



2025 YILI
BİLGİ TEKNOLOJİLERİ DAİRE BAŞKANLIĞI
BİRİM İÇ DEĞERLENDİRME RAPORU

İÇİNDEKİLER

ÖZET	3
BİDR’NİN HAZIRLANMASINDA KATKISI OLANLAR.....	3
BİRİM HAKKINDA BİLGİLER	3
İletişim Bilgileri	3
Tarihsel Gelişimi	3
Misyonu, Vizyonu, Değerleri ve Hedefleri	4
Misyon	4
Vizyon.....	4
Değerler	4
Hedef	6
LİDERLİK, YÖNETİŞİM VE KALİTE.....	7
A.1. Liderlik ve Kalite.....	7
A.1.4. İç Kalite Güvencesi Mekanizmaları	7
A.1.5. Kamuoyunu Bilgilendirme ve Hesap Verebilirlik	8
A.2. Misyon ve Stratejik Amaçlar	9
A.2.2. Stratejik amaç ve hedefler.....	9
A.3. Yönetim Sistemleri.....	9
A.3.1. Bilgi Yönetim Sistemi.....	9
A.3.4. Süreç yönetimi	14
A.4. Paydaş Katılımı	15
A.4.1. İç ve dış paydaş katılımı	15
EĞİTİM VE ÖĞRETİM	15
B.3. Öğrenme Kaynakları ve Akademik Destek Hizmetleri	15
B.3.4. Dezavantajlı gruplar	21

ÖZET

Birim İç Değerlendirme Raporu (BİDR), Bilgi Teknolojileri Daire Başkanlığı'nın altyapısının ve süreçlerinin bir analizini sunmaktadır.

Raporun amacı, mevcut Bilgi Teknolojileri sistem altyapısını ve süreçlerini değerlendirmek, iyileştirme önerileri sunmak ve altyapının güvenliğini artırmak için yapılan iyileştirme alanları hakkında bilgi vermektedir. Bu raporun hazırlanması ile birim iç değerlendirme süreçleri ile Bilgi Teknolojileri hedeflerine uygun bir strateji geliştirilmesine katkı sağlamaktır.

BİDR raporu, Ankara Medipol Üniversitesi Bilgi Teknolojileri Daire Başkanlığı tarafından 2025 yılına kadar yapılan faaliyetleri ve iyileştirme çalışmalarını kapsamaktadır.

BİDR'İN HAZIRLANMASINDA KATKISI OLANLAR

Recep TOPRAK-Bilgi Teknolojileri Daire Başkanı

Şermin BEKTAŞ- Kurumsal Uygulamalar ve Yazılım Destek Ekip Lideri

BİRİM HAKKINDA BİLGİLER

İletişim Bilgileri

Bilgi Teknolojileri Daire Başkanı

Recep TOPRAK

Tel: 0312 508 8730

E-posta : recep.toprak@ankaramedipol.edu.tr

Tarihsel Gelişimi

- Bilgi Teknolojileri Daire Başkanlığı ISO 27001 Bilgi Güvenliği Sertifikasını almasının ardından 2025 yılında Bilgi Güvenliği Yönetim Sistemini günlük iş süreçlerine yerleştirilmesine ve sürdürülebilirliğini sağlamaya odaklanmıştır. Bu kapsamda erişim yönetimi, kullanıcı yetkilendirmeleri ve sistemsel değişiklikleri bilgi güvenliği yaklaşımıyla ele almaya odaklanmıştır.
- ISO 27001 kapsamında oluşturulan politikalar, prosedür ve uygulamaların aktif şekilde işletilmesine devam edilerek bilgi güvenliği yaklaşımının kurumsal yapının bir parçası haline gelmesini hedeflenmiştir.
- Bilgi güvenliği süreçleri, mevcut iş akışları ve kalite yönetimi anlayışı ile uyumlu şekilde yürütülmeye başlanmıştır.

- Bilgi Teknolojileri Daire Başkanlığı bünyesinde süreçlerin izlenmesi ve gerektiğinde iyileştirilmesine yönelik çalışmalar sürdürülmüştür.
- Yürütülen çalışmalar üniversitemizin bilgi varlıklarının korunması, veri gizliliğinin sağlanması ve kurumsal risklerin yönetilmesi konularındaki yaklaşımı güçlendirmiştir.

Misyonu, Vizyonu, Değerleri ve Hedefleri

Misyon

“Bilgi Teknolojileri Daire Başkanlığı olarak, kurumumuzun iş stratejilerini desteklemek amacıyla güvenilir, yenilikçi ve etkili bilgi teknolojileri hizmetleri sağlamayı taahhüt ediyoruz. Teknoloji standartlarını benimseyerek, sürekli iyileştirme anlayışıyla hareket ediyor ve çalışanlarımızın ve öğrencilerimizin bilgi teknolojileri alanındaki ihtiyaçlarına çözümler sunuyoruz. Güçlü bir ekip ruhu ile, bilgi teknolojileri aracılığıyla kurumun hedeflerine ulaşmasına katkıda bulunuyoruz.”

Vizyon

“Bilgi Teknolojileri Daire Başkanlığı olarak, teknolojik liderlikte öncü olmayı, sürekli olarak teknoloji çözümleri sunmayı ve organizasyon genelinde dijital bilişim sağlayacak noktaya ulaşmayı hedefliyoruz. Öğrenci memnuniyetini odak noktamız yaparak, yenilikçi projeler ve stratejiler geliştirerek kurumunuzun sürdürülebilir bir teknoloji altyapısı oluşturmak için çalışıyoruz. Ekip çalışmasına dayalı, sağlık ve eğitim bilişimi alanında kurumumuzun vizyonunu gerçekleştirmeyi taahhüt ediyoruz.”

Değerler

1. Verimlilik

Bilgi Teknolojileri, iş süreçlerini hızlandırarak zaman ve maliyet tasarrufu sağlamaktadır. Otomasyon ve dijitalleşme sayesinde manuel işlemler azalmakta, operasyonel verimlilik artmaktadır.

2. Erişilebilirlik

Bilgiye her yerden ve her zaman erişim imkânı sunarak kullanıcıların kesintisiz çalışma ve bilgiye ulaşım süreçlerini desteklemektedir.

3. Güvenlik

Verilerin korunmasını sağlamak amacıyla güçlü şifreleme, erişim kontrolü ve siber güvenlik önlemleri uygulanmaktadır. Yetkisiz erişimlerin önlenmesi ve veri bütünlüğünün sağlanması hedeflenmektedir.

4. İnovasyon

Yeni fikirlerin geliştirilmesini ve uygulanmasını destekleyen Bilgi Teknolojileri organizasyonların dijital dönüşüm süreçlerini hızlandırmaktadır.

5. Kesintisiz İletişim

Kişiler, cihazlar ve sistemler arasında kesintisiz iletişim sağlanarak bilgi akışı hızlandırılmakta ve operasyonel süreçler daha etkin yönetilmektedir.

