ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ AÇISINDAN TÜRKİYE' DE HUKUK BÜROLARINDA BİLGİ GÜVENLİĞİ YÖNETİMİ

Berker KILIÇ

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

ARALIK 2019

Berker KILIÇ tarafından hazırlanan “ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ AÇISINDAN TÜRKİYE’ DE HUKUK BÜROLARINDA BİLGİ GÜVENLİĞİ YÖNETİMİ” adlı tez çalışması aşağıdaki jüri tarafından OY ÇOKLUĞU ile Gazi Üniversitesi ADLİ BİLİŞİM Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Yrd.Doç.Dr. Nursel YALÇIN

Bilgisayar ve Öğretim Teknolojisi Eğitimi Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan : Doç.Dr. Bünyamin CİYLAN

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Üye : Doç.Dr. Olgun DEĞİRMENCİ

Hukuk Ana Bilim Dalı, TOBB Ekonomi ve Teknoloji Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Tez Savunma Tarihi: 09/12/2019

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Doç. Dr. Aslıhan TÜFEKÇİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Berker KILIÇ

09/12/2019

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ AÇISINDAN TÜRKİYE' DE HUKUK BÜROLARINDA BİLGİ GÜVENLİĞİ YÖNETİMİ

(Yüksek Lisans Tezi)

Berker KILIÇ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Aralık 2019

ÖZET

Bilgi güvenliği açısından haberleşme, enerji, bankacılık/finans, kritik kamu hizmetleri, ulaştırma ve su yönetimi alanları kritik alt yapılar olarak görülmektedir. Ancak, özel nitelikli kişisel verilerin işlenmesi ve veri sorumlusu sıfatı ile avukatların müvekkillerine karşı, kişisel verilerinin gizliliğinden sorumlu olmaları nedeni ile günümüzde hukuk alanının da kritik bir alan olarak değerlendirilmesi mümkündür. Bu çalışmada, hukuk bürolarının İnsan Kaynakları, Bilişim Teknolojileri Ekipman ve Bilişim Teknolojileri İletişim altyapıları ile ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi alt amaçları arasındaki anlamsal farklılıkları belirlenmiş, 0-100 aralığında genellenebilir bir eşitlik geliştirilerek, hukuk bürolarının ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile uyum seviyeleri ölçülmüştür. Çalışmada, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi amaç ve alt amaçları paralelinde geliştirilen öz değerlendirme anketi kullanılmıştır. Farklı şehirlerden 452 hukuk bürosuna uygulanmış, elde edilen sonuçlar, hukuk bürolarının İnsan Kaynakları, Bilişim Teknolojileri Ekipmanları ve Bilişim Teknolojileri İletişimi özellikleri açılarından değerlendirilmiştir. Değerlendirme sürecinde iki farklı yöntem izlenmiştir. Hukuk bürosunun İnsan Kaynakları, Bilişim Teknolojileri Ekipman ve Bilişim Teknolojileri İletişim özellikleri ile ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi 35 alt amacı arasındaki anlamsal farklılıklar analiz edilmiştir. Veriler Kolmogorov-Smirnov ve Shapiro-Wilk normallik testleri ile normal dağılım göstermedikleri görülmüştür. alt grup sayısı ikiden fazla olan özellikler için Kruskal Wallis, iki olan alt gruplar için Mann Whitney U testleri uygulanarak anlamsal farklılıklar analiz edilmiştir. Diğer taraftan, hukuk bürolarının ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi 14 amacı ile regresyon analizi yapılmış ve hukuk bürolarının Bilgi Güvenliği Yönetim Sistemi puanlarını elde edebilmek için bir eşitlik geliştirilmiştir. Elde edilen anlamsal farklılıklar ve bilgi güvenliği puanları kullanılarak, hukuk büroları için ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kriterlerine uyumluluklarını arttırabilmeleri için güçlendirici ve tamamlayıcı model adı verilen iki model geliştirilmiştir. Katılımcı 452 hukuk bürosunun 0-100 aralığında yalnızca 10,381 puan alarak ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi' ne uyumluluklarının oldukça düşük olduğu görülmüştür. Ancak, hukuk bürolarının İnsan Kaynakları, Bilişim Teknolojileri Ekipman ve Bilişim Teknolojileri İletişim özellikleri ile anlamsal farklılıkların tespit edildiği ISO/IEC Bilgi Güvenliği Yönetim Sistemi alt amaçlarına odaklanan güçlendirici model ve tamamlayıcı modellerin uygulanması ile bu puanın artırılabileceği görülmüştür.

Bilim Kodu	: 92401
Anahtar Kelimeler	: ISO/IEC, ISO/IEC 27001, Bilgi Güvenliği, Hukuk Bürosu, Bilgi Güvenliği Yönetim Sistemi, BGYS, Bilgi Güvenliği Modeli
Sayfa Adedi	: 274
Danışman	: Yrd.Doç.Dr.Nursel YALÇIN

INFORMATION SECURITY MANAGEMENT IN LAW OFFICES IN TURKEY IN TERMS ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

(Master's Degree Thesis)

Berker KILIÇ

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

December 2019

ABSTRACT

In terms of information security, the fields of communication, energy, banking/finance, critical public services, transportation and water management are regarded as critical infrastructures. However, due to the fact that lawyers have a resposibility for the secrecy of personal data in the capacity of being resposible for processing of private qualified personal data and in charge of the data, today it is possible to be considered the field of law as a critical one as well. In this study, the semantic differences between Human Resources of Law Offices, the Equipment of Information Technologies and the infrastructures of Information Technologies Communication and the sub objectives of ISO/IEC 27001 Information Security Management System are determined, the adjustment levels related to ISO/IEC 27001 Information Security Management System with law offices are measured by developing a generalizable equality in range of 0-100. In the study, the self evaluation survey which is developed in paralel with the objective and sub objectives of ISO/IEC 27001 Information Security Management System is used. It is applied to 452 law offices from different cities, the obtained results are evaluated in terms of the features of Human Resources of Law Offices, the Equipment of Information Technologies and Information Technologies Communication. Two different methods are followed in the evaluation process. The semantic differences between Human Resources of the Law Office, the Equipment of Information Technologies and the feautures of Information Technologies Communication and 35 sub objectives of ISO/IEC 27001 Information Security Management System are analyzed. It is seen that the datas don't indicate a normal dispersion with Kolmogorov-Smirnov ve Shapiro-Wilk normality tests. The semantic differences are analyzed by applying Kruskal Wallis test for the feautures having sub groups more than two and Mann Whitney test for the ones having two sub groups. On the other hand, a regression analysis is performed with the 14 objectives of ISO/IEC 27001 Information Security Management System of law offices and an equality is developed for obtaining the points of Information Security Management System of law offices. By using obtained semantic differences and the points of Information Security, two models named as strengthening and supplementary model are developed for increasing the adjustments to the criteria of ISO/IEC 27001 Information Security Management System for law offices. It is seen that the adjustments of 452 participant law offices to ISO/IEC 27001 Information Security Management System are rather low by taking only 10,381 points in range of 0-100. Nevertheless, it is seen that these points can be increased by applying strengthening and supplementary model focused on the sub objectives of ISO/IEC Information Security Management System, by which the semantic differences between Human Resources of the Law Offices, the Equipment of Information Technologies and the feautures of Information Technologies Communication are detected.

Science Code : 92401

Key Words : ISO/IEC, ISO/IEC 27001, Information Security, Law Office, Information Security Management System, BGYS, Information Security Model

Page Number : 274

Counsellor : Yrd.Doç.Dr.Nursel YALÇIN

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren, kıymetli tecrübelerinden faydalandığım danışmanım Yrd.Doç.Dr. Nursel YALÇIN' a ayrıca, manevi desteği ile beni hiçbir zaman yalnız bırakmayan, işleri idare eden eşim Esra KILIÇ ve bilgisayarımı çalışmam için bana bırakan oğlum Ömer Karahan KILIÇ' a teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	Açıklamalar
m	Amaç sıra numarası
n	Madde sıra numarası
o	Katılımcı sıra numarası
EP	Madde evet puanı
KP	Madde kısmen puanı
HP	Madde hayır puanı
$MCP_{m.o.n}$	Madde cevap puanı
$KAP_{m.o}$	Bir amaç için bir katılımcının puanı
KAP_{m}	Bir amaç için tüm katılımcıların puanı
KAP_{o}	Tüm amaçlar için bir katılımcıların puanı
KAP	Tüm amaçlar tüm katılımcıların anket puanı
BGYSP	Bilgi güvenliği yönetim sistemi puanı
BGYSP100	0-100 aralığında bilgi güvenliği yönetim sistemi puanı

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ANSSI	Fransa Ulusal Siber Güvenlik Ajansı
BG	Bilgi güvenliği
BGRY	Bilgi güvenliği risk yönetimi
BGYS	Bilgi güvenliği yönetim sistemi
BİGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BMI	Federal Bilgi Teknolojileri Güvenliği Ofisi
BSI 100-3	Federal Bilgi Teknolojileri Güvenliği Ofisi 100-3
BT	Bilişim teknolojileri
BTE	Bilişim teknolojileri ekipman
BTE	Bilişim Teknolojileri Enstitüsü
BTİ	Bilişim teknolojileri iletişim

Kısaltmalar	Açıklama

CCTA	İngiltere Merkez Bilgi İşlem ve Telekomünikasyon Ajansı
COBIT	Bilgi ve ilgili teknolojiler için kontrol amaçları
CRAMM	CCTA risk analizi ve yönetimi metodu
CVSS-SIG-First	Ortak güvenlik açığı puanlama sistemi-özel ilgi grubu-birinci
DCSSI	Başbakan Bilgi Sistemleri Güvenliği Merkez Müdürlüğü
DDOS	Servis dışı bırakma saldırısı (Denial-of-Service Attack)
EBIOS	İhtiyaçların ifade edilmesi ve güvenlik amaçlarının belirlenmesi
ENISA	Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı
HIPAA	Sağlık sigortası taşınabilirliği ve sorumluluk yasası
IRAM	Bilgi riski değerlendirme metodolojisi
ISAMM	Bilgi güvenliği değerlendirme ve izleme yöntemi
IIEC	Uluslararası Elektroteknik Komisyonu
ISO	Uluslararası Standardizasyon Örgütü
ITIL	Bilgi teknolojileri altyapı kütüphanesi
İLTAREN	İleri Teknolojiler Araştırma Enstitüsü
KOBİ	Küçük ve orta boy işletme
KV	Kişisel veriler
KVKK	Kişisel Verileri Koruma Kanunu
MAGERIT	Bilgi sistemleri risk analizi ve yönetimi metodolojisi
MAGERIT	Bilgi teknolojileri analiz ve risk yönetimi metodolojisi
MARION	Bilgisayar risk analizi metodolojisi ve seviye optimizasyonu
MEHARI	Harmonize risk analizi yöntemi
MIGRA	İşletme riskinin yönetimi için entegre metodoloji
NIST SP 800-30	Ulusal Standartlar ve Teknoloji Enstitüsü özel yayın 800-30
OCS	Siber Güvenlik Dairesi (Office of Cybersecurity)
OCTAVE	Operasyonel olarak kritik tehdit, varlık ve güvenlik açığı değerlendirmesi
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü
OPM3	Kurumsal proje yönetimi olgunluk modeli
OWASP	Açık web uygulama güvenliği projesi
P-CMM	İnsan yeterliliği olgunluk modeli (People Capability Maturity Model)
PHI	Korunan sağlık bilgileri (Protected Health Information)
PUKÖ	Planla-Uygula-Kontrol et-Önlem al
PMMM	Proje yönetimi olgunluk modeli
PRINCE2	Kontrollü ortam projeleri (PRojects IN Controlled Environments)
Kısaltmalar	**Açıklama**

RA	Risk analizi
RD	Risk değerlendirme
RY	Risk yönetimi
SGE	Siber Güvenlik Enstitüsü
SREP	Güvenlik gereksinimleri mühendislik süreci
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1. GİRİŞ

Bilgi güvenliği (BG), bilgi alanındaki nesnenin (bilginin kendisi ve bulunabileceği tüm ortamlar) korunması, toplanması, oluşturulması, işlenmesi, bilginin dağıtılması ve kullanılması ve ayrıca ortaya çıkan sosyal ilişkilerin düzenlenmesi sistemi ile anlaşılır.

Günümüzde ticari işletmeler, kamu kurumları, her türde organizasyon kısaca kişisel verilerle çalışan bütün kuruluşların, kritik bilgilerinin manipülasyonu ve çalınması gibi çeşitli iç ve dış güvenlik tehditlerine maruz kalmaktadır. Olası bir iç veya dış müdahaleye ek olarak, doğal felaketler veya bilgisayar kullanıcılarının kasıtsız hataları da sonuçları itibariyle birer tehdit olarak ele alınmaktadır.

Siber saldırıların artışına paralel olarak planlı bir şekilde veri koruma ortamları ve süreçleri oluşturmak amaçlı bilgi varlıklarını yönetmek için etkili bir Bilgi Güvenliği Yönetim Sistemi (BGYS) oluşturması, uygulaması ve sürdürmesi zorunlu hale gelmiştir [87].

Kuruluşlar, bilgi varlıklarını korumak ve büyük para kayıplarını önlemek için bilgi güvenliğine giderek daha fazla yatırım yapmaktadırlar [88]. Ancak güvenlik ihlallerinin de sayısı artmaya devam etmektedir [89]. Çoğu kuruluş, yalnızca teknik bilgi güvenliği önlemleri olarak saldırı ve izinsiz giriş tespit sistemleri kullanmaktadır [90]. Ancak bazı kuruluşlar da veri alışverişi yaparak, bilgiyi paylaşarak ya da dış kaynak kullanımı ile diğer sistemlerle, insanlarla ve kuruluşlarla etkileşime girdikleri bir sistem içerisinde çalışıyor olabilirler [91]. Bu gibi durumlarda da, bilgileri gereğinden fazla miktarda detay içerecek şekilde paylaşılması durumu ortaya çıkarak bilgilerin gizliliği ve özel verilerin bütünlüğünü bozabilir veya paylaşım güvenilmeyen üçüncü taraflarla yapılmış olabilir.

BG olmadan kuruluşlar, itibar kaybı, pazar payı kaybı ve düzenleyici sansürle sonuçlanan etkin olmayan bilgi güvenliği yönetiminin neden olduğu hizmet kesintisi, veri sızması, finansal hatalar, başarılı iç ve dış saldırılar gibi çeşitli güvenlik sorunlarıyla karşı karşıya kalabilmektedirler [3].

BGYS' leri çoğunlukla büyük ölçekli kuruluşlara hitap eder. Ancak, küçük ölçekli ve kritik bilgilerin işlendiği kuruluşlar için de BGYS' nin kullanılabilir olması gereklidir. Küçük kuruluşların, büyükler gibi bir bilgi güvenliği altyapısı kurmaları onlar için yüksek maliyetli

olabilir fakat kritik bilgilerin korunması gereği, bilgi güvenliği risklerini azaltmaya yönelik gerekli optimal bir BG modeli geliştirilmiş olması gerekmektedir.

BG risklerini değerlendirmek için birçok yöntem vardır ve bunların çoğu tehditleri ve açıkları tespit etmeyi, bilinen tehditlerle ilişkili olasılık ve etkileri analiz etmeyi ve nihayetinde etki azaltmak için uygun eğitim seviyesini ve kontrolleri belirleme risklerini önceliklendirmeyi içerir. Örneğin Almanya'da Bilgi Güvenliği için Federal Daire tarafından önerilen IT-GrundsChutz yöntemi, beş gruba ayırmıştır (zorunlu sebepler, organizasyonel eksiklikler, insan hatası, teknik başarısızlık ve kasıtlı eylemler). Bu yöntemde, korunma önlemleri; altyapı, organizasyon, personel, yazılım ve donanım, iletişim ve acil durum planlaması şeklindedir [92]. National Institute of Standards and Technology Special Publication 800-30 (Ulusal Standartlar ve Teknoloji Enstitüsü Özel Yayın 800-30, NIST SP 800-30)' ün tavsiyelerinin kapsamlı bir risk değerlendirme (RD) programı için bir rehber olarak değerlendirildiği başka bir yöntemdir. Bu yöntemde, RD süreci, güvenlik riski yönetimi sürecinin ilk aşamasıdır ve dokuz aşamayı içerir [93]:

1) Sistem karakterizasyonu
2) Tehdit tespiti
3) Güvenlik açığı tespiti
4) Kontrol analizi
5) Olasılık tespiti
6) Etki analizi
7) Risk tespiti
8) Kontrol önerileri
9) Sonuç dokümantasyonu

Kuruluşların günlük operasyonlarında Bilgi Teknolojileri (BT) kullanımının artması, bilginin değeri ve kırılganlığının en üst düzeyde olmasına neden olmaktadır. Dahası, bulut bilişim gibi, dağıtılmış depolama ve hesaplama, bilgisayar fonksiyonlarının dış kaynak kullanımı konusundaki gelişmeler BG' ni daha önemli bir hale getirmiştir.

Bilgi Güvenliği (BG) risk analizi (RA) ve risk yönetimi (RY), sahip olunan varlıklar ve bunların arkasındaki teknolojiler hakkında, altyapının karşı karşıya olduğu tehditleri ve açıkları tanımak için kapsamlı bilgi gerektirir.

Bilgi Güvenliği Risk Yönetimi (BGRY) yöntemleri temel olarak risklere odaklanır, ancak bazı sorunlardan zarar görür: açık bir metodolojinin olmaması, BG risklerinin göz ardı edilmesi, pahalı belgeler ve önerilen yaklaşımların uygulanması için derinlemesine bir anlayış ve uzmanlık ihtiyacı gereklidir.

Dutch A&K (Afhankelijkheids-en Kwetsbaarheidsanalyse) Analysis (Hollanda (Bağımlılık ve Güvenlik Açığı Analizi, Hollanda A&K Analizi) analizi, Österreichisches IT-Sicherheitshandbuch (Avusturya Bilgi Teknolojileri Güvenlik El Kitabı, Austrian IT Security Handbook), Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau (Bilgisayar Risk Analizi Metodolojisi ve Seviye Optimizasyonu, MARION), Information Security Assessment & Monitoring Method (Bilgi Güvenliği Değerlendirme ve İzleme Yöntemi, ISAMM) gibi bilgiler yalnızca yerel dillerde mevcuttur. Diğer BGYS' leri genel hatlarıyla incelendiğinde: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Bilgi Teknolojileri Analiz ve Risk Yönetimi Metodolojisi, MAGERIT) RA ve RY metodu kuruluşa has hiyerarşilerine göre varlıkları tanımlanır ve gruplandırılır. Ardından, potansiyel tehditleri analiz eder ve güvenlik hedeflerini yerine getirmek için gereken önlemleri alır. Benzer şekilde, Security Requirements Engineering Process (Güvenlik Gereksinimleri Mühendislik Süreci, SREP) [94], tehditleri ve bunları değerlendirmek için MAGERIT tablolarını modellemek için yanlış durum diyagramlarını kullanan, varlık bazlı tekrarlamalı ve artırımlı bir süreçtir. Sistematik yapılarına rağmen, her iki yöntem de, sistemden ya da çevresinden ya da paydaşlar arasındaki sosyal etkileşimlerden kaynaklanan etkileşimlerden kaynaklanan zayıflıkları göz ardı etmektedir. Information Risk Assessment Methodology (Bilgi Riski Değerlendirme Metodolojisi, IRAM) [95], kuruluşun bilgi sistemlerine ve bilgi tehditlerine odaklanan, atölye temelli ve araç destekli bir modeldir. Bu yaklaşım bilgi sistemlerinin önemini ve kritikliğini belirlemeye yardımcı olur. Bilgi güvenliği RA' nde kabul edilen tek doğru, gerçek ve her durumda kullanılabilir genel bir risk hesaplama formülünün var olmamasıdır.

Diğer BGYS sistemlerine de kısaca değinilecek olursa, PRojects IN Controlled Environments (Kontrollü Ortam Projeleri, PRINCE2), Organizational Project Management Maturity Model (Kurumsal Proje Yönetimi Olgunluk Modeli, OPM3), People Capability Maturity Model (İnsan Yeterliliği Olgunluk Modeli, P-CMM), Project Management Maturity Model (Proje Yönetimi Olgunluk Modeli, PMMM), Information Technology Infrastructure Library (Bilgi Teknolojileri Altyapı Kütüphanesi, ITIL) ve Control Objectives

for Information and Related Technologies (Bilgi ve İlgili Teknolojiler İçin Kontrol Amaçları, COBIT) gibi BGYS' leri mevcuttur [4].

Kişilerin kimliğini belirleyen kişisel verilerine ek olarak kritik bilgilerinden birisi de kişilerin suç ve suça ilişkin hukuki bilgileridir. Hukuk alanında kişiyi vekaleten temsil eden avukatlar, kişinin bu kapsamdaki her türlü bilgisine sahiptir. Bu temsil ile avukatın kişinin suçuna yahut mağduriyetine ilişkin sahip olduğu kişisel bilgilerini koruması önemlidir. Kişisel Verilerin Korunması Kanunu (KVKK), Avukatlık Kanununu ve ilgili diğer kanunlarının bu doğrultuda maddeleri mevcuttur. KVKK açısından avukat, müvekkilinin kişisel bilgilerini koruma yükümlülüğü bakımından veri sorumlusudur.

Bilgi Güvenliği Yönetim Sistemleri alanında, kuruluşların kaynaklarını ve varlıklarını korumayı amaçlayan çeşitli kılavuzlar, standartlar ve platformlar geliştirilmiştir (International Organization for Standardization/International Electrotechnical Commission (Uluslararası Standardizasyon Örgütü/Uluslararası Elektroteknik Komisyonu, ISO/IEC) 27000 [59], NIST-SP 800 [96], Common Vulnerability Scoring System- Special Interest Group-First (Ortak Güvenlik Açığı Puanlama Sistemi-Özel İlgi Grubu-Birinci, CVSS-SIG-First [97], MAGERIT [98], ITIL ve COBIT [99], vb.)

Kuruluşların türüne ve ihtiyacına bağlı olarak kullanılan farklı RD yöntemleri vardır. Bazı metodolojiler, kullanım için oldukça farklı olduklarından büyük kuruluşlar ve deneyimli çalışanlar gerektirir. Metodolojilerin çoğu, ticari olarak geliştirilmiştir, bu nedenle, bazıları pazarlama amacı dışında halka açık değildir. Bir kuruluşun RD için bir metodoloji kullanması gerekir, genellikle doğru olanı seçilmeden önce farklı metodolojileri karşılaştırmayı amaçlar.

Kuruluşların artan BG ve kullandıkları varlıkları ile ilgili endişeleri vardır. BG, kuruluşların varlıklarını korumayı amaçlayan bir dizi prosedür ve süreç, teknoloji ve insandır [100]. Kuruluşlarda çeşitli riskler mevcuttur ve kuruluşlar belirlenen riskleri kaldırmak veya azaltmak için güvenlik kontrollerini kullanmak amacıyla bu risklerin nasıl değerlendirileceğini belirleyen önemli bir sorunla karşı karşıyadır. Standart bir metodoloji veya kuruluş tarafından kullanılabilecek prosedür yoktur. Çok sayıda RD yöntemi ve çerçevesi vardır ve BG için istekli olan kuruluşlar, farklı metodolojileri karşılaştırmalı ve ihtiyaçlarına uygun en iyi yöntemi seçmelidir. RD firmaları, risklerin ciddiyetini ölçmekte

ve zararı azaltmak ve güvenlik önlemlerine yapılan yatırımdan maksimum faydayı elde etmek için güvenlik kontrolleri geliştirmektedir. Genel olarak, risklerin tanımlanmasının ardından kuruluşlar tehdidin değerini, ortaya çıkma ihtimalini ve tehdidin kuruluşta ortaya çıkarabileceği etkiyi belirler. Riskin ciddiyeti, aynı anda hem niteliksel, hem niceliksel hem de her iki yöntem uygulanarak elde edilebilecek tehdit ve tehdit oluşumunu birleştirerek belirlenebilir.

Kuruluşlar, bilgisayar korsanlarının, kötü niyetli ve dürüst olmayan çalışanlar ve fiziksel güvenliği ihlal etme gibi çeşitli yollarla güvenlik tehditleriyle karşı karşıya kalabilirler. Finansal kuruluşlar, önemsiz güvenlik olayları nedeniyle bazen fark edilmeyen güvenlik ihlali nedeniyle finansal zarar görür [101]. Daha önce belirtildiği gibi, BG riskini belirlemek için kuruluşlar tarafından benimsenebilecek standart bir metodoloji veya prosedür yoktur, kuruluşlar genellikle RD için ayrıntılı adımlar atmaktadır. Kuruluşlardaki riskleri değerlendirmek için en değerli bilgilere yönelik riskler önceliklendirilir ve ardından varlıklar için tehdidin ciddiyeti değerlendirilir [5].

ISO/IEC 27002, ISO/IEC tarafından ortaklaşa yayımlanan bir standarttır. ISO/IEC 27002, ISO/IEC 27K paketinin bir parçasıdır. ISO/IEC 27001, gereksinimleri içeren standarttır, ISO/IEC 27002 ise standardın uygulanmasına rehberlik eden uygulama kodudur [2].

Çalışmada, BGYS standartlarının veya çerçevelerinin benimsenmesini etkileyen kilit faktörlerine genel bir bakış sunmak için, BGYS ' ni uygulamadaki zorluklar ve engeller hakkındaki mevcut literatürün sistematik bir incelemesi yapılmıştır. BGYS' nin ne olduğu, neden önemli olduğu ve kuruluşlarda nasıl elde edilebileceği hakkında temel bir anlayış edinmek için, genel olarak bir BGYS teorisi açıklanmaktadır. Daha sonra, en popüler BGYS standartlarının ve çerçevelerinin bir özeti sunulmaktadır. Ayrıca, BG yönetimini etkileyen kilit faktörlerin ve BGYS standartlarının veya çerçevelerinin benimsenmesine ilişkin mevcut araştırmaların sınırlarının eleştirel bir şekilde gözden geçirilmesi sağlanmıştır. Literatür taramasının amacı, BG etkileyen anahtar faktörler aracılığıyla araştırma soruları için bir temel oluşturmaktır.

Her standart için, kuruluşların işin doğasına, BG olgunluk seviyesine, kuruluşun büyüklüğüne ve bütçesine bağlı olarak seçecekleri birçok uygulama rehberi vardır. Ancak, bu standartlardan veya çerçevelerden birine tamamen uyumun sağlanması zordur.

Bu çalışma ile özel bir kuruluş türü olarak hukuk bürolarının ISO/IEC 27001 BGYS çerçevesinde değerlendirilmesi yapılacaktır. Değerlendirme iki açıdan gerçekleştirilmiştir. Birincisi hukuk bürolarının mevcut ISO/IEC 27001 kontrolleri ile uyumluluğu insan kaynakları, bilişim teknolojileri ekipman (BTE) ve bilişim teknolojileri iletişim (BTİ) özellikleri açısından değerlendirilmiş ve anlamlı farklılıklar araştırılmıştır, ikincisi ise ISO/IEC 27001 kontrollerine uyumlulukları bir puana dönüştürülerek incelenmiştir ve değerlendirilmiştir.

Değerlendirmede yapılan puanlama hem bir yeterlilik göstergesi hem de hukuk büroları için kurulacak bir BGYS sisteminde ISO/IEC 27001 Standardında yer alan uyum sağlanabilecek kriterlerin seçiminde yol gösterici olacaktır.

Bu araştırma, BGYS standartlarının ve çerçevelerinin benimsenmesinin düşük olduğu ve BGYS standartlarının ve çerçevelerinin benimsenmesini etkileyen faktörlerin araştırılması olgusunu veya gerçeğini açıklamaya odaklanmaktadır. Araştırma sorularına cevap vermek için yüksek düzeyde yapılandırılmış bir veri toplama stratejisi izleyerek bu araştırma için nicel yöntem kullanılmıştır. Bu araştırmada Mono Yöntemi nicel çalışması benimsenmiştir. Yani tek bir veri toplama tekniği kullanılmıştır.

Araştırmada, ISO/IEC 27001 BGYS çerçevesinde hazırlanan öz değerlendirme anketi kullanılmıştır. Öz değerlendirme anketi ile elde edilen bilgilerden hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özellikleri açılarından ISO/IEC 27001 BGYS alt amaçları arasında bir ilişki olup olmadığı araştırılmış ve öz değerlendirme sonucu hukuk bürolarına özel bir bilgi güvenliği modelinin optimum gereksinimleri ölçülmüştür.

Ankette ISO/IEC 27001 BGYS içerisinde yer alan 14 Amaç, 35 Alt Amaç ve 113 kontrol için 294 anket maddesi hazırlanmıştır.

Çalışma ile ISO/IEC 27001 BGYS' nin de alt amaç seviyesinde aşağıdaki sorulara cevap aranmış ve bu doğrultuda hukuk bürolarında ISO/IEC 27001 BGYS kurulumuna ilişkin seçilecek kontroller ile bir model ve puan hesaplama yöntemi geliştirilmiştir.

Araştırma Problemi 1: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 2: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Organizasyonu - İş Organizasyon" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 3: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 4: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - İstihdam Öncesi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 5: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - Çalışma Esnasında" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 6: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 7: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Varlıkların Sorumluluğu" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 8: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Bilgi Sınıflandırması" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 9: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Ortam İşleme" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 10: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 11: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Kullanıcı Erişim Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 12: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Kullanıcı Sorumlulukları" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 13: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 14: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Kriptografi - Kriptografik Kontroller" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 15: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 16: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Fiziksel ve Çevresel Güvenlik - Teçhizat" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 17: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - İşlem Prosedürleri ve Sorumlulukları" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 18: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Kötücül Yazılımlardan Koruma" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 19: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Yedekleme" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 20: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Kaydetme ve İzleme" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 21: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - İşletimsel Yazılımın Kontrolü" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 22: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Teknik Açıklık Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 23: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Bilgi Sistemleri Tetkik Hususları" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 24: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Haberleşme Güvenliği - Ağ Güvenliği Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 25: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Haberleşme Güvenliği - Bilgi Transferi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 26: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 27: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 28: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Test Verisi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 29: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 30: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 31: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 32: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 33: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 34: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 35: Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Uyum - Bilgi Güvenliği Gözden Geçirmeleri" düzeyleri anlamlı farklılaşmakta mıdır?

Araştırma Problemi 36: ISO/IEC 27001 içerisinde yer alan 14 Amaç düzeyinde hukuk büroları için optimal bir BGYS modeli ortaya koyulabilir mi?

Sağlık, haberleşme, enerji, bankacılık/finans, kritik kamu hizmetleri, ulaştırma, su yönetimi, telekomünikasyon ve enerji gibi sektörler hali hazırda BGYS açısından kritik sektörler olarak ele alınmaktadır. Ancak, bu alanlara ek olarak, özellikle kişisel veriler (KV) ve buna bağlı kişilerin sosyal yaşamları, sosyal itibarları ile ilgili olan hukuki konularda kritik bir alan/sektör olarak tanımlanmamıştır.

Bilgi günümüzde değeri olan bir nesneye yani metaya dönüşmüştür. Bu nedenle, bilginin artık bir veri bütününden ziyade, alınabilir, satılabilir bir nesneye dönüşmüş olması BG gereksinimini de artırmıştır.

Hukuk büroları açısından bakıldığında, müvekkilleri açısından soruşturma yahut kovuşturmaya dahil olan bilgiler, yani bir dosya bütünü, hem fiziksel hem de elektronik ortamda bir değerdir.

Bu değer müvekkil açısından imaj ve itibar olarak değerlendirilebileceği gibi, avukat açısından da işlediği ve geliştirdiği ekonomik değeri olan anlamlı bir veri bütünüdür. Yani nesnel bir değeri vardır.

Ayrıca, avukatın, müvekkilin kişisel bilgilerini koruma yükümlülüğü nedeni ile de müvekkiline karşı sorumlu olduğu düşünülmektedir.

Hukuk bürolarının BG gereksinimi, her ne kadar az sayıda çalışan ve ekipmana sahip yapılar olması nedeni ile kapsamlı ve maliyetli bir şekilde değerlendirmeye uygun olmasa da, işlenen verilerin kritik önemi, iş sürekliliği gereksinimi ve iş kapasitesine bağlı iş verimliliği gereksinimleri açısından değerlendirildiğinde, yönetilmesi gereken bir seviyededir.

RY uzun zaman önce her türlü kuruluşu bünyesine katmış olup artık bilgisayarlar işe girdiği için BG risklerinin göz önünde bulundurulması zorunlu hale gelmiştir. Ayrıca, bilgisayarlar artık neredeyse tüm kritik işlemden sorumludur, bu nedenle BT riski, günümüzde kuruluşların ana risklerinden biri haline gelmiştir [30].

Hukukun da bir kritik sektör olduğu varsayımı ve güncel BG mevzuatının gelişme yönü göz önünde bulundurularak hukuk alanındaki KV' in korunmasına yönelik yaptırımı olan hukuki gelişmeler olacağı beklenmektedir.

Bu varsayımın ilk göstergeleri Cumhurbaşkanlığı 2019/12 Sayılı Genelgesi ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından Bilgi ve İletişim Güvenliği Rehberi hazırlanacağından bahsedilmekle birlikte henüz yayınlanmamıştır [138], ayrıca TBMM tarafından kabul edilen 11' nci Kalkınma Planı' da BG' ne atıf yapan çok sayıda maddenin var olması [136] bu alandaki ilerleyen dönemlerde yasal zorunluluklarla karşılaşılması olasılığını göstermektedir.

Araştırma katılımcılarının çoğunluğu Samsun, İstanbul, Ankara ve İzmir ilinde faaliyet gösteren hukuk bürolarından oluşmaktadır. Katılımcıların çoğunluğa kıyasla küçük illerden ve ilçelerden olmamasına rağmen, hukuk bürolarının benzer şekilde faaliyet gösterdiği kabul edilerek, büronun faaliyet gösterdiği şehrin sonuçlar üzerindeki etkisi çalışma kapsamına dahil edilmemiştir.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde, bir meta olarak bilgi tanımlanmış ve BG riski açıklanmıştır. Kuruluşların BG risklerine yaklaşım teorileri değinilmiş ve RA süreci özetlenmiştir. Riskin hesaplanabilirliği, hesaplama bileşenleri ve riski etki seviyesine göre sınıflandırılması yapılmıştır. Son olarak KV' in de meta bilgi olmasına değinilmiştir.

