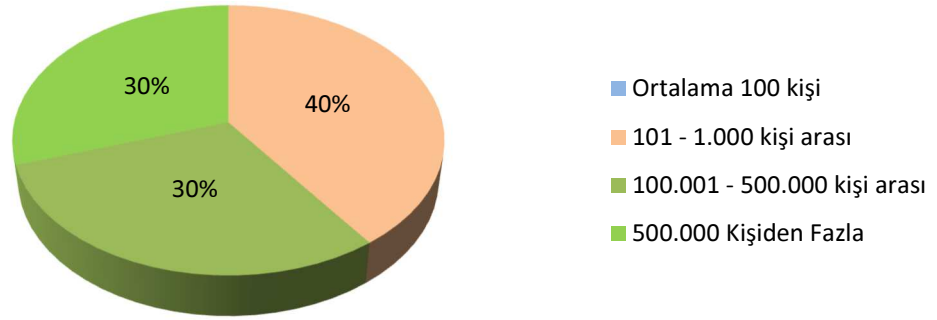
Kurumunuz bünyesinde kaç adet veri merkezi mevcuttur?



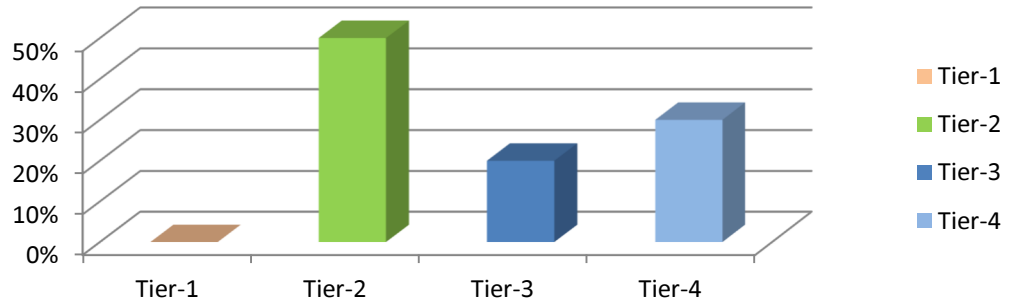
Veri Merkez(ler)inden ne kadarına ait Felaket Kurtarma Merkezi (FKM) mevcuttur ?



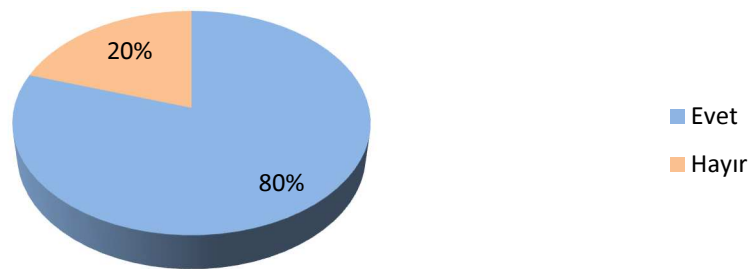
Kurumunuzun Veri merkez(ler)i, aylık ortalama kaç kişiye hizmet vermektedir?



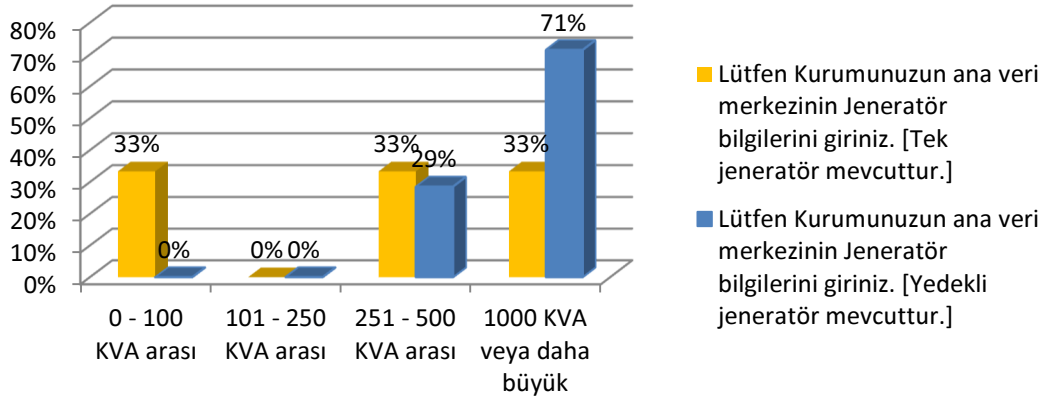
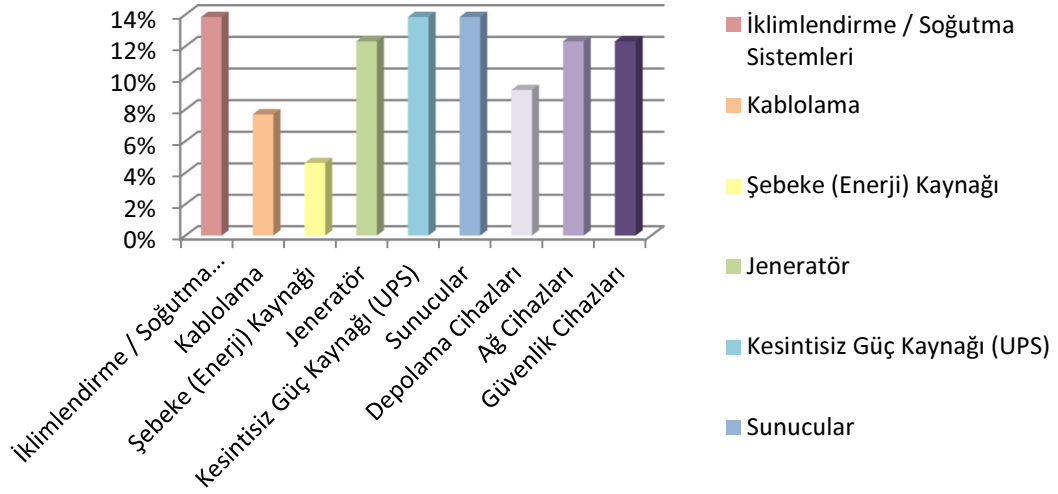
Kurumunuzun Veri merkez(ler)inin TIA standartlarına göre hangi seviyede olduğunu düşünüyorsunuz?



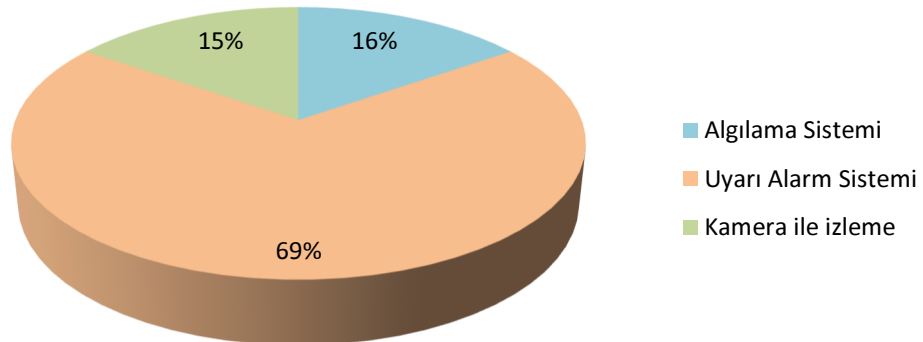
Kurumunuzun Veri merkez(ler)inin enerji alt yapısı, soğutma sistemleri, su basması v.b. ile ilgili izleme sisteminiz var mıdır?



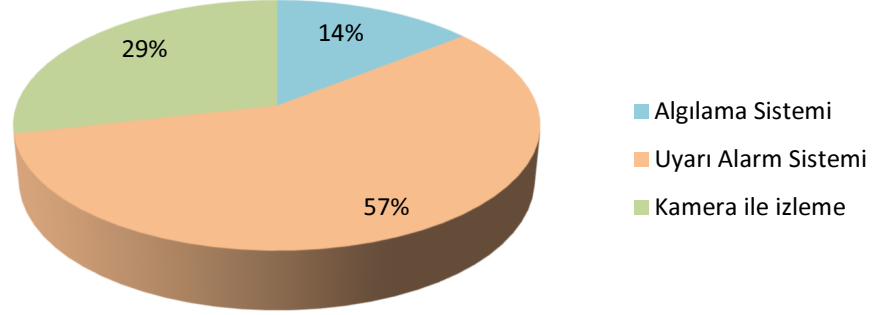
Kurumunuzun Veri merkez(ler)i bileşenlerinden hangileri yedeklidir?