6. Otomasyon

Tekrarlanan işlerin otomatizme edilerek insan hatasının azaltılması ve iş gücünün daha stratejik alanlara yönlendirilmesi sağlanmaktadır.

7. Esneklik

Farklı sektör ve ihtiyaçlara göre uyarlanabilir çözümler sunarak organizasyonların değişen koşullara hızlı bir şekilde adapte olmasını mümkün kılmaktadır.

8. Maliyet Tasarrufu

Bilgi Teknolojileri, dijitalleşme ile operasyonel giderleri düşürerek işletmelere uzun vadede maliyet avantajı sağlamaktadır.

9. Hızlı Karar Alma

Bilgi Teknolojileri Daire Başkanlığı olarak yönetmiş olduğumuz sistemleri uzaktan izleyerek ve alarm mekanizmasını oluşturularak hata oluştuğunda proaktif yaklaşarak hızlı çözüm sağlamaktadır.

10. İş Sürekliliği

Felaket kurtarma, veri yedekleme ve yüksek erişilebilirlik çözümleri ile iş süreçlerinin kesintisiz devamlılığı sağlanmaktadır.

11. Ölçeklenebilirlik

Bilgi Teknolojileri altyapıları, küçük işletmelerden büyük kuruluşlara kadar büyümeye uygun şekilde yapılandırılabilir.

12. Kullanıcı Deneyimi

Kullanıcı dostu dijital hizmetlerin etkinleştirilmesiyle çalışan memnuniyeti artırılmakta, daha iyi hizmet süreçleri oluşturulmaktadır.

13. Uzaktan Çalışma İmkânı

Hibrit ve uzaktan çalışma modellerini destekleyerek çalışanların esnek çalışma ortamlarına uyum sağlamalarına olanak tanımaktadır.

14. Çevresel Sürdürülebilirlik

Kâğıt tüketiminin azaltılması, enerji verimli sistemlerin kullanılması ve dijitalleşmenin artırılması ile çevresel etkilerin minimize edilmesi hedeflenmektedir.

15. Uyumluluk ve Regülasyonlar

Bilgi güvenliği ve sektör standartlarına uyum sağlanarak yasal düzenlemelere uygunluk temin edilmektedir.

16. Eğitim ve Öğrenme Kolaylığı

Online eğitim platformları ve uzaktan eğitim çözümleri ile bilgiye erişim kolaylaştırılmakta, çalışanların sürekli gelişimi desteklenmektedir.

Yukarıda belirtilen kalite değerleri, Bilgi Teknolojilerinin organizasyonlara sunduğu stratejik avantajları ve sürdürülebilir iş süreçleri oluşturmadaki rolünü ortaya koymaktadır.

Hedef

Bilgi Teknolojileri Daire Başkanlığı ISO 27001 Bilgi Güvenliği Sertifikasını almasının ardından 2025 yılında Bilgi Güvenliği Yönetim Sistemini günlük iş süreçlerine yerleştirilmesine ve sürdürülebilirliğini sağlamaya odaklanmıştır. Bu kapsamda erişim yönetimi, kullanıcı yetkilendirmeleri ve sistemsel değişiklikleri bilgi güvenliği yaklaşımıyla ele almaya odaklanmıştır.

Bilgi güvenliği politika ve süreçlerinin günlük operasyonlara daha etkin şekilde entegre edilmesi, risk temelli yaklaşımın kurumsal karar alma mekanizmalarında gözetilmesi önceliklerimiz arasında yer almaktadır.

Bilgi güvenliği veri koruma süreçlerinde sürekliliğin sağlanması, mevcut kontrollerin etkinliğinin korunması ve ihtiyaçlar doğrultusunda iyileştirilmesi hedeflenmektedir.

Dijitalleşme ve otomasyon çalışmalarının mevcut sistemlerle uyumlu ve güvenli şekilde yaygınlaştırılması, hizmet kalitesinin artırılması ve operasyonel süreçlerin daha verimli hale getirilmesi amaçlanmaktadır.

Kaynakların etkin kullanımı doğrultusunda mevcut altyapının izlenmesi, maliyet etkin çözümlerin değerlendirilmesi ve sistemler arası entegrasyonların güvenli biçimde sürdürülmesi hedeflenmektedir.

Yapılan çalışmalarla kurumumuzun bilgi güvenliği, iş sürekliliği ve dijital dönüşüm hedeflerine katkı sağlayan, güvenli ve sürdürülebilir bir bilişim altyapısının geliştirilmesine devam edilmesi amaçlanmaktadır.

LİDERLİK, YÖNETİŞİM VE KALİTE

A.1. Liderlik ve Kalite

A.1.4. İç Kalite Güvencesi Mekanizmaları

Bilgi Teknolojileri Kalite Temsilcisi, iç kalite güvencesi sisteminin sürdürülmesi ve geliştirilmesi süreçlerinde aktif rol almaktadır. 2024 yılında gerçekleştirilen Bilgi Güvenliği Farkındalık Eğitimi önceki rapor döneminde kayıt altına alınmıştır. 2025 yılı içerisinde ise bilgi güvenliği süreçlerine ilişkin farkındalığın artırılmasına yönelik bilgilendirmeler yapılmıştır.

[1_OD2]

Bu kapsamda, idari ve akademik personele yönelik bilgilendirme e-postalarının gönderilmesi ve süreçlere ilişkin toplantıların gerçekleştirilmesi planlanmıştır. Bilgi güvenliği kapsamında, e-posta güvenliğine yönelik anti-malware koruması, gelişmiş tehdit tespiti, zararlı bağlantıların engellenmesi ve veri güvenliğini destekleyen mekanizmalar hakkında personele daha sık bilgilendirme yapılması hedeflenmiştir. Söz konusu faaliyetlerin kayıt altına alınarak iç kalite güvencesi kapsamında izlenmesi amaçlanmıştır. [2_OD2][3_OD3][4_OD3]

Bilgi Teknolojileri Daire Başkanlığı'na ait web sitesinde yer alan Vizyon ve Misyon, Bilgi Güvenliği, BT Hizmet Yönetimi (ITSM), Anket Yönetimi (LimeSurvey), Öğrenci

Danışmanlığı (MEBİS), Livechat ve Elektronik Belge Yönetim Sistemi (EBYS) başlıkları önceki rapor döneminde oluşturulmuştur [\[OD3\]](#). 2025 yılı içerisinde söz konusu içeriklerin erişilebilirliğinin ve sürekliliğinin sağlanmasına yönelik izleme faaliyetleri yürütülmüş, mevcut yapı korunmuştur.