2.1. Meta Olarak Bilgi

Bilgi, insan düşünme ve yorumlamanın bir sonucudur [104]. Çoğu durumda bilgi, insanlara gizli bilgi olarak dahil edilmekle birlikte, bu bilgi, bir tür açık bilgi biçimine, yani yazılı veya sözlü dilden dışsallaştırılarak başkalarıyla paylaşılabilmektedir [105]. Bilgi, kullanımı ve paylaşılmasıyla bir şirkete değer verir; bu, bilgi alan kişilerin paylaşılan bilgileri yorumlayabilmelerini ve bunları öğrenme ve yansıtma için kullanabilmelerini gerektirir [106].

Bilginin kullanımı ve paylaşılması, bilgiye sahip insanlar arasında iletişimi gerektirir. Günümüzde bilgi paylaşımını destekleyecek çok sayıda teknik araç vardır. Bunlar arasında, belki coğrafi olarak birbirlerinden ayrı olan insanlar arasındaki yüz yüze iletişimi taklit etmek için tasarlanmış farklı bilgi sistemleri ve sosyal medya araçları vardır. Ayrıca tekrar kullanabilmek ve paylaşabilmek için bir taraftan da depolanmaktadır. Bilgiye bağlı riskleri tanımlamanın ve yönetmenin sistematik bir yolu, bilginin birleşik bir korunma düzeyi oluşturulmasına yardımcı olacaktır. Ancak araştırmalar bunun en azından yaygın olarak örgütlerde bulunmadığını göstermektedir [107].

Bir kuruluş çalışanlarının bilgisinden rekabet avantajı yarattığında, bilgi kuruluşun en büyük varlığı olur. Bu fikir, kuruluşun bilgiye dayalı bakış açısının bel kemiğidir [108]. Bilgi bir kuruluşun kaynağı olarak kabul edildiğinde, kendisine sahip olan bireylere bağlı olduğu, aynı zamanda kişiden kişiye bireysel ve kollektif seviyelerde aktarılması mümkün olan bir şey olarak kabul edilir [109]. Bilgi kuruluşun içinde bulunduğu durumu anlamak için kullanılırken, kuruluş aynı zamanda yeni bilgiler de yaratmakta ve bu bilgiye dayanarak kararlar alınmaktadır [14].

Bilginin aşağıdaki gibi birçok tanımı vardır [15]:

i. Bilgi birisi hakkındadır veya bir şey onlar hakkında gerçeklerden oluşur.
ii. Girdi verilerinin bir programla işlenmesi yoluyla bir bilgisayardan çıktı olarak önemli veya faydalı bilgiler elde edilebilir.
iii. Bilgi, bir kuruluş için değerli olan ve dolayısıyla uygun şekilde korunması gereken diğer önemli ticari varlıklar gibi bir varlıktır.
iv. Bilgi birçok biçimde olabilir. Kağıda basılabilir veya yazılabilir, elektronik olarak saklanabilir, posta yoluyla iletilebilir veya elektronik araçlar kullanılarak, filmlerde gösterilen veya görüşme sırasında konuşulabilir.

ISO/IEC 17799' a dayanan BG tanımı "gizliliğin korunması, bilgilerin bütünlüğü ve kullanılabilirliğinin yanı sıra, orijinallik, hesap verebilirlik, reddedilmeme ve güvenilirlik gibi diğer özellikler de söz konusudur" şeklinde yapılmıştır [15].

2.2. Bilgi Güvenliği Riski

BG bir kuruluştaki veri ve işlem prosedürlerinin bütünlüğünü ve gizliliğini sağlamak için sistemleri, işlemleri ve iç kontrolleri birleştirmektir. BT' nin ortaya çıkmasıyla birlikte, bilgi sistemlerinde kullanıcıların rolleri, bilgi işlem olanaklarına erişim için BT uzmanlarından, düzenli operasyonlar için BT dışındaki personele, dışarıdan belirsiz bireylere doğru gelişmektedir. Yani, internetteki yetkisiz kullanıcıların ciddi tehdidi ile BG daha önce görülmemiş zorluklarla karşı karşıya kalmaktadır ve etkili BG yönetimi en büyük endişelerden biri haline gelmiştir [102].

Bir BGRY çerçevesi, değerlendirilenler ve kimin dahil edilmesi gerektiğine ilişkin kuralları belirlemektedir. Risk derecelerini ölçmek, nitelemek ve karşılaştırmak için kritere karar verir ve değerlendirme ve faaliyetlerin takibi sonucu belgeleri oluşturulur. Bir çerçevenin amacı, bir kuruluşun kritik bilgi ve donanımsal varlıklar için potansiyel riski hem niteliksel hem de niceliksel olarak anlamasını sağlayacak bir risk ölçümü yapmaktır [103]. Kritik bir RD çerçevesi, bir organizasyonun bilgi işlem ortamı için güvenlik riskini etkin bir şekilde tanımlar. Sonunda, RY çerçevesi, güvenlik seviyesini iyileştirme planları sunar ve güvenlik risklerini kabul edilebilir seviyelere getirecek önlemleri önerir [33].

2.3. Risk Kavramı ve Risk Yönetimi

Risk bir zarara, bir kayba, bir tehlikeye yol açabilecek bir olayın oluşma olasılığı olarak tanımlanabilir. Risk için belirsizlik durumu, riskin gerçekleşeceği varlık ve bu varlığın bulunduğu bir ortam olmalıdır.

Risk istenmeyen bir olayın nedeni, olasılığı ve sonucuna bağlı olarak ortaya çıkar. Başka bir ifadeyle, risk bir tehdidin, bir zafiyetin yani zayıflıkların ve bir sonucun birleşimidir. RY ise risklerin belirlemesi ve bunları engellenemeye yönelik tedbirlerin uygulanması sürecidir. RY sürecinin en önemli kısımları RD ve riskin gerçekleşmesi durumunda uğranılan zararın telafi edilmesidir. RD, risk tanımlaması ve risk analizinden oluşan bir risk yönetimi alt sürecidir.

Biz farkında olsak da olmasak da, yaptığımız tüm faaliyetlerde risk vardır. Temel düzeyde, risk genellikle bir olayın meydana geldiği belirsizlik ve fiilen meydana gelmesi durumunda etki/önem/sonuç ile ilişkilendirilir. Tanım genellikle içeriğe özgüdür ve bir kuruluşun sonuçla nasıl başa çıktığı konusunda geniş bir çeşitlilik ortaya çıkarmaktadır [11].

Kuruluşların BG risklerine yaklaşımı farklı teorilere bağlı olabilir [8]. Bu teoriler;

2.3.1. Güvenlik politikası teorisi

Bir BG politikasının oluşturulmasının, uygulanması ve sürdürülmesinin BG' ni sağlayacağı düşünülür. Ancak her duruma uygun genel ve tutarlı bir güvenlik politikası teorisi yoktur.

2.3.2. Risk yönetimi teorisi

Risk yönetimi teorisi, RA ve değerlendirmesi yoluyla, BG' ne ilişkin risklerin tahmin edilebileceğini ve gerekli önlemlerin alınabileceğini, risk ortaya çıksa dahi bunun en az zararla atlatılabileceğini öngörmektedir. Bu teoride amaç tüm risklere karşı önlem almak değil, BG' nin kabul edilebilir bir seviyede olmasıdır. Uygulamaya geçilen BGYS, kontrol ve iyileştirme prosedürleri ile izlenir ve iyileştirmeler yapılarak kabul edilebilir riskin daha alt seviyelere indirilmesine çalışılır.

2.3.3. Kontrol ve denetim teorisi

Kontrol ve denetim teorisi, kuruluşların BGYS' leri kurmaları gerektiğini söylemektedir. Sistem uygulamaya sokulduktan sonra ise, sistemin verimliliğini ölçmek için performans ölçümleri yapılması gerektiğini öngörmektedir. Bir diğer bakış açısı ile performans ölçümü ve iyileştirme süreci de BGYS' nin bir parçası olduğu için bu teori Risk Yönetimi Teorisinin bir parçasıdır.

2.3.4. Yönetim sistemi teorisi

Yönetim sistemi teorisi, kuruluşun bilgi varlıklarını kontrol etmek ve korumak için belgelenmiş bir BGYS sistemi oluşturması ve sürdürmesi gerektiğini öngörmektedir.

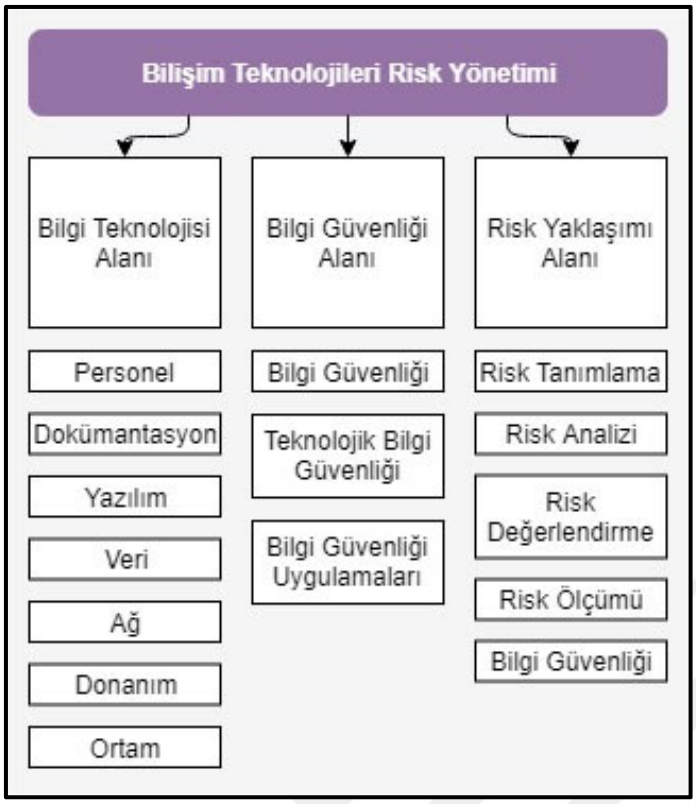
2.3.5. Acil durum teorisi

Acil durum teorisi, kuruluş içindeki ve dışındaki risk faktörlerinin etkilerinin önlenmesi ve beklenmedik durumların yönetilebilmesini öngörmektedir. BG' nin sağlanabilmesi için bir veya daha fazla bilgi güvenliği teorisinin birleşimi ile güvenlik politikası eylemleri, RY eylemleri, kontrol ve denetim eylemleri, sistem yönetimi eylemlerinin uygulanmasına dayanmaktadır.

Şekil 2.1.' de görüldüğü gibi risk yaklaşımı bütünlüğünün alt alanı, yüksek seviyede risk tanımlaması, risk analizi, risk değerlendirmesi, risk çözümü ve risk izleme gibi hususları içermektedir [6].

2.3.6. Risk tanımlaması

Risk belirleme, araştırılacak gerçek bir BT ortamının soyut bir modelinin derlenmesi, böylece net sınırların belirlenmesi sürecidir. Böyle bir ortam, hem açık bağlantı hem de kapalı bağımsız sistemler dahil olmak üzere bir veya daha fazla bilgi sistemine işaret etmektedir. Varlıklar ve/veya yükümlülüklerin yanı sıra tehditler ve güvenlik açıkları da tanımlanmaktadır.



Şekil 2.1. Risk yönetimi kavramları [6]

2.3.7. Risk analizi

Buradaki temel amaç, belirli bir bilgisayarlı sistem üzerindeki etkiyi ve bunun sonucunda kurum üzerindeki etkiyi, bir kesinti veya istenmeyen bir olay meydana geldiğinde hesaplamaktır [110].

Dinamik risk yönetiminin üç aşamasını mümkün kılan genel amaçlı üst düzey fonksiyonlar şunlardır [31]:

Saldırı modellemesi: Çevredeki elementlerin zaman ve mekan içinde algılanması, anlamlarının anlaşılması ve yakın gelecekte durumlarının yansıtılması olarak tanımlanan durum farkındalığı işlevinin ortaya koyulmasıdır.

Risk modellemesi: Bir RD yaklaşımı kullanarak, yöneticinin tanımlanmış herhangi bir tehdidin veya devam eden saldırı riskini tanımlamasını ve ölçmesini sağlayan özellikleri, bunun yanı sıra, bu riskleri azaltan olası müdahale mekanizmalarının etkinleştirilmesi ve

yayılmasından kaynaklanan sistemler/işler/ görevler üzerindeki olası etki ve maliyetler vb. gibi belirlemesidir.

Tepki modellemesi: Tepki modellemesinin kullanılması, tespit edilen riskleri azaltmak için müdahale olanakları öneren, tespit edilen riskleri kabul edilebilir bir seviyenin altına düşürmek için en uygun müdahale olanaklarının seçilmesine olanak sağlayan özellikleri ve ardından izlenen veya korunan BT sistemlerine uygulanacak etki azaltma eylemlerini hesaplanmasını içermektedir.

2.3.8. Risk değerlendirmesi

RA sırasında belirlenen risk faktörleri, her bir bilgi teknolojisi alanı için, yani çevre ile ilgili tüm risklerin gruplanması için bir risk ölçümü hesaplamak üzere konsolide edilmektedir. Bu sonuçların sunulması, nihayetinde risk çözümü karar verilmesini kolaylaştırmak için büyük önem taşımaktadır [6].

RY, genel bir BG programının ayrılmaz bir parçasını oluşturur. RA, varlıkların bilinen değerlerinden hesaplanan risk düzeylerinin ve bu varlıklara yönelik tehdit düzeylerinin gerçekleşme olasılıklarının ve zayıf noktalarının yani güvenlik açıklarının tespitini ve değerlendirilmesini içerir [7].

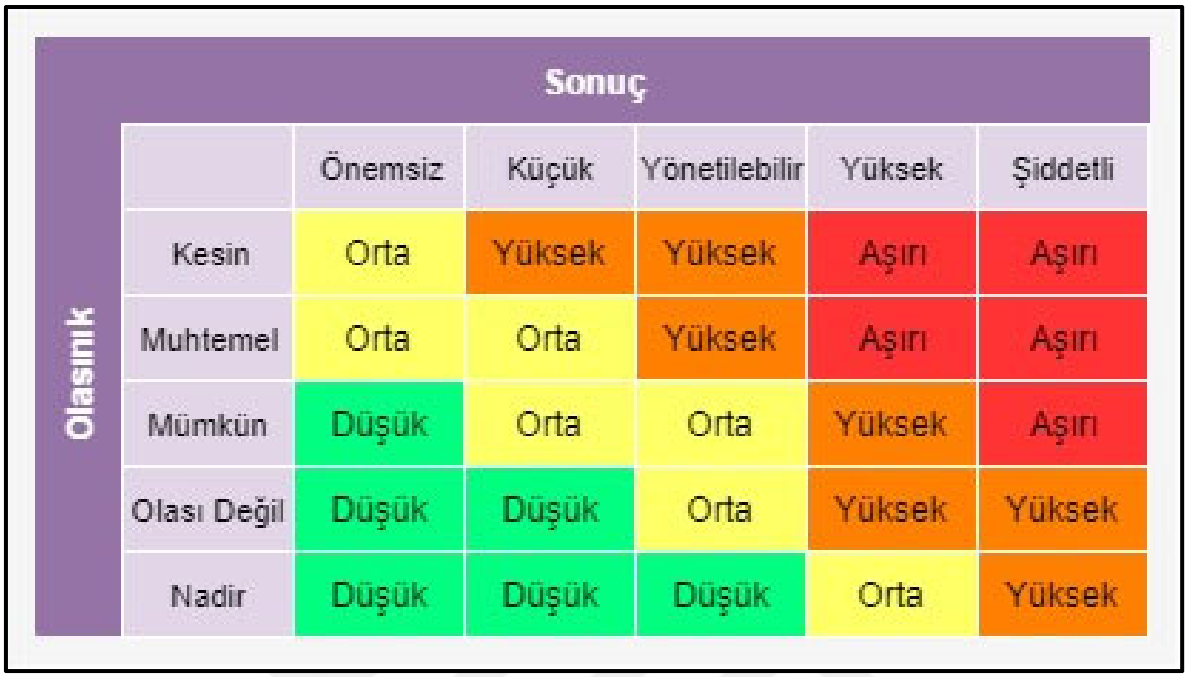
RY, varlıklara yönelik belirlenmiş risklerin haklı gösterdiği karşı önlemlerin belirlenmesi, seçilmesi ve benimsenmesini ve bu risklerin kabul edilebilir seviyelere indirilmesini içerir. Böylece riskin ölçülmesi bir tehdit, güvenlik açığı ve varlık değerlerinin bir ürünü olarak belirlenebilir [7]:

Risk = Varlık x Tehdit x Güvenlik açığı

İş ortamlarını ve kaynaklarını göz önünde bulundurarak bir kuruluştaki karar vericiler [7];

i. Risk azaltma (belirli önlemlerin alınması ile risklerin azaltılması),
ii. Risk kabulü (karşı önlemlerin varlık değerlerinden daha maliyetli olması durumunda, kalan riskin veya hatta başlangıç seviyesinin kabul edilmesi),
iii. Risk transferi (riski sigorta veya dış kaynak kullanımı yoluyla başka bir kuruma aktarmak),

stratejilerinden bir veya birkaçını izleyebilirler.



Şekil 2.2. Risk değerlendirme matrisi [18]

Şekil 2.2.' de görüldüğü gibi matrisin bir tarafında sonuçlar, diğer yanda da gerçekleşme ihtimalleri vardır. Matrisde kullanılan sıralama şunlardır: düşük, orta, yüksek ve aşırı. Daha kolay yorumlanabilmesi için farklı renklerle işaretlenmiştir [18].

RD, somut bir duruma ilişkin risk değerinin ve iki faktöre bağlı olarak tanınan bir tehdidin, olasılık ve etkinin belirlenmesidir. Risk seviyesi, iki risk faktörünün ürünü olup BT risk değerlendirmesi, nitel veya nicel bir yaklaşımla yapılabilmektedir [30].

Risk büyüklüğü zarara neden olan güvenlik açığının istismar olasılığına dayanır, güvenlik açığının daha sık meydana gelmesi sistemi daha riskli kıldığından güvenlik açığının sıklığı da sistemdeki güvenlik açığının ortaya çıkmasına dayanmaktadır [40].

2.3.9. Risk çözümü

Risk çözümünün amacı bir tehdidin gerçekleştirilme sıklığını ve tehdidin sonucunun derecesini, yani potansiyel zararı en aza indirmektir [110].

İstismarın şiddetiyle beraber sayısal risk seviyesi ölçümünde, uyarıların toplam sayısı, istismardan etkilenen birimler, güvenlik açığı taraması esnasında tespit edilen değişkenler parametreler gibi birçok faktörü göz önünde bulundurulmaktadır [40].

Risk, etki seviyesine göre sınıflandırılabilir [23]. Bu seviyeler;

Yüksek/Felaket: Bu seviyede, sistem kaybı, projenin kurtarılamaz hale gelmesi, büyük sorun, teslim tarihinin kaçırılmasına neden olan zamanlamalara neden olmaktadır. Bu seviyedeki risklerin sonucunda maliyet aşımı bütçenin %50' sinden daha büyük olmaktadır.

Orta/Kritik: Bu seviyede, düzeltilebilir işletme kapasitesine sahip projeyle ilgili önemli sorunlar ortaya çıkmaktadır. Bu seviyedeki risklerin sonucunda maliyet aşımı %10' u aşmaktadır (% 50'sinden az).

Düşük/Marjinal: Bu aşamada, küçük problemli proje, operasyonel kapasite geri kazanılabilir kaybı, lansman tarihi maliyetini etkilemeyen iç zamanlamalara neden olmaktadır. Bu seviyedeki risklerin sonucunda maliyet veya zaman diliminin %10' undan azını aşmaktadır.

RA, gerçek değerlerin mi yoksa soyut seviyelerin mi kullanıldığına bağlı olarak, nicel veya nitel olabilir. Risk tedavisi, risklerle başa çıkacak önlemlerin seçilmesi ve uygulanması için bir alt süreçtir. Dört alternatif vardır: risk azaltma, risk transferi, riskten kaçınma ve risk kabulü. Risk azaltma, riski azaltmaya yardımcı olan eylemlerden oluşmaktadır (yani, riskli bir olayın oluşma olasılığını, etkisini veya her ikisini azaltma). Risk transferi, potansiyel zarar yükünü başka bir tarafla paylaşmaktır. Sigorta risk transferi için bir olasılıktır. Riskten kaçınma, riskli bir olaydan kaçınma kararıdır (örneğin, işletmenin riskli bir kısmından çekilme). Risk kabulü, tahmini zararların meydana gelebileceğini kabul etmektir. Doğal olarak, risk kabulü açıkça herhangi bir karar alınmadan otomatik olarak uygulanır [29].

RY kuralları, RY süreci için genel metodolojileri içermektedir. Süreçle ilgili tarafların tanımı, ana terimlerin tanımları, destekleyici belgeler ve fazların üst düzey tanımları gibi, süreçle ilgili örgütsel sorulara özellikle dikkat edilmektedir. Her ne kadar bu kurallar sıklıkla RD ve risk tedavi aşamalarına odaklanmasına rağmen, tedavilerin uygulanması, sonuçların iletilmesi, izleme ve değerlendirme, bakım ve iyileştirme gibi diğer faaliyetleri de içmektedir. Bu bağlamda, genel siber risk yönetimi süreci, yaygın olarak bilinen Planla-

Uygula-Kontrol Et-Önlem Al (PUKÖ) döngüsünün özel bir uygulaması olarak görülebilmektedir [29].

Bu yöntem, analizin aynı anda birkaç kriter kullanılarak yapıldığı çok özellikli değerlendirmeye dayanmaktadır. Örneğin, farklı tehditlerin etkisi dört kriter kullanılarak değerlendirilir: verimlilik kaybı, gelir kaybı, yasal cezalar ve itibar gibi. Bir tehdit için genel etki, bu kayıpların ağırlıklı bir toplamından oluşmaktadır. En uygun koruma stratejisinin seçimi için benzer bir analiz yapılır. Karşı önlemler, riski ne kadar iyi azalttıklarına, ne kadar maliyetli olduklarına ve ne kadar bakım gerektirdiğine bağlı olarak seçilmektedir [29].

2.3.10. Risk izleme

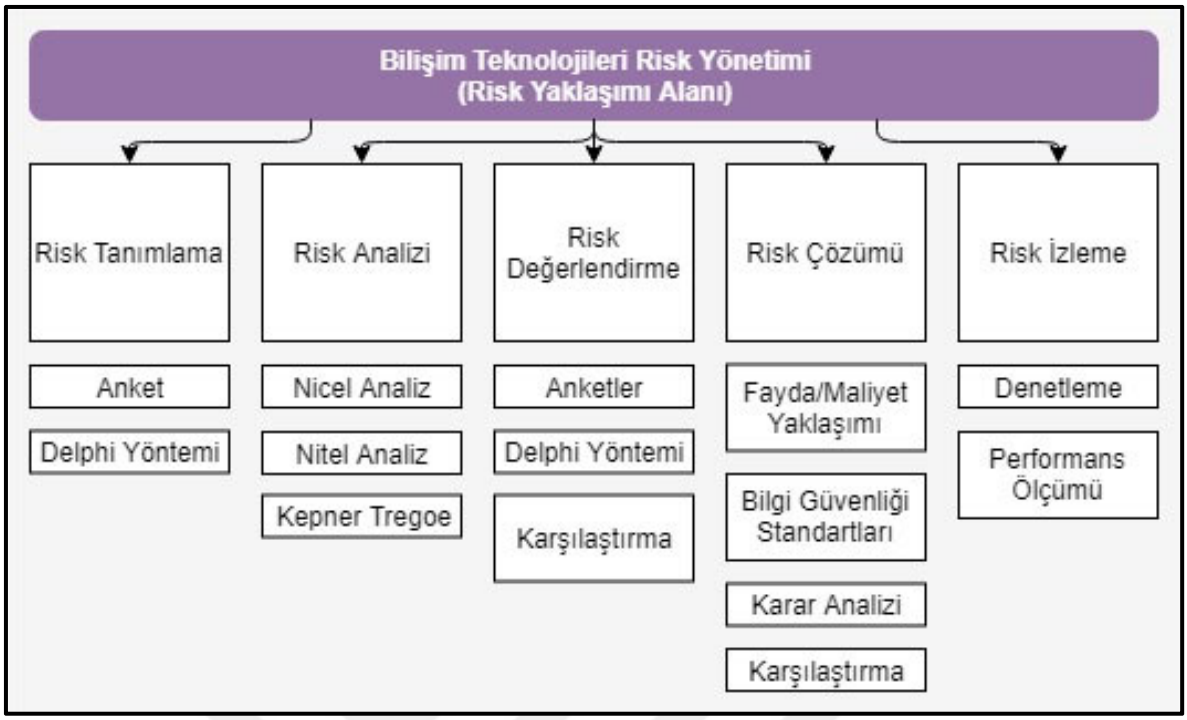
Devam eden bir risk izleme fonksiyonu büyük öneme sahip olmalıdır. Böyle bir eylem, karşı önlemlerin yalnızca etkili ve zamanında uygulanmasını değil, aynı zamanda uygunluğunu ve çalışmasını da sağlamaktadır [6].

Şekil 2.3.' de, risk yaklaşım alanına ilişkin analiz yöntemleri gösterilmiştir.

RY' ne yönelik herhangi bir yaklaşım, kapsamlı ve dinamik bir şekilde, bilgi teknolojisi alanının bütünlüğünü mümkün olduğunca ele almalıdır [6].

Kurumsal operasyonlara (görev, işlevler, imaj veya itibar dahil), kurumsal varlıklar, bireyler, diğer kuruluşlar veya bir bilgi sisteminin işletilmesinden veya kullanımından kaynaklanan uluslararası RY süreci aşağıdaki maddelerden oluşmaktadır [111].

i. Risk değerlendirmesi yapılması
ii. Bir risk azaltma stratejisinin uygulanması
iii. Bilgi sisteminin güvenlik durumunun sürekli izlenmesi için tekniklerin ve prosedürlerin kullanılması
iv. Toplam RY programının belgelenmesi



Şekil 2.3. Risk yönetim kavramları alt alanları [6]

BG, bilgi sistemlerinin gizliliğini, bütünlüğünü ve hazır bulunma durumunu, teknoloji, farkındalık, eğitim, öğretim ve planın uygulanmasındaki yayılma ve işlenme durumunu kayıt altında tutmalıdır [18].

Risk, olasılık ve etki olmak üzere ikiye ayrılabilir. Risk, olasılık ve etki kalemlerinin ürünüdür [23]. Bir riskin sonucunu ortaya çıkaracak olumsuz durumu sayısal bir puan olarak ifade etmek gerekirse, riskin gerçekleşme ihtimali ile vereceği zarar yani riskin etkisi risk puanını ifade etmede kullanılabilecektir.

Risk Puanı = Olasılık x Etki

Olasılık seviyesi tanımları [23]:

- Yüksek/Çok büyük olasılık: Bu riskin ortaya çıkma ihtimalinin yüksek olması, bu nedenle sorun yaratma (70%<Risk Puanı).
- Orta/Olası: Bu gibi riskler arada bir soruna dönüşebilir (30%<Risk Puanı<70%).
- Düşük/İyileştirilemez: Bunun bir problem olma olasılığı çok fazla değil (0%< Risk Puanı<30%).

ISO/IEC 27001 standardı, RD ve risk telafisi de dahil olmak üzere RY için tüm adımları tanımladığından, bir RY kılavuzu olarak da görülebilmektedir [29].

2.4. Kişisel Verilerin Korunması

KV' nin tanımlanmış veya tanımlanabilir bir birey hakkında herhangi bir bilgi olduğu kabul edilir [112]. Tanımlanabilirlik kimliği doğrudan veya dolaylı olarak belirlenebilen herhangi bir kişi anlamına gelmektedir.

El ile veya otomatik olarak KV' in toplanması, depolanması ve işlenmesi izni, sahiplerinin mahremiyet alanına girer ve bu nedenle, bu işlemlerden sorumlu kuruluşların, onları korumak için yasalarca zorunlu tutulması gerekir [35].

Bu hali ile KV belirli bir kişiyi gösterebilmesi ve nesnel ve işlenebilir olması nedeni ile meta bir bilgi olarak adlandırılabilmektedir.

Avrupa'da veri korumayla ilgili düzenlemeler açısından değişim girişimlerini desteklemiştir. Buna göre, 2012' de Avrupa Komisyonu, KV' in korunması için her ülkede (aktarılmaya gerek kalmadan) doğrudan uygulanacak yeni bir düzenleme önermiştir [113]. Bu düzenleme 2016 yılında Avrupa Birliği (AB) tarafından onaylanmıştır, böylece Mayıs 2016' da yürürlüğe giren ve başvurusu mecburi üyelerin uygulanması zorunlu olan Genel Veri Koruma Yönetmeliği 25 Mayıs 2018' de sonuçlanmıştır [112].

Ülkemizde ise bu konudaki gelişmeler oldukça yeni olup, 30823 Sayılı Resmi Gazete' de yayınlanan 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi ile bilgi ve iletişim güvenliğine ilişkin bir takım tedbirler sıralanmıştır [137]. Her ne kadar genelgede yer alan tedbirlerin uygulanmasına ilişkin bir rehber yayınlanacağından bahsedilmiş olsa da çalışmanın tamamlandığı tarih itibariyle henüz yayınlanmıştır.

Genelgede, "bilginin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir [137]" ifadesi ile ilerleyen dönemlerde ülkemizde de bilgi güvenliği alanında yasal düzenlemelerin ve başta kamu kurum ve kuruluşları olmak üzere, KV' e sahip işletmelerin uyması zorunlu olan bilgi güvenliği düzenlemeleri, beklenen bir durum haline getirmektedir.

3. İLGİLİ ARAŞTIRMALAR

Bu bölümde, BG yönetim süreci sertifika aşamasına kadar özetlenmiştir. Belli başlı ulusal ve uluslararası BGYS' leri için karşılaştırma tabloları oluşturulmuş ve değerlendirilmiştir. AB ve ülkemizde BG' den sorumlu kurumlara değinilmiştir. Kritik sektörlerde BG ve BG' nin maliyeti konularına değinilmiş ve kritik bir sektör olarak hukuk alanına değinilmiştir.

3.1. Bilgi Güvenliği Yönetimi

Son yıllarda, siber riske artan bir ilgi duyulmakta ve siber riskin işletmeler ve toplumlar üzerinde ciddi etkiye yol açabileceği için uğraşılması en zor konular arasında olduğu düşünülmektedir. Sosyal ağların, mobil cihazların, kablosuz teknolojilerin ve bulut hizmetlerinin yayılmasıyla iş dünyasında ve günlük gerçeklikte BT' nin genişlemesi, kırılganlığın artmasına neden olmuştur. Birçok şirket BG' ni büyük bir iş riski olarak görülmektedir. Geniş güvenlik önlemi uygulamasına rağmen, ihlallerden kaynaklanan kayıplar hala oldukça yüksektir [29].

Gizlilik, bilginin yetkisiz kişilerin, kuruluşların veya süreçlerin bilgisine sunulmaması veya ortaya çıkarılmamasıdır. [114].

Bütünlük, veri bütünlüğüne ve sistem bütünlüğüne ayrılmaktadır. Veri bütünlüğü, verilerin yetkisiz bir şekilde değiştirilmediği veya imha edilmediği anlamına gelmektedir [115]. Sistem bütünlüğü, bir sistemin amaçlanan işlevini sistemin kasıtlı veya kazayla yetkisiz müdahaleden arındırılmış, zarar görmemiş bir şekilde yerine getirmesidir [116]. Uygunluk ise, talep üzerine erişilebilir ve kullanılabilir olma özelliği olup yetkili bir başka kullanıcıdan temin edilmektedir [15].

Kurumsal bir BG yapısı kurmak için aşağıdaki adımlar izlenebilir [12]. Bu adımlar hukuk büroları gibi küçük bir işletme olarak görülebilecek yapılar için de geçerlidir.

Hazırlık: İlgili iş ortakları da gözetilerek, veriler hazırlanır ve tespit edilen sorunlar da bu aşamaya dahil edilir.

Veri toplama ve analizi: Mevcut yapılar, kaynaklar, ilgili çalışanlar ve tesislerin bir envanterini içerir. Toplanan veriler, potansiyel zayıflıkları bulmak için uygun bir RD ile analiz edilir.

İş süreç geliştirme: Analiz sonucu elde edilen girdilerle yeni süreçler yaratılır. Risklerin süreçlerle birlikte nasıl yönetilebileceği ve iş süreçlerinin mümkün olduğu kadar etkili ve uygulanabilir tutulması düşünülür.

Anlayış ve planlama: Uygun bir anlayış tanımını ve yaklaşan faaliyetlerin planlanmasını içerir. BG önlemleriyle mevcut iş süreçlerinin bir araya getirilir. Burada önemli olan önlemlerin süreçleri yavaşlatma ve benzeri açılardan olumsuz etkilememesidir. Planlama içerisinde risk öngörülerinin gerçekleşmesi durumunda bununla ilgilenecek sorumluların ve acil eylem planlarının da yer alması gerekir.

Uygulama: Önemli olan, çalışanların bu konuda bilinçli ve eğitilmiş olmasıdır. Çalışanların riskten kaçınma ve riskin gerçekleşmesi durumunda uymaları gereken prosedürler kendilerine anlatılmış ve gerekli ise riskin sonuçları konusunda sorumlulukları belirlenmiş olmalıdır.

İzleme ve bakım: Sürecin uygulanması sırasında, yapılan ölçümlerle süreç sürekli izlenir ve karar verilen kalite ve bilgi güvenliği düzeyi korunur. Tekrarlanan riskler belirlenerek ek güvenlik tedbirlerinin alınması amacıyla ek eylemler gerçekleştirilebilir.

Harici sertifika: Zorunlu olmasa da kurumun güvenlik yönetim süreçlerini bir sertifikasyon aracılığı ile tescil edebilmesi mümkündür. Hassas bilgilerle çalışan, kuruluşlar açısından güvenlik gereksinimlerinin tam olarak yerine getiriliyor olması ve bunun sertifikalanmış olması, kuruluştan faydalananlar açısından bir tercih kriteri olacağı unutulmamalıdır.

3.2. Bilgi Güvenliği Yönetim Sistemlerine Genel Bir Bakış

Uygulamada ulusal ve uluslararası çok sayıda BGYS bulunmaktadır [50]. Belli başlı BGYS' leri aşağıdaki şekilde özetlenebilir.