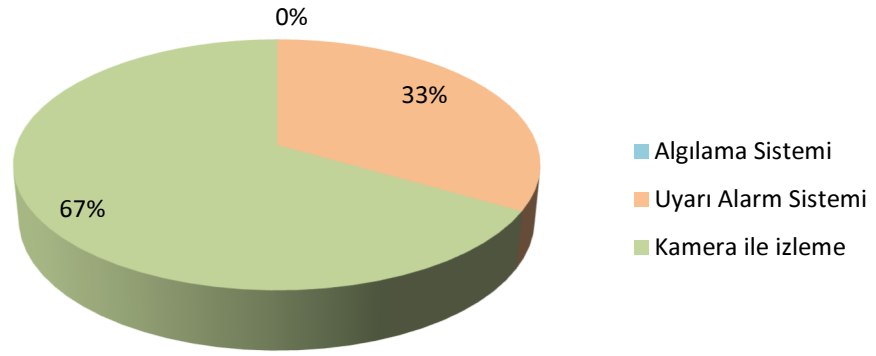
Yangın Önlemleri



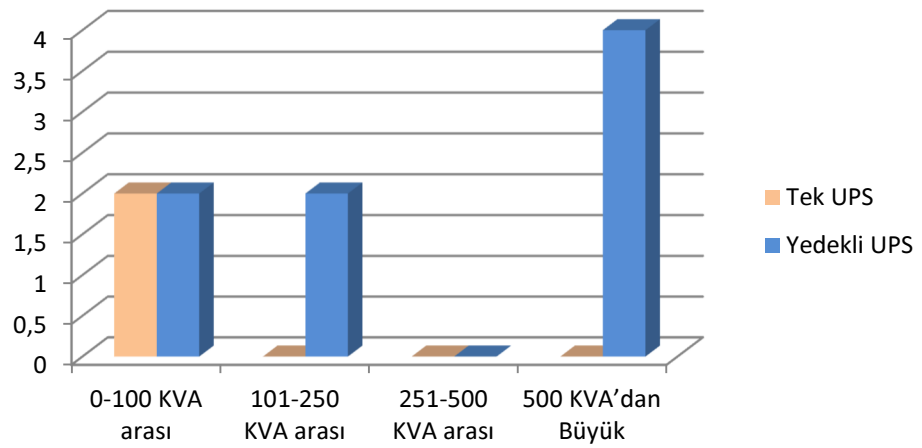
Su Baskını Önlemleri



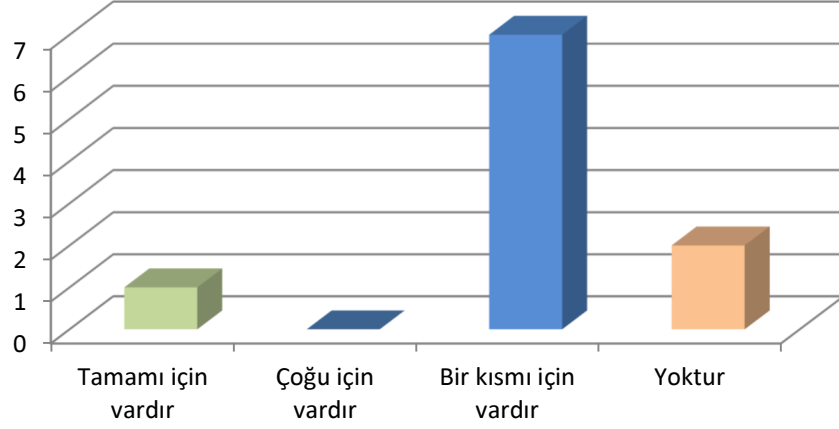
Deprem Önlemleri



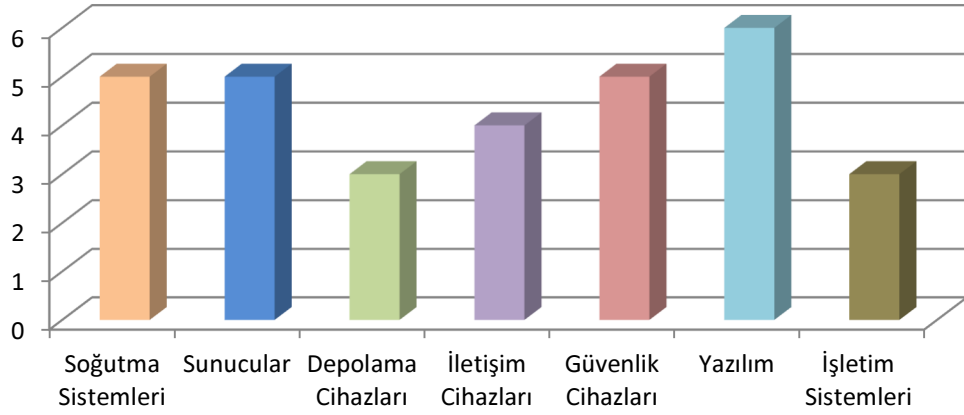
Veri Merkezi Kesintisiz Güç Kaynağı



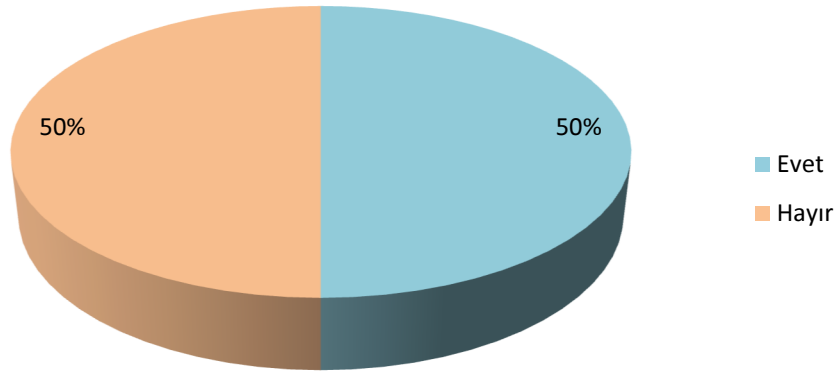
Kurumunuzun Veri merkez(ler)inin hizmet sürekliliği ve işletilmesine ilişkin özel sektör ile hizmet anlaşmanız mevcut mudur?



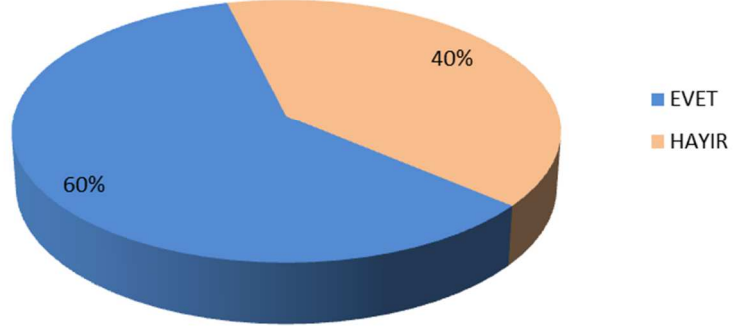
Hizmet Anlaşmaları



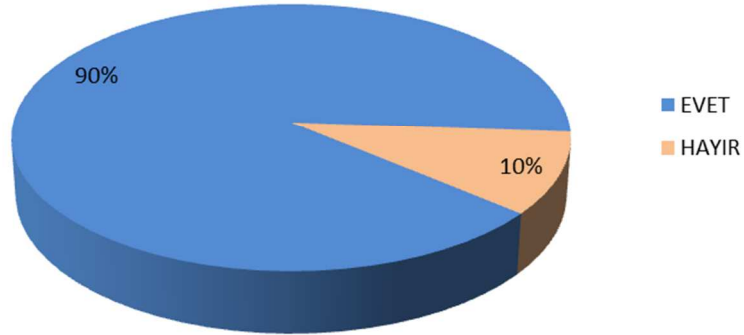
BGYS var mı ?



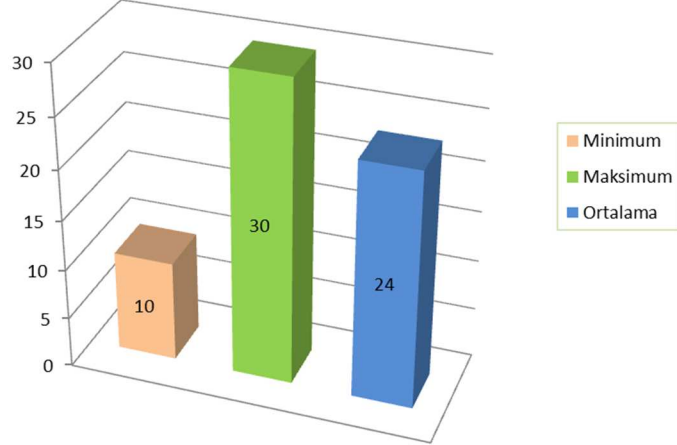
Kurumunuzun Bilgi Güvenliđi Yönetim sistemi
ve buna bađlı kurum içi yönerge /
yönetmeliklerimiz var mıdır?



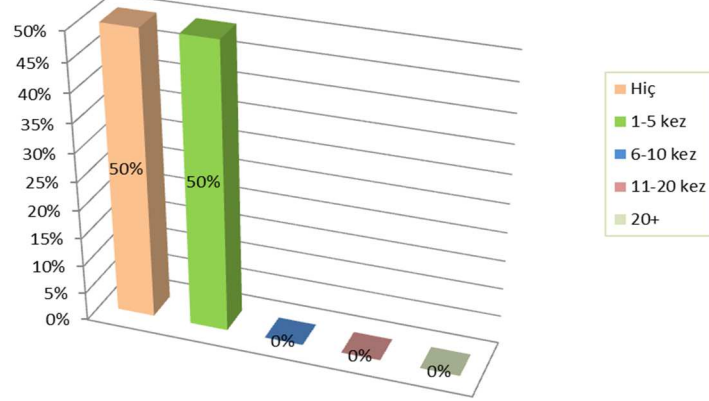
Kurumunuzun Veri merkez(ler)ine uygun
(FM200 gazlı) yangın söndürme sistemi var
mıdır?