GLPI'nin ITSM (Information Technology Service Management) özellikleri, üniversitemizde BT hizmet taleplerinin etkin şekilde yönetilmesini sağlamaktadır. Öğrenci ve personelden MEBİS ve diğer BT hizmetlerine ilişkin gelen talepler, GLPI üzerinden kayıt altına alınarak izlenmektedir. **[5_OD3]**

2025 yılı içerisinde ITSM süreçleri kapsamında; e-posta ile iletilen taleplerin otomatik olarak sisteme yönlendirilmesi sağlanmış, talepler ekip içerisinde sınıflandırılarak ilgili personellere atanmıştır. Ayrıca istatistiksel takip mekanizmaları kullanılarak tekrarlayan talep ve sorun başlıkları analiz edilmiş, süreç iyileştirmelerine girdi oluşturacak değerlendirmeler yapılmıştır. GLPI sayesinde taleplerin anında kaydedilmesi, önceliklendirilmesi ve izlenmesi, öğrencilerin ve personellerin sorunlarına daha hızlı çözümler bulmamıza olanak sağlamaktadır. Bu sayede ITSM, kurum içindeki teknolojik hizmetleri etkili bir biçimde yöneterek kurumsal performansı artırmaktadır. [\[OD3\]](#)**[6_OD4]**

Olgunluk Düzeyi (4) Paydaş katılım mekanizmalarının işleyişi izlenmekte ve bağlı iyileştirmeler gerçekleştirilmektedir.

[1](2)A.1.4.egitim_ve_toplanti_takibi.pdf

[2](2)A.1.4.trendmicro_sandbox.pdf

[3](3)A.1.4.trendmicro_sandbox-1.pdf

[4](3)A.1.4.trendmicro_sandbox-2.pdf

[5](3)A.1.4.itsm_kullanim_kilavuzu.pdf

[6](4)A.1.4.itsm_takip_raporu.pdf

A.1.5. Kamuoyunu Bilgilendirme ve Hesap Verebilirlik

Web Sitesi Bilgilendirme Ankara Medipol Üniversitesi web sitesinde vizyonumuz, misyonumuz ve değerlerimize ilişkin bilgilendirme yapılmaktadır. [\[OD2\]](#)

Web sitesinde yer alan duyurular 06.05.2019 tarihinden itibaren yayınlanmaya başlanmış olup, toplamda 1136 adet duyuru bulunmaktadır. Bunlardan 4 tanesi arşivlenerek saklanmakta, 1132 tanesi ise yayınlanmaya devam etmektedir. Eposta bilgilendirme sistemi, kurumsal iç iletişimin etkin ve zamanında yürütülmesini sağlamak amacıyla kullanılmaya devam etmektedir. 2025

yılı içerisinde, kurum personelinin önemli duyuru ve bilgilere zamanında erişimini sağlamak amacıyla eposta sistemi aktif olarak kullanılmıştır. Bu kapsamda; etkinlik duyuruları, sistem güncellemeleri, politika ve süreç bilgilendirmeleri, toplantı davetleri ve eğitim odaklı içerikler belirlenen eposta listeleri aracılığıyla ilgili hedef kitlelere iletilmiştir. E-posta sistemi, iç haberleşmenin güçlendirilmesi, iş takibinin desteklenmesi ve kurumsal bilgilendirme süreçlerinin sürdürülebilirliğinin sağlanması amacıyla kullanılmaya devam etmektedir.

[1_OD3]

Olgunluk Düzeyi (4) Kurumun kamuoyunu bilgilendirme ve hesap verebilirlik mekanizmaları izlenmekte ve paydaş görüşleri doğrultusunda iyileştirilmektedir.

[1](3)A.1.5.mailing_bilgilendirme.pdf

A.2. Misyon ve Stratejik Amaçlar

A.2.2. Stratejik amaç ve hedefler

Ankara Medipol Üniversitesi'nin 2026-2030 Stratejik Planı'nda yer alan kurumsal kapasitenin, altyapının ve kalite süreçlerinin güçlendirilmesi hedefleri doğrultusunda, Bilgi Teknolojileri birimi olarak dijital altyapının etkin yönetimi ve sürdürülebilirliğini sağlamaya yönelik çalışmalarımız planlı ve sistematik bir şekilde yürütülmektedir.

A.3. Yönetim Sistemleri

A.3.1. Bilgi Yönetim Sistemi

Bilgi yönetimi, kurumun tüm verilerinin toplanması, işlenmesi, depolanması ve dağıtılması süreçlerini kapsar. Bu süreçte kurum kaynakları dış ve iç tehditlere karşı korunarak güvenli bir şekilde yönetilmesi planlanmaktadır. Bilgi güvenliği verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için kritik bir öneme sahiptir. Bu bağlamda, sunucu güvenliği için yazılım ve donanımsal koruma önlemleri alınmıştır.

Kurumun ihtiyaçları doğrultusunda seçilen Trend Micro Deep Security güvenlik yazılımı, önceki yıllarda olduğu gibi bu raporlama döneminde de aktif olarak kullanılmaya devam etmektedir. Yazılım, daha önce tanımlanan yapılandırma ve etkinleştirilen modüller ile çalışmasını sürdürmektedir.

- Web İtibarı Modülü, kritik verilerin korunması amacıyla zararlı ve sahte web sitelerine erişimi engellemektedir. **[1_OD3]**
- Uygulama Kontrolü Modülü, yetkisiz yazılım yüklemelerini ve sistem yöneticisi dışındaki değişiklikleri engelleyerek güvenliği artırmaktadır. **[2_OD3]**.

- Bütünlük İzleme Modülü, Windows ve Linux tabanlı sunucularda dosya bütünlüğünü izlemekte, yetkisiz değişiklikler için uyarılar üretmektedir. [3_OD3]
- İzinsiz Giriş Önleme Modülü ise sunuculara yönelik saldırıları tespit ederek hizmet sürekliliğini tehdit edebilecek girişimleri engellemektedir. [4_OD3]

Trend Micro Apex One (Uç Nokta Güvenliği) çözümü, 2025 yılında da sunucu sistemleri ve son kullanıcı cihazlarında kullanılmaya devam etmektedir. Söz konusu sistem, kötü amaçlı yazılım, casus yazılım ve Truva atı türü tehditlere karşı koruma sağlayarak hizmet sürekliliğini desteklemektedir. [5_OD4]

Mevcut raporlama döneminde, Apex Central yönetim konsolu üzerinden son kullanıcıların zafiyet tespit edilmiş uygulamaları kullanmaları engellenmiş olup uç nokta güvenliği ek kontrollerle güçlendirilmiştir. [6_OD3]

2025 yılında Trend Micro Deep Discovery (Ağ Güvenliği) çözümü kullanılmaya devam etmektedir. Sistem, kötü amaçlı yazılımların tespit edilmesi ve tehdit istihbaratının diğer güvenlik katmanlarıyla paylaşılması işlevlerini aynı şekilde sürdürmektedir. Ön filtreleme teknolojisi ile ağ gecikmelerinin önüne geçilmektedir. Ek genişletilmiş algılama ve yanıt (XDR) yetenekleri ile tehditlerin tespit ve engellenmesi sağlanmaktadır. [7_OD3][8_OD3]