3.2.1. Avusturya BT güvenlik el kitabı

Avusturya BT Güvenlik El Kitabı, Avusturya Federal İdari İşleri tarafından 1998 yılında yayınlanmış ve iki parçadan oluşmaktadır. Birinci bölüm BT güvenlik yönetimi sürecinin tanımı, risk analizi, güvenlik kavramlarının tanımı, güvenlik planının uygulanması ve takip eden adımlardan oluşmaktadır. İkinci bölümde 230 temel güvenlik önlemi yer almaktadır. İlk geliştirilme aşamasında devlet kurumlarına yönelik olmasına rağmen günümüzde tüm kurumlara hitap etmektedir. Avusturya BT Güvenlik El Kitabı risk yönetimi ile ilgili riskin tanımlanması, risk analizi, risk değerlendirme, ölçme, işleme, kabulü ve iletişimi konuları kapsamaktadır [117].

3.2.2. Hollanda A&K analizi

A&K Analizi Hollanda Hükümeti tarafından 1996 yılında tamamlanıp duyurulmuş ve o tarihten beri güncellenmemiştir. Hollanda Hükümeti tarafından desteklenen yöntem Hollanda devlet kurumlarının yanı sıra Hollanda' daki diğer kurumlar tarafından da kullanılmaktadır [117].

3.2.3. Ortak güvenlik açığı puanlama sistemi - Özel ilgi grubu - Birinci (CVSS-SIG-First)

Cisco Systems, Symantec, ISS, Qualys, Microsoft, CERT/CC ve eBay gibi çeşitli BT güvenlik şirketlerini içeren Amerika Birleşik Devletleri (ABD) Ulusal Güvenlik Bakanlığı tarafından başlatılan ortak çalışmadır [9].

3.2.4. Bilgi güvenliği değerlendirme ve izleme yöntemi (ISAMM)

Belçika Telindus Grup tarafından 2002 yılında yayınlanmış olup, bir kurumdaki bilgi güvenliği yönetim sistemini destekleyen nitel yönteme dayalı risk analiz metodudur. Kurumlara bu yöntem ilgili varlık ve tehditlerin tanımlanması, tanımlanan güvenlik açıklıklarına göre tehditlerin olasılık ve etkilerinin ölçülmesi, risklerin sunumu ve bu risklerin kabul edilebilir ya da kabul edilemez olmalarına karar verilmesi, kabul edilemez riskler için alınacak önlemlere karar verilmesi ve risk iletişim sürecinin grafik ve raporlarla desteklenmesi konularında yardımcı olmaktadır [20].

3.2.5. Bilgi teknolojileri temel koruma kılavuzu (IT-Grundschutz)

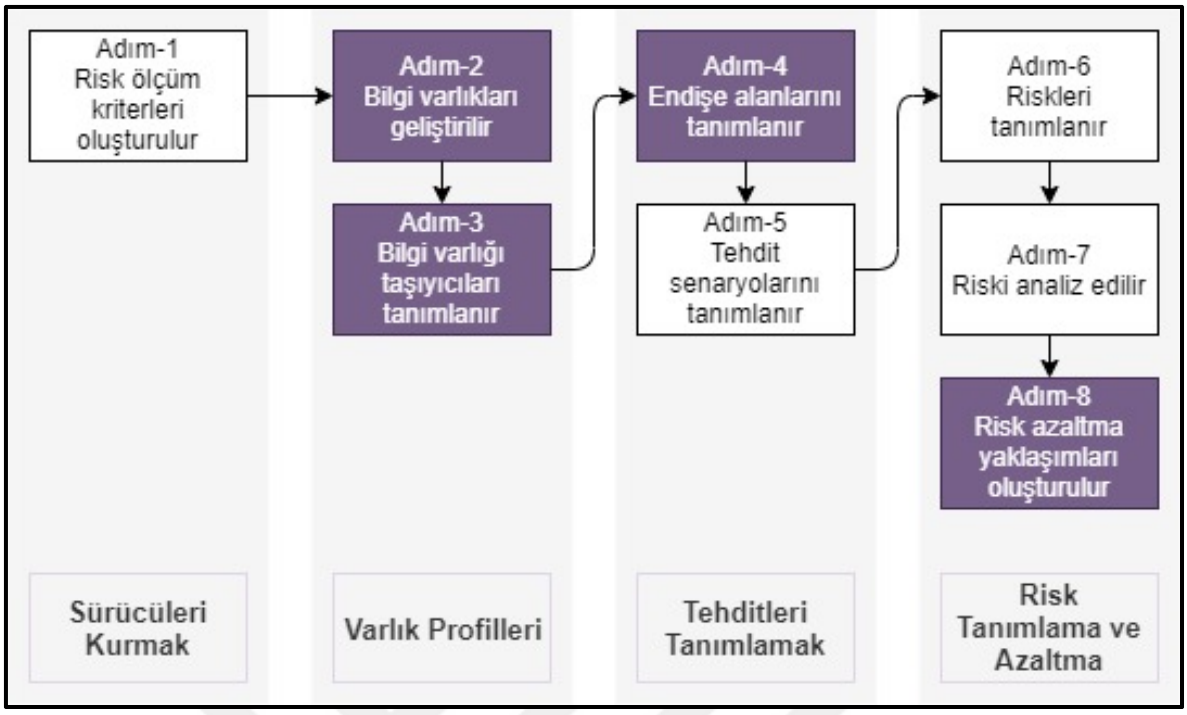
IT-Grundschutz (Bilgi Teknolojileri Temel Koruma Kılavuzu, IT- Grundschutz) Almanya Bilgi Güvenliği Bakanlığı tarafından 1993 yılında kurumlara BGYS kurmak için tasarlanmış bir yöntemdir. Son sürümü 2005 yılında yayınlanmış olup Alman hükümeti için merkezi BT güvenlik hizmeti sağlayıcısıdır. IT-Grundschutz' un amacı kurumlara BT güvenlik yönetimi için bir çerçeve sağlamaktır. Belirli bir etki alanında gerekli BT güvenlik seviyesine ulaşmak için uygulanabilir BT güvenlik süreci ve detaylı teknik öneriler içeren bir yönteme sahiptir [20].

3.2.6. Operasyonel olarak kritik tehdit, varlık ve güvenlik açığı değerlendirmesi (OCTAVE)

İleri hesaplama içeren ağır riskli bir risk metodolojisidir. Operationally Critical Threat, Asset, and Vulnerability Evaluation (Operasyonel Olarak Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi, OCTAVE) Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü' nde geliştirilmiştir. OCTAVE teknik riske değil kuruluş içi riske odaklanmaktadır. OCTAVE iki versiyona sahiptir: Büyük kuruluşlar için OCTAVE ve küçük kuruluşlar için OCTAVE-S, her iki modelleme de, modelleme sonuçlarını belgelemek için özel uygulama katalogları, profiller ve çalışma sayfalarına sahiptir [9]. OCTAVE, güvenlik RY için risk temelli bir stratejik değerlendirme ve planlama tekniğidir. Organizasyondaki farklı düzeylerdeki bilgilerden faydalanılarak kritik varlıklar ve tehditleri belirlenir. Açıklıklar kurumsal ve teknolojik olarak belirlenir. Kurumun misyonunu ve önceliklerini destekleyecek şekilde bir uygulama-tabanlı koruma stratejisi ve risk azaltma planları geliştirilmektedir [20]. OCTAVE yöntemi, BG için risk bazlı bir stratejik değerlendirme ve planlama yöntemidir [27]. Temel Modeli Şekil 3.1.' de görülen OCTAVE, kurumsal risklerin değerlendirilmesine odaklanmaktadır ve teknolojik riskleri ele almamaktadır [47].

3.2.7. Açık web uygulama güvenliği projesi (OWASP)

Open Web Application Security Project (Açık Web Uygulama Güvenliği Projesi, OWASP), web uygulaması güvenliği alanında serbestçe erişilebilir makaleler, metodolojiler, belgeler, araçlar ve teknolojiler yaratan çevrimiçi bir topluluktur [9].

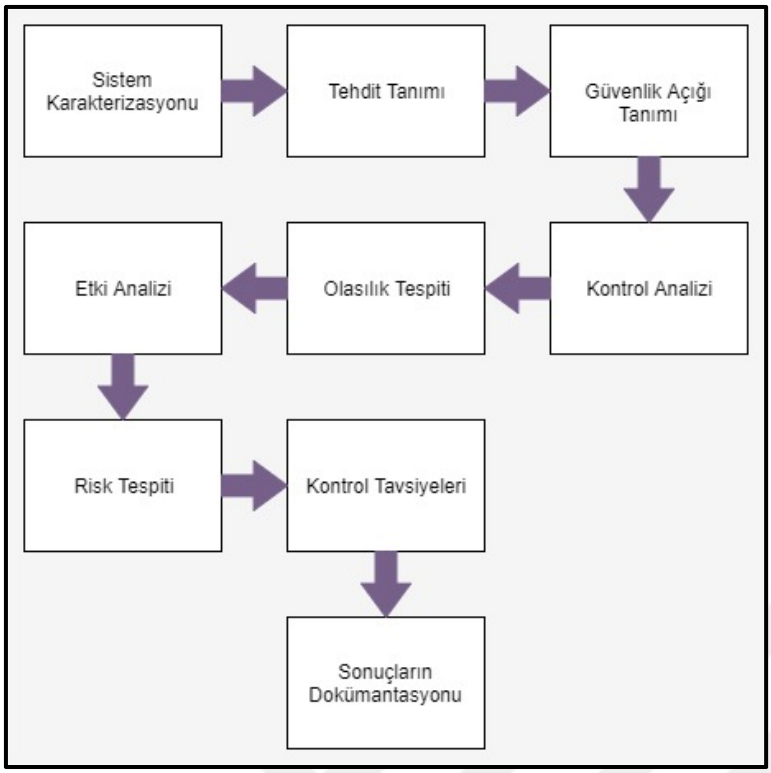


Şekil 3.1. OCTAVE temel modeli [44]

3.2.8. Ulusal standartlar ve teknoloji enstitüsü - Özel yayın (NIST-SP 800-30)

SP 800-30, ABD' de NIST tarafından 2002 yılında yayınlanmıştır. SP 800-30, BT için RY' ne genel bir bakış sağlar ve sistem geliştirme yaşam döngüsünün nasıl desteklediğini belirtir. Ayrıca RD yöntemi ve BT sisteminin bir RD yürütülmesi konusunu dokuz temel adımda açıklar. Dokuz adım sistemin tanımlanması, tehditlerin tanımlanması, açıklıkların tanımlanması, kontrol analizleri, olasılıkların belirlenmesi, etki analizi, riske karar verilmesi, kontrol önerileri ve raporlama şeklindedir. SP800-30 risk azaltma seçenekleri ve risk azaltma stratejileri de dahil olmak üzere, süreci, kontrol uygulanması için yaklaşımı, kontrol kategorilerini, fayda-maliyet analizini ve artık riskleri de değerlendirmektedir. Son olarak, başarılı bir RY programı ve devam eden bir risk ölçme ve değerlendirme süreci için gerekli faktörleri açıklamaktadır [118].

Şekil 3.2.' de görülen SP 800-30 modeli, bilişim sistemlerinin etkin RY sürecinin geliştirilmesi için risk temelli bir yaklaşım olup işletme süreçleri ve BG faaliyetleri arasındaki bağlantıda temel prensipleri belirlemektedir [10].

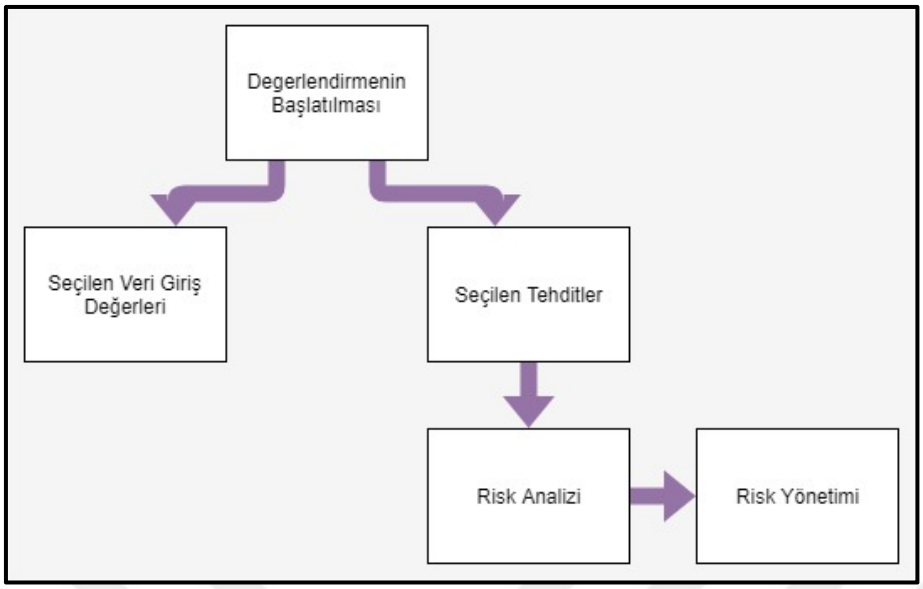


Şekil 3.2. NIST SP 800-30 temel modeli [9]

3.2.9. CCTA risk analizi ve yönetimi metodu (CRAMM)

Central Communication and Telecommunication Agency (İngiltere Merkez Bilgi İşlem ve Telekomünikasyon Ajansı, CCTA) tarafından geliştirilen nitel bir güvenlik RY yaklaşımıdır [119]. CCTA Risk Analysis and Management Method (CCTA Risk Analizi ve Yönetimi Metodu, CRAMM) yaklaşımında RY süreci, Şekil 3.3' de de görüleceği üzere üç aşamada tanımlanmaktadır [10]:

i. Varlıkların tanımlanması ve değerlenmesi (verileri, uygulama yazılımını ve fiziksel varlıkları tanımlar)
ii. Tehdit ve güvenlik açığı değerlendirmesi (tehditleri ve zayıf noktaları tanımlar)
iii. Risk hesaplama (her varlık için riski hesaplar)



Şekil 3.3. CRAMM temel modeli [43]

3.2.10. Harmonize risk analizi yöntemi (MEHARI)

MEthod for Harmonized Analysis of RIsk (Harmonize Risk Analizi Yöntemi, MEHARİ) Fransız Bilgi Güvenliği Uzmanları Birliği tarafından geliştirilen RA ve RY' ne dayalı bir yaklaşımdır. MEHARI' de RA beş aşamada tamamlanır: Bağlam kuruluşu, destek analizi ve varlık sınıflaması, risk tanımlaması, RA ve RD. RY dört aşamada tamamlanır. Bu aşamalar risk değerlendirmesi, risk çözümü, risk kabulü ve risk iletişimi şeklindedir [10].

3.2.11. Bilgi sistemleri risk analizi ve yönetimi metodolojisi (MAGERIT)

Methodology for Information Systems Risk Analysis and Management (Bilgi Sistemleri Risk Analizi ve Yönetimi Metodolojisi, MAGERIT) 1997 yılında İspanya Bakanlığı Kamu İdaresi tarafından yayınlanmıştır. 2005 yılında yayınlanan MAGERIT v2 sürümü ile beraber Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü, OECD) içindeki Bilgi Sistemleri Güvenliği için OECD Yönergeleri ve Ağlar' ın 6. Kuralında RD gerekli bir adım olarak değerlendirilmeye başlanmıştır. MAGERIT v2 ile ilişkili olan EAR ve PILAR isimli yazılımları sayesinde farklı standart ve formatta grafiksel araçlar sunmaktadır [20].

3.2.12. İşletme riskinin yönetimi için entegre metodoloji (MIGRA)

Metodologia Integrata per la Gestione del Rischio Aziendale (İşletme Riskinin Yönetimi İçin Entegre Metodoloji, MIGRA), 1999 yılında yayınlanmış olan nitel bir RD ve RY modeli olup BT ve diğer maddi duran varlıklara uygulanmaktadır. MIGRA analistlere tehditler, saldırılar, güvenlik önlemleri ve güvenlik çemberi bileşenleri arasındaki ilişkileri anlamalarında yardımcı olmaktadır. Böylece yöntem, her güvenlik önleminin risk ve maliyet açısından değerlendirilmesini sağlayarak uygulanıp uygulanmaması kararında yardımcı olmaktadır [120].

3.2.13. İhtiyaçların ifade edilmesi ve güvenlik amaçlarının belirlenmesi (EBIOS)

Expression des Besoins et Identification des Objectifs de Sécurité (İhtiyaçların İfade Edilmesi ve Güvenlik Amaçlarının Belirlenmesi, EBIOS), Kamu ve özel sektörde yaygın olarak kullanılan Direction Centrale de la Sécurité des Systémes d'Information, Premier Ministre (Başbakan Bilgi Sistemleri Güvenliği Merkez Müdürlüğü, DCSSI) yaklaşımıdır. Yaklaşım, RA sürecinin beş aşamada tamamlandığı BT sistemlerinin güvenlik gereksinimlerine ve hedeflerine dayanmaktadır [121]:

i. Bağlam ve çevresel analiz
ii. Güvenlik gereksinimlerinin değerlendirilmesi
iii. Riskli analiz
iv. Risk amaçlarının belirlenmesi
v. Güvenlik gereksinimlerinin belirlenmesi

EBIOS uluslararası standartlar olan ISO/IEC 27001, ISO/IEC 15408, ve ISO/IEC 17799 ile uyumlu olup AB, Fransa, Tunus, Luksemburg da özel sektör firmaları tarafından tercih edilen bir yöntemdir [20].

BG' de yalnızca bir standartla uyumluluk yeterli olmayabilir. Bir standarttaki gereklilikler ve teknik kontroller güncel değilse ve yeni tehditler ve güvenlik açıkları ile yeterince başa çıkamıyorsa, sertifikalandırılan sistem detaylı bir değerlendirme sonunda bile hala tespit edilmemiş kusurlara sahip olabilmektedir. Bu nedenle, bir standardın güvencesini garanti etmedeki etkinliği, sadece ihtiyaç duyduğu değerlendirmenin derinliğine veya kontrollerin

açıklandığı ayrıntıya dayanarak değerlendirilemez [17]. Bu nedenle, herhangi bir BG standardı ile uygulanabilir uyumu sağlamak için kapsamı ve olası boşlukların tanımlanması gerekmektedir [16].

BT güvenlik standartlarının çalışması, son yıllarda spesifik çerçevelerin benimsenmesine ilişkin kılavuzlar [122, 123] veya çoklu standartların karşılaştırılması [124-126] şeklinde gelişmiştir. Bu çalışmaların çoğu, farklı çerçevelerde bulunan genel özelliklerin karşılaştırılması ile sınırlı kalmıştır ve kontrollerini, ihmallerini veya birbirlerini nasıl tamamladıkları veya birbirleriyle nasıl örtüştüklerini dikkate almamıştır. Üst üste binme ve boşluklar özellikle göz önüne alındığında bile, sınırlamalar ve eksiklikler hakkında derinlemesine bir açıklama yapılmamıştır [17].

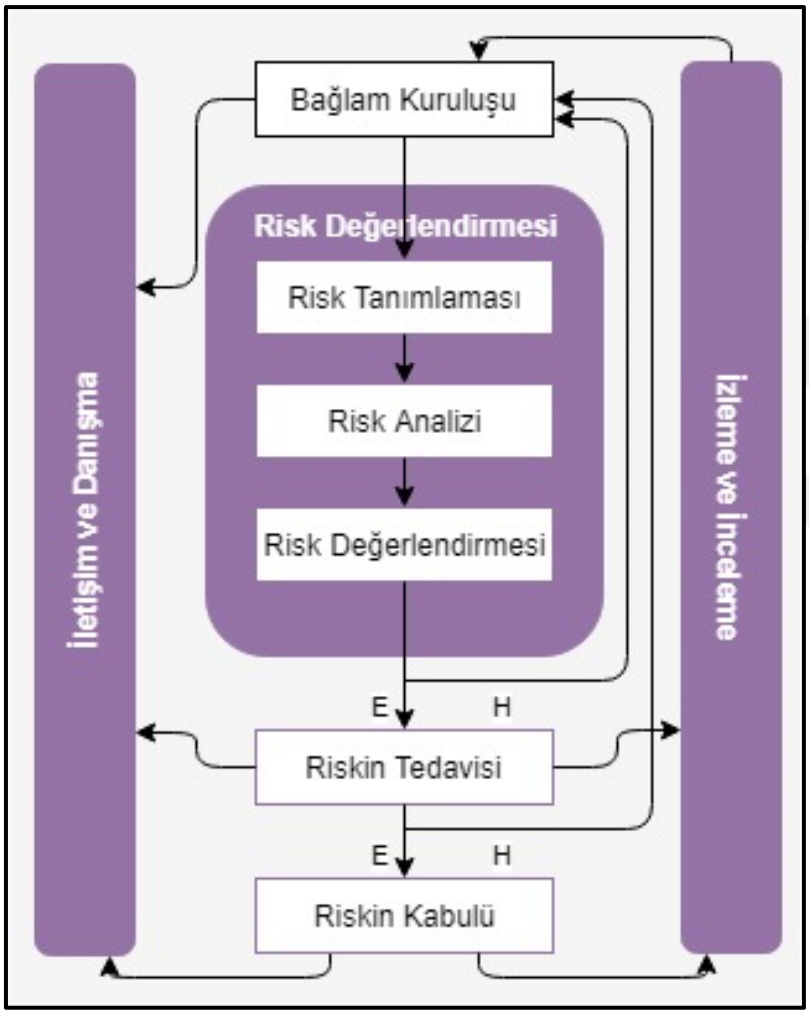
Modern RD metodolojilerinin ve araçlarının çoğu varlığa dayalıdır, yani tüm RD sürecine bir altyapının varlıklarının değeri (veri, bilgi veya kaynaklar) üzerinden yaklaşmaktadırlar. Bilgi teknolojisi sistemlerinin sertifikasyonu için uluslararası bir standart olan ISO/IEC 27001 [58], süreç bazlı RD' den yararlanma yeteneğini açıkça ortaya koymaktadır. Bu standartlara ek olarak, 2016/1148 numaralı Avrupa Parlamentosu ve Konsey Direktifi, hizmet odaklı bir RY' nin varlığına ihtiyaç duyulduğunu belirtmektedir. Bu direktifte amaç, vatandaş hizmetleri için gerekli olanı korumak olduğundan dolayı süreçlere öncelikli odaklanmayı süreçlerin içine yerleştiren bir yaklaşımı ifade etmektedir. Bu tür hizmetler (işlemler) tekli veya çoklu altyapılarla sağlanabilmektedir [25].

EBIOS, MEHARI, CRAMM, Bundesamt für Sicherheit in der Informationstechnik (Federal Bilgi Teknolojileri Güvenliği Ofisi, BSI) 100-3 ve OCTAVE gibi yöntemler, uzman görüşüne dayanan, ancak sonuçlara bir derece öznellik getiren nitel yaklaşımı takip etmektedir. MAGERIT gibi kantitatif veya hibrid yaklaşımı izleyen yöntemler belirsizlik altında karar vermeyi desteklemek için kullanılan matematiksel bir kanıt sağlamakta, ancak yüksek kaliteli girdi verileri ve iyi geliştirilmiş bir proje modeli gerektirmektedir [25].

3.3. Bilgi Güvenliği Yönetim Sistemleri

BT sistemlerinde RY ve güvenlik yönetimi son yıllarda dünyadaki hemen hemen tüm ülkelerde önemli bir konu haline gelmiştir. Güvenlik analizi ve yönetimi alanında, son 10 yılda çeşitli ISO/IEC standartları belirlenmiştir. ISO/IEC standartlarında Bilgi Güvenliği

Risk Yönetim Süreci Şekil 3.4.' de görüldüğü şekildedir [1, 58-61]. Standartların yanı sıra, risk analizi ve yönetimini sağlayan bazı yöntemler geliştirilmiştir. Dünya çapında 200' den fazla yöntem vardır, ancak bunların %80' inden fazlası pratik olarak kullanılmamakta veya halka açık değildir. Diğerleri arasında sadece birkaç tanesi dünya çapında kabul görmektedir. Kabulleri, standartlara, tavsiyelere vb. uyumluluktan ve güncelleme ve destek faaliyetlerinden kaynaklanmaktadır [24].



Şekil 3.4. Bilgi güvenliği risk yönetim süreci [61]

Verimli BG, izlenen sistemlerdeki istenmeyen olaylara veya olaylara neden olan senaryoların ayrıntılı bir tanımlanmasına dayanmaktadır. RD' ye dayanan güvenlik standartları (örneğin, ISO/IEC 27K serisi [58, 61]) bir kuruluşun tanımlanmış varlıkları üzerinde güvenlik açığı olan olumsuz eylemleri gerçekleştirmek için kaynak yada tanımlanmış bir risk olasılığı gibi tehdidi sık sık tanımaktadır. BT sistemine olası ve devam etmekte olan saldırıların kapsamlı ancak doğru bir şekilde azaltılmasını sağlamak için,

riskleri sürekli olarak ölçen ve izlenen sistemde hedeflenen BG tehditlerine nasıl yanıt vereceğine karar veren bir yanıt çerçevesine dayanan bir güvenlik yönetim sistemi geliştirilmiştir. Bu çerçeveye dinamik RY müdahale sistemi denilmektedir [31].

BGYS iş hedeflerini gerçekleştirmek için BG' ni kurmak, uygulamak, yönetmek, işletmek, gözlemlemek, gözden geçirmek, sürdürmek ve geliştirmek için olan sistematik bir yaklaşımdır [127]. BGYS analiz ve tasarım metotlarını, BT kullanıcılarını, topluluk yönetim problemlerini ve etik problemleri kombine eden bir yapıya sahiptir [128].

3.3.1. Uluslararası standartlar

Çizelge 3.1.' de yer alan uluslararası standartlara bakıldığında, hemen hemen hepsinin Küçük ve Orta Boy İşletmeler (KOBİ) ile büyük boy işletmelere uygun olduğu, yani her türde kuruluş tarafından kullanılabilir olduğu görülmektedir. BGYS odaklarının RD ve RY, esnekliklerinin ise esnek ve esnek değil arasında değişken olduğu görülmektedir. Tamamı tüm sektörlere hitap eden BGYS' lerinin yaklaşımlarının açık bir şekilde birbirlerinden farklı oldukları görülmektedir.

Örneğin, ISO/IEC 27001 BGYS' de yaklaşım varlık ve kontrol tabanlı olduğu görülmektedir.

Çizelge 3.1. Uluslararası risk değerlendirme ve yönetim standartları kriterleri [36]

	KRİTER	**ISO/IEC 27001**	**OCTAVE**	**CRAMM**	**NIST SP 800-30**
1	**Ölçek**	KOBİ' ler ve Büyük Organizasyonlarda kuruluşun BGYS' sini kapsar	Büyük Organizasyonlarda kuruluşun tamamını kapsar	KOBİ' ler ve Büyük Organizasyonlarda kuruluşun BT ile ilgili risklerini kapsar	KOBİ' ler ve Büyük Organizasyonlarda kuruluşun BT ile ilgili risklerini kapsar
2	**Odak**	RD ve RY	RD ve RY	RD	RD
3	**Esneklik**	Kısmen Esnek	Esnek	Esnek Değil	Kısmen Esnek
4	**Karmaşıklık**	Orta	Düşük	Yüksek	Düşük
5	**Yaklaşım**	Varlık ve Kontrol Tabanlı	Risk Bazlı Değerlendirme ve Planlama	Varlıkların Niteliklerine Dayalı Yaklaşım	BT İle İlgili Risk Bazlı Yönetim

Çizelge 3.2. (devam) Uluslararası risk değerlendirme ve yönetim standartları kriterleri [36]

6	**Araç Desteği**	Hayır	Evet	Evet	Bilinmiyor
7	**Yayın Tarihi/ Son Güncelleme**	2005/2013	1999/2005	1985/2011	2000/2012
8	**Hedef**	Tüm Sektörler	Tüm Sektörler	Tüm Sektörler	Tüm Sektörler

3.3.2. Ulusal standartlar

Çizelge 3.2.' de yer alan ulusal standartlara bakıldığında, hemen hemen hepsinin KOBİ ve büyük boy işletmelere yani her türde kuruluş tarafından kullanılabilir olduğu görülmektedir. BGYS odaklarının RD ve RY, esnekliklerinin ise esnek ve esnek değil arasında değişken olduğu görülmektedir.

Çizelge 3.2. Ulusal risk değerlendirme ve yönetimi standartları kriterleri [36]

	Kriter	**BSI 100-3**	**MAGERIT**	**MEHARI**	**MONARC**
1	**Ölçek**	KOBİ' ler ve Büyük Organizasyonlarda kuruluşun BGYS' sini kapsar	Büyük Organizasyonlarda kuruluşun tamamını kapsar	Orta ve Büyük Organizasyonlarda kuruluşun tamamını kapsar	KOBİ' ler ve Büyük Organizasyonlarda kuruluşun tamamını kapsar
2	**Odak**	RD ve RY	RD	RD	RD ve RY
3	**Esneklik**	Kısmen Esnek	Kısmen Esnek	Kısmen Esnek	Kısmen Esnek
4	**Karmaşıklık**	Orta	Düşük	Düşük	Düşük
5	**Yaklaşım**	Varlık ve kontrol temelli	Varlık tabanlı	Formül ve parametrelere dayalı analiz	İşletmeye bilgi varlıkları ve risk senaryolarına dayalı
6	**Araç Desteği**	Evet	Evet	Evet	Evet
7	**Yayın Tarihi/ Son Güncelleme**	2004/2008	1997/2013	1998/2010	2016/2016
8	**Hedef**	Tüm Sektörler	BT ve İletişim Organizasyonları	Büyük ve Orta Boy İşletmeler	Tüm Sektörler

3.4. AB Ülkelerinde ve Türkiye' de Bilgi Güvenliğinden Sorumlu Kurumlar

Fransa: Fransız Siber Güvenlik Stratejisi, Ulusal Dijital Güvenlik Stratejisi olarak adlandırılarak tamamen BG konularından daha geniş bir perspektife sahiptir. Agence nationale de la sécurité des systèmes d'information (Fransa Ulusal Siber Güvenlik Ajansı, ANSSI) BG' nin sivil tarafının lider ajansıdır. Fransız BG' nin örgütsel yapısını ANSSI etrafında toplanmıştır. Bu kurum, devlet kurumlarına BG yardımcı olmaktan, endüstriler ve kritik altyapılar için BG standartlarını düzenlemekten ve siviller için bilinçlendirme kampanyaları ve eğitimi düzenlemekten sorumludur [34].

Finlandiya: Finlandiya BG yaklaşımı bütünsel, kapsamlı ve kapsayıcı bir yapıya sahiptir. Tüm paydaşlarının siber esnekliğini, hazırlıklı olmalarını ve farkındalıklarını artırmaya yöneliktir. Özel olarak, BG politikaları ve bunun yanı sıra kritik bilgi altyapısının korunması, siber suçların önlenmesi, uluslararası işbirliği ve uzmanlığın geliştirilmesinden sorumludur. Finlandiya' nın özel BG ve BG çerçevesi, ulusal güvenlik çerçevesini yansıtmaktadır. Bu nedenle, sivil hükümet politika-stratejik boyutu yönlendirirken, operasyonel sorumluluklar ilgili bakanlıklara, kurumlara ve paydaşlar dağıtılmaktadır. Bununla birlikte, koordinasyonu ve izlenmesi, Savunma Bakanlığı' nın bünyesinde bulunan ve başkanlık edilen Güvenlik Komitesi içerisinde merkezileştirilmiştir [34].

Almanya: Almanya BG için bütüncül bir yaklaşım benimsemektedir. Bundesamt für Sicherheit in der Informationstechnik (Federal Bilgi Teknolojileri Güvenliği Ofisi, BMI) politika geliştirme perspektifinden yola çıkmasına rağmen, operasyonel sorumluluk istihbarat topluluğundan, kolluk kuvvetlerinden ve kamu-özel irtibat bürosundan özel bir dizi kurum ve ofise devredilmiştir. Hem BG hem de BG politika geliştirme ve gözetim sorumluluklarına ve bu politikanın operasyonelleştirilmesine ayrılmıştır. BG politikaları geliştirme ek olarak, Şansölye Ofisi ve Federal Dışişleri Bakanlığı arasında bölünmüştür. Belirli operasyonel görevler, Federal Bilgi Güvenliği Ofisi ve Federal İstihbarat Servisi gibi belirli uzmanlık alanlarına sahip ajanslara devredilmiştir. Bununla birlikte, BG' de genel liderlik, İçişleri Bakanlığı' ndadır [34].

İngiltere: İngiltere' de BG, siber alanın sağladığı ekonomik ve sosyal fırsatların, kurumsal, kişisel/vatandaş ve ulusal çıkarlar için minimum risk ile herkese açık olmasını sağlamak anlamına gelmektedir. BG politikası, sivil, cezai adalet ve askeri/savunma konularını

kapsamaktadır. Politika oluşturma ve BG' deki genel liderlik Bakanlar Kurulu Ofisi' nden, özellikle Office of Cybersecurity (Siber Güvenlik Dairesi, OCS) sorumluluğundadır. Operasyonel eylemler Devlet İletişim Merkezi altında çalışan İstihbarat Toplama ve Güvenlik Sağlama Merkezi ve Savunma Bakanlığı sorumluluğundadır [34].

Avrupa Birliği: The European Union Agency for Cybersecurity (Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı, ENISA) AB, üye devletler, özel sektör ve AB vatandaşları için bir ağ ve bilgi güvenliği uzmanlığı merkezidir. ENISA, bilgi güvenliğinde iyi uygulamalar hakkında tavsiye ve öneriler geliştirmek için bu gruplarla birlikte çalışmaktadır. İlgili AB mevzuatının uygulanmasında üye devletlere yardım etmekte ve Avrupa' nın kritik bilgi altyapısı ve ağlarının direncini arttırmak için çalışmaktadır. ENISA, AB' de ağ ve bilgi güvenliğini iyileştirmeye yönelik sınır ötesi toplulukların gelişimini destekleyerek üye devletlerdeki mevcut uzmanlığı arttırmayı amaçlamaktadır [36].