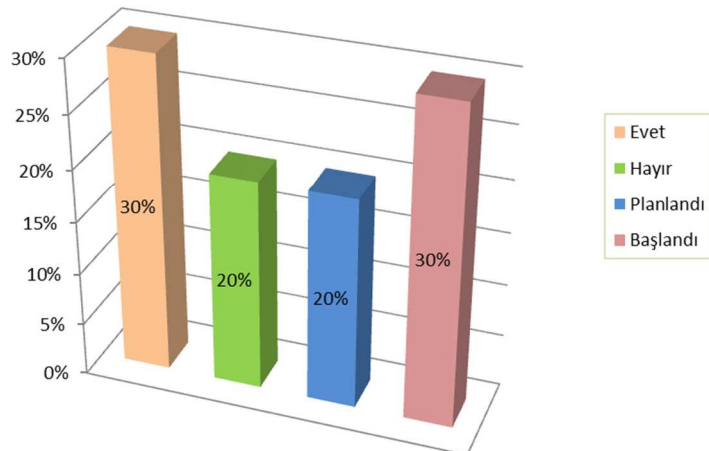
Kurumunuz veri merkezlerinizde herhangi sebeple son bir yıl boyunca hizmet kesintisi yaşandıysa ortalama kesinti süresi dakika cinsinden nedir?



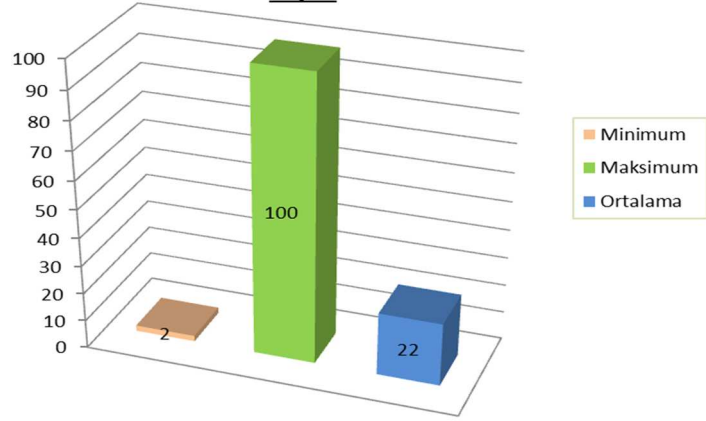
Kurumunuzun Veri merkez(ler)inizde (siber saldırı, teknik arıza vb) herhangi sebeple son bir yıl boyunca ortalama kaç kez hizmet kesintisi yaşandı?



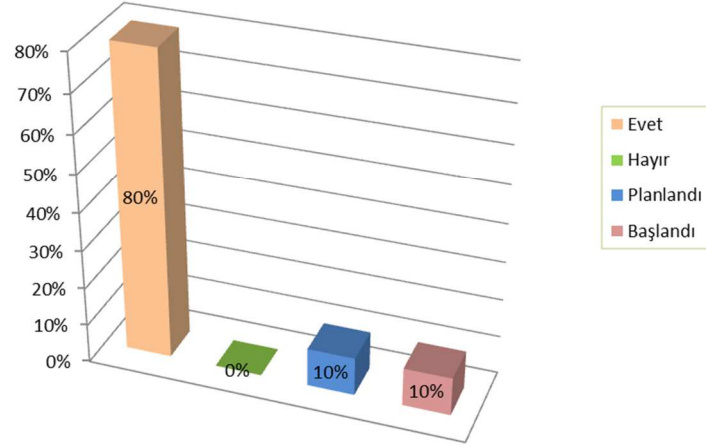
İş Sürekliliği Yönetim Sisteminiz mevcut mudur?



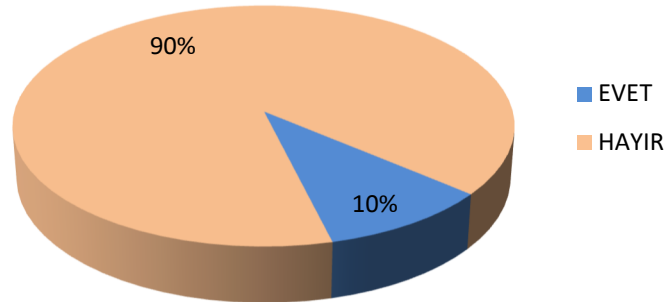
Kurumunuzun Veri merkez(ler)inde kurum personeline ve dışarıya hizmet veren portal sayısı nedir?



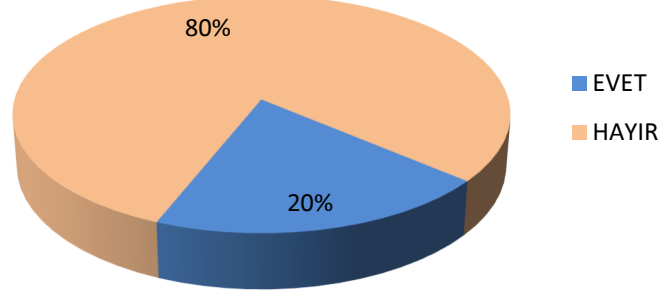
Kurumunuzun veri yedekleme stratejisi var mıdır?



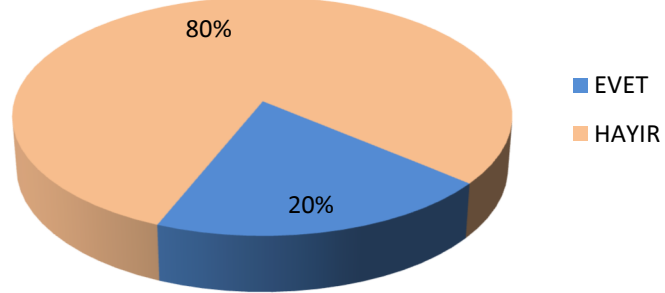
Kurumunuzun Veri merkez(ler)i hizmetleri sunulurken karşılaşılan sorunların çözümünde idari açıdan sıkıntı yaşıyor musunuz?



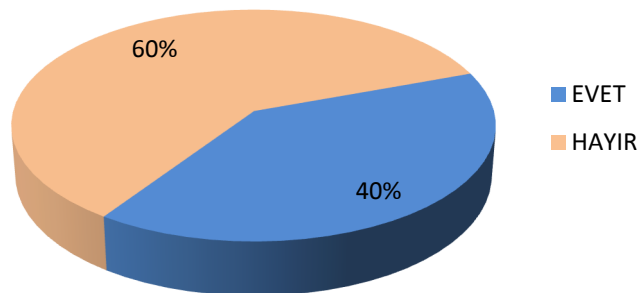
Kurumunuzun Veri merkez(ler)i hizmetleri sunulurken karşılaşılan sorunların çözümünde mali açıdan sıkıntı yaşıyor musunuz?



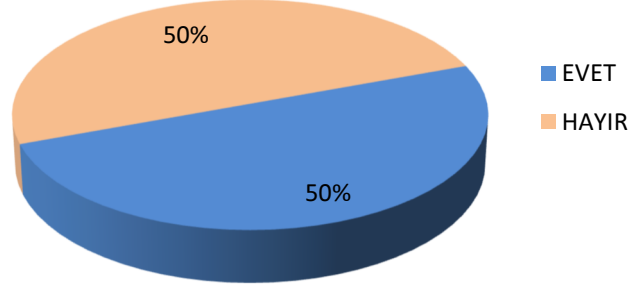
Kurumunuzun Veri merkez(ler)i hizmetleri sunulurken karşılaşılan sorunların çözümünde teknik açıdan sıkıntı yaşıyor musunuz?



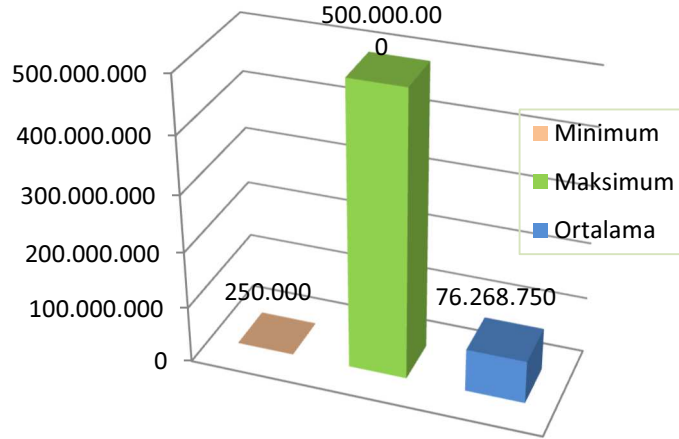
Kurumunuzda Veri Merkez(ler)i ile ilgili mevzuat var mıdır?