2025 yılında kurum ağ güvenliği mimarimiz kapsamında FortiGate güvenlik duvarı cihazı aktif olarak kullanılmaya devam etmektedir. FortiGate cihazı, sunuculara gelen ve giden trafiği izleyerek yalnızca belirlenen güvenilir kaynaklardan erişime izin vermekte, yetkisiz tüm erişim taleplerini engellemektedir. Ayrıca VIP (Virtual IP) yapılandırması sayesinde dış ağdan gelen trafik kontrollü şekilde iç ağdaki ilgili sunuculara yönlendirilmektedir. Cloudflare üzerinden gelen trafik, FortiGate cihazı üzerindeki VIP tanımları aracılığıyla iç sistemlere aktarılmakta ve bu süreç güvenlik politikaları çerçevesinde yönetilmektedir. [9_OD3]

2025 yılı itibarıyla, yapılan iyileştirmelerle DDoS (Dağıtık Hizmet Engelleme) saldırılarına karşı koruma mekanizmaları da geliştirilmiştir. Önceki yıllarda yalnızca ağ seviyesindeki (Layer 3/4) koruma kullanılırken, bu yıl uygulama katmanı (Layer 7) koruma modeli devreye alınmıştır. Böylece HTTP/HTTPS tabanlı uygulama odaklı saldırılar analiz edilerek anomali tespiti yapılmakta ve kötü niyetli istekler, hizmet sürekliliğini etkilemeden dinamik olarak engellenmektedir.

Aynı kapsamda, SSL sertifikalarının yönetimi de merkezi FortiGate cihazı üzerinden SSL Offload sistemi ile gerçekleştirilmeye başlanmış, böylece sertifika yükleme ve yönetim süreçleri basitleştirilmiş ve operasyonel verimlilik artırılmıştır. Bu yenilikler, geçen yıl raporlanan altyapı ve güvenlik süreçlerinin üzerine yapılan geliştirmelerin bir parçasıdır.

[10_OD4]

Güvenlik Bilgisi ve Olay Yönetimi (SIEM) kapsamında kullanılan Günlük İnceleme Modülü, kurumumuzun güvenlik altyapısını izlemek, tehditleri tespit etmek ve bu tehditlere karşı zamanında müdahale etmek için 2025 yılında da etkin bir şekilde görev yapmaktadır. Günlük İnceleme Modülü, sunucularda meydana gelen tüm olayları kaydeden günlük dosyalarını düzenli olarak analiz etmektedir. Özellikle güvenlik açısından kritik veriler sürekli izlenmekte ve potansiyel tehditler karşısında uyarılar üretilmektedir. İzlenen günlüklerde belirli bir olay veya anomali tespit edildiğinde, önleyici aksiyonları tetiklemek amacıyla uyarılar gönderilmektedir. Bu uyarılar, güvenlik ekibinin hızlı bir şekilde müdahale etmesini sağlamaktadır. Örneğin, bir sunucuya yapılan yetkisiz giriş denemelerinin sayısı belirlenen eşiği aştığında sistem otomatik uyarı oluşturmaktadır. [11_OD4]

Uyarı Türleri

- **Yetkisiz Giriş Denemeleri:** Birden fazla başarısız giriş denemesi potansiyel bir saldırı girişimini gösterebilir. Güvenlik ekibine derhal uyarı gönderilmektedir.
 - **Kritik Yapılandırma Değişiklikleri:** Sistem yöneticisi dışında yapılan değişiklikler sunucu güvenliğini tehdit edebilir; tespit edilip uyarı oluşturulmaktadır.
 - **Hata Mesajları:** Sunucularda meydana gelen sistem hataları veya yapılandırma problemleri, güvenlik zafiyetlerine yol açabilir; izlenerek gerekli müdahale yapılmaktadır.
- 2025 yılında, 2024 yılı BİDR raporunda belirtilen değerlendirmeler dikkate alınarak modülün etkinliği sürdürülmektedir.

Bilginin elde edilmesi, kaydedilmesi, güncellenmesi ve paylaşılmasına ilişkin tanımlı süreçler Varlık Envanteri Sayımı [12_OD3] kurumda bulunan tüm dijital varlıkların (sunucular, ağ cihazları, yazılımlar, donanımlar vb.) düzenli olarak sayılmasını ve takip edilmesini sağlayan kritik bir güvenlik prosedürüdür. Bu süreç, bilgi güvenliği yönetimi açısından önemli bir adımdır. Mevcut varlıkların tam listesine sahip olmak, güvenlik açıklarını tespit etmek ve siber saldırılara karşı hazırlıklı olmak için gereklidir. Varlık envanteri sayımı, kurumda yer alan tüm cihazlar ve yazılımlar üzerine yapılan taramalarla gerçekleştirilir. Bu sayede, her bir varlığın

durumu, özellikleri ve güvenlik durumu hakkında bilgi edinilmektedir. Envanter listesi, sürekli olarak güncellenir ve herhangi bir kayıp, değişiklik ya da yeni eklenen varlıklar raporlanır.

Bilgi güvenliği ve güvenilirliğini sağlamaya yönelik süreçler ve uygulamalar kapsamında, kurumumuz belirli dönemlerde kurum içi ve kurum dışı, sahip olduğu tüm sistemlerin ve bilgilerin kötü amaçlı kişi/kişilerin erişiminden kaynaklı kaybolması veya zarar görmesinden korumak amacıyla zafiyet sızma testleri yaptırmaktayız. Sızma Testi Raporu [13_OD3] Test sırasında, kurumun sistemleri üzerinde gerçekçi saldırı senaryoları simüle edilerek, zafiyetler tespit edilmeye çalışılır ve sızma testi raporu hazırlanır. Bu rapor, testin kapsamını, tespit edilen açıkları ve bu açıkları gidermek için alınması gereken aksiyonları içerir.

Kurum içindeki süreçlere yönelik geliştirdiği uygulamaları 2025 yılında da kullanmaya devam etmektedir. Kurum içi yazışmalar için EBYS [OD3], eğitim-öğretim faaliyetleri için MEBİS otomasyonu [OD3] ve Sürekli Eğitim Merkezi Yönetim Sistemi [OD3], dijitalleşme kapsamında sınav süreçleri için **E-Sınav Plan (Moodle Aktarım)** E-Sınav Plan Yazılımı üzerinde yapılan geliştirmeler kapsamında, görevlilerimizin sisteme yükledikleri sorular PDF formatına dönüştürülerek çıktı alınabilmekte ve yüz yüze sınavlarda kullanılabilir. [14_OD3] [15_OD3] [16_OD3] Öğrencilere yönelik **Anket Yönetimi (LimeSurvey)** [OD4] Sistemi kurumumuza ait sunucular üzerinde barındırılmakta olup, arayüz tasarımı ihtiyaçlar doğrultusunda birimimiz tarafından revize edilmiştir. Ayrıca LiveChat [OD3] ve Yurt Bilgi Sistemi [17_OD3] uygulamaları üzerinden öğrencilere yönelik hizmetler sürdürülmektedir.