Türkiye: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) Türkiye' nin en yetkin Ar-Ge merkezi olma özelliğiyle BİLGEM, Türkiye' de BG ve BT alanında teknolojik bağımsızlığı sağlamak için, askeri ve sivil BG' ni, bütünlüğünü, güvenli bir şekilde iletilmesini ve saklanmasını sağlayan teknolojik Ar-Ge çalışmaları gerçekleştirmektedir. 40 yılı aşan bilgi birikimi, deneyimi ve 1600' ü aşan personeliyle merkez, uluslararası standartlarda bilimsel ve teknolojik araştırmalar gerçekleştirmektedir [49].

BİLGEM' in temel faaliyetlerini Araştırma-Geliştirme, Test ve Değerlendirme, Prototip Üretimi ve Eğitim oluşturmaktadır. Merkezin ileri elektronik, bilişim teknolojileri, kriptoloji, siber güvenlik, yazılım teknolojileri, bilgi güvenliği, elektronik harp ve telekomünikasyon alanlarında bugüne kadar yüzlerce başarılı projeye imza atan enstitülere sahiptir. Bu enstitüler şu şekildedir: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), Bilişim Teknolojileri Enstitüsü (BTE), İleri Teknolojiler Araştırma Enstitüsü (İLTAREN), Siber Güvenlik Enstitüsü (SGE) ve Yazılım Teknolojileri Araştırma Enstitüsü (YTE) [49].

Ülkemizde BG' den sorumlu, 2012 yılında kurulan Siber Güvenlik Kurulu' nun başlıca görevleri şunlardır;

i. BG ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak
ii. Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak
iii. BG ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek
iv. Kanunlarla verilen diğer görevleri yapmak

olarak sıralanmıştır. Kurul, Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığında çeşitli bakanlıklar ve kurumlardan gelen üyelerin katılımından oluşmaktadır [138].

20/10/2012 tarih, 28447 sayılı Resmi Gazetede yayınlanan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince ulusal BG sağlanmasına ilişkin politika, strateji ve eylem planlarını hazırlamak ve koordinasyonunu sağlamak görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir [50].

3.5. Kritik Sektörlerde Bilgi Güvenliği

BG, kendisini bilimsel bir araştırmaya hazırlayan net bir şekilde ayrılmış akademik çalışma alanı değildir. Aksine, BG, teknikten davranışsal ve kültüre kadar çok sayıda disiplini birleştirmektedir. Bilimsel çalışma, tehditlerin hızla gelişen doğası, kontrollü deneyler yapma zorluğu ve teknik değişim ve yenilikçilik hızı ile daha da karmaşıklaşmaktadır. Kısacası, BG bir bilimden çok daha fazlasıdır [38].

Teknolojiye ek olarak, BG ayrıca insanların veriye ve işlemlere erişiminin olduğu anlamına da gelmektedir. Erişim yetkili veya yetkisiz olabilir. Siber saldırganlar, kötü niyetli etkinlikler gerçekleştirerek kişisel veya finansal kazanç için güvenlik açığından yararlanmaya çalışan bireyler veya gruplardır. Amatörlerin, bilgisayar korsanlarının ve organize bilgisayar korsanlarının, zarar verme niyetlerine bağlı olarak hedefleri her türde kuruluşlardır. Tehditler ayrıca kuruluşların içinden, ayrıcalıklı kullanıcılardan veya son kullanıcılardan gelebilmektedir. Siber saldırganların temel amaçları manipüle, tahrip, bozma ve çalmaktır [39].

Kritik altyapı sağlayıcıları, haberleşme, enerji, bankacılık/finans, kritik kamu hizmetleri, ulaştırma ve su yönetimi alanlarını kapsamaktadır. Kritik altyapılar, ulusal güvenlik için büyük önem taşımaktadır. Bu nedenle bu temel hizmetlerin sürekliliğini sağlamak için ulusal güvenlik stratejileri ve politikaları tarafından güçlü bir şekilde desteklenmesi gerekmektedir. Coğrafi bir yere bağlı olarak, kritik altyapılar ayrıca, Internet Servis Sağlayıcılarına bağımlılıklarını kritik hale getiren özel sektöre ait altyapıya (telekomünikasyon ağları) da büyük ölçüde dayanabilirler [46].

Örneğin kritik kamu hizmetleri kapsamında olan sağlık alanına ait özel güvenlik standartlarına kısaca değinilecek olursa [27]:

- BS EN 45502-1 (2015): Genellikle Aktif İmplante Edilebilir Tıbbi Cihazlar için geçerli olan gereksinimleri tanımlamaktadır. Ayrıca, belirli Aktif İmplant Yapılabilir Tıbbi Cihazlar için standartlar vardır.
- AAMI TIR57 (2016): Bir tıbbi cihaz için BG RY gerçekleştirme yöntemleri konusunda rehberlik sağlayarak tıbbi cihaz üreticilerini desteklemektedir. Asıl amaç cihazın gizliliğini, bütünlüğünü ve/veya kullanılabilirliğini veya cihazın işlediği bilgileri gizleyebilecek güvenlik tehditlerinden kaynaklanan riskleri yönetmektir.
- 1996 Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası: ABD' nde, Protected Health Information (Korunan Sağlık Bilgileri, PHI)' nin gizliliğini ve güvenliğini korumak için gerekenleri belirleyen bir sağlık mevzuatıdır. The Health Insurance Portability and Accountability Act (Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası, HIPAA) mevzuatı, kurumun bilgilerini şifresiz göndermesi için dosyaya yetki belgesi yazmamışsa, sağlıkla ilgili bilgileri içeren hastalara gönderilen e-postaların aktarım sırasında şifrelenmesi gerektiğini zorunlu kılmaktadır.

TUBİTAK, BİLGEM tarafından hazırlanan, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı' nın Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması başlığı altında, bu stratejik eylem kapsamında devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek riskleri azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmıştır [50].

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kamu bilişim sistemlerine ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ilave

olarak küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dahil olmak üzere ulusal siber uzayın ülkemiz ölçeğindeki bütün bileşenlerini kapsamaktadır [50].

BG kapsamında stratejik amaçların en doğru şekilde tanımlanabilmesi için BG riskleri gerçekçi bir biçimde değerlendirilmiş ve belirlenen başlıca riskler aşağıda sıralanmıştır [50]:

1. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak saldırılar sonucunda kritik hizmetlerin kesintiye uğraması.
2. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak saldırılar sonucunda, vatandaşlara ait kişisel bilgilerin veya kamuya ait gizli bilgilerin ele geçirilmesi, ifşa edilmesi, değiştirilmesi veya yok edilmesi.
3. Kuruluşlara ait ticari sırların ele geçirilmesi, ifşa edilmesi, değiştirilmesi veya yok edilmesi.
4. Propaganda kuruluşların itibarının zarar görmesi veya hassas bilgi/verinin ifşa edilmesi, değiştirilmesi veya yok edilmesi.
5. E-ticaret yapan kuruluşların, e-posta hizmeti veren kuruluşların, sosyal medya hizmeti veren kuruluşların saldırılar sonucunda hizmet verememesi nedeniyle maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin ele geçirilmesi, ifşa edilmesi, değiştirilmesi veya yok edilmesi.
6. E-ticaret yapan kuruluşların, finans sektörü veya çevrimiçi ödeme ya da para transferine imkan veren diğer kuruluşların müşterilerine ait hassas bilgilerin ele geçirilmesi nedeni ile itibar kaybına uğraması, toplumda güven kaybı oluşması, bu hizmetlerden faydalanan müşterilerin maddi kayba uğraması.
7. Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
8. Toplumun internete ve sosyal ağlara olan bağımlılığı, BG alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, mobil ve sabit bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle kötücül yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.
9. Her türlü kurum ve kuruluşta dolandırıcılık amaçlı saldırılarla karşı karşıya kalınması.

10. Her türlü kuruluşta, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığı ile verilen hizmet ve faaliyetlerin kesintiye uğraması.

Tubitak BİLGEM tarafından gerçekleştirilen Ulusal Bilgi Sistemleri Güvenlik Projesi kapsamında hazırlanan aşağıdaki kılavuzlar ile teknik anlamda yol gösterici olmaya çalışılmıştır [51-56].

- Bilgi sistemleri kabul edilebilir kulanım politikası oluşturma kılavuzu
- Sosyal mühendislik: zafiyetler ve korunma yöntemleri kılavuzu
- Erişim kontrol politikası oluşturma kılavuzu
- Web sunucu (IIS7.0 ve IIS7.5) güvenliği kılavuzu
- Ağ mimarisi güvenliği kılavuzu
- Denial-of-Service Attack (Servis Dışı Bırakma Saldırısı, DDOS) ile mücadele kılavuzu

3.6. Bilgi Güvenliğinin Maliyeti

Fayda-maliyet analizi ve BG maliyet değerlendirmesinin yapılması, kuruluşların ne kadar etkili tedbirler alacağını ve kuruluşun, alınan tedbirlerin işe yaramaması durumunda kayıplarını nasıl azaltacağını belirlemede yardımcı olmaktadır. Fayda-maliyet değerlendirme ve BG değerlendirme yöntemlerinin çoğu süreçlere, yaşam döngüleri adımlarına ve teknik güvenlik standartlarının özel gereksinimlerine yoğunlaşmaktadır.

Fayda-maliyet analizinin amacı, BG için harcanan maliyetlerin, sağlanması beklenen faydadan daha düşük olmasını sağlamaktır. BG, kuruluşların doğrudan kar etmesini sağlayan bir faaliyet değildir. Ancak, BG maliyetinin göz ardı edilmesi durumunda ortaya çıkabilecek potansiyel zarardan kaçınılmasının sağlayacağı fayda değerlendirmektedir.

BG perspektifinden BG maliyetlerini sınıflandırılmasında uygulanan yaklaşımlar şunlardır [28]:

- Bilanço odaklı yaklaşım: Bu yaklaşım BT ile ilgili bütçe planlama yolu ile bilgi güvenliği uygulama maliyetlerini hesaplamayı sağlar. Maliyet kalemleri personel maliyetleri, donanım, yazılım, dış kaynak kullanımı ve yönetilen güvenlik servisleridir.

- Güvenlik önlemi yaşam döngüsü yaklaşımı: BG çözümleri BT yaşam döngüsüne göre değerlendirilir. BG maliyetlerini satın alma maliyetleri, kurulum maliyetleri, işletme maliyetleri ve değişim olmak üzere dört unsur belirler.
- Bilgi teknolojisi güvenliği süreç odaklı yaklaşım: BG maliyetlerini personel maliyetleri, danışmanlık maliyetleri, işletme maliyetleri ve risk maliyetleri oluşturur. Yöntem, tek bir bilgi güvenliği gereksinimine veya kontrol değerlendirmesine odaklanır.
- ISO/IEC 27001 odaklı yaklaşım: Uluslararası bir BG standart olan ISO/IEC 27001 dünya çapında yaygın olarak kullanılmaktadır. BG uygulamasına ISO/IEC 27001 kontrolleri bakış açısıyla bakılması önerilmektedir.

3.7. Kritik Bir Sektör Olarak Hukuk Alanı

Çoğu kuruluş kritik ve hassas bilgilere sahiptir. Kuruluşlar ne kadar düzenli çalışırlarsa çalışsınlar, operasyonlarını tehlikeye atan, hatta kesintiye uğramasına neden olan, önemli verilerinin kaybına veya çalınmasına neden olan olaylarla karşılaşmaları muhtemeldir. Çoğu durumda, bu olaylar kuruluşun maddi kayıplarına veya itibarlarının kaybına neden olabilmektedir. Benzer şekilde, vatandaşlar da zaman zaman çevrimiçi dolandırıcılık veya kişisel kimlik hırsızlığı gibi olaylarla ilgili olaylar yaşamaktadır. Bu nedenle, kilit bir varlık olarak bilgi, ortaya çıkan tehditlerden korunmalıdır. BG, bilgilerin gizliliği, bütünlüğü ve kullanılabilirliği ile ilgilenen alandır. BG' nin odak noktası, kuruluşun kurumsal sistemlerini oluşturan varlıklar da dahil olmak üzere, hem kendi personeli hem de iş ortakları, satıcılar, müşteriler ve diğer paydaşları destekleyen tüm organizasyondur [26].

Bir kuruluş günümüz teknolojik bağlamında etkin bir BG olmadan faaliyet göstermesi zordur. Düşük güvenlikli kuruluşlar, ortakları için de tehdit oluşturmaktadır. Öte yandan, tüketicilerin bir kuruluşa duydukları güven, KV' inin güvenliğine de bağlı olacaktır [26].

Birçok ülkede, mevzuat ve yönetmelikler BG konusunda kuruluşları cezai olarak sorumlu kılmakta ve bazı durumlarda uygun risk kontrol ve BG önlemlerini uygulamaları ve sürdürmeleri konusunda başarısız olmaları durumunda hesap verebilir olmalarını istemektedir [26]. BG riski ölçüm sistemlerinin etkililiğinde önemli bir konudur [129, 130]. ISO/IEC 27001, BGYS' i sağlamak, yönetmek ve geliştirme ihtiyacını belirten uluslararası bir standarttır ayrıca BG kontrolünde ve ölçümünde de referans olarak kullanılmaktadır [19].

BG, gizlilik, bütünlük ve geçerlilik sağlamak için bilgisayar sistemlerini yetkisiz erişim, kullanım, rahatsızlık ve tahribattan korumayı sağlamak olarak tanımlanabilir [93].

Kuruluşun bilgi işlem ortamını güvence altına alma ihtiyacının artması ile birlikte, güvenlik RY sürecini doğru bir şekilde tanımlayan bir RY çerçevesine ihtiyaç duyulmaktadır. BG yönünde risklerin azaltılması ile aynı temel amaç olsa da, RY çerçevelerinin hepsinin çok farklı bakış açıları vardır ve sorunları farklı şekilde ele almaktadırlar. Bilgi her organizasyon için kritik bir varlıktır ve bu nedenle BG risklerini azaltma konusunda stratejik planların geliştirilmesi ve uygulanması her kurumun operasyonunun önemli bir parçası olmalıdır [33].

Hukuk büroları da, özellikle hassas KV' i işlemesinden dolayı gerek ilgili müvekkillerin gerekse kurumsal ve ilgili avukatların itibarlarının korunabilmesi için BG konusunu bir öncelik olarak görmeli ve temel bir takım tedbirleri almalıdır.

Hukuk büroları açısından da uygun bir RA ve değerlendirme süreci şu adımlardan oluşabilir:

Adım 1: Risk Değerlendirmesi - Bilgi Teknolojileri Sistemi İşin Kritik Süreçlerini, Değer Üretimini ve Değerini Korumasını Destekliyor mu?

Hukuk büroları çoğunlukla avukatların gider ortağı oldukları belirli bir yönetimi olmayan kuruluşlardır. Bu nedenle, net bir yönetimden bahsedilmesi mümkün olmasa da, yerine getirilmesi gereken yönetimsel fonksiyonlar büro avukatları arasında gerçekleştirilmektedir. Diğer taraftan, büroda çalışan her bir avukatın kendi gelir ve giderlerinden sorumlu olması nedeni ile de, BG' nin bir kuruluş maliyeti olarak değil, paylaşılan bir gider olarak değerlendirilmesi gerekmektedir.

Bilgi varlıklarının avukatlar için ne olduğunu bulmak yerine, büro ortağı avukatların, büro için değer yaratan planlanmış ve var olan iş süreçlerini anlamaları ve hangi değer yaratan ya da değer koruyan süreçlerin BT tarafından desteklendiğine karar vermeleri gerekmektedir. Değer koruması, gündelik faaliyetlerle ilgili olmayan beklenmedik maliyetlerin ve iş kesintilerinin önlenmesi yahut büronun, avukatların veya müvekkillerin itibar kaybına uğrayabilecekleri durumlar olarak görülebilir. Kısmen ortak kullanılan, BT sisteminin hangi kısmının değer yaratma ve hangi kısmının destekleme faaliyetlerinde kullanıldığının belirlenmiş olması önemlidir.

Eğer BT tarafından değer yaratma ve değerin korunması önemli değil ve yeterli ölçüde korunmuyorsa, daha fazla analiz için bir bilgi güvenliği uzmanının sürece dahil edilmesi gerekli değildir. Kritik iş süreçlerinde kullanılmayan bir bilgi sistemi, genel BG önlemleri alınarak ve izlenerek de korunabilir [48]. Kritik iş süreçlerinde kullanılan, yani iş sürekliliğinin sekteye uğramasına, eski haline getirilmesi için maliyete ve/veya büro, avukat ve müvekkillerin itibarlarının zarar görmesine neden olabilecek bilgi sistemleri ise tehditlere ve güvenlik açıklarına karşı koruma, denetim ve izlemeye tabi tutulmalıdır.

Adım 2: Risk Değerlendirmesi - İşle İlgili Kritik Bilgi Sisteminin Analizi

Tehdit ve kırılganlık değerlendirmesi, sisteme sızma olasılığının tahmini ile ilgili işlemler, teknik bir süreç olmasından dolayı bir güvenlik uzmanı tarafından yerine getirilmelidir. Güvenlik uzmanı riskleri belirtebilir, güvenlik olayları meydana gelirse teknik sonuçları açıklayabilir ve sistemi kurtarmak için gereken zamanı ve diğer gerekli kaynakları önerebilir [48].

Adım 3: Risk Değerlendirmesi - Etkiler ve Risk Tolerans Seviyeleri [48]

2. adımdaki çıktılar sistemin güvenli olmadığını gösterdiğinde, o zaman hukuk bürosu 3. adımla devam etmelidir. Potansiyel güvenlik olayının hukuk bürosuna etkileri, büroyu paylaşan avukatlar tarafından tahmin edilebilmelidir. İş sürekliliğini etkileyen ve maddi kayba neden olan faktörleri anlamak, büronun, avukatların ve müvekkillerin itibarlarına zarar verebilecek risklerin neler olabileceğinin öngörülebilmesi gerekmektedir.

İtibar riski, müvekkillerin, büro avukatları ile çalışıp çalışmama kararlarını etkiliyor mu? Olası bir iş kesintisi bir hafta sonu ek çalışma ile telafi edilebilir mi yoksa geri dönülemez zarara uğramak söz konusu olabilir mi? BG riskleri nedeni ile gerçekleşen riskler, risklere karşı tedbir almaktan daha mı pahalıya mal olmaktadır? Büroda meydana gerçekleşebilecek BG riskleri büronun ve avukatların yasal düzenlemelerle uyumlu çalışmasına engel olmakta mıdır? BG risklerini kabul edilen risk tolerans düzeyinde tutmak için BG maliyetlerini en aza indirmek için nelere yatırım yapılmalıdır?

Büroda giderilmesi gereken risklere karar verildiğinde, risk giderme alternatifleri belirlenmeli ve tahmin edilmelidir. Büroyu paylaşan avukatlar, riskleri giderme alternatifleri

öneren teknolojik tavsiyelere ihtiyaç duyar. RD' ni yapan güvenlik uzmanı, sistemdeki mevcut güvenlik açıkları konusunda bir anlayışa sahip olduğundan, uzman ayrıca saldırganların güvenlik açıklarından yararlanmalarının nasıl önlenebileceği konusunda öneride bulunabilir. Sızmayı önlemek ve/veya sonuçta ortaya çıkan olumsuz etkiyi en aza indirgemek için büroların seçim yapabilecekleri farklı alternatifler vardır. Alternatiflerin bir kısmı yedek, bir kısmı tamamlayıcı tedbirler olabilir. Bu tedbirlerin bir kısmı teknik tedbirler bir kısmı ise teknik olmayan tedbirler olabilir.

Dosyaların şifrelenmesini bir kural haline getirmek teknik bir tedbirken bu kural sonrasında ise şifreleme ve şifre çözme konusunda insanları eğitmek teknik olmayan bir tedbirdir [48]. Her ikisinin de uygulanabilmesi için de maddi kaynak gereklidir. Güvenlik önlemleri alternatiflerini karşılaştırılabilir hale getirmek için büro açısından teknik veya operasyonel yeterlilikleri değerlendirilmelidir.

Bu aşamadaki zorluk, riskleri azaltan güvenlik tedbirlerinin kalitesinin ve verimliliğinin görünmemesidir. Hukuk büroları gibi küçük kuruluşların güvenlik çözümlerinin yeteneklerini ve verimliliğini test edecek kaynakları yoktur. Çoğunlukla, kontrollerin etkinliği ile ilgili olarak erişilebilir kaynaklarda yer alan bilgilere ve kontrollerle uyumlu öz değerlendirmelere güvenmek zorundadırlar. Güvenlik ürünleri hakkındaki bilgileri, farklı kaynaklardan bilgi alarak ve tanıtılan etkinlik konusunda kritik öneme sahip olarak doğrulamaya çalışabilirler.

Birden fazla önlem birleştirildiğinde, ortak etkinlikleri değerlendirilmelidir. Örneğin, masaüstü güvenlik çözümünün %50 riski önlediği ve güvenlik duvarı güvenlik çözümünün de bazı saldırıların %80' ini önlediği tahmin ediliyorsa, bu önlemlerin her ikisi birlikte uygulandığında, koruma en az %80 olmalıdır. Eğer birbirini tamamlayıcı ürünler seçilmişse bu oran %80' inin üzerinde olmalıdır. Alternatif önlemleri seçerken ve önlemlerin etkinliğini tahmin ederken, çözümün sağlayıcısı tarafından sağlanan lisansın veya desteğin uzunluğunu göz önünde bulundurmak da önemlidir. Güvenlik riskleri her geçen gün artmakta ve çeşitlenmektedir. Bu nedenle güncel bir güvenlik sistemine sahip olmak çok önemli [48]. Hukuk büroları gibi küçük işletmeler bir takım güvenlik kontrolleri uygulamak için sahip oldukları veya ihtiyaç duydukları insan kaynaklarını da göz önünde bulundurmalıdır. Bilgi sistemlerini günlük olarak takip edecek bir uzmanları yoksa, günlük izleme gerektiren çözümleri düşünmemelidirler.

Hukuk büroları gibi küçük kuruluşlarda BG yatırım problemini çözmek için girdi bilgisi el altında bulunmamaktadır. Ancak, güvenlik önlemlerinin uygulanması ve işletilmesi ile ilgili tüm maliyetler dikkate alınmalıdır.

4. ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE HUKUK BÜROLARI AÇISINDAN DEĞERLENDİRME

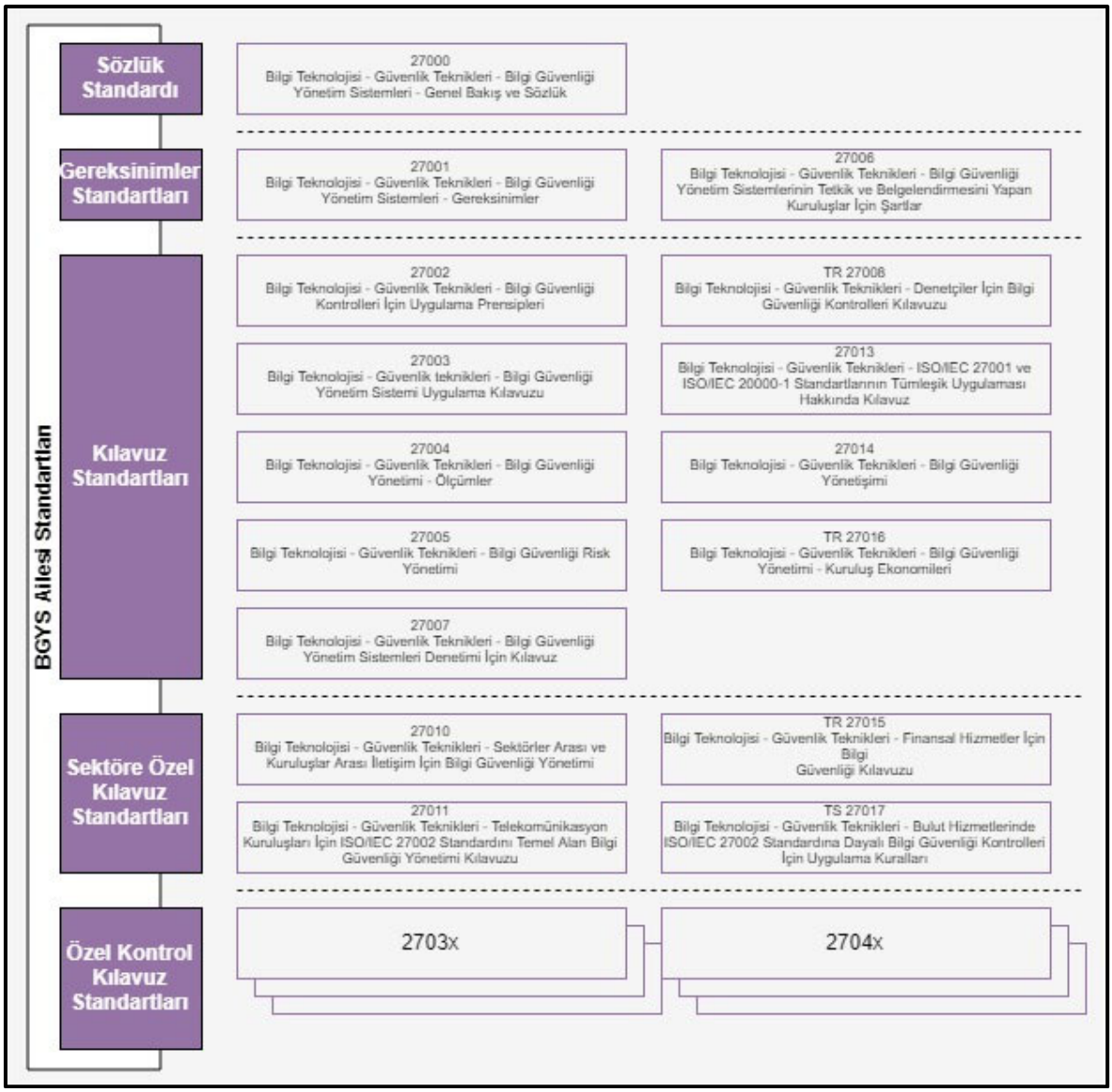
Bu bölümde, ISO/IEC 27K standartları ailesine kısa bir bakış yapılmış, özelde ise ISO/IEC 27001 BGYS' nin yapısına ve standardın iç işleyiş sürecine değinilmiştir. ISO/IEC 27001 BGYS sürecinin iyi yapılandırılmış bir süreç olarak ele alınması durumunda hangi alt başlıklar üzerinde durulması gerekeceği açıklanmıştır. ISO/IEC 27001 BGYS standardı yapısal olarak incelendikten sonra standardın içeriği hakkında literatüre yer verilmiş ve standardın sertifikasyon ayağı istatistiksel açıdan incelenmiştir. ISO/IEC 27001 BGYS sertifikasyonu dışında, dünya genelinde var olan diğer ulusal ve uluslararası BG sertifikalarına değinilmiştir. Devamında ülkemizdeki iller bazında barolara bağlı avukat sayılarına ait istatistikler incelenmiş, bir hukuk bürosu açısından BG' nin önemine değinilmiştir.

4.1. ISO/IEC 27K Ailesine Genel Bir Bakış

ISO/IEC 27K standartları ailesi BGYS standart ailesi birbiriyle ilişkili yayınlanmış veya gelişim aşamasında olan standartları kapsar ve birkaç önemli yapısal bileşenleri içermektedir. ISO/IEC 27001 BGYS gereklilikleri sağlayan bütün içerisindeki en tanınmış standarttır [19].

ISO/IEC 27001, kuruluşun BG işletimi tarafından korumayı sağlayan kuruluşu bilgi varlığıyla ilişkili olan risk kontrol ve risk önleme için bir takım kontrolleri içeren düzenleyici gereklilikler sağmaktadır [19].

ISO/IEC 27K ailesine ait standartların genel amaçları şekil-4.1.' de görüldüğü gibidir.



Şekil 4.1. ISO/IEC 27K ailesi standartları [57]

Şekilde 4.1.' de görüldüğü ISO/IEC 27000 standardı, sözlük standardı olup, diğer ISO/IEC 27K standartları için genel tanımları içermektedir. ISO/IEC 27001 ve 27002 standartları BGYS gereksinimlerini tanımlayan standartlardır.

ISO/IEC 27002, 27003, 27004, 27005, 27007, 27008, 27013, 27014, 27016 standartları BGYS kılavuzlarını tanımlamaktadır. ISO/IEC 27010, 27011, 27015, 27017 standartları, belirli kritik sektörler için BGYS kılavuzlarını tanımlamaktadır. ISO/IEC 2703x ve 2704x standartları ise, kontrol tabanlı özel kılavuzları tanımlamaktadır. ISO/IEC 27K ailesine ait tüm standartların bir listesi Çizelge 4.1.' de görüldüğü şekildedir.

Çizelge 4.1. ISO/IEC 27K ailesi standartları [57-86]

ISO/IEC 27000:2014 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Sözlük
ISO/IEC 27001:2013 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler
ISO/IEC 27002:2013 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri
ISO/IEC 27003:2010 TR	Bilgi Teknolojisi - Güvenlik teknikleri - Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu
ISO/IEC 27005:2011 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Risk Yönetimi
ISO/IEC 27006:2015 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemlerinin Tetkik ve Belgelendirmesini Yapan Kuruluşlar İçin Şartlar
ISO/IEC 27007:2013 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Kılavuz
ISO/IEC 27008:2011 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Denetçiler İçin Bilgi Güvenliği Kontrolleri Kılavuzu
ISO/IEC 27011:2008 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Telekomünikasyon Kuruluşları İçin ISO/IEC 27002 Standardını Temel Alan Bilgi Güvenliği Yönetimi Kılavuzu
ISO/IEC 27013:2012 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - ISO/IEC 27001 ve ISO/IEC 20000-1 Standartlarının Tümleşik Uygulaması Hakkında Kılavuz
ISO/IEC 27014:2013 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetişimi
ISO/IEC 27015:2014 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Finansal Hizmetler İçin Bilgi Güvenliği Kılavuzu
ISO/IEC 27017:2015 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Bulut Hizmetlerinde ISO/IEC 27002 Standardına Dayalı Bilgi Güvenliği Kontrolleri İçin Uygulama Kuralları
ISO/IEC 27018:2015 EN	Bilgi Teknolojisi - Güvenlik teknikleri - PII (Kişi Tanımlama Bilgisi) İşleyen Açık Bulut Ağlarda Kişi Tanımlama Bilgisinin Korunması İçin Uygulama Prensipleri
ISO/IEC 27031:2014 EN	Bilgi Teknolojisi - Güvenlik Teknolojileri - Bilgi ve İletişim Teknolojileri İçin İş Sürekliliği Yönergeleri
ISO/IEC 27033-1:2015 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 1: Genel Bakış ve Kavramlar

Çizelge 4.2. (devam) ISO/IEC 27K ailesi standartları [57-86]

ISO/IEC 27033-2:2012 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 2: Ağ Güvenliğinin Tasarımı ve Uygulanması İçin Tavsiyeler
ISO/IEC 27033-3:2010 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 3: Referans Ağ Oluşturma Senaryoları - Tehditler, Tasarım Teknikleri ve Kontrol Konuları
ISO/IEC 27033-4:2014 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 4: Güvenlik Ağ Geçitleri Kullanılarak Ağlar Arasında Güvenli İletişim
ISO/IEC 27033-5:2013 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 5: Sanal Özel Ağlar (VPNs) Kullanılarak Ağlar Arasında Çapraz Güvenli İletişim
ISO/IEC 27035:2011 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği İhlal Olayı Yönetimi
ISO/IEC 27036-1:2014 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Tedarikçi İlişkileri İçin Bilgi Güvenliği - Bölüm 1: Genel Bakış ve Kavramlar
ISO/IEC 27036-2:2014 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Tedarikçi İlişkileri İçin Bilgi Güvenliği - Bölüm 2: Gereksinimler
ISO/IEC 27036-3:2013 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Tedarikçi İlişkileri İçin Bilgi Güvenliği - Bölüm 3: Bilgi ve İletişim Teknolojisi Tedarik Zinciri Güvenliği İçin Tavsiyeler
ISO/IEC 27039:2015 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Saldırı Tespit Sistemlerinin Seçimi, Kurulumu ve İşletimi (IDPS)
ISO/IEC 27040:2015 EN	Bilgi Teknolojisi - Güvenlik Teknikleri - Depolama Güvenliği
ISO/IEC 15408-1:2009 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Teknolojisi (BT) Güvenliği İçin Değerlendirme Kriterleri - Bölüm 1: Giriş ve Genel Model
ISO/IEC 15408-2:2009 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Teknolojisi (BT) Güvenliği İçin Değerlendirme Kriterleri - Bölüm 2: Güvenlik Fonksiyonel Bileşenleri
ISO/IEC 15408-3:2013 TR	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Teknolojisi (BT) Güvenliği İçin Değerlendirme Kriterleri - Bölüm 3: Güvenlik Garanti Bileşenleri
ISO/IEC 20000-1:2013 TR	Bilgi Teknolojisi - Hizmet Yönetimi - Bölüm 1: Özellikler

4.2. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Yapısı

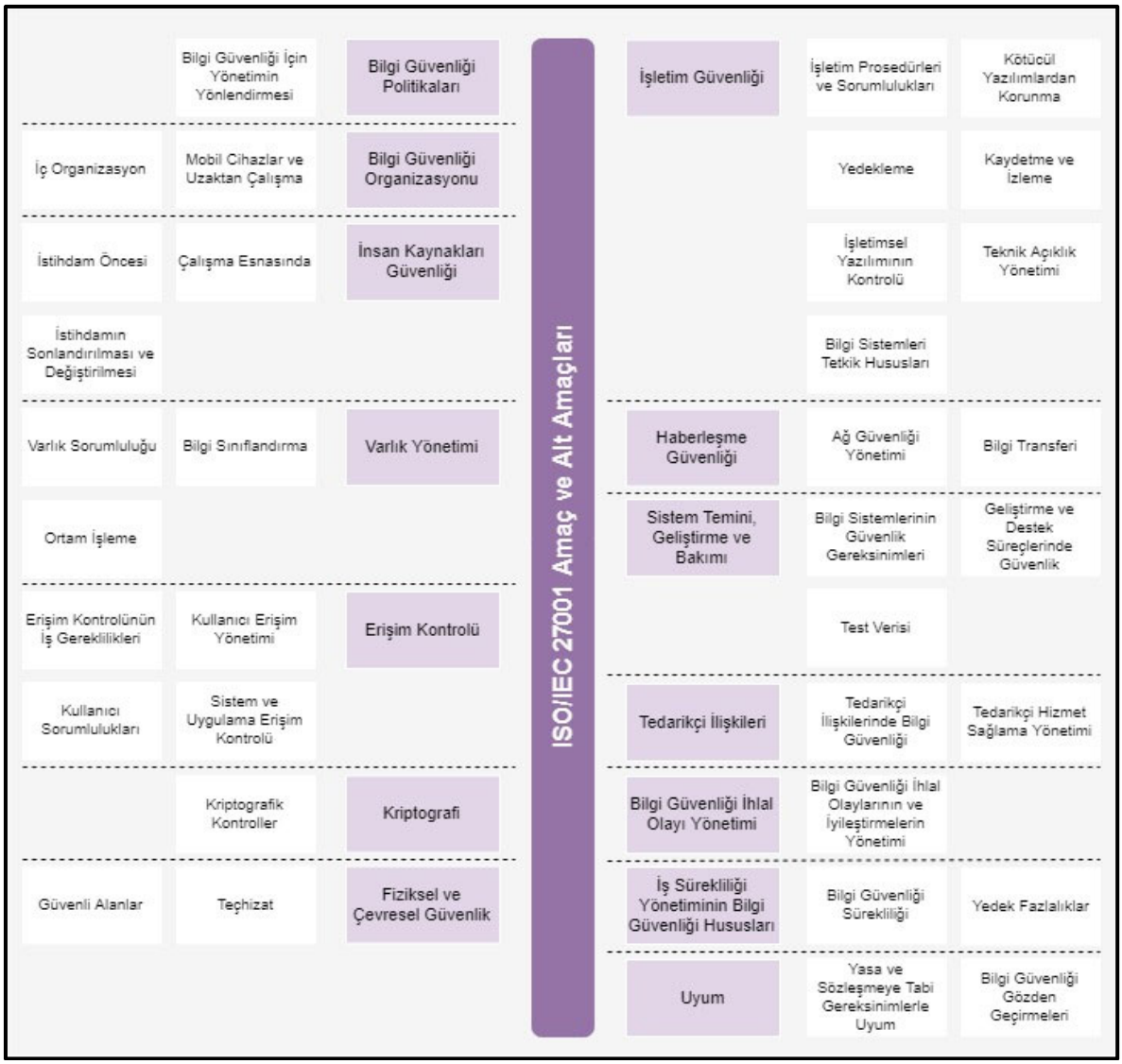
ISO/IEC 27001 standardı, "Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler" başlığına sahip olup, içeriğinde BGYS kriterleri amaç ve alt amaçlar halinde kategorize edilmiştir. Standarda ait amaç ve alt amaçlar arası kategorik yapı şekil 4.2.' de görüldüğü şekildedir.