Mevcut veri merkez(ler)inizin bir başka kamu kurumunun fiziki çatısı altında yer alıp, sistem ve verilerin sorumluluğunun yine şu anda olduğu gibi sizin kontrolünüzde olması gibi bir durum karşınıza çıksa idi, böyle bir çalışma modelini tercih eder miydin



Kurumunuzun 2013 yılı BİM yatırım bütçesi yaklaşık ne kadar idi? (TL)



EK-D: İLGİLİ MEVZUAT ÖRNEKLERİ

ADALET BAKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN HÜKMÜNDE KARARNAMENİN DEĞİŞTİRİLEREK KABULÜ HAKKINDA KANUN

(1)

Kanun Numarası : 2992
Kabul Tarihi : 29/3/1984
Yayımlandığı R. Gazete : Tarih : 7/4/1984 Sayı : 18365
Yayımlandığı Düstur : Tertip : 5 Cilt : 23 Sayfa : 59

Adli Sicil ve İstatistik Genel Müdürlüğü:

Madde 12 – Adli Sicil ve İstatistik Genel Müdürlüğünün görevleri şunlardır:

c) Adli sicil ve adli istatistik hizmetlerinin yerine getirilmesi için bilgi işlem sistemini kurmak ve geliştirmek,

ADLÎ SİCİL YÖNETMELİĞİ

Resmi Gazete Tarihi: 07.09.2005 Resmi Gazete Sayısı: 25929

Adlî sicil bilgileri verilebilecek olanlar

Madde 9 — Adlî sicil bilgileri, kullanılış amacı ve verileceği merci belirtilmek suretiyle; ilgili kişiye veya vekâletnamede açıkça belirtilmek koşuluyla vekiline, kamu kurum ve kuruluşlarına, kamu kurumu niteliğindeki meslek kuruluşlarına verilebilir.

Arşiv bilgilerinin istenmesi

Madde 12 — Arşiv bilgileri;

Kullanılış amacı belirtilmek suretiyle, kişinin kendisi veya vekâletnamede açıkça belirtilmiş olmak koşuluyla vekili,

Bir soruşturma veya kovuşturma kapsamında mahkeme, hâkim veya savcılıklar,

Yetkili seçim kurulları,

(Değişik bent:RG-20/4/2013-28624) Özel kanunlarda gösterilen hâllerde ilgili kamu kurum ve kuruluşları,

tarafından istenebilir.

Kanunda açıkça belirtilmediği takdirde, kişi hakkında alınacak bir karar veya yapılacak bir işlemle ilgili olarak, bir yakınının adlî sicil ve arşiv kayıtları istenemez ve bu bilgiler, kişiyi herhangi bir haktan yoksun bırakmak için dayanak olarak kullanılamaz.

Onsekiz yaşından küçüklerle ilgili adlî sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere mahkeme, hâkim veya savcılıklarca istenebilir.

Adlî sicil ve arşiv bilgisi sorgulama yetkisi

Madde 15 – (Başlığıyla birlikte değişik:RG-20/4/2013-28624)

Bir suça ilişkin soruşturma ve kovuşturma kapsamında adlî sicil ve arşiv kayıtlarında;

Mahkeme, hâkim, askerî hâkim, Cumhuriyet başsavcılığı ve askerî savcılık doğrudan doğruya,

Kolluk ve diğer kamu kurum ve kuruluşları Adalet Bakanının onayı ile, sorgulama yapabilirler.

Kamu kurum ve kuruluşları, görev ve yetkileri kapsamında, mevzuatın adlî sicil ve arşiv kaydı alınmasını öngördüğü hâllerde, Adalet Bakanlığının izniyle, kendi iş ve işlemlerine esas olmak üzere ve sadece o iş ve işleme münhasır olarak, ilgili kişiler hakkında, Adlî Sicil Paylaşım Sisteminden sorgulama yapabilir.

Gerçek kişiler, kendileriyle ilgili adlî sicil ve arşiv kaydını, güvenli elektronik imza veya güvenli kimlik doğrulama araçlarını kullanarak sorgulayabilirler. Sorgulama sonucu oluşturulan elektronik imzalı doğrulama kodunu da içeren adlî sicil ve arşiv kaydı belgesi, elektronik ortamda ilgisine güvenli şekilde ulaştırılır.

Adlî Sicil Paylaşım Sistemi veritabanındaki bilgilerin tamamı hiçbir kuruma veya kişiye verilemez.

Adlî Sicil Paylaşım Sisteminin işletilmesinde, kanunlarda ve uluslararası sözleşmelerde yer alan özel hayatın gizliliğine ilişkin hükümler esas alınır. Kamu kurum ve kuruluşları, adlî sicil bilgilerinin gizliliğini korumakla yükümlüdürler.

Adlî Sicil Paylaşım Sistemine erişecek kamu kurum ve kuruluşları ile bağlantı, e-Devlet Kapısı üzerinden ve/veya noktadan noktaya iletişim şekillerinden biri kullanılarak sağlanır. Veri iletişiminin doğru, hızlı, kesintisiz ve güvenli olması için gerekli tedbirler alınır.

Kamu kurum ve kuruluşları ile gerçek kişilerin, Adlî Sicil Paylaşım Sistemine erişimleri, internet tarayıcıları veya internet servisleri üzerinden gerçekleştirilir.

Adlî Sicil Paylaşım Sisteminden yapılabilecek sorgulamalar, sorgulama sonucu olarak gönderilen bilgiler, kamu kurum ve kuruluşlarının erişeceği internet servisleri ve gerçek kişilerce erişilebilecek internet sayfaları, Genel Müdürlükçe belirlenir ve verilen yetkiler dışında işlem yapılması ve bilgi alınması engellenir.

Adlî Sicil Paylaşım Sistemi veri tabanından yedi gün - yirmidört saat hizmet verilir.

Genel Müdürlük, Adlî Sicil Paylaşım Sistemine erişecek kamu kurum ve kuruluşları kullanıcıları ile gerçek kişilerin kontrol edilmesi, verilen yetki çerçevesinde bilgi alınması ve gerekli bilgilerin Adlî Sicil Paylaşım Sistemi veri tabanında tutulması için her türlü tedbiri alır. Adlî Sicil Paylaşım Sisteminden yapılan her türlü işlemin tarihi, saati, işlemi yapan birim ve kullanıcı, yapılan sorgulama bilgileri izleme bilgisi olarak tutulur. Tutulan izleme bilgisi sorgu sonucunu da içerir.

Adlî Sicil Paylaşım Sisteminden yararlanmak isteyen kamu kurum ve kuruluşlarının, Bakanlığa yazılı olarak başvurması ve başvurularda, talep edilen bilgilerin kullanılma gerekçesinin ve yasal dayanağının belirtilmesi zorunludur.

Bakanlık, Adlî Sicil Paylaşım Sistemi veri tabanında tutulan bilgileri, bu Yönetmelikte belirlenen usul ve esaslara göre Bakanlık ile kamu kurum ve kuruluşları arasında yapılacak protokol çerçevesinde paylaşımına açabilir. Bu bilgilerin protokollerde belirtilen esaslar doğrultusunda kullanılması zorunludur.

Onikinci fıkrada belirtilen protokolde aşağıda belirtilen hususlara yer verilir:

Kamu kurum ve kuruluşları ve kullanıcıların yetkileri,

Bilgilere erişim şekli,

Bilgilere erişim süresi,

Kamu kurum ve kuruluşlarının Adlî Sicil Paylaşım Sistemi veri tabanını kullanma amacı,

Sorumluluk,

Eğitim,

Taraflarca uygun görülecek diğer hususlar.

Sorgulamanın usul ve esasları Bakanlık ile sorgulama talep eden kamu kurum ve kuruluşları arasında yapılacak protokolde belirlenir.

TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ İLE

ODALAR VE BORSALAR KANUNU

Kanun Numarası : 5174

Kabul Tarihi : 18/5/2004

Yayımlandığı R.Gazete : Tarih : 1/6/2004 Sayı :25479

Yayımlandığı Düstur : Tertip : 5 Cilt : 43

Odalara kayıt zorunluluğu

Madde 9- Ticaret siciline kayıtlı tacirler ve 5 inci maddeye göre sanayici ve deniz taciri sıfatını haiz tüm gerçek ve tüzel kişiler ile bunların şubeleri ve fabrikaları, bulundukları yerdeki odaya kaydolmak zorundadırlar. **Meslek gruplarına göre yapılacak üye kayıtları, elektronik ortamda Bakanlık ve Birlik bünyesinde düzenlenen ortak veri tabanında güncel olarak tutulur.**

Bir merkeze bağlı olduğu halde, ister merkezin bulunduğu odanın, ister başka odanın çalışma alanı içinde olan müstakil sermayesi ve müstakil muhasebesi bulunan ve/veya muhasebesi merkezde tutulduğu ve müstakil sermayesi bulunmadığı halde kendi başına sınaî faaliyet ve ticarî muamele yapan yerler ve satış mağazaları bu Kanunun uygulanması bakımından şube sayılır.

Sanayi odası kurulan illerde sanayiciler, sanayi odasına kaydolmakla ticaret odasına kaydolma yükümlülüğünü de yerine getirmiş olurlar. Sanayi işletmesi sahiplerinin, sınaî nitelikli işlerinin gereği olarak meşgul oldukları ticaret işleri

bunların sanayici vasfını ortadan kaldırmaz; bunlar isterlerse ticaret odasına da kaydolabilirler.