Kurum içi izleme ve takip süreçleri için Digital Signage-RubuPlus [18_OD3], RoomScope Oda Yerleşim ve Takip Yazılımı [19_OD3], CCTV Kamera NVR Takip Sistemi [20_OD3], Personel Devam Kontrol Sistemi (PDKS) [21_OD3], Yemekhane Kartlı Geçiş Sistemi [22_OD3] ve Plaka Okuma Sistemi (PTS) [23_OD3] kullanılmaya devam edilmekte olup, bu sistemler aracılığıyla süreçler dijital ortamda izlenmektedir. [24_OD3]

Kurum içi dersliklerde karşılaşılabilecek sorunlara hızlı çözüm sunabilmek amacıyla her dersliğe kare kod ile entegre edilmiş bir WhatsApp destek hattı oluşturulmuştur. Akademisyenlerimiz ve öğrencilerimiz, karşılaştıkları herhangi bir sorun ile ilgili olarak bu destek hattı üzerinden başvuruda bulunmakta; saha destek ekibimiz tarafından anlık olarak destek sağlanmaktadır. Sistem, bu kapsamda 2025 yılında da kullanılmaya devam etmektedir. [25_OD3]

Infra Alert Yazılımı yazılım ile sistem ve ağ (network) altyapısına ait bilgiler merkezi olarak izlenmektedir. Yazılım üzerinden altyapı bileşenlerinin durumu takip edilmekte, düzenli sağlık

kontrolleri (health check) yapılmakta ve ihtiyaç duyulan durumlarda gerekli işlemler uygulanmaktadır. [26_OD3]

Mezun Bilgi Sistemi Mezun Bilgi Sistemi; Ankara ve İstanbul yerleşkeleri özelinde mezunlara ait bilgilerin merkezi, sistematik ve sürdürülebilir bir yapıda yönetilmesini sağlayan stratejik bir kurumsal altyapıdır. Sistem aracılığıyla mezunların eğitim geçmişi, iletişim bilgileri ve istihdam durumları düzenli olarak güncellenmekte ve izlenmektedir.

Ayrıca sistem üzerinden duyuru, anket ve veri toplama süreçleri etkin bir şekilde yürütülmekte; elde edilen veriler kurumsal izleme, değerlendirme ve raporlama çalışmalarında kullanılmaktadır.

Mezun Bilgi Sistemi, mezunlarla kurumsal bağın güçlendirilmesi, mezun başarılarının izlenmesi, program çıktılarının değerlendirilmesi ve sürekli iyileştirme süreçlerinin desteklenmesi açısından kalite güvence sisteminin önemli ve vazgeçilmez bir bileşenidir. [27_OD3]

KBYS – Kalite Bilgi Yönetim Sistemi üniversitemize ait kurumsal verilerin merkezi bir yapıda toplandığı, analiz edildiği ve raporlandığı bütünlük bir bilgi yönetim sistemidir. Sistem, kalite güvence süreçlerinin etkin, izlenebilir ve sürdürülebilir bir şekilde yürütülmesini desteklemek amacıyla tasarlanmıştır.

KBYS aracılığıyla akademik ve idari birimlere ait performans göstergeleri, faaliyet raporları, stratejik plan verileri, iç değerlendirme çıktıları ve kanıt dokümanları sistematik olarak kayıt altına alınmaktadır. Böylece veriye dayalı karar alma mekanizmaları güçlendirilmekte ve süreç yönetiminde şeffaflık sağlanmaktadır.

Sistem, kalite süreçlerinin planlama, uygulama, kontrol etme ve önlem alma (PUKÖ) döngüsü çerçevesinde düzenli olarak izlenmesine imkân tanımakta; iç ve dış değerlendirme süreçlerinde ihtiyaç duyulan rapor ve kanıtların hızlı ve güvenilir şekilde temin edilmesini sağlamaktadır.

KBYS, kurumsal hafızanın oluşturulması, süreçlerin standardizasyonu ve sürekli iyileştirme kültürünün yaygınlaştırılması açısından kalite güvence sisteminin temel ve stratejik bileşenlerinden biridir.

[28_OD3]

Olgunluk Düzeyi (3) Kurum genelinde temel süreçleri (eğitim ve öğretim, araştırma ve geliştirme, toplumsal katkı, kalite güvencesi) destekleyen entegre bilgi yönetim sistemi işletilmektedir.

[1](3)A.3.1. web_itibari.pdf

[2](3)A.3.1.uygulama_kontrolu.pdf

[3](3)A.3.1.butunluk_izleme.pdf

[4](3)A.3.1. izinsiz_girisi_onleme.pdf

[5](4)A.3.1. trendmicro_apexone(uc_nokta_guvenligi).pdf

[6](3)A.3.1.apex_central.pdf
[7](3)A.3.1.trendmicro_deep_discovery.pdf
[8](3)A.3.1. trendmicro_deep_discovery(ag_guvenligi).pdf
[9](3)A.3.1. guvenlik_duvari_(firewall).pdf
[10](4)A.3.1.ddos.pdf
[11](4)A.3.1. guvenlik_bilgisi_ve_olay_yonetimi_(siem).pdf
[12](3)A.3.1. varlik_envanteri_sayimi.pdf
[13](3)A.3.1. sizma_testi_raporu.pdf
[14](3)A.3.1. e-sinav_plan_(moodle_aktarim).pdf
[15](3)A.3.1. e-sinav_plan_(moodle_aktarim)-1.pdf
[16](3)A.3.1. e-sinav_plan_(moodle_aktarim)-2.pdf
[17](3)A.3.1.yurt_bilgi_sistemi.pdf
[18](3)A.3.1.digital signage_rubuplus.pdf
[19](3)A.3.1.roomscope_oda_plani.pdf
[20](3)A.3.1.cctv_kamera_nvr_takip_sistemi.pdf
[21](3)A.3.1.personel_devam_kontrol_sistemi_(pdks).pdf
[22](3)A.3.1.yemekhane_kartlı_geçiş_sistemi.pdf
[23](3)A.3.1. plaka_okuma_sistemi (pts).pdf
[24](3)A.3.1.yazilimler.pdf
[25](3)A.3.1. whatsapp_destek_hatti.pdf
[26](3)A.3.1. infraa_alert_yazilimi.pdf
[27](3)A.3.1.mezun_bilgi_sistemi.pdf
[28](3)A.3.1. kalite_bilgi_yonetim_sistemi.pdf