BG standartlarından bazıları öneri ve en iyi uygulamalar olarak tanımlanmıştır. Bazıları ise BG kriterleri olsa da, uyumluluk ilgili kuruluşlar için bir gerekliliktir. Kuruluşlar, ISO/IEC 27001 yayınından önce en çok ulusal BG kriterlerini, diğer ülkelerin BG standartlarını ya da BG' nin genel ilkelerini kabul etmişlerdir. Ulusal BG yönergelerinin birçoğu ISO standartlarıyla uyumludur. Bununla birlikte, bu ulusal BG kılavuz ilkelerinin çoğu, ISO/IEC 27001' in eski sürümleri ile uyumlu değildi veya belirli BG yönetimi kriterlerine sahiptirler [13].

ISO/IEC 27001 standardı, şekil 4.3.' de görülen, bir kuruluşun BGYS' nin etkinliğini planlamayı, uygulamayı, kontrol etmeyi, önlem almayı amaçlayan PUKÖ modeli olarak bilinen döngüsel bir model sunmaktadır. PUKÖ döngüsünün dört aşaması vardır. Bunlar [15];

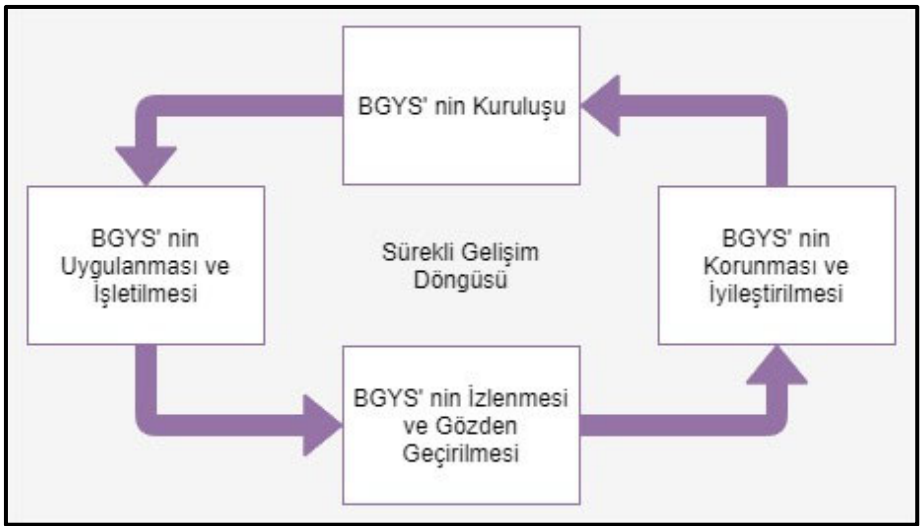
Planlama - BGYS' nin kuruluşu: İlk adım, risklerin tanımlanacağı, analiz edilip değerlendirileceği RD' yi tanımlamaktır. Daha sonra risk çözüm seçeneklerinin tanımlanması ve değerlendirilmesi takip edilmektedir. Kontrol hedefleri ve kontrolleri seçildikten sonra, yönetim artık riskleri onaylamalı ve BGYS' nin uygulanmasına izin vermelidir.

Uygulama - BGYS' nin uygulanması ve işletilmesi: Yönetim işlemleri, kaynaklar, öncelikler, roller ve sorumluluklar bu adımda tanımlanacaktır. Risk gerçekleşmesi durumunda ortaya çıkabilecek zararın ne şekilde düzeltilebileceği planının ilgili risklere göre belirlemesi ve kontrollerin buna göre yapılması gerekmektedir.



Şekil 4.2. ISO/IEC 27001 Ek-A amaç ve alt amaçları

Kontrol Etme - BGYS' nin izlenmesi ve gözden geçirilmesi: İzleme ve gözden geçirme prosedürleri geliştirilmeli ve yürütülmelidir. BGYS ve kontrollerin etkililiği ile RD metodolojisi ve gözden kaçan riskler dahil edilmeli ve gözden geçirilmelidir.



Şekil 4.3. ISO/IEC 27001 BGYS çerçevesi [37]

Önlem Alma - BGYS' nin korunması ve iyileştirilmesi: Bu adımda hem önleyici hem de düzeltici eylemlerin uygulanması BGYS' ni daha da iyileştirebilir. Ayrıca, belge ve kayıt kontrolünü zorlar ve BGYS' ni geliştirmek için BG olaylarını gözden geçirir.

Genellikle, ISO/IEC 27001, ISO/IEC 27002 ile birlikte uygulanır. ISO/IEC 27001 ve ISO/IEC 27002, gereksinimleri tanımlamakta ve BGYS için en uygun BG kontrollerini özetlemekte yardımcı olmaktadır. Bununla birlikte, hiçbir RD mekanizması ve BGYS uygulaması ile ilgili bir kılavuz bulunmamaktadır. Bu standartlar sadece yapılması gerekenleri ifade eder, ancak nasıl yapılacaklarından bahsetmez [15].

Aslında, güvenlik bakımının yeni bir kavramsal çerçevesi, bu yönergeleri izleyen herhangi bir BT altyapısının ve hizmetinin yetkili insanlar tarafından uygun bir şekilde erişilebilir ve güvenli hale getirilmesini önermiştir. Bununla birlikte, BT hizmetleri ve altyapının bakımı için ayrıntılı olarak tartışılmamış hiçbir güvenlik yönü yoktur [15].

Günümüzde, güvenlik, önerilen herhangi bir bakım modeli ve kılavuzları da dahil olmak üzere tüm BT hizmetlerinde ve altyapılarında endişe duyulan bir konudur. Bu nedenle, kuralları daha etkili ve kullanımı kolay hale getirmek için genel bir kapsama alanına ihtiyacı duyulmaktadır. Güvenlik bakımı, siber alanda, özellikle BT hizmetleri ve altyapı kullanımı için kuruluşlar için daha önemli hale gelmiştir.

14 amaç, 35 alt amaç alanında 114 kontrol hedefinden oluşan ISO/IEC 27001 Standardı sürekli gelişim döngüsü bağlamının içindeki BGYS tasarımına odaklanan ve standardın 5 ile 18 başlıkları arasındaki maddelerden oluşmaktadır.

4.2.1. Risk değerlendirmesi

Risk değerlendirmesi, tüm risk tanımlama, risk analizi ve risk değerlendirme sürecini tanımlamaktadır. İlk aşamada - Risk Belirleme - kuruluşun risk kaynaklarını, etki alanlarını, risk olaylarını ve sonuçlarını tanımlar. Buradaki temel amaç, tüm risklerin kapsamlı bir listesini oluşturmak, tercihen tüm riskleri veya kaçırılmış şansları belirlemeye odaklanmaktır. Ana kriter, risk kaynağının kuruluşun sorumluluğunda olup olmadığına bakılmaksızın, kuruluş üzerindeki etkisidir. Basamaklı efektler ve kümülatif etkiler de kapsam dahilinde olmalıdır. Kuruluş uygun araç ve yöntemler uygulamalı, ilgili geçmiş bilgileri entegre etmeli ve yetkili kişileri tanımlama aşamasına dahil etmelidir.

4.2.2. Risk tanımlaması

Risk tanımlamasında, ne tür olayların olabileceği ve daha sonra kayba yol açacağı incelenmektedir. Bu, kuruluşun kontrolü altında olan olayların yanı sıra dış etkenlere dayanan olayları da içermektedir. Risklerle ilişkili kuruluşun ilgili varlıkları tanımlanmalı, ayrıca, potansiyel tehditleri tanımlamak için bu varlıklar hakkında yeterli bilgi toplanmış olması gerekmektedir. Bu bağlamda, tehdidin kaynağı (ör. kasıtlı veya kasıtsız) veya türü (ör. yetkisiz eylemler, fiziksel hasar, teknik arızalar) gibi farklı hususların dikkate alınması gerekmektedir. Potansiyel tehditleri belirledikten sonra mevcut ve planlanan kontrollerin bir listesi oluşturulur. Bir kontrol, tanımlanan bir tehdidin, yani riskin ortaya çıkma olasılığını veya etkisini azaltmalı ve ayrıca kuruluş içinde uygulanabilirliğine göre değerlendirilmelidir. Ardından, mevcut güvenlik açıklarının bir listesi tanımalıdır. Güvenlik açıkları varlıklar ile ilgilidir ve teknik, kuruluşa özel veya sosyal eksiklikler nedeniyle mevcut olmalıdır. Yani bir güvenlik açığından yararlanan belirli bir tehdit olmadıkça, güvenlik açığı zararlı olarak kabul edilmez. Neticede gerçekleşebilir her güvenlik açığı riski için olası sonuçların değerlendirilmesi gerekmektedir. Bu sonuçların parasal maliyetlerine ek olarak kuruluşun itibarına verebileceği zararlar da göz önünde bulundurulmalıdır.

4.2.3. Risk analizi

Genel olarak, risk analizi nitel veya nicel olabilir. Nicel risk analizi kesin sayısal değerlere dayanırken, nitel yöntemler, olay senaryosunun sonuçlarını ve olasılığını tanımlamak için tanımlayıcı ölçekler (düşük, orta ve yüksek gibi) kullanılmaktadır. Risk analizinin türü, bir parçası olarak geliştirilen risk değerlendirme kriterleri ile tutarlı olmalıdır.

4.2.4. Bağlam kurulumu

Odak noktası risk analizi, olası sonuçların değerlendirilmesinin yanı sıra tanımlanan risklerin gerçekleşme ihtimallerini de göz önünde bulundurulmalıdır. Olasılıklar değerlendirirken, belirli bir tehdidin ne sıklıkta ortaya çıkabileceği ve ilişkili olabilecek diğer güvenlik açıkları da alınmalıdır. Bu bilgiler geçmiş verilerden değil aynı zamanda uzman görüşlerinden de toplanabilir. Sonunda, olasılık ve sonuçların birleşimi her risk için risk seviyelerinin hesaplanmasını sağlayacaktır.

4.2.5. Risk değerlendirmesi

Tüm olası risklerin risk seviyeleri, tanımlanan risk değerlendirme kriterleri ile karşılaştırılır. Bu, tanımlanan risklerin birbirleriyle ilişkilendirilmesini ve kuruluş için en önemli risklerin belirlenebilmesini sağlar. Bunun sonucunda, risk değerlendirme kriterlerine göre önceliklendirilen risklerin bir listesi oluşturulabilir.

4.2.6. Risk gidermek

ISO/IEC 27005' te risk tedavisi dört olası seçenekten oluşan bir yapıda tanımlanmaktadır:

i. Risk değişikliği
ii. Risk tutma
iii. Riskten kaçınma
iv. Risk paylaşımı

Bu seçenekler birbirini dışlayan seçenekler değildir. Hatta bu seçeneklerin bütünleşik olarak kullanılmasının gerektiği durumlar da olabilir. Bu bağlamdaki herhangi bir karar, riskin ilgili taraflarca nasıl algılandığına ve iletişim kurmanın en iyi yoluna dayanmaktadır. En yaygın

risk tedavi yöntemi, yeni kontrollerin geliştirilmesi veya mevcut kontrollerin modifikasyonu ile sağlanabilmektedir. Yeni kontrollerle ilgili her türlü kararın, mevcut kaynaklar ve önceki adımlarda türetilen genel şartlarla ilişkili olarak, zamansal, finansal ve teknik kısıtlamalar da dikkate alınarak hazırlanmalıdır. Belirli bir riskin çok yüksek olarak değerlendirilmesi durumunda, en uygun yöntem riski tamamen ortadan kaldıracak tedbirler alınması olabilir. Ayrıca, risk kuruluşun yönetimsel kararlarına bağlı olarak tamamen veya kısmen, bir sigorta şirketi gibi harici bir ortakla da paylaşılabilinir.

4.2.7. Risk kabulü

Risklerin kabulü, kuruluşun iş süreçlerine entegrasyon için çok önemlidir ve sorumlu yöneticiler bireysel kararı ile onaylanmalıdır. Her bir risk için, bu riskin belirli koşullarına dayanarak, örneğin riski kabul ederek yüksek maliyetten kurtulmak gibi açık bir fayda ile riskin kabulüne karar verilmiş olmalıdır. Ancak her durumda, riskin kabulüne ilişkin kararlar kayıt altına alınmış olmalıdır.

4.2.8. Risk iletişimi ve danışma

Risk iletişimi, bir risk yönetimi sürecinin uygulanmasında kilit bir faktördür. Bu nedenle, bu süreç tüm risk yönetimi süreci boyunca devam etmektedir. Mevcut risklerle ilgili bilgiler sürekli olarak toplanmakta ve aynı zamanda risklerden potansiyel olarak etkilenen çalışanlar risk yönetimi sürecinin mevcut sonuçları hakkında bilgilendirilmektedir. Özellikle risk tedavi planı ile ilgili olarak, bireysel çalışanların desteği çok önemlidir.

4.2.9. Bilgi güvenliği risk izleme ve gözden geçirme

Mevcut risk durumuna ilişkin doğru bakış açısı elde etmek için tüm risklerin ve bunların faktörlerinin, yani varlıkların, varlıkların değerinin, etkilerinin, tehditlerin, ve meydana gelme olasılıklarının güncel tutulması gereklidir. Bunu sağlamak için devam eden bir izleme, inceleme ve değerlendirme süreci başlatılmalıdır.

4.3. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

NIST, ENISA veya ISO gibi uluslararası standart geliştirme kuruluşları, süreçlerin ve hizmetlerin amaçlarına uygun olmasını sağlamak için tutarlı bir şekilde kullanılabilen gereksinimleri, şartnameleri, kuralları ve özellikleri sağlamaktadırlar [43].

BT yönetiminin uygulanması kuruluşun iş gereksinimlerine ve genellikle risk yönetimi iyileştirme, iletişim ve iş ile ilgili BT arasındaki bağlantılarda meydana gelen nedenlere uygun olmalıdır. ISO/IEC 27001, BG' nin oluşturulmasını, uygulanmasını, işletilmesini, izlenmesini, korunmasını ve iyileştirilmesini amaçlanan iş riski yaklaşımına dayalı bir kuruluşun yönetim sisteminin bir parçasıdır [32].

ISO/IEC 27001, teknik güvenliği tanımlayan standarttır, ancak gerçekte bir yönetim sistemi olduğu için, BG' nin teknik standardı değildir. BGYS uygulamasının sadece veri güvenliğinde çalışanlar tarafından ihtiyaç duyulduğunu varsayan birçok kuruluş vardır. Bu durum tüm sektörlerde veri güvenliği konusunda farkındalık eksikliğine neden olmaktadır. Bilgiyi korumak sadece BG için yeni cihazlar veya uygulama kullanmaya başlamak demek değildir. Aynı zamanda cihaz ve uygulamaların kullanımındaki tüm işlemlerin de kontrol edilmesi ve BGYS standartlarına uygun hareket edilmesi demektir [32].

BGYS sağlayan ISO/IEC 27001, dünyada kuruluşlar tarafından BG politikalarının yönetimi ve kuruluşun BG' nin uygulanmasında kullanılan standarttır. ISO/IEC 27001, paydaşlar için esnek bir şekilde kuruluş içi ve kuruluş dışı olarak tasarlanmıştır, böylece standart daha fazla alana odaklanabilmektedir [32].

Bazı ülkeler için ulusal bir BG rehberinin benimsenmesi, ulusal BG seviyesini arttırmak ve BG alanının önemine daha fazla dikkat çekmek için bir motivasyon görevi görmektedir. Bunun yanı sıra, ulusal bir BG kılavuzuna sahip olmak, uluslararası bir BGYS standardına uyum sağlamada da hızlandırıcı etki gösterebilir. Diğer taraftan bazı ülkelerde ise, güvenlik gerekliliklerini yerine getirmek için ulusal bir BG kılavuzunun yeterli olduğu düşünülmektedir. Dil gibi, uluslararası iletişimin kapsamı, eğilimler ve kamusal düzenlemeleri gibi ISO/IEC 27001' in kabul oranını etkileyen bazı faktörler vardır. Bunun yanı sıra, ulusal BG yönergelerinin amacı ve odaklanmasının yanı sıra ISO/IEC 27001' e genellik ve benzerlik seviyesi de bu standart kabul oranını etkilemektedir [13].

Ülkemizde de Cumhurbaşkanlığı 2019/12 Sayılı Genelgesi ile, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından Bilgi ve İletişim Güvenliği Rehberi hazırlanacağından bahsedilmekle birlikte henüz yayınlanmamıştır [138]. Ayrıca TBMM tarafından kabul edilen 11' nci Kalkınma Planı' nda yer alan bilgi güvenliğine ilişkin çok sayıda madde mevcuttur [136].

Pek çok ülkede, ulusal bir BG Rehberi var olsa da ISO/IEC 27001, birçok endüstri alanında popülerdir, çünkü hassas bilgileri yapılandırılmış şekilde koruyarak pazar güvencesi ve BT yönetişimi sunmaktadır [13].

Kuruluşların BG özellikleri ve ihtiyaçları, uymak için çeşitli BG standartları ve ilkeleri olması nedeni ile bir BGYS oluşturmak için kendine özgü gereksinimler ve motivasyonlar sağlamaktadır. ISO/IEC 27001, sertifika veren ilk uluslararası BGYS' dır [58].

ISO/IEC 27001' in uygulanması, BG gereksinimlerine ve düzenli denetimlere göre, mevcut BG seviyesine kabul edilebilecek kuruluşlara çeşitli faydalar sağlamaktadır [58]. Kuruluşların hizmet verdiği kişilerin talebi, özellikle KV' leri kullanan kuruluşlar için ISO/IEC 27001 uygulamasının en önemli nedenlerinden biridir [131]. ISO/IEC 27001, güvenlik olaylarında, kabul edilebilir bir veri koruma düzeyi kanıtlamak için yönetime önemli ölçüde yardımcı olmaktadır [132].

Hukuk büroları açısından, hizmet verilen kişilerin yani müvekkillerin dava dosyaları kapsamında mevcut tüm verilerin kişisel bilgiler olduğu, bu bilgilerin korunmasından da müvekkilin dava vekaleti kapsamında avukatı ve hukuk bürosu sorumlu olduğu açıktır.

ISO/IEC 27001, kuruluşların yasal veya paydaşların gereksinimlerini karşılamaları veya genel olarak tekliflere başvuru için bir ön koşul olması için gerekli olan en iyi uygulamaların uzun süreli deneyimlerinin faydalarından yararlanmaktadır [58].

Çizelge 4.2.' de görüleceği üzere dünya genelinde 2016 yılında ISO/IEC 27001 sertifikasına sahip işletme sayısı 33.290' ken 2017 yılında bu sayının 6.211 (%19) artışla 39.501 ' yükselmiştir [133]. Bu durum, uluslararası alanda ISO/IEC 27001 sertifikasyonuna olan talebi açık bir şekilde göstermektedir.

Kuruluşların, bilgi güvenliği gereksinimlerinin ötesinde, sektörlerinde müşterilerine ve iş ortaklarına güven verebilmesi de günümüzde bir ihtiyaç haline gelmiştir.

Çizelge 4.2. incelenmeye devam edildiğinde ISO/IEC 27001 sertifikasına sahip işletme sayısı ülkemiz ve kıtalar bazında karşılaştırmaya tabi tutulduğunda, ülkemiz özelinde 2006-2015 yılları arasında düşük bir artış hızına sahip olduğu ancak, 2015 yılında 268 olan sertifikalı işletme sayısının 2016 yılında 500' e sıçradığı görülmüştür. Bu eğilimin yerel mi yoksa uluslararası bir eğilim olduğunu görmek üzere kıta verileri ile karşılaştırma yapıldığında, Afrika Bölgesi ile Orta ve Güney Amerika Bölgesi ile ülkemizin benzerlik gösterdiği görülmektedir.

2006-2017 yılları arasında tüm bölgeler için genel eğilimin ISO/IEC 27001 sertifikası alan kuruluş sayısının sürekli olarak bir artış yönünde olduğu, ancak 2016-2017 yıllarına ait sayılardan artışın yavaşladığı görülmektedir.

Çizelge 4.2. Türkiye ve kıta bölgelerinde ISO/IEC 27001 sertifikasına sahip kuruluş sayıları [134]

	Türkiye	**Afrika**	**Orta ve Güney Amerika**	**Kuzey Amerika**	**Avrupa**	**Batı Asya ve Pasifik**	**Orta ve Kuzey Asya**	**Orta Doğu**
2006	10	6	18	79	1.064	4.210	383	37
2007	27	10	38	112	1.432	5.550	519	71
2008	33	16	72	212	2.172	5.807	839	128
2009	86	47	100	322	3.563	7.394	1.303	206
2010	117	46	117	329	4.800	8.788	1.328	218
2011	100	40	150	435	5.289	9.665	1.497	279
2012	132	64	203	552	6.379	10.422	1.668	332
2013	181	99	272	712	7.952	10.116	2.002	451
2014	224	79	273	814	8.663	10.414	2.251	511
2015	**268**	**129**	**347**	1.445	10.446	11.994	2.569	606
2016	**500**	**224**	**564**	1.469	12.532	14.704	2.987	810
2017	531	301	620	2.108	14.605	17.562	3.382	923

BG alanında tek ve geçer sertifika sistemi ISO/IEC 27001 değildir. ISO/IEC 27001 dışındaki bazı ulusal ve uluslararası BGYS sertifikasyonları Çizelge 4.3' de özetlenmiştir.

Çizelge 4.3. Bilgi güvenliği yönetim sistemi sertifikaları [48]

Sertifika Adı	Kapsam ve Konu
ePrivacyseal	Gizlilik mührü programının önceden belirlenmiş kriterler kataloğuna uygun ürün veya hizmetleri onaylar.
EuroPrise	Programın konusu donanım (ör. bir donanım güvenlik duvarı), yazılım (ör. bir hastanede bir veritabanı uygulaması), BT tabanlı hizmetler ve verilerin otomatik olarak işlenmesi (ör. izinsiz veri işleme, web siteleri) gibi BT ürünleridir. Program, hizmetlerin değerlendirilmesi ve veri işlemenin canlı performansının denetlenmesini içerir. Değerlendirilen ürün ya tam bir üründür (ör. bir yazılım parçası) ya da bir ürünün parçasıdır.
CNIL Labels	Belgelendirme konusu, prosedürü veya ürünü, yayınlanan standartlardan birine uyum sağlayan herhangi bir gerçek veya tüzel kişi olabilir.
ICO Privacy Seal	Gizlilik mührünün amacı yalnızca sertifikalı kuruluşun İngiltere Veri Koruma Yasası' nın gereksinimlerine uygunluğunu göstermek değil, aynı zamanda kişisel bilgilerin işlenmesi konusunda yasal gerekliliklere uyumluluğu da göstermektir.
ISO/IEC 27001	Sertifikasyonun amacı, tek bir iş süreci, belirli bir hizmet veya bir kurumun tüm iş süreci olabilir. Sertifikalı kuruluş, BG risklerini istenen seviyelere kadar belirleyebilir, azaltabilir, hizmetlerine olan güveni artırabilir ve BG süreçlerini yönetebilir.
ISO/IEC 27018	ISO/IEC 27018 Davranış Kuralları, genel bulut bilgi işlem ortamı için ISO/IEC 29100' deki gizlilik ilkelerine uygun olarak KV' in korunmasına yönelik önlemlerin uygulanması için yaygın olarak kabul edilen kontrol hedefleri, kontroller ve kılavuzlar oluşturur. Bir bulut hizmeti sağlayıcısının BG risk ortamları kapsamında uyması gereken kişisel BG' ne ilişkin yasal gereksinimleri dikkate alarak ISO/IEC 27002' ye dayanan standartları belirler.
PrivacyMark System	Gizlilik İşaret Sistemi, Japonya' da güvenlik ve güvenliği sağlamak için mekanizmalar ve çerçeve altyapıları geliştirmeyi ve önermeyi amaçlayan kar amacı gütmeyen bir kuruluşlar tarafından işletilmektedir.
Privacy By Design Certification	Endüstriyel tasarım ile gizliliğin işlevselliğini artırmak ve tasarım ile gizliliğin günlük süreçlerine dahil edilmesi için çalışan şirket ve kuruluşlara yardımcı olmaktır.

4.4. Hukuk Bürolarında ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

Bilginin kapsamı ve değeri sürekli olarak arttığından, kuruluşların ve bireylerin, verilerin çalınması veya imha edilmesine maruz kalması artmaktadır. Bilgisayar ve mahremiyetle ilgili düzenlemelerin uyumluluk gereklilikleri ile birlikte BG' ne yönelik gittikçe daha

karmaşık bir hale gelmiş, Küresel tehditlerin yayılması, BG konusunda kuruluşların daha bütünsel bir yaklaşıma yönelmesine neden olmuştur [26].

Hukuk büroları da bunun istisnası bir ayrıcalığa sahip değildir, aksine, dilekçe yazımından, gerekli araştırmaların yapılmasına, dava açma süreçlerinden, müvekkiller ile iletişime kadar pek çok noktada hukuk büroları, kişiler açısından önemli, kişiye özel, hem avukat hem müvekkil açısından itibarlarının zarar görmesine yol açabilecek kritik KV ile çalışılmasından dolayı, pek çok kuruluşa kıyasla daha fazla riske sahip olduğundan bahsedilebilmek mümkündür.

Karar vericiler için, kuruluşun tüm seviyelerinde, BG risklerinin nasıl ele alınması gerektiğini anlamak önemlidir. Yalnızca kapsamlı ve sistematik bir yaklaşım, bir kuruluşun ihtiyaç duyduğu BG seviyesini sağlayabilmektedir. Bu yaklaşım, BG yönetimi için uluslararası referans, yani BG ile ilgili ISO/IEC 27K standartları ailesi tarafından verilmektedir [26].

ISO/IEC 27001, 27K ailesindeki anahtar standarttır. Bu standarda uyulması, bir kuruluşun BG riskleriyle ilgili hizmet alıcılara, tedarikçilere ve ayrıca düzenleyici ve adli makamlara doğru bir iletişim sağlamaktadır [26].

Faaliyet kapsamı, personel sayısı ve iş süreçlerinin çeşitliliği açısından, bir hukuk bürosunun ISO/IEC 27001 standardına tam olarak uyumlu olması beklenemeyeceği gibi, standarda uyum sağlama süreci de hem ek iş gücü ihtiyacı hem de maliyet açısından yüksek bir maliyetle karşılaşılmasına neden olabilecektir. Bu nedenle, hukuk bürolarının ISO/IEC 27001 standardının tüm kontrollerine uyum sağlamaktansa, mevcut durumlarının analiz edilmesi ve teknik açıdan kabul edilebilir bir seviyede kontrollerle uyumlu hale gelmesi en düşük iş gücü ve en düşük maliyetli çözüm olacaktır. Ancak, kontrollerin seçimi ISO/IEC 27001 Ek A' ya dayandırılmalıdır [26]. BGYS, kontrollerinin seçiminin, kuruluşun bilgi varlıklarını korumak ve hizmet alanlara güven vermek için yeterli ve orantılı olması gerekmektedir [15].

Bu çalışmada, ISO/IEC 27001 kontrolleri paralelinde hazırlanan öz değerlendirme anketi ile hukuk bürolarından mevcut durumları hakkında veri toplanmıştır. Toplanan veriler, hukuk bürolarının kontrollerle ne derecede uyumlu oldukları açısından analiz edilmiştir.

Yeni teknolojilerin gelişimiyle birlikte, yeni riskler de gelişmekte ve uygun bir şekilde yönetilmesi gerekmektedir. Güncel ve gelecekte ortaya çıkacak olan yeni risk türlerini bütünüyle destek sağlamak için kullanılan RD yöntemleri bu hızlı gelişimi takip etmek zorundadır [18].

BG günümüzde bilgi işlem başarısına katkıda bulunan en önemli konulardan birisidir. Etkili BG uygulama gerekliliği kamu, ticari ve kar amacı gütmeyen her türdeki kuruluşlarda ortaya çıkabilir.

Bilgi Toplumu Stratejisi 2006-2010 Faaliyet Planı, Başbakanlık Devlet Planlama Teşkilatı, 88 nolu maddesi, Ulusal Bilgi Sistemleri Güvenlik Programını tanımlamaktadır. Bu kapsamda, TÜBİTAK tarafından Türkiye' de dört kamu kurumunda ISO/IEC 27001 merkezli BGYS kuruluş danışmanlığı yapılmıştır [21].

Günümüzde, özel sektöre ek olarak, özellikle Sayıştay tarafından yapılan denetimler sonucunda, BGYS' nin kurulması ve kamu kurumlarında da ISO/IEC 27001 belgesi alınması neredeyse bir gereklilik haline gelmiştir [22].

Çoğu BGYS metodoloji ve araç genellikle kuruluşa özgüdür ve bir BT sisteminin belirli bölümleriyle ilgili değerlendirme raporları ve karşı önlemlerin alınmasına yöneliktir [25].

BG yatırımı yapan kuruluşlar, var olan tüm bilgi varlıklarını kapsayan, uygulanabilir, izlenebilir ve bilgi varlıklarını ve koruyabilecek bir BGYS amaçlamalıdır.

Günümüzün kuruluşlarında kilit bir varlık olarak bilgi, artan tehditlerden korunmalıdır. ISO/IEC 27001 standardına uygun bir BGYS kurmak, bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için ilk adımdır. Günümüz kuruluşlarında kilit bir varlık olarak bilgi, gereksiz artıştan da korunmalıdır [26].

Bu çalışmada, hukuk bürolarına uygulanan ISO/IEC 27001 kontrolleri paralelinde hazırlanan öz değerlendirme anketi aracılığı ile toplanan veriler analiz edilmiş ve hukuk bürolarının, ISO/IEC 27001 BGYS ile mevcut uyumluluk düzeyleri belirlenmiştir. Buna ek olarak, bir BGYS' nin ana ve alt amaçları açısından değerlendirilmiştir. Bu yolla hukuk büroları için minimum maliyet ve iş gücü ile ISO/IEC 27001 BGYS ile uyumlu bir BG modeli geliştirilmiştir.

Modeller yüksek düzeyde bir soyutlama seviyesinde olduğundan, bu yaklaşım, BG topluluğu içindeki etki alanı düzeyinde güvenlikle çalışan etki alanı analistleri ile aynı sorunları analiz eden güvenlik uygulayıcıları arasındaki bilgi güvenliği topluluğundaki boşluğu doldurmaya katkıda bulunmaktadırlar [26].

Kuruluşlar BT' ye ve bu teknolojilerden geliştirilen bilgi sistemlerine misyonlarını ve kuruluşlarının iş fonksiyonlarını başarıyla yürütmek için bağlıdırlar. Bilgi sistemleri süper bilgisayarlardan cep telefonlarına bir dizi çeşitli bilgisayar platformları oluşturucu bileşenler içerebilirmektedir [42].

Birçok kuruluşun karşılaştığı teknolojik genişleme nedeniyle, kuruluş varlıkları içinde dolaşımda olan çok çeşitli kritik bilgiler vardır. Bu genişleme, saldırganlar tarafından güvenlik açığı istismarına daha fazla duyarlılık sağlamaktadır. Bu nedenle kuruluşta var olan bilgilerin bütünlüğüne, gizliliğine ve kullanılabilirliğine katkıda bulunan kontrol ve politikaların tasarlanması son derece önemli hale gelmiştir. [45].

Standardizasyon perspektifinden bakıldığında, ISO/IEC 27001 kuruluşun sahip olduğu bilgi varlıklarının doğrudan kuruluşun kontrolü altında korunması olarak düşünmek mümkündür [46].

5. YÖNTEM

Çalışma için ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan kontrol listesi paralelinde hazırlanan 309 maddeden oluşan öz değerlendirme anketi (EK-1) kullanılmıştır. Anket maddeleri, ilk bölüm hukuk bürosunun İnsan Kaynakları, BTE ve BTİ özellikleri olmak üzere, ISO/IEC 27001 BGYS' nin 14 amaç ve 35 alt amacı paralelinde toplam 15 başlık altında katılımcılara sunulmuştur.