Sanayiciler, kendi sanayi ürünlerini satmak üzere birden fazla satış yeri açtıkları takdirde, fazlası için satış yerlerinin bulunduğu ticaret ve sanayi veya ticaret odasına da kaydolmak zorunda oldukları gibi; kendi sanayi ürünlerinin satışı dışında başka ticarî işlerle uğraştıkları takdirde, ticaret ve sanayi veya ticaret odasına da kaydolmakla yükümlüdürler.

Sermayesinin tamamı Devlete ve özel idarelere veya belediyelere veya bunların ortaklığına ait olan iktisadî müesseselerle bunların şubeleri, özel kanun veya sözleşme ile kurulmuş olup, Devletin ve özel idarelerin veya belediyenin iştiraki bulunan tüzel kişiliği haiz müesseseler veya bunların şubeleri ve fabrikaları, bulundukları ildeki odalara kaydolmak zorundadırlar.

Ticaret siciline kayıtlı gerçek ve tüzel kişilerden 5 inci maddede belirtilen deniz tacirleri ile beşinci fıkra hükmünde belirtilenlerden deniz ticaretiyle uğraşanlar, bulundukları ildeki deniz ticaret odasına kaydolmak zorundadırlar. Bu kapsamda sayılanlar, deniz ticaret odasına kaydolmakla diğer odalara kaydolma yükümlülüğünü de yerine getirmiş sayılırlar. Ancak, bu kapsamdakiler, deniz ticaret odasına kaydolmasını gerektiren faaliyetler dışında başka işlerle de uğraştığı takdirde, ayrıca ilgili odaya da kaydolmak zorundadır.

Odalara kaydı zorunlu olan gerçek ve tüzel kişilerle bunların şubeleri, kamu kurumu niteliğindeki başka meslek kuruluşlarına, birlik ve teşekküllere üye olmaya ve aidat ödemeye mecbur tutulamaz.

Bu maddede düzenlenen kayıt zorunluluğunu bir ay içinde yerine getirmeyenler, odalar tarafından re'sen kaydedilir ve durum kendilerine tebliğ edilir.

Borsaya kayıt zorunluluğu

Madde 32- Ticaret borsası kotasyonuna dahil maddelerin alım veya satımı ile uğraşanlar, bulundukları yerin borsasına kaydolmak zorundadırlar. Buna uymayanların kayıtları, borsaca re'sen yapılır ve kendilerine tebliğ edilir. **Meslek gruplarına göre yapılacak bu üye kayıtları, elektronik ortamda Bakanlık ve Birlik bünyesinde düzenlenen ortak veri tabanında güncel olarak tutulur.**

Borsaya kayıt zorunluluğunda olanların durumlarında meydana gelen ve Türk Ticaret Kanununa göre tescil ve ilânı gereken her türlü değişikliğin, gerçekleşmesinden itibaren bir ay içinde kayıtlı oldukları borsalara bildirilmesi

gerekir. İlgili sicile tescili zorunlu olup da kanunî şekil ve sürede tescil ettirilmemiş olan bir hususu haber alan ilgili borsa, bu zorunluluğu yerine getirmeyenlerin durumlarını gerekli sicil değişikliklerinin yapılması için ilgili sicil memurluğuna bildirir. Sicil memurluğu, bu bildirim üzerine gerekli işlemleri yapmakla yükümlüdür.

Merkezî borsa çalışma alanı dışında bulunmakla beraber, borsa çalışma alanı içinde faaliyet gösteren gerçek ve tüzel kişilerin, ticaret veya esnaf siciline tescil edilmiş ya da edilmemiş şube, irtibat bürosu, fabrika, temsilcilik, depo, alım satım yeri ve buna benzer ünitelerinin de borsaya kaydolmaları gerekir.

İçinde bulunulan yıldan önceki son iki yıldan itibaren adresleri ve durumları tespit edilemeyen ve içinde bulunulan yıldan önceki son iki yılda, borsa maddeleri üzerine alım satımı bulunmayan üyelerin isimleri, borsa meclisi kararıyla meslek grupları ve seçmen listelerinden silinir, aidat tahakkukları durdurulur ve bunlar borsa hizmetlerinden yararlanamazlar.

Yukarıdaki fıkrada anılan borsa meclisi kararını takip eden yılbaşından itibaren iki yıl içinde, ilgilinin üyesi bulunduğu borsaya müracaatla adres ve durumunu bildirmemesi halinde, borsa yönetim kurulunun teklifi ve meclis kararıyla borsadan kaydı silinir. Bu süre içinde durumunu bildirenlerin aidat tahakkukları başlatılır. Ancak bunlar aidat borçlarını ödemedikçe seçmen listelerine tekrar kaydedilemezler.

Borsaya dahil maddelerin üretici veya seri halde üretim yapmaksızın doğrudan tüketiciye satış yapan imalatçıları, borsalara kaydolmaksızın dahi kendi mallarını borsada satabilirler.

Seçimlere ilişkin genel esaslar

Madde 81- Oda, borsa ve Birlik organları ile şubelerinin seçimleri, bu Kanunda yazılı esas ve usullere göre, elektronik ortamda Bakanlık ve Birlik bünyesinde düzenlenen ortak veri tabanında Birliğe bağlı oda ve borsa meslek gruplarına göre seçme ve seçilme niteliklerini haiz olan üyeleri gösteren oda, borsa ve Birlik veri tabanından alınan güncel üye listeleriyle yargı gözetiminde yapılır.

Bir yerde birden fazla ilçe seçim kurulu bulunduğu takdirde, görevli hâkim il seçim kurulunca belirlenir. Birlik organları seçimlerinde görevli hâkim, merkez ilçe seçim kurulu başkanıdır.

İlçe seçim kurulu başkanı, oda ve borsanın üye ve meslek grubu sayısına ve Birlik organları seçimlerinin gereklerine göre seçim sandıklarının yer ve sayısını,

tarihini ve oy kullanma süresini, oy pusulasının şeklini ve seçimle ilgili diğer hususları belirler. Seçimlerde kullanılacak araç ve gereçler, ilçe seçim kurulundan sağlanır.

Seçim sandık kurulu

Madde 82- İlçe seçim kurulu başkanı, elektronik ortamda Bakanlık ve Birlik bünyesinde düzenlenen ortak veri tabanından sağlanan seçme ve seçilme niteliklerini haiz olan listeleri incelemek ve seçimleri yapmak üzere kamu görevlileri veya aday olmayan üyeler arasından bir başkan ile iki üyeden oluşan bir seçim sandık kurulu oluşturur ve aynı şekilde üç yedek üyeyi de belirler. Birlik organlarının seçiminde, seçim sandık kurulu için bir başkan ve dört üye ile beş yedek üye, kamu görevlileri veya aday olmayan delegeler arasından merkez ilçe seçim kurulu başkanı tarafından belirlenir.

Seçim sandık kurulu başkanının yokluğunda kurula en yaşlı üye başkanlık eder. Seçim sandık kurulu, seçimlerin Kanunun öngördüğü esaslara göre yürütülmesi, yönetimi ve oyların tasnifi ile görevli olup, bu görevleri seçim ve tasnif işleri bitinceye kadar aralıksız olarak devam eder.

İlçe seçim kurulu başkanı hâkime ve seçim sandık kurulu başkan ve üyelerine 298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanunda belirtilen esaslara göre ücret ödenir. Bu ücretlerle, diğer seçim giderleri seçimi yapan oda, borsa veya Birlik tarafından karşılanır.

Seçimler sırasında seçim sandık kurulu başkan ve üyelerine karşı işlenen suçlar, Devlet memurlarına karşı işlenmiş gibi cezalandırılır.

Oda ve borsa organlarının seçimleri

Madde 84- Oda ve borsa organlarının seçimleri, bu Kanun hükümlerine göre aşağıda belirtilen esas ve usullere uygun olarak, ekim ayında başlar kasım ayı içinde bitirilir.

a) Gruplandırma işlemleri ve meslek komitelerinin seçimi:

1) Meslek komiteleri seçiminden en az yirmi gün önce oda ve borsaların yönetim kurulları tarafından, seçilme hakkına sahip olanlarla, seçme hakkına sahip olanları gösteren, elektronik ortamda Bakanlık ve Birlik bünyesinde düzenlenen veri

tabanında yer alan meslek gruplarına göre hazırlanan listeler, üç nüsha olarak kuruluşun bulunduğu yerdeki ilçe seçim kurulu başkanına sunulur.

TÜRK TİCARET KANUNU ⁽¹⁾

Kanun Numarası : 6102
Kabul Tarihi : 13/1/2011
Yayımlandığı R.Gazete : Tarih: 14/2/2011 Sayı : 27846
Yayımlandığı Düstur : Tertip : 5 Cilt : 50

I - Genel olarak ⁽¹⁾

MADDE 24- (1) Ticaret sicili, Gümrük ve Ticaret Bakanlığının gözetim ve denetiminde ticaret ve sanayi odaları veya ticaret odaları bünyesinde kurulacak ticaret sicili müdürlükleri tarafından tutulur. Bir yerde oda mevcut değilse veya yeterli teşkilatı yoksa, ticaret sicili, Gümrük ve Ticaret Bakanlığınca belirlenecek bir odadaki ticaret sicili müdürlüğü tarafından tutulur.