A.3.4. Süreç yönetimi

BT Hizmet Yönetimi (ITSM) (Information Technology Service Management) sistemi, Ankara Medipol Üniversitesinde görev yapan akademik ve idari personel ile öğrencilerin yaşadıkları sorunların kaydedilmesi, takibi ve çözüm süreçlerinin yönetilmesi amacıyla kullanılmaktadır. Sistem, bu kapsamda 2025 yılında da kullanılmaya devam etmektedir. [\[OD4\]](#)

BioPro (Teknik Bakım) sistemi, Bilgi Teknolojileri Daire Başkanlığı'na ait ürünlerin depo giriş ve çıkış süreçlerinin takibini sağlamaktadır. Depodan çıkan sarf malzemeler, barkodlama sistemi ile üniversitemizde teslim edilecek ve kurulacak ürünlerimizin lokasyonlarına göre izlenebilir hale getirilmektedir. Talep üzerine teslim edilen ürünler ilgili kişilere zimmetlenmekte ve bu bilgiler sistem üzerinde kaydedilmektedir. Zimmet kayıtları, yalnızca

elektronik ortamda tutulmakla birlikte, aynı zamanda fiziki olarak dosyalanarak birimimizde arşivlenmektedir.

Bu kapsamda, 2024 yılı BİDR raporumuzda belirtilen uygulamalar bu yıl da değişiklik göstermemiştir. [\[OD3\]](#)

Olgunluk Düzeyi (3) Kurumun genelinde tanımlı süreçler yönetilmektedir.

A.4. Paydaş Katılımı

A.4.1. İç ve dış paydaş katılımı

Bilgi Teknolojileri Daire Başkanlığı'nın iç ve dış paydaşları bulunmaktadır. Üniversite paydaşları olan öğrenci, akademik ve idari personelin talep, istek ve şikayetlerini bildirebilecekleri bir yapı mevcuttur. Bu talepler Bilgi Yönetim Sistemi olan BT Hizmet Yönetimi (ITSM) uygulaması [\[1_OD4\]](#), MEBİS arabirimi [\[2_OD3\]](#), mobil uygulama [\[3_OD3\]](#), birimlere ait destek e-posta adresleri ve çağrı merkezi telefonu üzerinden iletilebilmektedir. Bildirilen istek veya arıza talepleri ilgili birimlere direkt olarak aktarılmakta, verilen cevaplar ve sunulan çözümler kayıt altına alınmaktadır. Alınan raporlarla verilen destek hizmetleri takip edilmekte ve iyileştirme yapılabilecek noktaların tespiti için birimlerde incelenmektedir.

Geçen yılki BİDR raporunda belirtildiği üzere, bu uygulamalar ve süreçler bu yıl da aynı şekilde devam etmektedir.

Olgunluk Düzeyi (4) Paydaş katılım mekanizmalarının işleyişi izlenmekte ve bağlı iyileştirmeler gerçekleştirilmektedir.

[\[1\]\(4\)A.4.1.mail_talep.pdf](#)

[\[2\]\(3\)A.4.1.mebis_talep.pdf](#)

[\[3\]\(3\)A.4.1.mobil_talep.pdf](#)

EĞİTİM VE ÖĞRETİM

B.3. Öğrenme Kaynakları ve Akademik Destek Hizmetleri

B.3.3. Tesis ve Altyapılar

Bulut Veri Depolama Projesi, İnternet üzerinden erişilebilen ve çeşitli veri depolama hizmetlerini sunan bir projedir. Bu proje, kullanıcıların verilerini güvenli bir şekilde saklamalarını, yedeklemelerini ve paylaşımlarını sağlar. Büyük bulut veri depolama

sağlayıcıları genellikle sunucu altyapısını yönetir ve kullanıcılara geniş depolama alanı ve diğer ilgili hizmetleri sunar. Bulut Veri Depolama ile dosya paylaşımlarının web arayüzünden yapılabilmesi hedeflenmiştir. "cloud.ankaramedipol.edu.tr" web arayüzü üzerinden dosya paylaşımları, güncel olarak SMB 2.0 ve 3.0 protokolleri kullanılarak devam etmektedir. 2024 yılı BİDR raporunda belirtildiği üzere, proje bu yıl da aynı şekilde devam etmektedir.

[1_OD3]

Trend Micro Deep Security Sunucu Güvenliği Projesi, sunuculara kullanım amacı dışında erişimlerin kısıtlanması, güvenlik açıklarının kapatılması ve zararlı yazılımların tespit edilerek engellenmesini hedeflemektedir. Bilgi güvenliği açısından kritik olan sunucuların güvenliğini sağlamak, düzgün çalışmalarını ve verimliliklerini korumak açısından önemlidir. Linux ve Windows işletim sistemleri için ayrı ayrı belirlenen güvenlik kuralları, gerçek zamanlı ve manuel tarama planlarıyla uygulanmaktadır ve kurum içindeki tüm sunucular için güncel olarak bu kurallar yürürlükte. **[2_OD3]**

2025 yılında da proje aynı şekilde devam etmektedir. Zabbix, üniversitemiz bünyesinde bulunan sunucu, ağ cihazları, sanal altyapılar ve uygulamaların performans, erişilebilirlik ve kaynak kullanım durumlarının merkezi olarak izlenmesini sağlayan açık kaynak kodlu bir izleme ve alarm yazılımıdır. Sistem üzerinden CPU, bellek, disk, ağ trafiği ve servis durumları anlık olarak takip edilmekte; belirlenen eşik değerlerin aşılması durumunda ilgili birimlere otomatik uyarılar iletilmektedir. Zabbix izleme altyapısı 7.0.5 LTS sürümü ile çalıştırılmış olup, güvenlik ve sürdürülebilirlik planlamaları kapsamında 2026 yılı itibarıyla 8.0.0 sürümüne geçiş tamamlanmıştır. BT altyapımızda kullanılan izleme sistemi en güncel stabil versiyonuna yükseltilmiş; bu güncelleme ile birlikte performans iyileştirmeleri, gelişmiş dashboard yapısı, daha detaylı alarm yönetimi ve güncel güvenlik iyileştirmeleri devreye alınmıştır. Yeni versiyon sayesinde sunucu, servis ve ağ izleme süreçleri daha stabil, hızlı ve güvenli şekilde yürütülmekte olup, gerçekleştirilen bu çalışma sistem sürekliliğini ve proaktif izleme kabiliyetimizi artırmıştır. **[3_OD4]**

Trend Micro Apex One Son Kullanıcı Bilgisayarı Güvenliği Projesi, kullanım amacı dışında erişimlerin kısıtlanması, güvenlik açıklarının kapatılması ve zararlı yazılımların tespit edilerek engellenmesini hedeflemektedir. Üniversite genelinde kullanıcı bilgisayarlarına yüklenen Apex One ajanları güncel tutulmakta ve haftalık otomatik taramalar ile eski sürümler

güncellenmektedir. Bu yıl yapılan güncelleme ile zaafiyet içeren uygulamalar engellenmiştir. Proje, 2025 yılında aynı şekilde devam etmektedir. [4_OD4][5_OD4]