5.1. Evren ve Örneklem

Araştırmanın çalışma evrenini 31/12/2018 Tarihi itibariyle aktif olarak 79 İl Barosuna kayıtlı avukatların çalıştığı hukuk büroları oluşturmaktadır. Evrene ait bilgiler TBB web sitesinden alınmıştır. Türkiye' de aktif olarak herhangi bir hukuk bürosuna bağlı olarak 116.779 avukat bulunmaktadır. Bu avukatlara ait cinsiye ve bağlı olunan Baro bilgileri Çizelge 5.1.' de verilmiştir. Her bir baroya bağlı avukatların toplam kaç hukuk bürosunda çalıştığına dair veriye ulaşılamamıştır.

Çizelge 5.1. 31/12/2018 tarihi itibariyle Türkiye' de Barolara bağlı avukat sayıları [152]

BARO ADI	ERKEK	KADIN	TOPLAM	ORAN(%)
ADANA BAROSU	1.557	1.128	2.685	2,30
ADIYAMAN BAROSU	224	84	308	0,26
AFYONKARAHİSAR BAROSU	303	171	474	0,41
AĞRI BAROSU	117	39	156	0,13
AKSARAY BAROSU	166	88	254	0,22
AMASYA BAROSU	139	84	223	0,19
ANKARA BAROSU	8.629	7.483	16.112	13,80
ANTALYA BAROSU	2.447	1.880	4.327	3,71
ARTVİN BAROSU	56	43	99	0,08
AYDIN BAROSU	672	493	1.165	1,00
BALIKESİR BAROSU	706	458	1.164	1,00
BARTIN BAROSU	56	56	112	0,10
BATMAN BAROSU	281	95	376	0,32
BİLECİK BAROSU	78	56	134	0,11
BİNGÖL BAROSU	91	32	123	0,11

Çizelge 5.1. (devam) 31/12/2018 tarihi itibariyle Türkiye' de Barolara bağlı avukat sayıları [152]

BİTLİS BAROSU	87	34	121	0,10
BOLU BAROSU	106	72	178	0,15
BURDUR BAROSU	139	95	234	0,20
BURSA BAROSU	1.987	1.421	3.408	2,92
ÇANAKKALE BAROSU	295	206	501	0,43
ÇANKIRI BAROSU	56	40	96	0,08
ÇORUM BAROSU	237	139	376	0,32
DENİZLİ BAROSU	751	466	1.217	1,04
DİYARBAKIR BAROSU	908	407	1.315	1,13
DÜZCE BAROSU	134	95	229	0,20
EDİRNE BAROSU	268	169	437	0,37
ELAZIĞ BAROSU	253	98	351	0,30
ERZİNCAN BAROSU	80	71	151	0,13
ERZURUM BAROSU	336	169	505	0,43
ESKİŞEHİR BAROSU	589	519	1.108	0,95
GAZİANTEP BAROSU	1.149	522	1.671	1,43
GİRESUN BAROSU	183	136	319	0,27
GÜMÜŞHANE BAROSU	54	17	71	0,06
HAKKARİ BAROSU	101	14	115	0,10
HATAY BAROSU	839	373	1212	1,04
IĞDIR BAROSU	61	42	103	0,09
ISPARTA BAROSU	257	144	401	0,34
İSTANBUL BAROSU	22.258	20.941	43.199	36,99
İZMİR BAROSU	4.521	4.255	8.776	7,52
K.MARAŞ BAROSU	519	233	752	0,64
KARABÜK BAROSU	91	71	162	0,14
KARAMAN BAROSU	88	53	141	0,12
KARS BAROSU	117	51	168	0,14
KASTAMONU BAROSU	133	92	225	0,19
KAYSERİ BAROSU	962	636	1.598	1,37
KIRIKKALE BAROSU	145	90	235	0,20
KIRKLARELİ BAROSU	161	104	265	0,23
KIRŞEHİR BAROSU	100	48	148	0,13
KİLİS BAROSU	53	27	80	0,07
KOCAELİ BAROSU	911	769	1.680	1,44
KONYA BAROSU	1.479	903	2.382	2,04

Çizelge 5.1. (devam) 31/12/2018 tarihi itibariyle Türkiye' de Barolara bağlı avukat sayıları [152]

KÜTAHYA BAROSU	241	121	362	0,31
MALATYA BAROSU	424	186	610	0,52
MANİSA BAROSU	638	373	1.011	0,87
MARDİN BAROSU	291	147	438	0,38
MERSİN BAROSU	1.287	866	2.153	1,84
MUĞLA BAROSU	725	694	1.419	1,22
MUŞ BAROSU	90	37	127	0,11
NEVŞEHİR BAROSU	129	62	191	0,16
NİĞDE BAROSU	119	77	196	0,17
ORDU BAROSU	268	157	425	0,36
OSMANİYE BAROSU	238	167	405	0,35
RİZE BAROSU	92	58	150	0,13
SAKARYA BAROSU	447	285	732	0,63
SAMSUN BAROSU	722	436	1.158	0,99
SİİRT BAROSU	108	32	140	0,12
SİNOP BAROSU	66	52	118	0,10
SİVAS BAROSU	280	214	494	0,42
ŞANLIURFA BAROSU	876	259	1.135	0,97
ŞIRNAK BAROSU	163	30	193	0,17
TEKİRDAĞ BAROSU	483	361	844	0,72
TOKAT BAROSU	214	143	357	0,31
TRABZON BAROSU	343	262	605	0,52
TUNCELİ BAROSU	29	10	39	0,03
UŞAK BAROSU	246	133	379	0,32
VAN BAROSU	443	145	588	0,50
YALOVA BAROSU	120	85	205	0,18
YOZGAT BAROSU	132	59	191	0,16
ZONGULDAK BAROSU	279	193	472	0,40
TOPLAM	65.423	51.356	116.779	100,00
ORAN	56,02	43,98		

Türkiye toplamında 116.779 avukat olduğu, bunların 65.423' ünün erkek (%56,02), 51.356' sının kadın (%43.98) olduğu görülmüştür.

En çok avukatın olduğu üç ilin İstanbul (43.199-%36,99), Ankara (16.112-%13,80), İzmir (8.776-%7,52) olduğu, bu üç ilde bulunan avukat sayısının Türkiye' deki avukatların % 58,30' u olduğu görülmüştür.

Hukuk bürolarının ve avukatların bağlı oldukları baroya göre herhangi bir özel statüye yahut ayrıcalığa sahip olmamaları ve araştırma konusu olan ISO/IEC 27001 BGYS açısından belirleyici bir özellik olmamasından dolayı, baro bazında erişilen hukuk bürosu ve avukat sayıları araştırmada incelenmemiştir.

Çalışma evreninin tüm Türkiye' yi kapsaması nedeni ile, yüz yüze ve posta yolu ile anket uygulama yöntemleri kullanılmış, 452 hukuk bürosu ile çalışılmıştır.

Örnekleme hatasını en aza indirgeyebilmek için farklı örnekleme yöntemleri kullanılmıştır.

Basit Tesadüfi Örnekleme: Sosyal medya ve Internet araştırmaları sonucu iletişim bilgilerine ulaşılan, farklı illerden avukatlarla görüşülmüş, posta ve telefon aracılığı ile anketler uygulanmıştır.

Kartopu Örneklemesi: Samsun ili içinde ve dışında halihazırda tanınan avukatların bulunduğu hukuk bürolarına anket uygulanmıştır. Bu avukatların referansları aracılığı ile farklı hukuk bürolarında çalışan avukatlar aracılığı ile anket uygulanmıştır. Samsun ilindeki anket uygulamaları yüz yüze yapılmıştır.

Küme Örneklemesi: Samsun ili içerisinde hukuk bürolarının yoğun olduğu adliye bölgesinde hukuk büroları doğrudan ziyaret edilmiş, sosyal medya aracılığı ile hukuk ve avukat grupları aracılığı ile rastgele ulaşılan avukatlar aracılığı ile posta yolu ile çalıştıkları hukuk bürolarına anket uygulanmıştır.

5.2. Veri Toplama Aracı

Araştırma, Hukuk Bürolarının ISO/IEC 27001 BGYS' ne uyumları konusunda bilgi toplamak için hazırlanan ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan Amaç, Alt Amaç ve Kontroller paralelinde hazırlanan Öz Değerlendirme Anketi kullanılmıştır.

Anketin, hukuk bürosunun ISO/IEC 27001 BGYS' ye uyum sağlama düzeyleri araştırma amacı taşımasından dolayı, yani anketi dolduran kişinin, kişisel görüş ve nitelikleri ile ilgili olmamasından dolayı yaş, cinsiyet, avukatlık kıdemi gibi bireysel verilerin toplanmasına ihtiyaç duyulmamıştır.

Literatürde BGYS' lerini etkileyen ana faktörlerin İnsan Kaynakları, kullanılan Bilgi Teknolojileri Ekipmanı (BTE) ve Bilgi Teknolojileri İletişimi (BTİ) ile ilgili olmasından dolayı, ankette hukuk bürolarının bu özellikleri de tespit edilmiştir.

ISO/IEC 27001 BGYS, 14 Alt Amaç, 35 Alt Amaç ve 113 Kontrolden oluşmaktadır. Hazırlanan ankette hiçbir kontrol atlanmamak şartıyla, kontrolün yapısına göre değişen sayıda, toplam 294 anket maddesi hazırlanmıştır. ISO/IEC 27001 BGYS amaç ve alt amaçlarına ilişkin anket madde sayıları Çizelge 5.2.' de gösterilmiştir.

Çizelge 5.2. ISO/IEC 27001 referans kontrol amaç ve alt amaçları ile anket madde eşleştirmeleri

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	**Alt Amaç Sayısı**	**Kontrol Sayısı**	**Anket Madde Sayısı**
5. Bilgi Güvenliği Politikaları	1	2	8
5.1. Bilgi güvenliği için yönetimin yönlendirmesi		2	8
6. Bilgi Güvenliği Organizasyonu	2	7	12
6.1. İç organizasyon		5	8
6.2. Mobil cihazlar ve uzaktan çalışma		2	4
7. İnsan Kaynakları Güvenliği	3	6	15
7.1. İstihdam öncesi		2	3
7.2. Çalışma esnasında		3	10
7.3. İstihdamın sonlandırılması ve değiştirilmesi		1	2
8. Varlık Yönetimi	3	10	18
8.1. Varlıkların sorumluluğu		4	6
8.2. Bilgi sınıflandırması		3	7
8.3. Ortam işleme		3	5
9. Erişim Kontrolü	4	14	25
9.1 Erişim kontrolünün iş gereklilikleri		2	3
9.2. Kullanıcı erişim yönetimi		6	13
9.3. Kullanıcı sorumlulukları		1	2
9.4. Sistem ve uygulama erişim kontrolü		5	7
10. Kriptografi	1	2	5

Çizelge 5.2. (devam) ISO/IEC 27001 referans kontrol amaç ve alt amaçları ile anket madde eşleştirmeleri

10.1. Kriptografik kontroller		2	5
11. Fiziksel ve Çevresel Güvenlik	2	15	42
11.1. Güvenli alanlar		6	12
11.2. Teçhizat		9	30
12. İşletim Güvenliği	7	13	42
12.1. İşlem prosedürleri ve sorumlulukları		4	9
12.2. Kötücül yazılımlardan koruma		1	2
12.3. Yedekleme		1	7
12.4. Kaydetme ve izleme		3	13
12.5. İşletimsel yazılımının kontrolü		1	2
12.6. Teknik açıklık yönetimi		2	6
12.7. Bilgi sistemleri tetkik hususları		1	3
13. Haberleşme Güvenliği	2	7	22
13.1. Ağ güvenliği yönetimi		3	10
13.2. Bilgi transferi		4	12
14. Sistem Temini, Geliştirme ve Bakımı	3	13	47
14.1. Bilgi sistemlerinin güvenlik gereksinimleri		3	10
14.2. Geliştirme ve destek süreçlerinde güvenlik		9	31
14.3. Test verisi		1	6
15. Tedarikçi İlişkileri	2	5	18
15.1. Tedarikçi ilişkilerinde bilgi güvenliği		3	8
15.2. Tedarikçi hizmet sağlama yöntemi		2	10
16. Bilgi Güvenliği İhlal Olayı Yönetimi	1	7	14
16.1. Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi		7	14
17. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	2	4	12
17.1. Bilgi güvenliği sürekliliği		3	8
17.2. Yedek fazlalıklar		1	4
18. Uyum	2	8	14
18.1. Yasal ve sözleşmeye tabi gereksinimlerle uyum		5	9
18.2. Bilgi güvenliği gözden geçirmeleri		3	5
TOPLAM	35	113	294

5.3. Veri İşleme

Katılımcılara hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özellikleri ile ilgili sorular yöneltilen ilk bölümünde 1-5 sorularda sayısal değerler girmeleri istenmiştir. 6-15 aralığında

yine İnsan Kaynakları, BTE ve BTİ özelliklerine ilişkin evet ve hayır şeklinde yanıtlamaları istenen sorular yöneltilmiştir.

ISO/IEC 27001 kontrollerine ilişkin 35 alt amaç anket içerisinde amaçlar paralelinde hazırlanan 14 soru grubu olarak katılımcılara yöneltilmiştir. Her bir alt amaca ait soru grubunun başlangıcında, katılımcılara gruptaki soruları cevaplayıp cevaplamamalarının gerektiğini belirlemek üzere evet/hayır seçenekli sorular sorulmuştur.

Grup sorusuna hayır cevabını veren katılımcılar, grup içerisindeki soruların tamamına hayır cevabını vermiştir.

Grup içerisindeki anket maddelerine katılımcılardan her soruya karşılık evet, kısmen ve hayır cevaplarından birini işaretlemeleri istenmiştir. Evet cevapları 2, kısmen cevapları 1 ve hayır cevapları 0 puan olacak şekilde her bir katılımcının anketteki alt amaçlarda bulunan sorulara verdikleri puanlar toplanmış ve o alt amaçtaki soru sayısına bölünerek katılımcıların alt amaçlardaki düzeyleri belirlenmiştir. Bu şekilde bir katılımcı herhangi bir alt amaçtaki düzeyi maksimum 2, minimum 0 puan olabilmektedir. Aynı durum 452 katılımcı bazında düşünülerek katılımcıların genel alt amaçlardaki seviyeleri tespit edilmiştir. Yani alt amaçlardaki genel düzeyleri hesaplanırken, katılımcıların o alt amaçtan elde ettiği puanlar toplanarak katılımcı sayısına bölünmüştür.

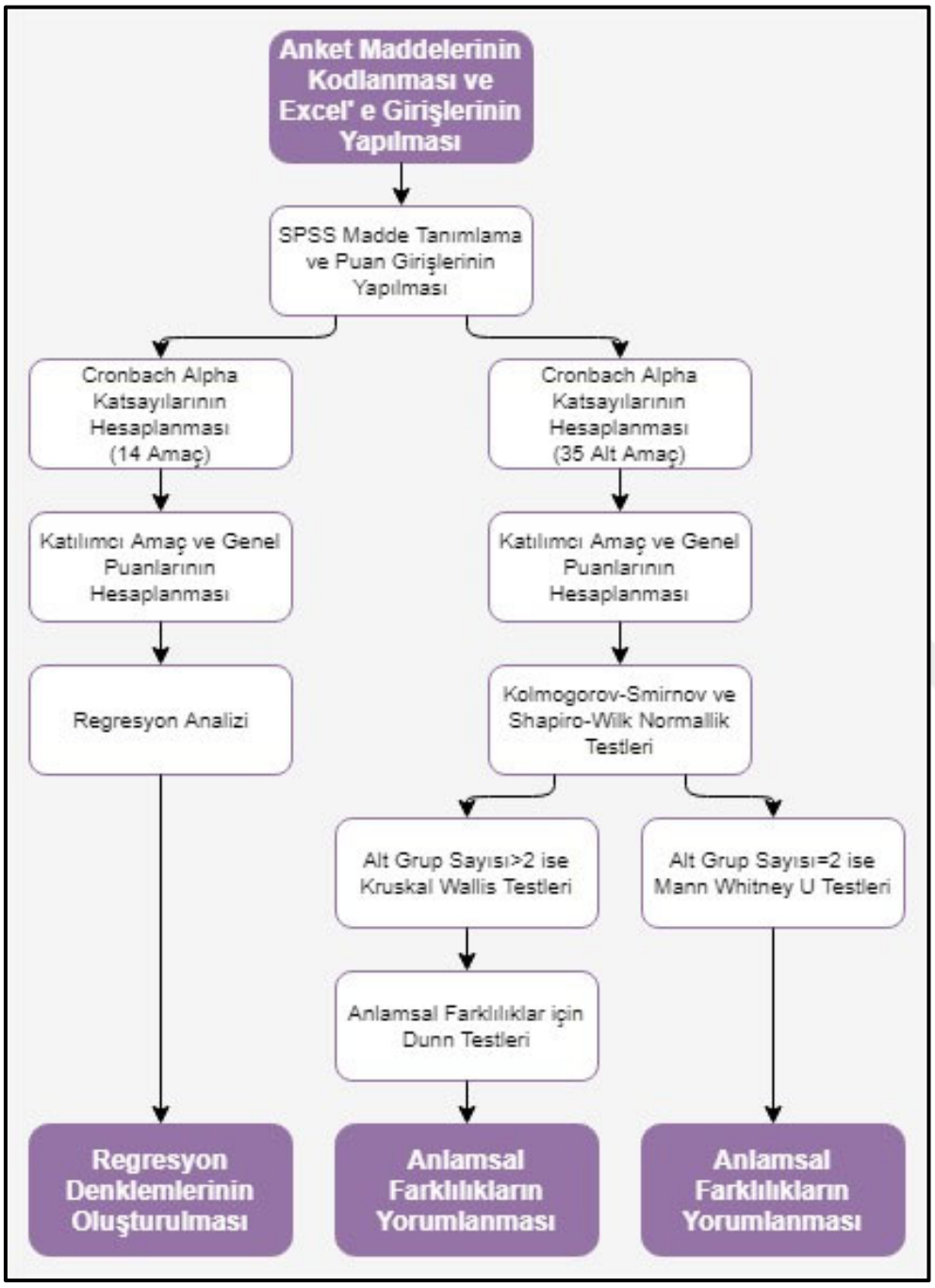
Katılımcıların amaç puanlarının hesaplanmasında da aynı yöntem kullanılmış, her bir katılımcının anketteki amaçta bulunan sorulara verdikleri puanlar toplanmış ve o amaçtaki soru sayısına bölünerek katılımcıların amaçtaki düzeyleri belirlenmiştir. Bu şekilde bir katılımcı herhangi bir amaçtaki düzeyi maksimum 2, minimum 0 puan olabilmektedir. Aynı durum 452 katılımcı bazında düşünülerek katılımcıların genel amaç seviyeleri tespit edilmiştir. Yani amaçtaki genel düzeyleri hesaplanırken, katılımcıların o amaçtan elde ettiği puanlar toplanarak katılımcı sayısına bölünmüştür.

Şekil 5.1.’ de yer alan veri işleme işlemleri sonrasında veri analiz işlemlerine geçilmiştir.

5.4. Verilerin Analizi

Uygulanan anket neticesinde elde edilen verilerin analizi Şekil-5.1’ de görülen adımlarla bu bölümde yapılmıştır. Verilerin analizinin yapılabilmesi için anket formları önce Excel’ e

daha sonra uygun kodlamalar yapılarak IBM SPSS 25.0 programına aktarılmıştır. Analizlerde tanımlayıcı istatistikler Frekans (n), Yüzde (%), Sıra Ortalaması (SO), Ortalama ($\bar{X}$) ve Standart Sapma (SS) olarak belirtilmiştir.



Şekil 5.1. Anket veri işleme ve analiz süreci

Güvenilirlik analizi, daha önceden belirlenmiş bir ölçek türüne göre hazırlanmış ankete verilen yanıtların tutarlılığını ölçen analiz türüdür. Likert tipi ölçümlerde ölçeğin iç tutarlılığını belirlemede Cronbach Alfa yöntemi kullanılır.

- 0,00≤α≤0,40 ise ölçek güvenilir değildir.
- 0,40≤α≤0,60 ise ölçek düşük güvenilirliktedir.
- 0,60≤α≤0,80 ise ölçek oldukça güvenilirdir.
- 0,80≤α≤1,00 ise ölçek yüksek derecede güvenilir bir ölçektir.

Ölçeğin Cronbach Alfa değerinin 0,4'den büyük olması gerekmekte ve 1 tam değerine yaklaştıkça güvenilirlik seviyesinin yükseldiği kabul görmektedir. Cronbach Alfa değerinin düşük çıkması testin homojen olmadığını yani birkaç özelliği bir arada ölçtüğünü gösterir. Her bir araştırma problemi için alt amaç soru gruplarına ait Cronbach Alfa değerleri Çizelge 5.3.' te gösterilmiştir.

Çizelge 5.3. Analizlerde kullanılan alt amaç madde gruplarının Cronbach Alfa değerleri

Alt Amaç Soru Grubu	Madde Sayısı	Cronbach Alfa Değeri
Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi	8	,769
Bilgi Güvenliği Organizasyonu - İç Organizasyon	8	,812
Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma	4	,733
İnsan Kaynakları Güvenliği - İstihdam Öncesi	3	,986
İnsan Kaynakları Güvenliği - Çalışma Esnasında	10	,815
İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi	2	,957
Varlık Yönetimi - Varlıkların Sorumluluğu	6	,995
Varlık Yönetimi - Bilgi Sınıflandırması	7	,980
Varlık Yönetimi - Ortam İşleme	5	,957
Erişim Kontrolü - Erişim Kontrolü İçin İş Gereksinimi	3	,907
Erişim Kontrolü - Kullanıcı Erişim Yönetimi	13	,809
Erişim Kontrolü - Kullanıcı Sorumlulukları	2	,959
Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü	7	,891
Kriptografi - Kriptografik Kontroller	5	,767
Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar	12	,921
Fiziksel ve Çevresel Güvenlik - Teçhizat	30	,959
İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları	9	,840
İşlem Güvenliği - Kötücül Yazılımlardan Koruma	2	,874
İşlem Güvenliği - Yedekleme	7	,916
İşlem Güvenliği - Kaydetme ve İzleme	13	,785
İşlem Güvenliği - İşletimsel Yazılımının Kontrolü	2	,906
İşlem Güvenliği - Teknik Açıklık Yönetimi	6	,898

Çizelge 5.3. (devam) Analizlerde kullanılan alt amaç madde gruplarının Cronbach Alfa değerleri

İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları	3	,806
Haberleşme Güvenliği - Ağ Güvenliği Yönetimi	10	,608
Haberleşme Güvenliği - Bilgi Transferi	12	,927
Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri	10	,870
Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik	31	,912
Sistem Temini, Geliştirme ve Bakımı - Test Verisi	6	,902
Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği	8	,949
Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi	10	,960
Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi	14	,846
İş Sürekliliğinin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği	8	,962
İş Sürekliliğinin Bilgi Güvenliği Hususları - Yedek Fazlalıklar	4	,917
Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum	9	,833
Uyum - Bilgi Güvenliği Gözden Geçirmeleri	5	,915

Cronbach Alfa değerleri incelendiğinde sonuçların ,608 ile ,995 arasında olduğu görülmüş ve analizlerde kullanılan ölçeklerin güvenilir oldukları anlaşılmıştır.

5.5. Analiz Türünün Belirlenmesi

ISO/IEC 27001 BGYS 14 amaç ve 35 alt amacından elde edilen, hukuk bürolarına ait anket sonuçları, 2 farklı açıdan incelenmiştir.

Birincisi, hukuk bürolarının İnsan Kaynakları, BTE, ve BTİ özellikleri ile ISO/IEC 27001 BGYS kontrolleri arasındaki ilişkilerin analizi, ikincisi ise, ISO/IEC 27001 BGYS kontrolleri aracılığı ile, hukuk bürolarının BGYS Puanı olarak isimlendirilen, ISO/IEC 27001 BGYS kontrollerine uyum düzeylerini ifade etmek üzere hesaplanan puan değerinin tespiti için yapılan regresyon analizidir.

Regresyon analizi ile bir BGYS Puanı hesaplamaktaki amaç, öz değerlendirme anketini herhangi bir zamanda yanıtlayan hukuk büroları için de ISO/IEC 27001 BGYS' ne uyum seviyelerini diğer hukuk büroları ile kıyaslanabilir bir puan hesaplayabilmektir.

Verilerin normal dağılıma uygun olup olmadığını belirlenmek amacıyla çeşitli normallik testleri uygulanabilir. Bu testler arasında en bilinenleri ve en güçlüleri Kolmogorow-Smirnov, Shapiro-Wilk normallik testleridir. Bu testler sonucunda elde edilen anlamlılık düzeyi p<,05 düzeyinde ise verilerin normal dağılmadığına karar verilir. ISO/IEC 27001 BGYS 35 alt amacından elde edilen hukuk bürolarına ait genel puanlara ayrı ayrı Kolmogorov-Smirnov ve Shapiro-Wilk normallik testleri yapılmış ve sonuçlar Çizelge 5.4.' te verilmiştir.

Çizelge 5.4. Alt amaçlara ait Kolmogorov-Smirnov ve Shapiro-Wilk normallik test sonuçları

Alt Amaç Soru Grubu	Kolmogorov-Smirnov			Shapiro-Wilk		
	İsta tistik	S.D	p	İsta tistik	S.D	p
Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi	,483	452	,000	,499	452	,000
Bilgi Güvenliği Organizasyonu - İç Organizasyon	,516	452	,000	,369	452	,000
Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma	,531	452	,000	,304	452	,000
İnsan Kaynakları Güvenliği - İstihdam Öncesi	,508	452	,000	,451	452	,000
İnsan Kaynakları Güvenliği - Çalışma Esnasında	,479	452	,000	,435	452	,000
İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi	,504	452	,000	,419	452	,000
Varlık Yönetimi - Varlıkların Sorumluluğu	,409	452	,000	,620	452	,000
Varlık Yönetimi - Bilgi Sınıflandırması	,450	452	,000	,487	452	,000
Varlık Yönetimi - Ortam İşleme	,431	452	,000	,547	452	,000
Erişim Kontrolü - Erişim Kontrolü İçin İş Gereksinimi	,466	452	,000	,385	452	,000
Erişim Kontrolü - Kullanıcı Erişim Yönetimi	,530	452	,000	,301	452	,000
Erişim Kontrolü - Kullanıcı Sorumlulukları	,363	452	,000	,707	452	,000
Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü	,371	452	,000	,567	452	,000
Kriptografi - Kriptografik Kontroller	,323	452	,000	,773	452	,000
Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar	,454	452	,000	,585	452	,000
Fiziksel ve Çevresel Güvenlik - Teçhizat	,496	452	,000	,313	452	,000
İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları	,534	452	,000	,319	452	,000
İşlem Güvenliği - Kötücül Yazılımlardan Koruma	,287	452	,000	,777	452	,000
İşlem Güvenliği - Yedekleme	,308	452	,000	,753	452	,000
İşlem Güvenliği - Kaydetme ve İzleme	,430	452	,000	,600	452	,000

Çizelge 5.4. (devam) Alt amaçlara ait Kolmogorov-Smirnov ve Shapiro-Wilk normallik test sonuçları

İşlem Güvenliği - İşletimsel Yazılımının Kontrolü	,475	452	,000	,519	452	,000
İşlem Güvenliği - Teknik Açıklık Yönetimi	,418	452	,000	,593	452	,000
İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları	,485	452	,000	,443	452	,000
Haberleşme Güvenliği - Ağ Güvenliği Yönetimi	,518	452	,000	,328	452	,000
Haberleşme Güvenliği - Bilgi Transferi	,281	452	,000	,829	452	,000
Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri	,455	452	,000	,500	452	,000
Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik	,309	452	,000	,617	452	,000
Sistem Temini, Geliştirme ve Bakımı - Test Verisi	,503	452	,000	,362	452	,000
Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği	,526	452	,000	,322	452	,000
Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi	,485	452	,000	,426	452	,000
Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi	,324	452	,000	,651	452	,000
İş Sürekliliğinin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği	,428	452	,000	,589	452	,000
İş Sürekliliğinin Bilgi Güvenliği Hususları - Yedek Fazlalıklar	,497	452	,000	,472	452	,000
Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum	,272	452	,000	,828	452	,000
Uyum - Bilgi Güvenliği Gözden Geçirmeleri	,381	452	,000	,708	452	,000
S.D: Serbestlik Derecesi						

Çizelge 5.4.' e göre Kolmogorov-Smirnov ve Shapiro-Wilk testlerinde anlamlılık kısmındaki değerlerin p<,05 olmasından dolayı verilerin normal dağılıma sahip olmadıkları anlaşılmış ve analizlerde nanparametrik testler kullanılmıştır.

ISO/IEC 27001 BGYS alt amaçlarına ait puanlar ile İnsan Kaynakları, BTE ve BTİ özelliklerinin katılımcılardan değer girilmesi istenen 1-5 sorularda 2' den fazla alt gruba sahip oldukları için Kruskal Wallis testleri, 6-15 sorular içinse İnsan Kaynakları, BTE ve BTİ özelliklerinin analizinde 2 alt gruba sahip oldukları için Mann Whitney U testleri kullanılmıştır. İstatistiksel anlamlılık değeri p<,05 olarak kabul edilmiştir.

Kruskal Wallis testi sonucu herhangi bir değişkenin alt grupları arasında farklılık tespit edilirse (p<,05 olarak bulunursa), bu farklılığın hangi alt gruplar arasında olduğu çeşitli yöntemlerle araştırılabilir. Bu yöntemlere post-hoc testleri denir. Analizlerde post-hoc testi olarak Dunn çoklu karşılaştırma testi (Bonferroni testi) kullanılmış, alt gruplar arası farklılık yorumlanmıştır. Mann Whitney U testi iki grup arasındaki farklılaşmayı gösterdiği için ek bir analiz gerekmeksizin doğrudan yorumlama yapılmıştır.

6. BULGULAR

Bu bölümde, ISO/IEC 27001 BGYS alt amaçları seviyesinde 35 araştırma problemi ile 35 alt amacın, hukuk bürosunun 15 anket maddesinden oluşan İnsan Kaynakları, BTE, BTİ özellikleri açısından analizi yapılmış, elde edilen bulgular istatistiksel açıdan sunulmuştur.

Diğer taraftan, ISO/IEC 27001 BGYS amaçları seviyesinde, 14 alt amaç için regresyon analizi yapılmış ve hukuk bürolarının ISO/IEC 27001 BGYS' ye uyum düzeylerini ifade etmek üzere regresyon formülü elde edilmiştir.

6.1. Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ Özellikleri

Anket sorusunu cevaplayan 452 hukuk bürosunun İnsan Kaynakları, BTE ve BTİ özelliklerine ait bilgiler analiz edilerek yüzde ve frekans değerleri Çizelge 6.1.' de verilmiştir.

Çizelge 6.1. Hukuk bürolarına ait insan kaynakları, BTE ve BTİ özellikleri yüzde oranları çizelgesi

İnsan Kaynakları, BTE ve BTİ Özellikleri		N	%
1. Bürodaki çalışan avukat sayısı?	Bir	48	10,6
	İki	196	43,4
	Üç	92	20,4
	Dört	52	11,5
	Beş+	64	14,2
2. Bürodaki çalışan personel sayısı?	Bir	144	31,9
	İki	112	24,8
	Üç	108	23,9
	Dört+	88	19,5
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	84	18,6
	Bir	68	15,0
	İki	252	55,8
	Üç	48	10,6
4. Büroda kullanılan bilgisayar sayısı?	İki	116	25,7
	Üç	76	16,8
	Dört	40	8,8
	Beş	84	18,6
	Altı+	136	30,1

Çizelge 6.2. (devam) Hukuk bürolarına ait insan kaynakları, BTE ve BTİ özellikleri yüzde oranları çizelgesi

5. Büroda kullanılan yazıcı sayısı?	Bir	256	56,6
	İki	132	29,2
	Üç	64	14,2
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	232	51,3
	Evet	220	48,7
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	240	53,1
	Evet	212	46,9
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	236	52,2
	Evet	216	47,8
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	264	58,4
	Evet	188	41,6
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	196	43,4
	Evet	256	56,6
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	240	53,1
	Evet	212	46,9
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	208	46,0
	Evet	244	54,0
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	272	60,2
	Evet	180	39,8
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	236	52,2
	Evet	216	47,8
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	220	48,7
	Evet	232	51,3

452 hukuk bürosunun İnsan Kaynakları, BTE ve BTİ özellikleri incelendiğinde büyük oranda 2 avukatın (%43,4) çalıştığı, 1 personelin (%31,9) çalıştığı ve 2 yardımcı personelin (%55,8) çalıştığı tespit edilmiştir. Büroda kullanılan bilgisayar sayısının büyük oranda 6 ve üzeri (%30,1) olduğu, yazıcı sayısının ise büyük oranda 1 (%56,6) olduğu anlaşılmıştır.

452 hukuk bürosunun %48,7' si büroda bilgisayar ağına bağlı mobil cihazlar kullandığını, %46,9' u çalışanlarına büro ağında kişisel mobil cihazlarını kullanmalarına izin verdiğini, %47,8' i büro ve avukatlık hizmetleri için özel bir paket programı kullandığını, %41,6' sı büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi sahibi olduğunu, %56,6' sı büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerinin alındığı anlaşmalı bir tedarikçilerinin olduğunu, %46,9' u büro bilişim

güvenliği konusunda danışmanlık aldıkları bir tedarikçilerinin olduğunu, %54' ü büroda kablolu bilgisayar ağı kullandıklarını, %39,8' i büroda kablosuz bilgisayar ağı kullandıklarını, %47,8' i büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop ve cep telefonu bağlanmasına izin verdiklerini, %51,3' ü büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop ve cep telefonu bağlanmasına izin verdiklerini belirtmiştir.

6.2. Hukuk Bürolarının Alt Amaçlardaki Düzeylerine Ait Tanımlayıcı İstatistikler

452 hukuk bürosunun alt amaçlarındaki genel düzeylerine ait tanımlayıcı istatistikler hesaplanarak Çizelge 6.2.' de büyükten küçüğe doğru sırlanarak verilmiştir.