(2) Ticaret sicili kayıtlarının elektronik ortamda tutulmasına ilişkin usul ve esaslar Kanunun 26 ncı maddesine göre çıkarılacak yönetmelikte gösterilir. Bu kayıtlar ile tescil ve ilan edilmesi gereken içeriklerin düzenli olarak depolandığı ve elektronik ortamda sunulabilen merkezi ortak veri tabanı, Gümrük ve Ticaret Bakanlığı ile Türkiye Odalar ve Borsalar Birliği nezdinde oluşturulur.

(3) Ticaret sicili müdürlüğünün kurulmasında aranacak şartlar ve odalar arasında sicil işlemleri ile ilgili olarak varlığı gerekli işbirliğinin sağlanmasına ilişkin esaslar, Gümrük ve Ticaret Bakanlığınca çıkarılacak bir tebliğle düzenlenir.⁽¹⁾

(4) **(Ek: 26/6/2012-6335/3 md.)** Ticaret sicili kayıt işlemlerinin elektronik ortamda yapılması için toplanması ve işlenmesi gerekli olan kişisel veriler, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuata uygun bir şekilde korunur.

AFET VE ACİL DURUM YÖNETİMİ BAŞKANLIĞININ
TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN

Kanun Numarası : 5902
Kabul Tarihi : 29/5/2009
Yayımlandığı R.Gazete : Tarih: 17/6/2009 Sayı : 27261
Yayımlandığı Düstur : Tertip : 5 Cilt : 48

Bilgi Sistemleri ve Haberleşme Dairesi Başkanlığı

MADDE 13/B- (Ek:24/10/2011-KHK-661/87 md.)

(1) Bilgi Sistemleri ve Haberleşme Dairesi Başkanlığının görevleri şunlardır:

a) Afet ve acil durum yönetim merkezlerinin, ortak haberleşme ve bilgi sistemlerinin standardını belirlemek ve denetlemek.

b) Afet ve acil durumlara ilişkin her türlü bilgi, haberleşme, tahmin ve erken uyarı sistemlerini kurmak, kurdurmak, bakım ve onarımını yapmak veya yaptırmak, işletmek veya işletilmesini sağlamak.

c) E-Devlet uygulamalarının Başkanlık ile ilgili çalışmalarını yapmak, koordine etmek ve yürütmek.

ç) Afet ve acil durumlara yönelik coğrafi bilgi sistemini kurmak veya kurdurmak, formatlarını hazırlamak, il afet ve acil durum müdürlükleri arasındaki bilgi standartlarını oluşturmak.

d) Bilişim teknolojisindeki gelişmelere uygun olarak daha etkin ve verimli bilgi, belge ve iş akışı düzenini kurmak, buna yönelik yazılımları üretmek veya sağlamak.

e) Başkanlığın bilişim altyapısı ve haberleşme sisteminin kurulumu, bakımı, ikmali, geliştirilmesi ve güncellenmesi ile ilgili işleri yürütmek, bunlarla ilgili güvenlik tedbirlerini almak, kripto merkezini kurmak, kurdurmak ve işletmek.

f) Bilişim teknolojisinin gelişimini izlemek, bilgi işlem donanım ve yazılımının kullanılmasında diğer kamu kurum ve kuruluşlarıyla işbirliği yapmak.

g) Başkanlık birimleri ve diğer ilgili kuruluşlarla işbirliği yaparak bilgi işlem sisteminin etkin ve verimli bir şekilde çalışmasını sağlamak.

ğ) Afet ve acil durumlara yönelik veri tabanlarını kurmak, kurdurmak ve işletmek, uygulama yazılımlarını yapmak veya yaptırmak.

h) Başkanlığın internet sayfaları, elektronik imza ve elektronik belge uygulamaları ile ilgili teknik çalışmaları yapmak veya yaptırmak.

ı) Başkanlık hizmetleriyle ilgili bilgileri toplamak ve ilgili birimlerle işbirliği içinde veri tabanları oluşturmak.

i) Başkan tarafından verilecek benzeri görevleri yapmak.

DEVLET İSTİHBARAT HİZMETLERİ VE MİLLİ İSTİHBARAT TEŞKİLATI KANUNU

Kanun Numarası : 2937

Kabul Tarihi : 1/11/1983

Yayımlandığı R.Gazete : Tarih : 3/11/1983 Sayı : 18210

Yayımlandığı Düstur : Tertip : 5 Cilt : 22 Sayfa : 830

Ek Madde 1 – (Ek: 17/4/2014-6432/11 md.)

Millî İstihbarat Teşkilatı uhdesindeki istihbari nitelikteki bilgi, belge, veri ve kayıtlar ile yapılan analizler, Türk Ceza Kanununun İkinci Kitap Dördüncü Kısım Yedinci Bölümünde yer alan suçlar hariç olmak üzere, adli mercilerce istenemez.

6 ncı maddenin birinci fıkrasının (e) bendine göre kimlikleri değiştirilenler, MİT'in görev ve faaliyetlerine yardımcı olanlar veya istihbarat hizmetlerinde istifade edilenler, kamu görevlisi olup olmadıklarına bakılmaksızın; görev, faaliyet ve yardımları sebebiyle sorumlu tutulamaz.

Teşkilat uhdesindeki bilgi ve belgelerin gizlilik derecelerinin ve sürelerinin tespit edilmesine, birim ve kısımlara ayrılmasına, kullanıma veya paylaşımına açılmasına ve bunların akademik çalışmalar ile her türlü yayın ve edebî eserde kullanılmasına Müsteşar tarafından oluşturulacak bir Komisyonca karar verilir.

**GELİR İDARESİ BAŞKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA
KANUN**

Kanun Numarası : 5345
Kabul Tarihi : 5/5/2005
Yayımlandığı R.Gazete : Tarih: 16/5/2005 Sayı : 25817
Yayımlandığı Düstur : Tertip : 5 Cilt : 44

Uygulama ve Veri Yönetimi Daire Başkanlığı⁽¹⁾

Madde 11- Uygulama ve Veri Yönetimi Daire Başkanlığının görevleri şunlardır:

a) İşlemlerin hızlı ve etkin bir şekilde yürütülmesi için gerekli bilgi işlem sistemlerini kurmak, teknolojik gelişmelere uygun bir şekilde geliştirmek ve bilişim faaliyetlerini yürütmek.

b) Başkanlığın taşra teşkilatının görev ve çalışma esasları ile ilgili yönetmelik ve yönergeleri, diğer birimlerle işbirliği yapmak suretiyle hazırlamak ve uygulanmasını izlemek.

c) Taşra birimlerinin kuruluşuna ilişkin işlemleri yürütmek.

d) Merkez ve taşra teşkilatının iş ve işlem akışlarını düzenlemek ve verimliliğini artırmaya yönelik tedbirler almak.

e) Taşra birimlerinin iş ve işlemlerinde koordinasyon ve uygulama birliğini sağlamak.

f) İdare ve mükelleflerce kullanılacak belge ve formlarla vergi beyannamelerini hazırlamak.

g) Tüm ekonomik faaliyetlere ilişkin ulusal mali bilgi alt yapısını tek merkezden geliştirmek, yönetmek ve bu bilgileri ilgili birimlerin kullanımına sunmak.

h) Kurumsal veri tabanını oluşturmak ve ulusal veri alt yapısının hazırlanmasına katkıda bulunmak.

i) Mükellefiyet, vergilendirme, denetim ve risk analizine yönelik her türlü bilgi, veri ve istatistiği toplamak ve işlemek.

j) Vergilendirme, denetim, planlama ve kayıt dışı ekonomiyle mücadele konularında veri sağlamak.

k) (Ek: 18/2/2009-5838/20 md.) 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu kapsamındaki kamu idarelerine verilmesi gereken her türlü beyanname, bildirge ve benzeri belgeleri, bu idarelerin mevzuatı gereğince elektronik ortamda bunlar adına almak.