Kaynak Planlama Uygulaması Veri Tabanı Yenileme Projesi, kalite süreçlerimiz kapsamında belirlenen hedefler doğrultusunda yürütülmekte olup, veri tabanının sürekli ve kesintisiz erişilebilir olması sağlanmaktadır. Sürekli Erişilebilirlik kapsamında MEBİS uygulamasına ait veri tabanı “Always On” prensibi ile çalışmakta, yüksek erişilebilirlik altyapısı sayesinde birincil sunucuda yaşanabilecek problemlerde veri tabanı erişimi otomatik olarak ikincil sunucuya devredilmekte ve hizmet sürekliliği temin edilmektedir. [6_OD3]

Web sitesi veri tabanı sunucusunda yapılan güncellemeler ve değişiklikler sırasında web sitelerinin kesintisiz erişilebilirliği hedeflenmişti. Bu doğrultuda, kurum içi web siteleri için veri tabanı kurulumu yapılmış, yüksek erişilebilirlik sağlanmış ve birincil sunucuda yaşanacak problemlerde veri tabanı erişimi ikincil sunucuya otomatik olarak devredilerek veri kaybı önlenmiştir. 2024 yılı itibarıyla geçiş süreci tamamlanmış, senkronizasyon problemleri giderilmiş ve veri bütünlüğü sağlanmıştır. Proje 2025 yılında da aynı şekilde devam etmektedir. [7_OD3]

Veeam Yedekleme Yenileme Projesi kapsamında sunucu yedeklemeleri günlük olarak alınmakta ve sistem yönetimi ekibi, sunucuların aktif hale getirilememesi durumunda yedekten hızlı bir şekilde kurtarma işlemini sağlamaktadır. Sunucu yedekleri ana sistemden bağımsız veri depolama alanlarına taşınmış, proxy sunucular ile yük dağılımı sağlanmış ve yedekleme performansı optimize edilmiştir. Proje 2025 yılında da aynı şekilde devam etmektedir. [8_OD3]

Veeam Yedekleme Bulut Depolama Projesi kapsamında, kritik uygulama verileri ve veri tabanı yedekleri, kurum veri merkezinden bağımsız bir veri merkezinde tutulmakta ve haftalık yedekleme ile felaket kurtarma senaryosuna dahil edilmektedir. 2024 yılı BİDR raporunda belirtildiği üzere, proje 2025 yılında da aynı şekilde devam etmektedir.

[9_OD3]

İnternet hızı, geçen yılki BİDR raporunda belirtildiği üzere 2025 yılında da aynı şekilde devam etmektedir. [10_OD3]

Kız ve Erkek Konukevi ile Kampüs kablosuz ağ altyapısının iyileştirmesi kapsamında mevcut Access Point'lerin (AP) fiziksel konumları yeniden düzenlenmiş, kanal (MHz) ve çıkış gücü ayarları optimize edilerek kapsama alanı artırılmış ve kanal çakışmaları önemli ölçüde azaltılmıştır. Bu düzenlemeler sonucunda kullanıcı yoğunluğu dengelenmiş, bağlantı kararlılığı yükselmiş ve genel Wi-Fi performansı iyileştirilmiştir.

[11_OD3]

Personel Takip Sistemi (PDKS), 2024 yılı BİDR raporunda belirtildiği üzere, 2025 yılında da aynı şekilde devam etmektedir. **[12_OD2]**

2024 yılı BİDR raporunda belirtilen yapıya ilişkin herhangi bir değişiklik yapılmamış olup mevcut uygulama aynı şekilde sürdürülmektedir. Aktif Dizin ortamında bulunan sunucuların iç güvenlik duvarları, DeepSecurity çözümü aracılığıyla aktif olarak çalıştırılmakta ve güvenlik önlemleri etkin biçimde uygulanmaktadır. Özellikle Aktif Dizin sunucularında uygulanan güvenlik kontrolleri, her bir bilgisayar ve/veya servis grubu bazında merkezi olarak yönetilen politika kuralları aracılığıyla sağlanmaktadır. Yerel güvenlik duvarının kullanım amacı; dış ağlardan gelen bağlantıları filtreleyerek yalnızca tanımlı ve yetkilendirilmiş kurallar doğrultusunda erişime izin vermektir (Örnek: Web sunucularına yönelik oluşturulan kurallar kapsamında sadece ilgili web portları (80 ve 443) üzerinden erişim sağlanmaktadır). Bununla birlikte, sunucuların kullanım amacına bağlı olarak, merkezi güvenlik politika kurallarına ek olarak DeepSecurity üzerinde sunucu bazlı (tekil) güvenlik duvarı kuralları da tanımlanmıştır. 2025 yılında değişiklik yapılmamış olup mevcut uygulama düzenlenerek sürdürülmektedir.

[13_OD3]

DNS sorgularının yönetimi kapsamında, kurum dış IP adresine doğrudan yönlendirme yerine Cloudflare WAF altyapısı kullanılmakta olup IP gizlemesi sağlanmakta ve web uygulamalarına yönelik saldırılara karşı koruma sağlanmaktadır. 2025 yılında da belirtilen yapıya ilişkin herhangi bir değişiklik yapılmamış olup mevcut uygulama düzenlenerek sürdürülmektedir.

[14_OD3]

Medipol Eğitim Bilgi Sistemi (mebis.ankaramedipol.edu.tr); öğrenci ve personelin kayıt, ders, not, izin vb. işlemleri gerçekleştirdiği web tabanlı uygulamasıdır. Kurumun en yoğun erişim alan sistemlerinden biri olması sebebiyle, kesintisiz ve sağlıklı erişim altyapısının sağlanmasına yönelik gerekli teknik önlemler uygulanmaktadır. İlgili sistem için Load Balancing servisi

Cloudflare üzerinde yapılandırılmıştır. Kuruma ait iki ayrı internet servis sağlayıcısı üzerinden sağlanan bağlantı yapısı sayesinde, hatlardan birinde yoğunluk veya kesinti yaşanması durumunda diğer hat devreye alınarak hizmet sürekliliği sağlanmaktadır.

Ayrıca, belirtilen iki internet hattı için ayrı ayrı NAT IP (sunucunun dış dünyadan erişimini sağlayan dış IP adresi) tanımlamaları yapılmış olup, bu yapı kesintisiz erişim ve güvenli bağlantı altyapısını desteklemektedir. **[15_OD4]**

2025 yılı itibariyle, mevcutta kullanılan iki adet FortiGate 600E cihazı ile devam edilmektedir ve firewall lisansları 3 yıllık olarak yenilenmiştir. Yenilenen lisans kapsamında güvenlik servisleri güncel tutulmakta, ağ trafiği ise FortiAnalyzer üzerinden izlenerek kayıt altına alınmaktadır. **[16_OD4]**

2025 yılı itibariyle, Merkezi Log Yönetimi (SIEM) çözümü kapsamında herhangi bir değişiklik yapılmamış olup, 2024 yılı BİDR raporunda belirtildiği şekilde süreçler aynı yapıda devam etmektedir.