Çizelge 6.2. Hukuk bürolarının alt amaçlardaki düzeylerine ait tanımlayıcı istatistiksel değerler

Alt Amaçlar	N	Min.	Maks.	$\bar{X}$	SS
İşlem Güvenliği - Kötücül Yazılımlardan Koruma	452	,00	2,00	,7434	,7625
Erişim Kontrolü - Kullanıcı Sorumlulukları	452	,00	2,00	,6018	,7827
Haberleşme Güvenliği - Bilgi Transferi	452	,00	1,92	,5693	,6201
Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum	452	,00	2,00	,5516	,6022
Uyum - Bilgi Güvenliği Gözden Geçirmeleri	452	,00	2,00	,4743	,6676
Varlık Yönetimi - Varlıkların Sorumluluğu	452	,00	2,00	,4454	,7360
İşlem Güvenliği - Yedekleme	452	,00	2,00	,4197	,5519
Kriptografi - Kriptografik Kontroller	452	,00	2,00	,3947	,4850
İşlem Güvenliği - İşletimsel Yazılımının Kontrolü	452	,00	2,00	,3363	,6870
İnsan Kaynakları Güvenliği - İstihdam Öncesi	452	,00	2,00	,2979	,6883
Varlık Yönetimi - Ortam İşleme	452	,00	2,00	,2796	,5723
Varlık Yönetimi - Bilgi Sınıflandırması	452	,00	2,00	,2718	,6127
İşlem Güvenliği - Teknik Açıklık Yönetimi	452	,00	2,00	,2625	,4987
İş Sürekliliğinin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği	452	,00	2,00	,2323	,4366
Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar	452	,00	1,50	,2146	,4055
Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü	452	,00	2,00	,2111	,4268
İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi	452	,00	2,00	,1903	,5085
Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi	452	,00	2,00	,1871	,3042
İş Sürekliliğinin Bilgi Güvenliği Hususları - Yedek Fazlalıklar	452	,00	1,50	,1549	,3637

Çizelge 6.2. (devam) Hukuk bürolarının alt amaçlardaki düzeylerine ait tanımlayıcı istatistiksel değerler

Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik	452	,00	1,17	,1457	,2673
Erişim Kontrolü - Erişim Kontrolü İçin İş Gereksinimi	452	,00	2,00	,1327	,3884
Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi	452	,00	1,80	,1283	,3474
Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri	452	,00	1,60	,1257	,2911
Sistem Temini, Geliştirme ve Bakımı - Test Verisi	452	,00	1,67	,1180	,3645
Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi	452	,00	1,13	,1051	,2404
İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları	452	,00	1,00	,1003	,2546
İşlem Güvenliği - Kaydetme ve İzleme	452	,00	,54	,0994	,1765
Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği	452	,00	1,71	,0936	,3205
İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları	452	,00	,89	,0787	,2527
İnsan Kaynakları Güvenliği - Çalışma Esnasında	452	,00	1,00	,0743	,1974
Bilgi Güvenliği Organizasyonu - İç Organizasyon	452	,00	1,00	,0697	,2086
Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma	452	,00	1,25	,0575	,2053
Fiziksel ve Çevresel Güvenlik - Teçhizat	452	,00	1,60	,0555	,1958
Erişim Kontrolü - Kullanıcı Erişim Yönetimi	452	,00	,38	,0225	,0805
Haberleşme Güvenliği - Ağ Güvenliği Yönetimi	452	,00	,40	,0186	,0632

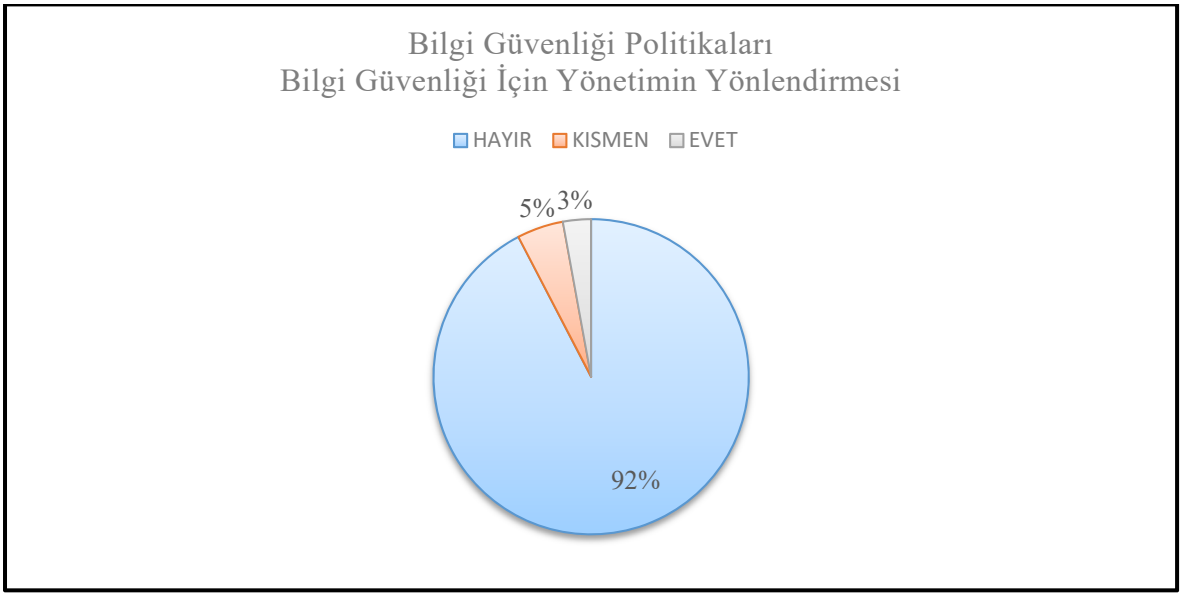
Hukuk bürolarının alt amaçlardaki düzeylerine ait ortalama puanlar incelendiğinde en yüksek ($\bar{X}$=,7434) puan ortalamasının İşlem Güvenliği - Kötücül Yazılımlardan Koruma alt amacında, en düşük puan ortalamasının ($\bar{X}$=,0186) İşlem Güvenliği - Ağ Güvenliği Yönetimi alt amacında olduğu görülmüştür. Hukuk bürolarının alt amaçlardaki düzeylerine ait puan ortalamalarının maksimum 2, minimum 0 olabildiği göz önüne alındığında hukuk bürolarının alt amaçlardaki düzeyleri genel itibariyle düşüktür denilebilir.

6.3. Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ Özellikleri İle ISO/IEC 27001 BGYS Alt Amaçlarının Analizi

Aşağıda, çalışmanın her bir araştırma problemi için, hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre alt amaçlarının analiz sonuçları yer almaktadır.

6.3.1. Bilgi güvenliği politikaları - Bilgi güvenliği için yönetimin yönlendirmesi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 8 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %3' ünün Evet, %5' inin Kısmen ve %92' sinin Hayır cevabını verdikleri görülmüştür (Şekil 6.1.).



Şekil 6.1. Bilgi güvenliği politikaları - Bilgi güvenliği için yönetimin yönlendirmesi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis (X^2 değeri) ve Mann Whitney U (U değeri) testleri uygulanmış sonuçlar, Çizelge 6.3.' te verilmiştir.

Çizelge 6.3. Bilgi güvenliği politikaları - Bilgi güvenliği için yönetimin yönlendirmesi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	206,33	,08	,29	X^2=4,121
	İki	226,74	,11	,25	p=,390
	Üç	223,72	,09	,21	
	Dört	235,27	,12	,22	
	Beş+	237,75	,13	,25	
2. Bürodaki çalışan personel sayısı?	Bir	232,94	,15	,33	X^2=17,890
	İki	221,00	,07	,16	p=,000
	Üç	201,61	,04	,15	
	Dört+	253,50	,15	,24	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	216,88	,09	,25	X^2=14,954
	Bir	234,97	,11	,21	p=,002
	İki	235,42	,13	,27	
	Üç	184,50	,00	,00	
4. Büroda kullanılan bilgisayar sayısı?	İki	233,05	,14	,32	X^2=15,159
	Üç	196,08	,03	,11	p=,004
	Dört	208,70	,06	,20	
	Beş	229,26	,12	,26	
	Altı+	241,44	,13	,22	
5. Büroda kullanılan yazıcı sayısı?	Bir	223,88	,11	,25	X^2=,558
	İki	230,80	,10	,21	p=,757
	Üç	228,13	,12	,27	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	232,19	,13	,28	U=24200
	Evet	220,50	,08	,19	p=,161
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	223,37	,11	,26	U=24688
	Evet	230,05	,10	,22	p=,424
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	223,92	,11	,27	U=24880
	Evet	229,31	,10	,21	p=,518
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	226,74	,12	,27	U=24752
	Evet	226,16	,09	,20	p=,945
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	211,44	,06	,17	U=22136
	Evet	238,03	,14	,28	p=,002
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	231,17	,13	,28	U=24320
	Evet	221,22	,08	,18	p=,233
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	233,04	,13	,28	U=24016
	Evet	220,93	,08	,20	p=,147
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	220,26	,08	,20	U=22784
	Evet	235,92	,14	,30	p=,066
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	215,08	,07	,19	U=22792
	Evet	238,98	,14	,29	p=,004
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	234,57	,13	,26	U=23744
	Evet	218,84	,08	,22	p=,059

Çizelge 6.3. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin;

- Büroda çalışan personel sayısına göre anlamlı farklılaştığı (X^2=17,890; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Üç" (201,61) olan hukuk bürolarının Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin "Bir" (232,94) olanlara göre daha düşük olduğu tespit edilmiştir (p=,033).
    - Büroda çalışan personel sayısı "Üç" (201,61) olan hukuk bürolarının Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin "Dört ve üzeri" (253,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=14,954; p=,002), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Üç" (184,50) olan hukuk bürolarının Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin "Bir" (216,88) olanlara göre daha düşük olduğu tespit edilmiştir (p=,015).
    - Büroda çalışan yardımcı personel sayısı "Üç" (184,50) olan hukuk bürolarının Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin "İki" (234,97) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=15,159; p=,004), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Üç" (196,08) olan hukuk bürolarının Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin "İki" (233,05) olanlara göre daha düşük olduğu tespit edilmiştir (p=,047).
    - Büroda kullanılan bilgisayar sayısı "Üç" (196,08) olan hukuk bürolarının Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin

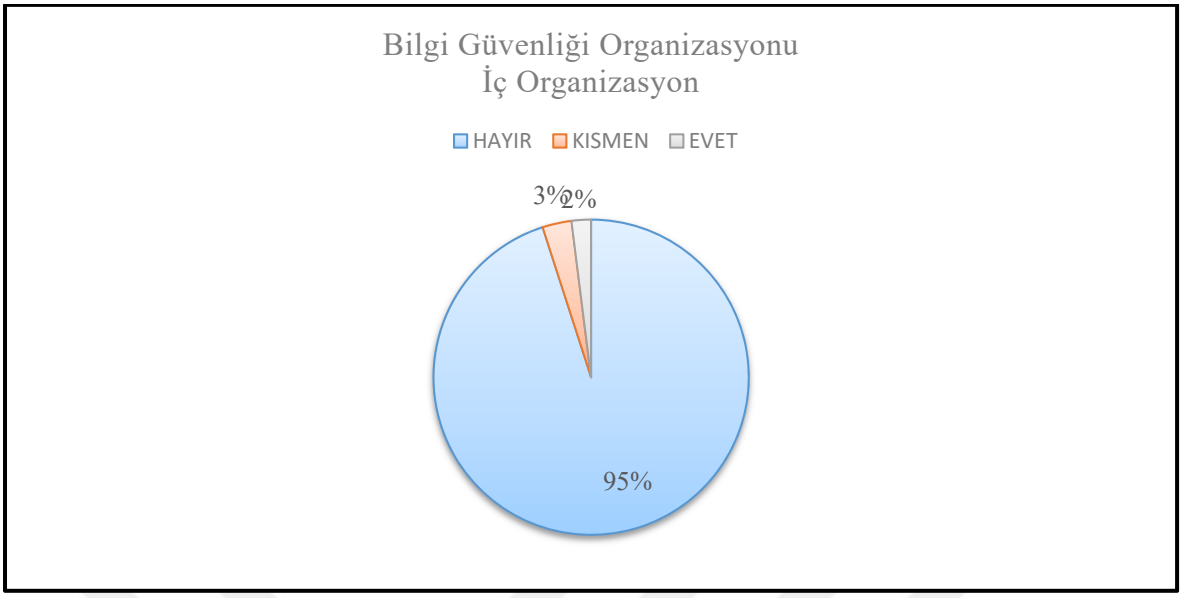
"Altı ve üzeri" (241,44) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).

Çizelge 6.3. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyinin;

- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22136; p=,002), tedarikçisi olan (238,03) hukuk bürolarının, olmayanlara (211,44) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22792; p=,004), bağlanmasına izin veren (238,98) hukuk bürolarının, vermeyenlere (215,08) göre daha yüksek olduğu tespit edilmiştir.

6.3.2. Bilgi güvenliği organizasyonu - İç organizasyon düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Organizasyonu - İç Organizasyon" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 8 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %2' sinin Evet, %3' ünün Kısmen ve %95' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.2.).



Şekil 6.2. Bilgi güvenliği organizasyonu - İç organizasyon alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.4.' te verilmiştir.

Çizelge 6.4. Bilgi güvenliği organizasyonu - İç organizasyon düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	237,67	,09	,26	X^2=21,007 p=,000
	İki	232,50	,08	,22	
	Üç	240,67	,12	,28	
	Dört	200,50	,00	,00	
	Beş+	200,50	,00	,00	
2. Bürodaki çalışan personel sayısı?	Bir	225,72	,07	,22	X^2=15,971 p=,001
	İki	224,86	,07	,21	
	Üç	209,46	,03	,17	
	Dört+	250,77	,12	,25	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	253,17	,13	,25	X^2=14,860 p=,002
	Bir	227,68	,08	,24	
	İki	218,75	,05	,20	
	Üç	218,83	,04	,14	
4. Büroda kullanılan bilgisayar sayısı?	İki	247,74	,13	,29	X^2=23,965 p=,000
	Üç	212,08	,03	,11	
	Dört	200,50	,00	,00	
	Beş	210,21	,01	,05	
	Altı+	234,15	,10	,24	

Çizelge 6.4. (devam) Bilgi güvenliği organizasyonu - İç organizasyon düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	231,97	,08	,22	X^2=9,831
	İki	228,50	,08	,24	p=,007
	Üç	200,50	,00	,00	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	223,74	,06	,19	U=24880
	Evet	229,41	,08	,23	p=,405
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	223,23	,06	,20	U=24656
	Evet	230,20	,08	,22	p=,307
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	230,91	,08	,22	U=24448
	Evet	221,69	,06	,20	p=,176
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	224,92	,07	,22	U=24400
	Evet	228,71	,07	,19	p=,583
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	218,58	,04	,16	U=23536
	Evet	232,56	,09	,24	p=,042
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	230,67	,08	,22	U=24440
	Evet	221,78	,06	,19	p=,193
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	235,31	,09	,24	U=23544
	Evet	218,99	,05	,18	p=,017
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	227,21	,07	,22	U=24288
	Evet	225,43	,06	,19	p=,799
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	230,53	,07	,20	U=24536
	Evet	222,09	,07	,22	p=,215
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	228,72	,07	,20	U=25032
	Evet	224,40	,07	,22	p=,526

Çizelge 6.4. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=21,007; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Dört" (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin "İki" (232,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,046).
    - Büroda çalışan avukat sayısı "Dört" (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin "Üç" (240,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,014).

  - Büroda çalışan avukat sayısı “Beş ve üzeri” (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “İki” (232,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,021).
  - Büroda çalışan avukat sayısı “Beş ve üzeri” (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “Üç” (240,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=15,971; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan personel sayısı “Üç” (209,46) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “Dört ve üzeri” (250,77) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=14,860; p=,002), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan yardımcı personel sayısı “İki” (218,75) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “Sıfır” (253,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=23,965; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Dört” (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “İki” (247,74) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
  - Büroda kullanılan bilgisayar sayısı “Beş” (210,21) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “İki” (247,74) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
  - Büroda kullanılan bilgisayar sayısı “Üç” (212,08) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin “İki” (247,74) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=9,831; p=,007), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

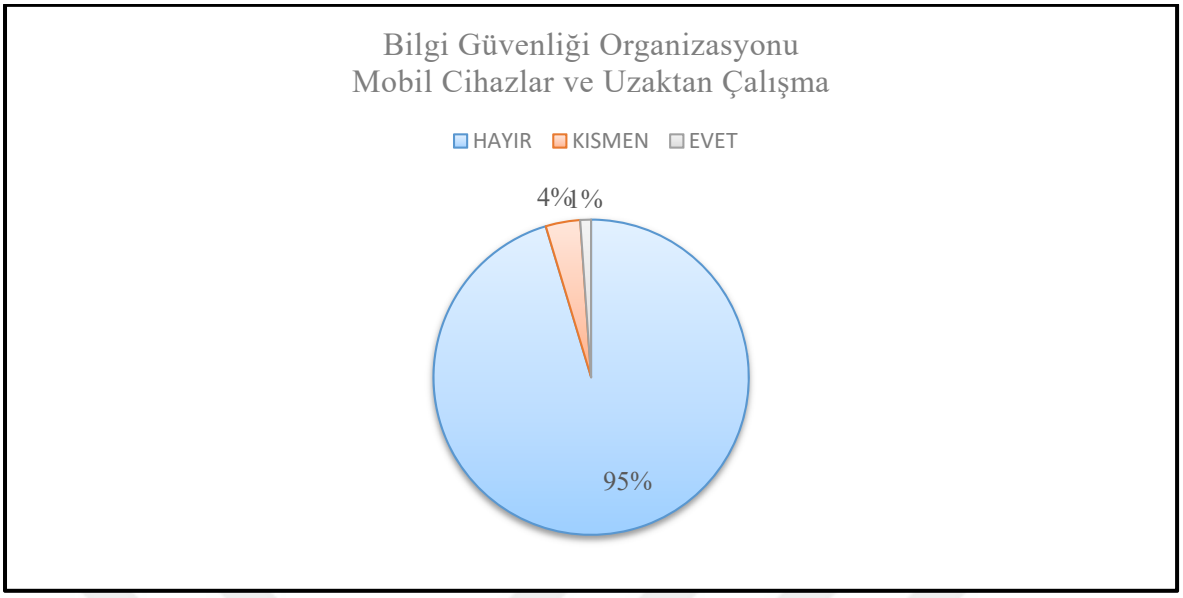
- Büroda kullanılan yazıcı sayısı "Üç" (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin "İki" (228,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,033).
- Büroda kullanılan yazıcı sayısı "Üç" (200,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin "Bir" (231,97) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).

Çizelge 6.4. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği Organizasyonu - İç Organizasyon düzeyinin;

- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U= 23536; p=,042), tedarikçisi olan (232,56) hukuk bürolarının, olmayanlara (218,58) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U= 23544; p=,017), kablolu bilgisayar ağı kullanan (218,99) hukuk bürolarının kullanmayanlara (235,31) göre daha düşük olduğu tespit edilmiştir.

6.3.3. Bilgi güvenliği organizasyonu - Mobil cihazlar ve uzaktan çalışma düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 2 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %1' inin Evet, %4' ünün Kısmen ve %95' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.3.).



Şekil 6.3. Bilgi güvenliği organizasyonu - Mobil cihazlar ve uzaktan çalışma alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.5.' te verilmiştir.

Çizelge 6.5. Bilgi güvenliği organizasyonu - Mobil cihazlar ve uzaktan çalışma düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	208,50	,00	,00	X^2=19,262
	İki	227,19	,07	,24	p=,001
	Üç	247,11	,11	,25	
	Dört	208,50	,00	,00	
	Beş+	222,88	,05	,19	
2. Bürodaki çalışan personel sayısı?	Bir	226,78	,05	,17	X^2=10,369
	İki	241,21	,12	,31	p=,016
	Üç	217,02	,03	,14	
	Dört+	218,95	,03	,16	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	220,02	,06	,27	X^2=1,886
	Bir	233,68	,06	,17	p=,596
	İki	226,50	,06	,19	
	Üç	227,67	,06	,22	

Çizelge 6.5. (devam) Bilgi güvenliği organizasyonu - Mobil cihazlar ve uzaktan çalışma düzeyinin analizi

4. Büroda kullanılan bilgisayar sayısı?	İki	240,09	,11	,30	X^2=25,502
	Üç	231,87	,07	,20	p=,000
	Dört	252,90	,13	,27	
	Beş	208,50	,00	,00	
	Altı+	215,26	,02	,13	
5. Büroda kullanılan yazıcı sayısı?	Bir	215,63	,03	,17	X^2=44,792
	İki	256,32	,14	,29	p=,000
	Üç	208,50	,00	,00	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	224,09	,05	,18	U=24960
	Evet	229,05	,07	,23	p=,390
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	223,30	,04	,16	U=24672
	Evet	230,12	,08	,25	p=,238
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	219,92	,03	,15	U=23936
	Evet	233,69	,08	,25	p=,017
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	229,11	,07	,23	U=24128
	Evet	222,84	,04	,17	p=,284
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	222,17	,05	,20	U=24240
	Evet	229,81	,07	,21	p=,189
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	223,77	,05	,22	U=24784
	Evet	229,59	,06	,20	p=,313
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	226,42	,07	,24	U=25360
	Evet	226,57	,05	,17	p=,980
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	221,56	,04	,15	U=23136
	Evet	233,97	,09	,27	p=,035
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	227,65	,06	,23	U=25216
	Evet	225,24	,05	,18	p=,676
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	225,15	,06	,23	U=25224
	Evet	227,78	,06	,19	p=,650

Çizelge 6.5. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=19,262; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (208,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin "Üç" (247,11) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).

- Büroda çalışan avukat sayısı “Dört” (208,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “Üç” (247,11) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=10,369; p=,016), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı “Üç” (217,02) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “İki” (241,21) olanlara göre daha düşük olduğu tespit edilmiştir (p=,021).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=25,502; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı “Beş” (208,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “İki” (240,09) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
    - Büroda kullanılan bilgisayar sayısı “Beş” (208,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “Dört” (252,90) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).
    - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (215,26) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “İki” (240,09) olanlara göre daha düşük olduğu tespit edilmiştir (p=,014).
    - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (215,26) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “Dört” (240,09) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=44,792; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı “Üç” (208,50) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “İki” (256,32) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

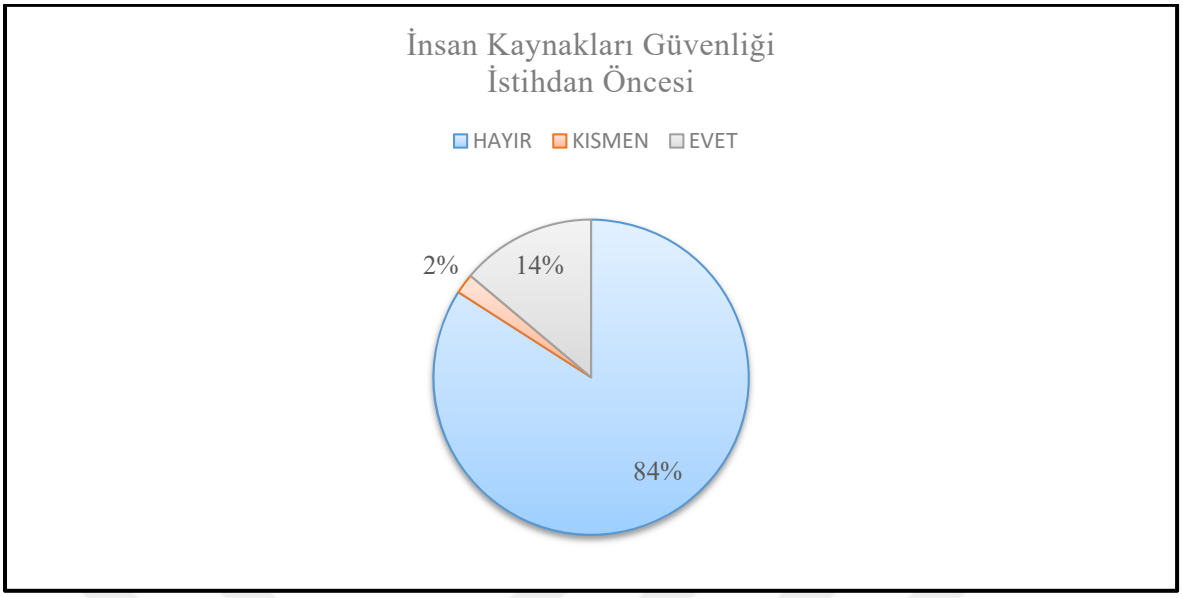
- Büroda kullanılan yazıcı sayısı “Bir” (215,63) olan hukuk bürolarının Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin “İki” (256,32) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.5. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=23936; p=,017), özel bir paket programı olan (233,69) hukuk bürolarının olmayanlara (219,92) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23136; p=,035), kablosuz bilgisayar ağı kullanan (233,97) hukuk bürolarının kullanmayanlara (221,56) göre daha yüksek olduğu tespit edilmiştir.

6.3.4. İnsan kaynakları güvenliği - İstihdam öncesi düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ iletişim özelliklerine göre “İnsan Kaynakları Güvenliği - İstihdam Öncesi” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 3 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %14’ ünün Evet, %2’ sinin Kısmen ve %84’ ünün Hayır cevabını verdikleri görülmüştür (Şekil 6.4.).



Şekil 6.4. İnsan kaynakları güvenliği - İstihdam öncesi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.6.' da verilmiştir.

Çizelge 6.6. İnsan kaynakları güvenliği - İstihdam öncesi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	247,50	,47	,86	X^2=6,859 p=,144
	İki	230,91	,33	,71	
	Üç	221,80	,26	,69	
	Dört	208,96	,15	,55	
	Beş+	218,25	,23	,63	
2. Bürodaki çalışan personel sayısı?	Bir	221,83	,26	,66	X^2=10,001 p=,019
	İki	216,21	,21	,63	
	Üç	223,39	,27	,67	
	Dört+	251,05	,50	,84	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	255,64	,54	,88	X^2=16,850 p=,001
	Bir	204,62	,12	,49	
	İki	225,74	,29	,68	
	Üç	210,50	,17	,58	
4. Büroda kullanılan bilgisayar sayısı?	İki	229,40	,32	,72	X^2=8,057 p=,090
	Üç	213,87	,19	,58	
	Dört	210,90	,17	,53	
	Beş	245,93	,46	,85	
	Altı+	223,68	,27	,67	

Çizelge 6.6. (devam) İnsan kaynakları güvenliği - İstihdam öncesi düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	225,75	,29	,69	X^2=6,697
	İki	238,14	,39	,77	p=,035
	Üç	205,50	,13	,50	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	216,98	,22	,60	U=23312
	Evet	236,54	,38	,77	p=,012
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	224,70	,28	,68	U=25008
	Evet	228,54	,31	,71	p=,624
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	236,26	,38	,76	U=23184
	Evet	215,83	,21	,60	p=,009
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	218,50	,23	,63	U=22704
	Evet	237,73	,39	,76	p=,015
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	222,58	,27	,66	U=24320
	Evet	229,50	,32	,72	p=,380
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	232,70	,35	,75	U=23952
	Evet	219,48	,24	,62	p=,091
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	223,96	,28	,66	U=24848
	Evet	228,66	,32	,72	p=,549
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	223,15	,27	,66	U=23568
	Evet	231,57	,34	,74	p=,292
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	228,74	,32	,71	U=24960
	Evet	224,06	,28	,68	p=,550
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	234,57	,36	,74	U=23744
	Evet	218,84	,24	,64	p=,044

Çizelge 6.6. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin;

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=10,001; p=,019), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "İki" (216,21) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin "Dört ve üzeri" (251,05) olanlara göre daha düşük olduğu tespit edilmiştir (p=,020).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=16,850; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

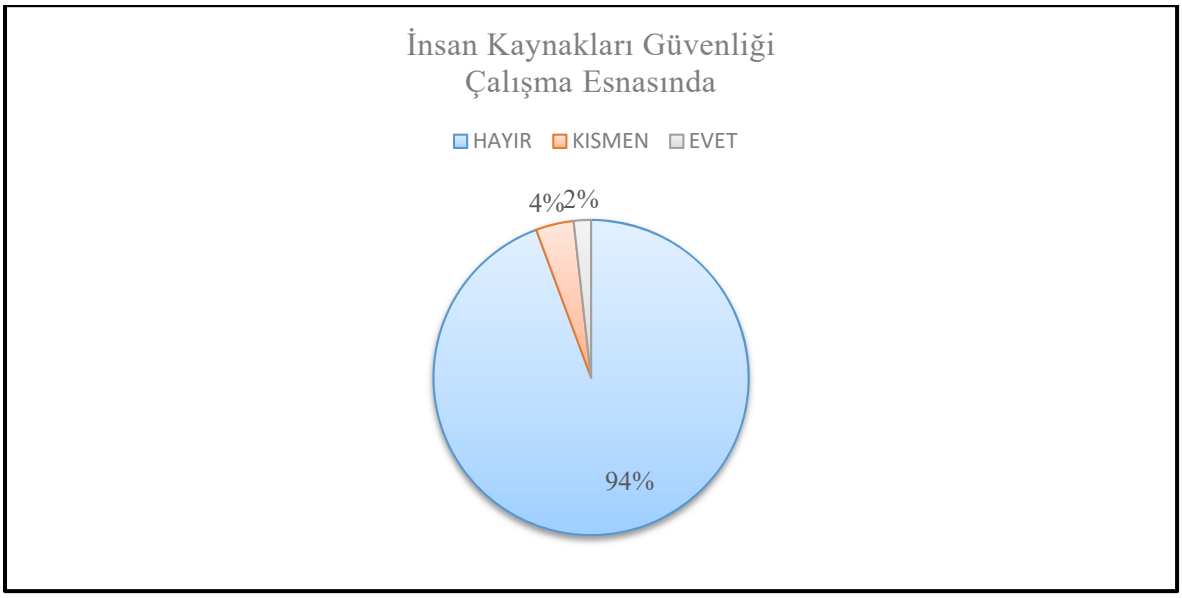
  - Büroda çalışan yardımcı personel sayısı “Bir” (204,62) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin “Sıfır” (255,64) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
  - Büroda çalışan yardımcı personel sayısı “Üç” (210,50) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin “Sıfır” (255,64) olanlara göre daha düşük olduğu tespit edilmiştir (p=,016).
  - Büroda çalışan yardımcı personel sayısı “İki” (225,74) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin “Sıfır” (255,64) olanlara göre daha düşük olduğu tespit edilmiştir (p=,026).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=6,697; p=,035), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan yazıcı sayısı “Üç” (205,50) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin “İki” (238,14) olanlara göre daha düşük olduğu tespit edilmiştir (p=,030).

Çizelge 6.6. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İnsan Kaynakları Güvenliği - İstihdam Öncesi düzeyinin;

- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23312; p=,012), bilgisayar ağında mobil cihazlar kullanan (236,54) hukuk bürolarının kullanmayanlara (216,98) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=23184; p=,009), özel bir paket programı olan (215,83) hukuk bürolarının olmayanlara (236,26) göre daha düşük olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=22704; p=,015), özel bir web sitesi olan (237,73) hukuk bürolarının olmayanlara (218,50) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23744; p=,044), bağlanmasına izin veren (218,84) hukuk bürolarının, vermeyenlere (234,57) göre daha düşük olduğu tespit edilmiştir.

6.3.5. İnsan kaynakları güvenliği - Çalışma esnasında düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - Çalışma Esnasında" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 10 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %2' sinin Evet, %4' ünün Kısmen ve %94' ünün Hayır cevabını verdikleri görülmüştür (Şekil 6.5.).



Şekil 6.5. İnsan kaynakları güvenliği - Çalışma esnasında alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.7.' de verilmiştir.