İÇİŞLERİ BAKANLIĞI TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN ⁽¹⁾

Kanun Numarası	: 3152
Kabul Tarihi	: 14/2/1985
Yayımlandığı R. Gazete	: Tarih : 23/2/1985 Sayı : 18675
Yayımlandığı Düstur	: Tertip : 5 Cilt : 24 Sayfa : 239

Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü

Madde 10 – Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünün görevleri şunlardır:

a) Ülke nüfusunun yapısı, nitelikleri, nüfus hareketleri ve bunlardaki gelişmelere göre takip edilecek politikaların tespitine dair çalışmaları ilgili kuruluşlarla işbirliği içinde yapmak, belirlenecek esasların yürütülmesini sağlamak,

b) Nüfus hareketlerini takip etmek ve değerlendirmek, merkezde bir nüfus bilgi bankası kurmak, aile ve hayat istatistiklerine ait verileri toplamak, ilgili kuruluşlarla işbirliği içerisinde yayınlamak,

c) Nüfus hizmetlerini düzenlemek, yürütmek, takip etmek, denetlemek ve değerlendirmek, usulüne göre tesis edilmemiş kayıtların silinmesini karara bağlamak, maddi hataları düzeltmek, aile kayıtlarını birleştirmek, mükerrer kayıtları birbirine göre tamamlamak ve diğerlerini silmek, nüfus hizmetleri ile ilgili olarak diğer bakanlık, kurum ve kuruluşlar arasında koordinasyon sağlamak,

d) Vatandaşlığın kazanılması, kaybı ve göçmen olarak kabule dair işlemleri yürütmek ve vatandaşlıkla ilgili kanunları uygulamak, vatandaşlık anlaşmazlıklarını karara bağlamak ve vatandaşlık incelemelerini yapmak,

e) (Ek: 15/3/2003-4825/1 md.) Nüfus cüzdanlarının yürürlük, değiştirme ve geçerlilik tarihlerini belirlemek ve nüfus cüzdanlarının üretiminde uygulanacak sistem ve teknolojiyi tespit etmek,

NÜFUS HİZMETLERİ KANUNU

Kanun Numarası : 5490
Kabul Tarihi : 25/4/2006
Yayınlandığı R.Gazete : Tarih : 29/4/2006 Sayı : 26153
Yayınlandığı Düstur : Tertip : 5 Cilt : 45

Nüfus kütüklerinin tutulması

MADDE 6- (1) Nüfus olayları, iletişim ağı kullanılarak nüfus müdürlüklerindeki aile kütüklerine ve merkezî veri tabanına tescil edilir.

(2) Bakanlık, doğal afet ve olağanüstü hallere karşı kesintisiz olarak hizmet verilmesini sağlamak amacıyla, merkezî veri tabanının yedeğinin farklı bir yerde tutulmasını sağlar.

Aile kütüklerinde bulunması gereken kişisel bilgiler

MADDE 7- (1) Her mahalle veya köy için ayrı aile kütüğü tutulur. Aile kütüklerinde aşağıdaki bilgiler bulunur:

- a) Türkiye Cumhuriyeti kimlik numarası.
- b) Kayıtlı bulunduğu il, ilçe, köy veya mahalle adı ile cilt, aile ve birey sıra numarası.
- c) Kişinin adı ve soyadı, cinsiyeti, baba ve ana adı ile soyadları, evli kadınların önceki soyadları.
- ç) Doğum yeri ile gün, ay ve yıl olarak doğum tarihi ve kütüğe kayıt tarihi.

d) Evlenme, boşanma, soybağının kurulması veya reddi, ölüm, vatandaşlığın kazanılması veya kaybedilmesi gibi kişisel durumda meydana gelen değişiklik veya yetkili makamlarca yapılan düzeltmeler.

e) Dini.

f) Medenî hali.

g) Yerleşim yeri adresi.

ğ) Fotoğrafı.

(a), (g) ve (ğ) bentlerinde belirtilen kayıtlar sadece elektronik ortamda tutulur.

(2) Türkiye'de aile kütüğü bulunmayan ve yabancı ülkelerde oturan vatandaşlar Bakanlığın göstereceği bir nüfus müdürlüğünde açılacak aile kütüğüne kaydedilir.

Gizlilik

MADDE 9- (1) Nüfus kayıtları ve bu kayıtların tutulmasına dayanak olan belgeler gizlidir. Bunlar, yetkili ve sorumlu memurlar ile teftiş ve denetim yetkisi olanlar dışında kimse tarafından görülüp incelenemez. Mahkemeler bu hükmün dışındadır.

(2) Nüfus kayıtlarına bu bilgileri işleyen memurlar ve Kimlik Paylaşımı Sistemi kapsamında nüfus kayıtlarından faydalanan diğer görevliler de bu gizliliğe uymak zorundadırlar. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

Kimlik ve Adres Paylaşımı Sistemlerinin kullanılması

MADDE 45- (1) Bakanlık, Kimlik Paylaşımı Sistemi ve Adres Paylaşımı Sistemi veri tabanlarında tutulan bilgileri bu Kanunda belirtilen esas ve usûller çerçevesinde kurumlar ile diğer kişilerin hizmetine açabilir. Yerleşim yeri adresi bilgileri ancak kurumlar ile 5411 sayılı Bankacılık Kanunu çerçevesinde faaliyette bulunan bankaların ve 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu çerçevesinde faaliyette bulunan sigorta ve emeklilik şirketleri ile Güvence Hesabının paylaşımına açılabilir. ⁽¹⁾⁽²⁾

(2) Kimlik Paylaşımı Sistemi veri tabanındaki bilgilerin tamamı veya bir kısmı toplu halde hiçbir kuruma veya diğer kişilere verilemez. Kurumlar ve diğer kişiler

kendi iş ve işlemlerine esas olmak üzere sadece kayıtlarını tuttukları kişilerin bilgilerini alabilirler.

(3) Kurumlar aldıkları bilgileri tanımlanmış hizmetlerin yerine getirilmesi dışında başka hiçbir amaçla kullanamaz; ilgilisi veya bu Kanunun 44 üncü maddesinde belirtilenler dışında kimseye veremez. Sistemin bütün aşamalarında görev yapan yetkililer de bu kurallara uymakla yükümlüdür. Bu yükümlülük, kamu görevlilerinin görevlerinden ayrılmalarından sonra da devam eder.

(4) Genel Müdürlükten alınan bilgilerin iş ve işlemlerde kullanılmasının hukukî sonuçları bilgiyi alan kurumun sorumluluğundadır.

(5) Bu Kanun ile kurulacak veri tabanlarının istatistik amaçlı kullanımında 10/11/2005 tarihli ve 5429 sayılı Türkiye İstatistik Kanunu hükümleri uygulanır.

Adres bilgilerinin tutulması ve adres standardı

MADDE 48- (1) Yerleşim yeri adresi ve diğer adreslere ait bilgilerin tutulmasına ilişkin politikanın oluşturulması, geliştirilmesi, yaygınlaştırılması, idarî birimlere göre genel uygulamaya geçiş tarihlerinin tespit edilmesi, ulusal adres veri tabanı ile MERNİS veri tabanının ilişkilendirilmesi ve adres bilgilerinin paylaşılmasına ilişkin işlemler Bakanlıkça yürütülür. Bakanlığın nüfus kütüklerindeki adres kayıtlarını tamamlamak maksadıyla işbirliği talebi kurumlarca karşılanır.

(3) Bakanlık, adrese ilişkin her türlü bilgiyi kurumlardan istemeye yetkilidir. Kurumlar söz konusu isteğe yirmi gün içinde cevap vermekle yükümlüdür.

Adres bilgisi ve güncellenmesi

MADDE 49- (1) İl özel idaresi ve belediyeler sorumluluk alanlarındaki adres bileşenlerini adres standardına uygun olarak tanımlayıp bunlara değiştirilemeyecek sabit tanıtım numarası vererek mahallindeki bütün adresleri kapsayacak şekilde adres bilgilerini oluşturmakla yükümlüdür. Herhangi bir sebeple sabit tanıtım numarası dışında adres bileşenlerinde yapılan değişiklikler de il özel idaresi ve belediyelerce takip edilerek ulusal adres veri tabanına işlenir.

(2) Ulusal adres veri tabanı Genel Müdürlükte tutulur. Genel Müdürlük, ulusal adres veri tabanındaki yerleşim yeri adresi bilgilerini nüfus kütüklerindeki kişi kayıtları ile ilişkilendirerek elektronik ortamda, yedekleme sistemleri ile birlikte güncel olarak tutar.

(3) (Mülga: 9/5/2012-6304/13 md.)

**ÖLÇME, SEÇME VE YERLEŞTİRME MERKEZİ BAŞKANLIĞININ
TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN**

Kanun Numarası : 6114
Kabul Tarihi : 17/2/2011
Yayımlandığı R.Gazete : Tarih: 3/3/2011 Sayı : 27863
Yayımlandığı Düstur : Tertip : 5 Cilt : 50

Sınav güvenliği

MADDE 9 – (1) Sınav soruları ile bunları hazırlamakla görevlendirilmiş olan kişilerin kimlikleri gizli tutulur. Başkanlık, gizliliğin sağlanması için gerekli bütün tedbirleri alır ve ilgili tüm kurumlarla işbirliği yapar. Soru havuzundaki sorular hiçbir koşul altında kısmen ya da tamamen üçüncü şahıslara verilmez. Adli ve idari soruşturma ve kovuşturmalarda soru havuzuna erişim için Bakanlar Kurulunun izni gereklidir.

**AİLE VE SOSYAL POLİTİKALAR BAKANLIĞININ TEŞKİLAT VE ÖREVLERİ
HAKKINDA KANUN HÜKMÜNDE KARARNAME⁽¹⁾**

Kanun Hük. Kar. nin Tarihi : 3/6/2011, No : 633
Yetki Kanununun Tarihi : 6/4/2011, No : 6223
Yayımlandığı R.G. Tarihi : 8/6/2011, No : 27958 Mük.
Yayımlandığı Düstur : Tertip : 5 Cilt : 50

Sosyal Yardımlar Bilgi Sistemi Veri Tabanı

MADDE 33- (1) Sosyal hizmetler ve yardımlar kapsamındaki kişilerin tespiti, ulusal politika ve stratejilerin oluşturulması ve sosyal yardımların objektif yararlanma

ölçütlerine göre belirlenmesi için veri sağlanması, mükerrer sosyal yardımların önlenmesi, bu alanda eşgüdümün sağlanması amacıyla sosyal güvenlik ve diğer ilgili veri tabanları ile bütünleşik yapıda, Türkiye Cumhuriyeti Kimlik Numarası temel alınarak Sosyal Yardımlar Bilgi Sistemi Veri Tabanı (Veri Tabanı) oluşturulur.