Merkezi log yönetimi ve danışmanlık hizmeti NSC iş birliği ile sürdürülmekte olup, log toplama ve korelasyon süreçlerinde Wazuh çözümü aktif olarak kullanılmaya devam etmektedir. **[17_OD3] [18_OD3] [19_OD3] [20_OD3] [21_OD3]**

2025 yılı itibariyle, eposta hesapları lisans optimizasyonu süreci herhangi bir değişiklik olmaksızın devam etmektedir.

Üniversitemiz ile ilişkisi kesilen ve Active Directory hesapları kapatılmış olan akademik ve idari personel, ücretli lisans gruplarından otomatik olarak çıkarılmakta ve Office 365 A1 lisansı atanmaktadır.

Ayrıca, Word, Excel ve benzeri Office uygulamalarını aktif olarak kullanmayan geçici görevlendirmeli akademik personel için de lisans optimizasyonu uygulaması sürdürülmekte olup, ilgili kullanıcılar lisans gruplarından çıkarılarak Office 365 A1 lisansına geçirilmektedir. 2025 yılı itibariyle, Microsoft Office 365 Çok Faktörlü Kimlik Doğrulama (MFA) uygulamasında herhangi bir değişiklik yapılmamış olup, 2024 yılında belirlenen politika doğrultusunda devam etmektedir.

Üniversitemizde bulunan öğrenci, akademisyen ve idari personelin Office 365 sistemlerine girişlerinde çok faktörlü kimlik doğrulama zorunlu olarak uygulanmaya devam etmekte ve kullanıcı hesaplarının güvenliği sağlanmaktadır. **[22_OD3]**

2025 yılı itibarıyla Single Sign-on (SSO) uygulamasında herhangi bir değişiklik yapılmamış olup, 2024 yılında belirlenen yapı ve entegrasyon politikası doğrultusunda sürdürülmektedir. Öğrenci, akademisyen ve personelin MEBİS sistemine erişiminde Active Directory ve Office 365 entegrasyonu devam etmekte; kullanıcıların tek kullanıcı adı ve şifre ile üniversite kaynaklarına güvenli erişimi sağlanmaktadır. [23_OD3]

2025 yılı itibarıyla SD-WAN (Yazılım Tabanlı Geniş Alan Ağı) Projesi kapsamında herhangi bir değişiklik yapılmamış olup, bir 2024 yılında oluşturulan yapı doğrultusunda uygulamaya devam edilmektedir. Türk Telekom ve Superonline internet erişim hatları üzerinden sağlanan yedekli yapı sürdürülmekte; hatlardan birinde kesinti yaşanması durumunda kurum internet erişimi diğer operatör üzerinden kesintisiz olarak sağlanmaktadır. [24_OD3]

MEBİS altyapısında servislerin sürekliliğini ve yüksek erişilebilirliğini sağlamak amacıyla Consul kullanılmaktadır. Consul sayesinde servis keşfi (service discovery) ve düzenli sağlık kontrolleri (health check) yapılmakta, çalışmayan servisler otomatik olarak sistem trafiğinden çıkarılmaktadır. Bu yapı sayesinde kesinti riski azaltılmakta ve sistemin kesintisiz, güvenilir şekilde çalışması sağlanmaktadır. [25_OD3]

Olgunluk Düzeyi (4) Tesis ve altyapının kullanımı izlenmekte ve ihtiyaçlar doğrultusunda iyileştirilmektedir

[1](3)B.3.3.bulut_veri_depolama_projesi.pdf

[2](3)B.3.3.trend_micro_deep_security_sunucu_guvenligi_projesi.pdf

[3](4)B.3.3.zabbix_sistem_izleme_projesi.pdf

[4](4)B 3.3.trend_micro_apex_one_son_kullanici_bilgisayari_guvenligi_projesi.pdf

[5](4)B.3.3.trend_micro_apex_one_son_kullanici_bilgisayari_guvenligi_projesi-1.pdf

[6](3)B.3.3.kaynak_planlama_uygulamasi_veri_tabani_yenileme_projesi.pdf

[7](3)B.3.3.web_sitesi_veri_tabani_yenileme_projesi.pdf

[8](3)B.3.3.veeam_yedekleme_yenileme_projesi.pdf

[9](3)B.3.3.veeam_yedekleme_bulut_depolama_projesi.pdf

[10](3)B.3.3.(i. internet_hizi_artirimi).pdf

[11](3)B.3.3.kiz_erkek_konukevi_ap_calismasi.pdf

[12](2)B.3.3.personel_takip_sistemi_(pdks).pdf

[13](3)B.3.3.(c. deepsec).pdf

[14](3)B.3.3. internete_acik_olan_sistemlerin_waf_uzerinden_calistirilmesi.pdf

[15](4)B.3.3.cloudflare_load_balance.pdf

[16](4)B.3.3. (g. universite_firewall_degisim_projesi).pdf

[17](3)B.3.3.siem.pdf

[18](3)B.3.3.-1_siem.pdf

[19](3)B.3.3.-2_siem.pdf

[20](3)B.3.3.-3_siem.pdf

[21](3)B.3.3.-4_siem.pdf

[22](3)B.3.3.(k. office365_mfa_(cok_faktorlu_kimlik_dogrulama_projesi)).pdf

[23](3)B.3.3.(l.single_sign-on_projesi).pdf

[24](3)B.3.3.(m. sdwan_(yazilim_tabanli_genis_alan_agi_projesi)).pdf

[25](3)B.3.3.consul.pdf

B.3.4. Dezavantajlı gruplar

2025 yılı itibarıyla MEBIS EqualWeb Eklentisi uygulamasında herhangi bir değişiklik yapılmamış olup, 2024 yılında sağlanan entegrasyon ve erişilebilirlik yapısı doğrultusunda sürdürülmektedir. EqualWeb eklentisi, öğrenci bilgi sistemine entegre şekilde çalışmaya devam etmekte; engelsiz üniversite uygulamaları kapsamında erişilebilirlik standartlarının korunması sağlanmaktadır. Öğrencilerin farklı engel durumlarına uygun olarak öğrenim kaynaklarına erişimi kolaylaştırılmakta, ekran okuma teknolojileri ve renk kontrastı iyileştirmeleri sayesinde çevrim içi içeriklere daha etkin ve kapsayıcı erişim imkânı sunulmaktadır. Bu kapsamda eğitimde eşitlik ve erişilebilirlik düzeyi muhafaza edilmektedir. [\[OD3\]](#)

Olgunluk Düzeyi (3) Dezavantajlı grupların eğitim olanaklarına erişimine ilişkin uygulamalar yürütülmektedir.