(2) Bakanlık birimleri ve kamu kurum ve kuruluşları ile 3294 sayılı Kanun hükümlerine göre kurulan vakıflar, yardım yapacakları kişilerin sosyal yardıma hak kazanıp kazanmadığını tespit amacıyla muhtaçlık durumlarını ve sosyal yardım alıp almadıklarını yardım yapılmadan önce Veri Tabanından sorgulamakla ve yapılan yardımların türü, miktarı ve ailenin diğer bireyleri de dâhil olmak üzere verildiği kişi ve verilme süresine ilişkin bilgiler ile yönetmelikle belirlenecek diğer konulara ilişkin bilgileri, yardım yapılmasına onay veren belgelerin oluşturulması ile eş zamanlı olarak Veri Tabanına işlemekle yükümlüdür.

(3) Bakanlık, Veri Tabanında tutulan bilgileri belirleyeceği usûl ve esaslar çerçevesinde kamu kurum ve kuruluşları ile mahalli idareler ve Türkiye Kızılay Derneğine açabilir.

(4) Veri Tabanındaki bilgilerin tamamı veya bir kısmı toplu hâlde hiçbir kuruma veya kişiye verilemez. Bakanlık Veri Tabanındaki bilgiler, elektronik ortamda, yedekleme sistemleri ile birlikte güncel olarak tutulur.

(5) Bu maddenin uygulanmasına ilişkin usûl ve esaslar Bakanlık tarafından hazırlanacak yönetmelikle belirlenir.

Sosyal Yardımlar Bilgi Sistemi Veri Tabanı

GEÇİCİ MADDE 8- (1) Bu Kanun Hükmünde Kararnamenin yürürlüğe girdiği tarihten itibaren iki yıl içinde, Sosyal Yardımlar Bilgi Sistemi Veri Tabanının oluşturulması ve kullanılması kapsamında;

a) Veri Tabanının altyapı çalışmaları Bakanlık bünyesinde yapılarak Veri Tabanı kurulur,

b) Sosyal yardım hizmeti sunmak üzere ödenek ayıran kamu kurum ve kuruluşları Veri Tabanına erişim konusunda teknik altyapılarını oluşturur. Ülke genelinde sosyal yardım hizmeti sunmak üzere ödenek ayıran kamu kurum ve kuruluşları ile Veri Tabanı arasında eş zamanlı işleyecek bir ağ altyapısı oluşturulur. Sosyal yardım hizmeti sunmak üzere ödenek ayıran kurumların Veri Tabanına ulaşabileceği bir merkezî bilgisayar programı Bakanlık tarafından hazırlanır. Veri

Tabanı, gerekli şifreleme ve kullanıcı eğitimi verilmesini müteakiben kamu kurum ve kuruluşlarının kullanımına açılır.

GÜMRÜK VE TİCARET BAKANLIĞININ TEŞKİLAT VE GÖREVLERİ HAKKINDA KANUN HÜKMÜNDE KARARNAME⁽¹⁾

Kanun Hük. Kar. nin Tarihi : 3/6/2011, No : 640

Yetki Kanununun Tarihi : 6/4/2011, No : 6223

Yayımlandığı R.G. Tarihi : 8/6/2011, No : 27958 Mük.

Yayımlandığı Düstur : Tertip : 5 Cilt : 50

Gümrükler Muhafaza Genel Müdürlüğü

MADDE 8- (1) Gümrükler Muhafaza Genel Müdürlüğünün görevleri şunlardır:

g) Kaçakçılıkla etkin mücadele etmek amacıyla ulusal ve uluslararası bilgi akışına dayalı veri tabanları oluşturmak, verileri işlemek, değerlendirmek ve risk analizi çerçevesinde kullanılabilecek nitelikte olanları Risk Yönetimi ve Kontrol Genel Müdürlüğüne iletmek.

GÜMRÜK KANUNU

Kanun Numarası : 4458

Kabul Tarihi : 27/10/1999

Yayımlandığı R.Gazete : Tarih : 4/11/1999 Sayı : 23866

Yayımlandığı Düstur : Tertip : 5 Cilt : 39

MADDE 12- 1. Gümrük idareleri ve diğer yetkili kurumlar gizli nitelikteki veya gizlilik esasına göre elde edilen bütün bilgileri saklamak zorundadır. Bu bilgileri veren kişinin veya makamın açık izni olmaksızın söz konusu bilgiler açıklanamaz. Şu kadar ki, gümrük idareleri verilerin korunmasına ilişkin yasal hükümler veya yargı kararlarının gereği olarak söz konusu bilgileri ilgili mercilere verirler.

SAĞLIK BAKANLIĞI VE BAĞLI KURULUŞLARININ
TEŞKİLAT VE GÖREVLERİ HAKKINDA
KANUN HÜKMÜNDE KARARNAME

Kanun Hük. Kar. nin Tarihi : 11/10/2011, No : 663

Yetki Kanununun Tarihi : 6/4/2011, No : 6223

Yayımlandığı R.G. Tarihi : 2/11/2011, No : 28103 Mükerrer

Yayımlandığı Düstur : Tertip : 5 Cilt : 51

Sağlık Bilgi Sistemleri Genel Müdürlüğü

MADDE 11- (1) Sağlık Bilgi Sistemleri Genel Müdürlüğünün görevleri şunlardır:

a) Sağlık alanında kullanılan bilişim sistemleri ve iletişim teknolojileri ile ilgili ülke çapında politika, strateji ve standartları belirlemek.

b) **Kişisel sağlık verileri ile ülke düzeyinde sağlık durumu ve sağlık hizmetlerine ilişkin veri ve bilgi akışını içeren her türden bilgi sistemleri ve projelerini yapmak ve yaptırmak.**

ç) Sağlık bilişimi ve teknolojisi alanında çalışacak kamu ve özel hukuk tüzel kişileri ile gerçek kişilerin uyacakları kuralları belirlemek, uygulamak, gerektiğinde bunların yazılım ve ürünlerinin uygunluğuna karar vermek ve müelliflerini yetkilendirmek.

Bilgi toplama, işleme ve paylaşma yetkisi

MADDE 47- (1) **(Değişik: 12/7/2013-6495/73 md.)** Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel

bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıta ile toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması hâlinde görevlerini yapmalarına yetecek derecede paylaşabilir.

(3) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.

KAYNAKÇA

- [1] Intel, "Intel IT's Data Center Strategy for Business Transformation", IT@Intel White Paper, Ocak, 2014.
- [2] IBM, "Defining a Blue Print for Smart Data Center", IBM, 2012.
- [3] U. E. P. Agency, "Data Center Report to Congress," U.S. Environmental Protection Agency, Tech. Rep., 2007.
- [4] Microsoft, "Data Center Presentation", Mart 2014.
- [5] IBM, "Data center operational efficiency best practices", IBM, 2012.
- [6] IBM, "Data Center as an Innovation Engine Presentation", IBM, 2013.
- [7] ESG, "IT Spending Intentions Survey 2014", The Enterprise Strategy Group, Şubat 2014.
- [8] EMC, "Lead Your IT Transformation", EMC, 2013.
- [9] ESG, "EMC IT: Leading the Transformation", The Enterprise Strategy Group, Şubat 2013.
- [10] Dünya Bankası, "Bilişim ve Ekonomik Modernizasyon Raporu". Dünya Bankası Washington DC, Mart 1993.
- [11] Bilgi Toplumu Tarihçesi, Kalkınma Bakanlığı Bilgi Toplumu Daire Başkanlığı. www.bilgitoplumu.gov.tr
- [12] "Türkiye Ulusal Enformasyon Altyapısı Anaplanı Sonuç Raporu", Ulaştırma Bakanlığı, Ekim 1999.
- [13] TBD Kamu-BİB, "e-Devlet Üst Yapısı", Çalışma Gurubu Raporu, Mayıs 2010.
- [14] "e-Türkiye Girişimi Eylem Planı", Başbakanlık, Ağustos 2002.
- [15] "e-Devlet'e Geçiş Sürecinde KamuNet Çalışmaları", Başbakanlık Devlet Planlama Teşkilatı KamuNet Teknik Kurulu Başkanlığı, Kasım 2002.

- [16] TÜBİTAK, “BTYK’nın 25. Toplantısı (2013/104 sayılı karar)”, 2013
- [17] E. Pinheiro, W.-D. Weber, L. A. Barroso, “Failure Trends in a Large Disk Drive Population”, Proceedings of the 5th USENIX Conference on File and Storage Technologies, Şubat 2007
- [18] Intel, “Reducing Data Center Cost with an Air Economizer”, Intel Information Technology, Ağustos 2008
- [19] IDC, “IDC Unveils Worldwide Internet of Things Spending Forecast”, Vertical Market, Şubat 2014.