Çizelge 6.7. İnsan kaynakları güvenliği - Çalışma esnasında düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	225,83	,07	,16	X^2=3,093
	İki	228,70	,07	,18	p=,542
	Üç	217,80	,05	,14	
	Dört	241,73	,12	,27	
	Beş+	220,38	,10	,28	

Çizelge 6.7. (devam) İnsan kaynakları güvenliği - Çalışma esnasında düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	226,22	,08	,20	X^2=1,582
	İki	229,21	,08	,21	p=,663
	Üç	231,69	,10	,24	
	Dört+	217,14	,04	,10	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	242,21	,10	,18	X^2=20,080
	Bir	214,97	,06	,22	p=,000
	İki	216,18	,05	,15	
	Üç	269,50	,21	,34	
4. Büroda kullanılan bilgisayar sayısı?	İki	234,78	,08	,17	X^2=24,223
	Üç	260,82	,15	,29	p=,000
	Dört	188,50	,00	,00	
	Beş	220,02	,06	,20	
	Altı+	215,44	,06	,18	
5. Büroda kullanılan yazıcı sayısı?	Bir	216,25	,05	,16	X^2=27,016
	İki	221,71	,06	,19	p=,000
	Üç	277,38	,21	,31	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	221,09	,08	,22	U=24264
	Evet	232,21	,07	,18	p=,165
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	227,07	,08	,21	U=25304
	Evet	225,86	,06	,18	p=,880
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	215,31	,05	,18	U=22848
	Evet	238,72	,10	,22	p=,003
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	225,77	,07	,18	U=24624
	Evet	227,52	,08	,22	p=,829
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	226,42	,08	,22	U=25072
	Evet	226,56	,07	,18	p=,986
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	227,33	,09	,22	U=25240
	Evet	225,56	,06	,17	p=,825
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	218,35	,05	,16	U=23680
	Evet	233,45	,09	,22	p=,060
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,35	,06	,19	U=21448
	Evet	243,34	,10	,20	p=,001
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	237,55	,09	,21	U=2280
	Evet	214,43	,06	,18	p=,004
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	234,28	,09	,23	U=23808
	Evet	219,12	,06	,16	p=,058

Çizelge 6.7. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin;

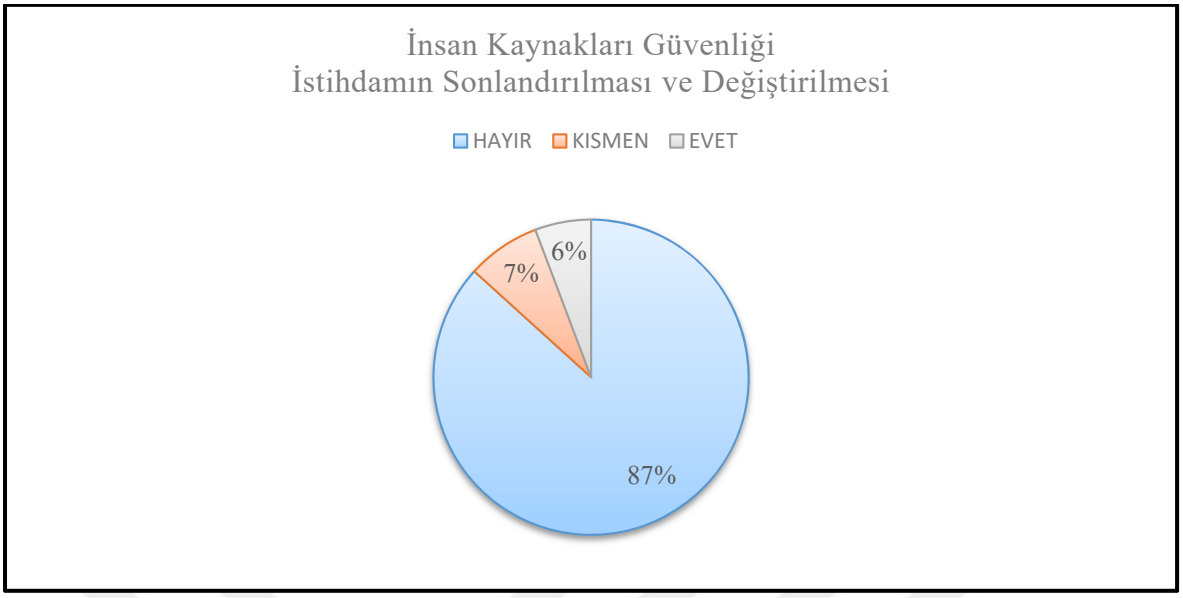
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=20,080; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Bir" (214,97) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (269,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
    - Büroda çalışan yardımcı personel sayısı "İki" (216,18) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (269,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=24,223; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Dört" (188,50) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "İki" (234,78) olanlara göre daha düşük olduğu tespit edilmiştir (p=,030).
    - Büroda kullanılan bilgisayar sayısı "Dört" (188,50) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (260,82) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (215,44) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (260,82) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).
    - Büroda kullanılan bilgisayar sayısı "Beş" (220,02) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (260,82) olanlara göre daha düşük olduğu tespit edilmiştir (p=,025).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=27,016; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "Bir" (216,25) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (277,38) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda kullanılan yazıcı sayısı "İki" (221,71) olan hukuk bürolarının İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin "Üç" (277,38) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.7. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İnsan Kaynakları Güvenliği - Çalışma Esnasında düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=22848; p=,003), özel bir paket programı olan (238,72) hukuk bürolarının olmayanlara (215,31) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21448; p=,001), kablosuz bilgisayar ağı kullanan (234,34) hukuk bürolarının kullanmayanlara (215,35) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22880; p=,004), bağlanmasına izin veren (214,43) hukuk bürolarının, vermeyenlere (237,55) göre daha düşük olduğu tespit edilmiştir.

6.3.6. İnsan kaynakları güvenliği - İstihdamın sonlandırılması ve değiştirilmesi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 2 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %6' sının Evet, %7' sinin Kısmen ve %87' sinin Hayır cevabını verdikleri görülmüştür (Şekil 6.6.).



Şekil 6.6. İnsan kaynakları güvenliği - İstihdamın sonlandırılması ve değiştirilmesi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.8.' de verilmiştir.

Çizelge 6.8. İnsan kaynakları güvenliği - İstihdamın sonlandırılması ve değiştirilmesi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	233,00	,25	,62	X^2=19,487
	İki	217,44	,13	,43	p=,001
	Üç	213,89	,11	,43	
	Dört	266,96	,50	,82	
	Beş+	234,63	,19	,40	
2. Bürodaki çalışan personel sayısı?	Bir	227,56	,24	,62	X^2=,062
	İki	226,93	,20	,52	p=,996
	Üç	225,61	,13	,33	
	Dört+	225,32	,18	,52	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	239,36	,31	,68	X^2=9,273
	Bir	219,68	,12	,33	p=,026
	İki	219,42	,14	,45	
	Üç	250,83	,33	,65	

Çizelge 6.8. (devam) İnsan kaynakları güvenliği - İstihdamın sonlandırılması ve değiştirilmesi düzeyinin analizi

4. Büroda kullanılan bilgisayar sayısı?	İki	218,98	,17	,54	X^2=3,498
	Üç	239,66	,21	,45	p=,478
	Dört	219,30	,20	,63	
	Beş	227,55	,21	,56	
	Altı+	227,03	,18	,47	
5. Büroda kullanılan yazıcı sayısı?	Bir	227,00	,21	,55	X^2=21,669
	İki	207,53	,06	,27	p=,000
	Üç	263,63	,38	,65	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	221,26	,15	,43	U=24304
	Evet	232,03	,24	,58	p=,148
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	231,37	,20	,50	U=24272
	Evet	220,99	,18	,53	p=,124
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	221,08	,15	,46	U=24208
	Evet	232,43	,23	,56	p=,128
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	225,77	,20	,54	U=24624
	Evet	227,52	,18	,47	p=,817
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	222,83	,18	,52	U=24368
	Evet	229,31	,20	,51	p=,388
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	231,33	,20	,49	U=24280
	Evet	221,03	,18	,54	p=,167
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	220,85	,16	,50	U=24200
	Evet	231,32	,21	,52	p=,161
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	223,88	,16	,46	U=23768
	Evet	230,46	,23	,58	p=,387
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	232,87	,23	,56	U=23984
	Evet	219,54	,15	,45	p=,074
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	234,72	,22	,52	U=23712
	Evet	218,71	,16	,51	p=,032

Çizelge 6.8. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=19,487; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Üç" (213,89) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Dört" (266,96) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).

  - Büroda çalışan avukat sayısı "İki" (217,44) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Dört" (266,96) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=9,273; p=,026), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan yardımcı personel sayı "İki" (219,42) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Sıfır" (239,36) olanlara göre daha düşük olduğu tespit edilmiştir (p=,046).
  - Büroda çalışan yardımcı personel sayı "İki" (219,42) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Üç" (250,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,012).
  - Büroda çalışan yardımcı personel sayı "Bir" (219,68) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Üç" (250,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,037).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=21,669; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan yazıcı sayısı "İki" (207,53) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Üç" (263,63) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda kullanılan yazıcı sayısı "Bir" (227,00) olan hukuk bürolarının İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin "Üç" (263,63) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).

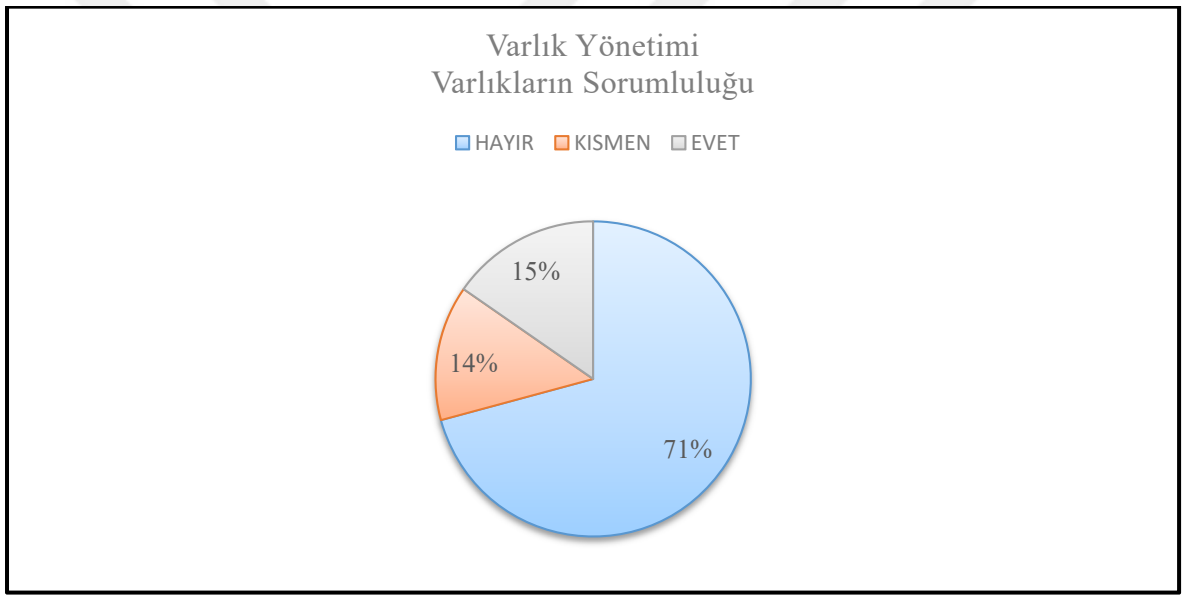
Çizelge 6.8. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi düzeyinin;

- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23712; p=,032),

bağlanmasına izin veren (218,71) hukuk bürolarının, vermeyenlere (234,72) göre daha düşük olduğu tespit edilmiştir.

6.3.7. Varlık yönetimi - Varlıkların sorumluluğu düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Varlıkların Sorumluluğu" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 6 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %15' inin Evet, %14' ünün Kısmen ve %71' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.7.).



Şekil 6.7. Varlık yönetimi - Varlıkların sorumluluğu alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U Testleri uygulanmış sonuçlar Çizelge 6.9.' da verilmiştir.

Çizelge 6.9. Varlık yönetimi - Varlıkların sorumluluğu düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	237,17	,58	,90	X^2=14,993
	İki	215,89	,39	,73	p=,005
	Üç	261,11	,65	,82	
	Dört	200,65	,23	,44	
	Beş+	222,25	,39	,71	
2. Bürodaki çalışan personel sayısı?	Bir	243,61	,56	,80	X^2=10,351
	İki	202,86	,30	,66	p=,016
	Üç	235,31	,48	,74	
	Dört+	217,77	,41	,73	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	236,40	,57	,87	X^2=10,626
	Bir	259,68	,65	,85	p=,014
	İki	213,93	,35	,65	
	Üç	228,17	,43	,79	
4. Büroda kullanılan bilgisayar sayısı?	İki	235,05	,51	,82	X^2=13,932
	Üç	205,03	,24	,52	p=,008
	Dört	273,70	,80	,92	
	Beş	208,21	,33	,66	
	Altı+	228,62	,47	,75	
5. Büroda kullanılan yazıcı sayısı?	Bir	226,41	,46	,75	X^2=2,337
	İki	234,80	,48	,75	p=,311
	Üç	209,75	,32	,70	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	229,64	,47	,77	U=24792
	Evet	223,19	,42	,71	p=,524
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	224,97	,42	,72	U=25072
	Evet	228,24	,47	,77	p=,747
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	235,11	,50	,77	U=23456
	Evet	217,09	,39	,71	p=,075
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	225,02	,42	,72	U=24424
	Evet	228,59	,48	,77	p=,728
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	220,66	,43	,76	U=23944
	Evet	230,97	,46	,73	p=,313
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	231,67	,50	,79	U=24200
	Evet	220,65	,39	,68	p=,277
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	233,42	,54	,83	U=23936
	Evet	220,60	,37	,65	p=,207
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,62	,35	,66	U=21520
	Evet	242,94	,59	,83	p=,008
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	228,70	,44	,70	U=24968
	Evet	224,09	,45	,79	p=,649
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	218,61	,38	,70	U=23784
	Evet	233,98	,51	,78	p=,129

Çizelge 6.9. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin;

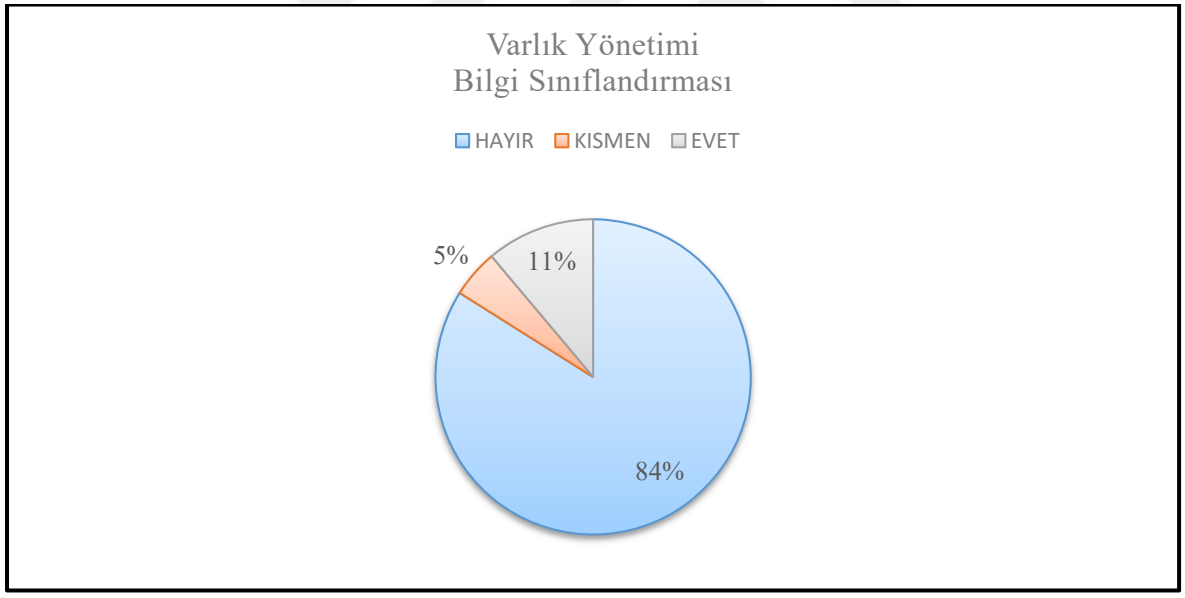
- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=14,993; p=,005), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Dört" (200,65) olan hukuk bürolarının Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin "Üç" (261,11) olanlara göre daha düşük olduğu tespit edilmiştir (p=,012).
    - Büroda çalışan avukat sayısı "İki" (215,89) olan hukuk bürolarının Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin "Üç" (261,11) olanlara göre daha düşük olduğu tespit edilmiştir (p=,009).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=10,351; p=,016), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "İki" (202,86) olan hukuk bürolarının Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin "Bir" (243,61) olanlara göre daha düşük olduğu tespit edilmiştir (p=,016).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=10,626; p=,014), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayı "İki" (213,93) olan hukuk bürolarının Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin "Bir" (259,68) olanlara göre daha düşük olduğu tespit edilmiştir (p=,011).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=13,932; p=,008), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Üç" (205,03) olan hukuk bürolarının Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin "Dört" (273,70) olanlara göre daha düşük olduğu tespit edilmiştir (p=,011).
    - Büroda kullanılan bilgisayar sayısı "Beş" (208,21) olan hukuk bürolarının Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin "Dört" (273,70) olanlara göre daha düşük olduğu tespit edilmiştir (p=,015).

Çizelge 6.9. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Varlık Yönetimi - Varlıkların Sorumluluğu düzeyinin;

- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21520; p=,008), kablosuz bilgisayar ağı kullanan (242,94) hukuk bürolarının kullanmayanlara (215,62) göre daha yüksek olduğu tespit edilmiştir.

6.3.8. Varlık yönetimi - Bilgi sınıflandırması düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Bilgi Sınıflandırma" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 7 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %11' inin Evet, %5' inin Kısmen ve %84' ünün Hayır cevabını verdikleri görülmüştür (Şekil 6.8.).



Şekil 6.8. Varlık yönetimi - Bilgi sınıflandırması alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Varlık Yönetimi - Bilgi Sınıflandırması düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.10.' da verilmiştir.

Çizelge 6.10. Varlık yönetimi - Bilgi sınıflandırması düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	229,17	,19	,37	X^2=4,621
	İki	231,85	,31	,67	p=,328
	Üç	214,50	,17	,46	
	Dört	210,50	,19	,56	
	Beş+	238,38	,45	,82	
2. Bürodaki çalışan personel sayısı?	Bir	224,78	,21	,51	X^2=18,821
	İki	208,57	,18	,53	p=,000
	Üç	216,94	,20	,54	
	Dört+	263,86	,58	,85	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	227,26	,21	,50	X^2=5,116
	Bir	233,21	,39	,78	p=,164
	İki	229,93	,28	,61	
	Üç	197,67	,17	,58	
4. Büroda kullanılan bilgisayar sayısı?	İki	228,98	,24	,55	X^2=4,230
	Üç	221,76	,20	,49	p=,376
	Dört	201,90	,20	,63	
	Beş	238,12	,28	,61	
	Altı+	227,09	,36	,74	
5. Büroda kullanılan yazıcı sayısı?	Bir	223,38	,28	,64	X^2=1,166
	İki	227,17	,19	,43	p=,558
	Üç	237,63	,42	,80	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	219,50	,23	,56	U=23896
	Evet	233,88	,32	,67	p=,107
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	212,50	,16	,47	U=22080
	Evet	242,35	,39	,73	p=,001
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	215,35	,23	,58	U=22856
	Evet	238,69	,32	,65	p=,009
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	225,44	,28	,64	U=24536
	Evet	227,99	,26	,59	p=,778
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	237,32	,36	,71	U=22968
	Evet	218,22	,21	,53	p=,034
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	224,07	,24	,58	U=24856
	Evet	229,25	,31	,66	p=,561
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	224,50	,27	,63	U=24960
	Evet	228,20	,27	,61	p=,679
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	224,71	,29	,64	U=23992
	Evet	229,21	,24	,58	p=,621
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	221,14	,22	,54	U=24224
	Evet	232,35	,33	,69	p=,209
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	227,74	,32	,69	U=25248
	Evet	225,33	,23	,54	p=,787

Çizelge 6.10. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Varlık Yönetimi - Bilgi Sınıflandırması düzeyinin;

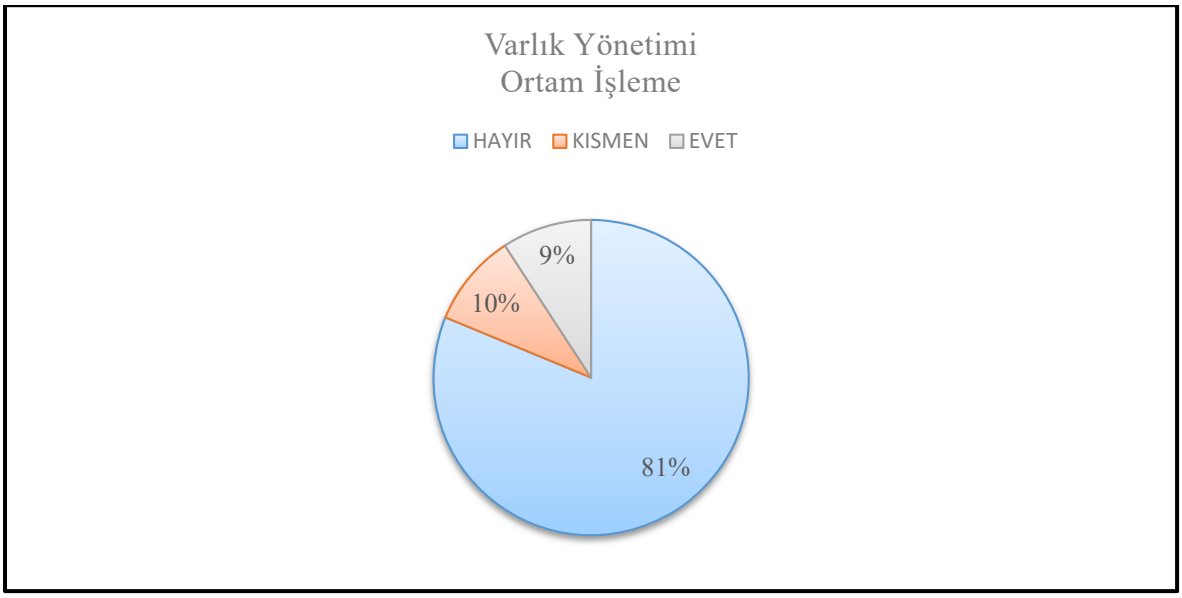
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=18,821; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "İki" (208,57) olan hukuk bürolarının Varlık Yönetimi - Bilgi Sınıflandırması düzeyinin "Dört ve üzeri" (263,86) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan personel sayısı "Üç" (216,94) olan hukuk bürolarının Varlık Yönetimi - Bilgi Sınıflandırması düzeyinin "Dört ve üzeri" (263,86) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
    - Büroda çalışan personel sayısı "Bir" (224,78) olan hukuk bürolarının Varlık Yönetimi - Bilgi Sınıflandırması düzeyinin "Dört ve üzeri" (263,86) olanlara göre daha düşük olduğu tespit edilmiştir (p=,014).

Çizelge 6.10. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Varlık Yönetimi - Bilgi Sınıflandırması düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22080; p=,001), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (242,35) hukuk bürolarının vermeyenlere (212,50) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=22856; p=,009), özel bir paket programı olan (238,69) hukuk bürolarının olmayanlara (215,35) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22968; p=,034), tedarikçisi olan (218,22) hukuk bürolarının, olmayanlara (237,32) göre daha düşük olduğu tespit edilmiştir.

6.3.9. Varlık yönetimi - Ortam işleme düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Ortam İşleme" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 5 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %9' unun Evet, %10' unun Kısmen ve %81' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.9.).



Şekil 6.9. Varlık yönetimi - Ortam işleme alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Varlık Yönetimi - Ortam İşleme düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.11.' de verilmiştir.

Çizelge 6.11. Varlık yönetimi - Ortam işleme düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	242,17	,30	,46	X^2=50,391 p=,000
	İki	201,36	,18	,51	
	Üç	207,63	,18	,49	
	Dört	297,12	,72	,83	
	Beş+	261,50	,36	,59	

Çizelge 6.11. (devam) Varlık yönetimi - Ortam işleme düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	224,39	,26	,54	X^2=18,595
	İki	219,43	,29	,65	p=,000
	Üç	259,02	,41	,68	
	Dört+	199,05	,13	,33	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	243,64	,34	,56	X^2=8,399
	Bir	197,79	,18	,53	p=,038
	İki	226,88	,30	,60	
	Üç	235,17	,23	,57	
4. Büroda kullanılan bilgisayar sayısı?	İki	221,33	,23	,48	X^2=9,053
	Üç	219,76	,16	,46	p=,060
	Dört	268,50	,66	,94	
	Beş	233,45	,30	,55	
	Altı+	218,03	,26	,57	
5. Büroda kullanılan yazıcı sayısı?	Bir	229,22	,34	,65	X^2=5,035
	İki	212,26	,16	,41	p=,081
	Üç	245,00	,28	,54	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	220,47	,27	,60	U=24120
	Evet	232,86	,29	,55	p=,189
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	237,57	,36	,67	U=22784
	Evet	213,97	,19	,43	p=,012
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	230,33	,25	,48	U=24584
	Evet	222,31	,31	,66	p=,396
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	212,71	,21	,53	U=21176
	Evet	245,86	,37	,63	p=,001
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	224,42	,28	,60	U=24680
	Evet	228,09	,28	,56	p=,699
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	232,73	,30	,59	U=23944
	Evet	219,44	,25	,57	p=,159
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	219,35	,28	,60	U=23888
	Evet	232,60	,28	,56	p=,161
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	231,15	,29	,56	U=23216
	Evet	219,48	,27	,60	p=,226
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	223,28	,27	,58	U=24728
	Evet	230,02	,29	,58	p=,475
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	227,26	,25	,52	U=25352
	Evet	225,78	,31	,62	p=,875

Çizelge 6.11. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Varlık Yönetimi - Ortam İşleme düzeyinin;

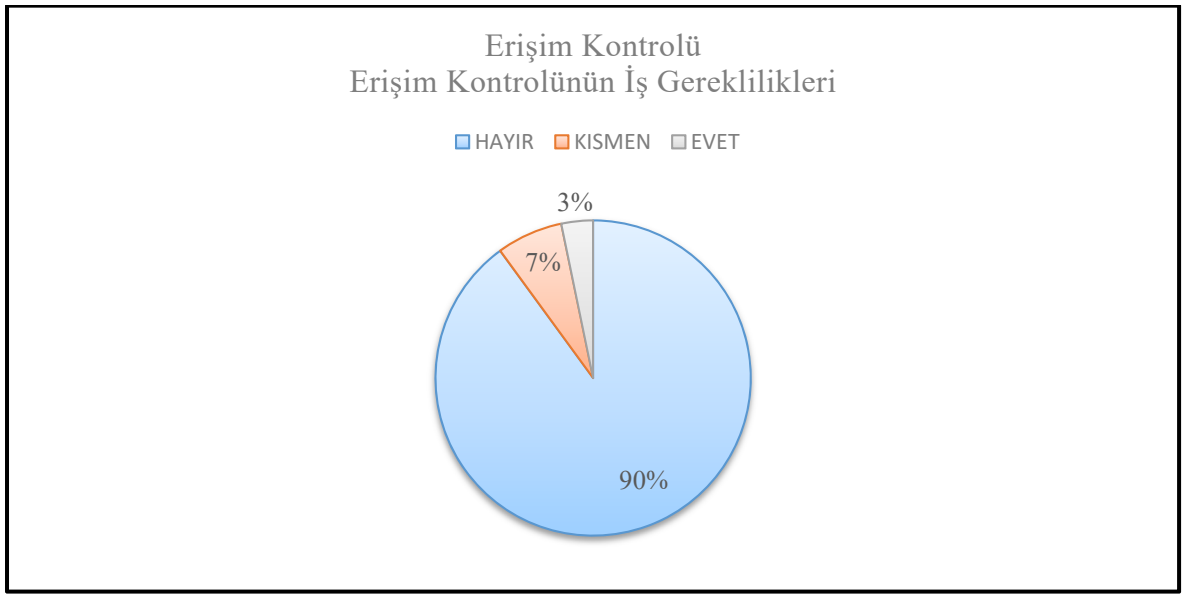
- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=50,391; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "İki" (201,36) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Beş ve üzeri" (261,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "İki" (201,36) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Dört" (297,12) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Üç" (207,63) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Beş ve üzeri" (261,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
    - Büroda çalışan avukat sayısı "Üç" (207,63) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Dört" (297,12) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=18,595; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Dört ve üzeri" (199,05) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Üç" (259,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan personel sayısı "İki" (219,43) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Üç" (259,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,020).
    - Büroda çalışan personel sayısı "Bir" (224,39) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Üç" (259,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,040).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=8,399; p=,038), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Bir" (197,79) olan hukuk bürolarının Varlık Yönetimi - Ortam İşleme düzeyinin "Sıfır" (243,64) olanlara göre daha düşük olduğu tespit edilmiştir (p=,030).

Çizelge 6.11. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Varlık Yönetimi - Ortam İşleme düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22784; p=,012), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (213,97) hukuk bürolarının vermeyenlere (237,57) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=21176; p=,001), özel bir web sitesi olan (245,86) hukuk bürolarının olmayanlara (212,71) göre daha yüksek olduğu tespit edilmiştir.

6.3.10. Erişim kontrolü - Erişim kontrolünün iş gereklilikleri düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 3 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %3' ünün Evet, %7' sinin Kısmen ve %90' ının Hayır cevabını verdikleri görülmüştür (Şekil 6.10.).



Şekil 6.10. Erişim kontrolü - Erişim kontrolünün iş gereklilikleri alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin anlamlı bir şekilde farklılaşıp

farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.12.' de verilmiştir.

Çizelge 6.12. Erişim kontrolü - Erişim kontrolü için iş gereksinimi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	244,67	,14	,26	X^2=15,649
	İki	234,38	,16	,43	p=,004
	Üç	208,33	,09	,35	
	Dört	243,12	,26	,60	
	Beş+	201,38	,02	,08	
2. Bürodaki çalışan personel sayısı?	Bir	232,78	,17	,45	X^2=2,793
	İki	231,43	,21	,55	p=,425
	Üç	221,09	,07	,19	
	Dört+	216,59	,05	,12	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	253,83	,22	,48	X^2=12,209
	Bir	229,56	,18	,50	p=,007
	İki	216,56	,08	,30	
	Üç	226,50	,17	,48	
4. Büroda kullanılan bilgisayar sayısı?	İki	236,64	,21	,53	X^2=19,742
	Üç	210,18	,04	,11	p=,001
	Dört	232,50	,10	,22	
	Beş	254,02	,22	,44	
	Altı+	208,21	,08	,35	
5. Büroda kullanılan yazıcı sayısı?	Bir	227,53	,15	,42	X^2=1,649
	İki	230,44	,15	,41	p=,438
	Üç	214,25	,04	,11	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	227,60	,13	,37	U=25264
	Evet	225,34	,13	,41	p=,777
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	234,23	,17	,45	U=23584
	Evet	217,75	,09	,31	p=,040
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	225,99	,12	,36	U=25368
	Evet	227,06	,15	,42	p=,894
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	226,29	,16	,47	U=24760
	Evet	226,80	,10	,24	p=,950
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	232,13	,21	,54	U=23984
	Evet	222,19	,07	,19	p=,218
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	227,17	,16	,44	U=25280
	Evet	225,75	,11	,33	p=,859
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	238,08	,22	,53	U=22968
	Evet	216,63	,06	,18	p=,008
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	218,00	,10	,34	U=22168
	Evet	239,34	,19	,46	p=,009
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	242,40	,19	,47	U=21736
	Evet	209,13	,07	,27	p=,000

Çizelge 6.12. (devam) Erişim kontrolü - Erişim kontrolü için iş gereksinimi düzeyinin analizi

15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	234,14	,18	,46	U=23840
	Evet	219,26	,09	,30	p=,063

Çizelge 6.12. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=15,649; p=,004), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (201,38) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin "İki" (234,38) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (201,38) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin "Dört" (243,12) olanlara göre daha düşük olduğu tespit edilmiştir (p=,009).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (201,38) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin "Bir" (244,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).
    - Büroda çalışan avukat sayısı "Üç" (208,33) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin "İki" (234,38) olanlara göre daha düşük olduğu tespit edilmiştir (p=,015).
    - Büroda çalışan avukat sayısı "Üç" (208,33) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin "Dört" (243,12) olanlara göre daha düşük olduğu tespit edilmiştir (p=,018).
    - Büroda çalışan avukat sayısı "Üç" (208,33) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin "Bir" (244,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,016).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=12,209; p=,007), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

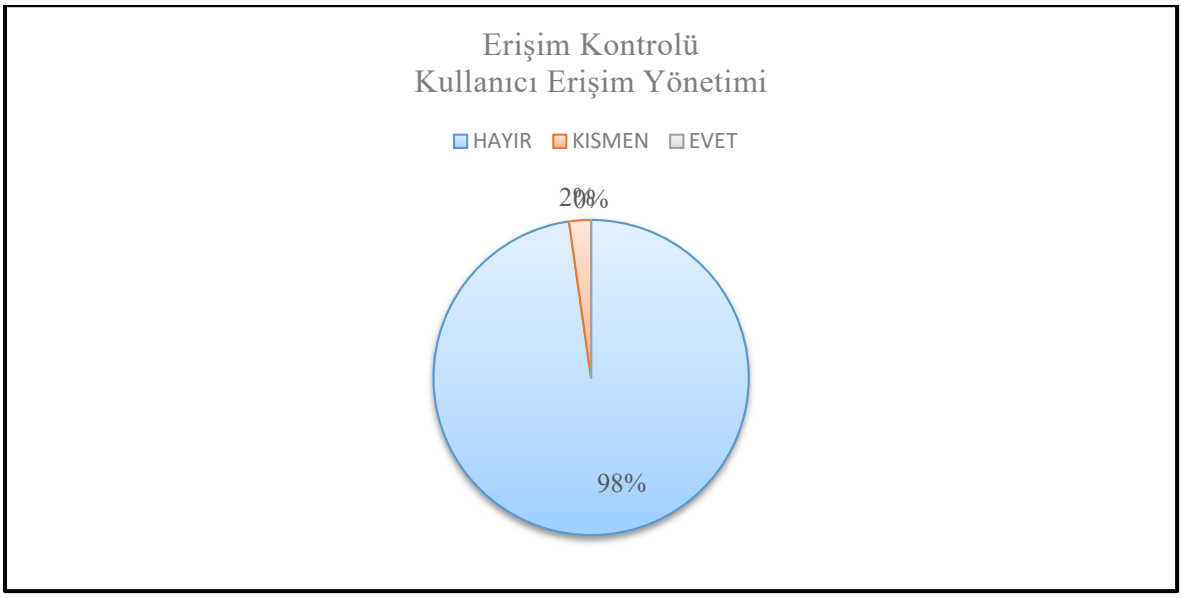
  - Büroda çalışan yardımcı personel sayısı “İki” (216,56) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin “Sıfır” (253,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=19,742; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (208,21) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin “Beş” (254,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
  - Büroda kullanılan bilgisayar sayısı “Üç” (210,18) olan hukuk bürolarının Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin “Beş” (254,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,011).

Çizelge 6.12. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23584; p=,040), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (217,75) hukuk bürolarının vermeyenlere (234,23) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22968; p=,008), kablolu bilgisayar ağı kullanan (216,63) hukuk bürolarının kullanmayanlara (238,08) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22168; p=,009), kablosuz bilgisayar ağı kullanan (239,34) hukuk bürolarının kullanmayanlara (218,00) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21736; p=,000), bağlanmasına izin veren (209,13) hukuk bürolarının, vermeyenlere (242,40) göre daha düşük olduğu tespit edilmiştir.

6.3.11. Erişim kontrolü - Kullanıcı erişim yönetimi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Kullanıcı Erişim Yönetimi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 13 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %0' ının Evet, %2' sinin Kısmen ve %98' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.11.).



Şekil 6.11. Erişim kontrolü - Kullanıcı erişim yönetimi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.13.' te verilmiştir.

Çizelge 6.13. Erişim kontrolü - Kullanıcı erişim yönetimi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	208,50	,00	,00	X^2=15,996
	İki	226,83	,02	,08	p=,003
	Üç	218,07	,01	,05	
	Dört	226,81	,03	,11	
	Beş+	250,88	,05	,12	

Çizelge 6.13. (devam) Erişim kontrolü - Kullanıcı erişim yönetimi düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	227,78	,03	,09	X^2=,318
	İki	224,57	,02	,08	p=,957
	Üç	225,17	,02	,08	
	Dört+	228,50	,02	,07	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	219,83	,02	,08	X^2=2,292
	Bir	234,97	,03	,10	p=,514
	İki	226,50	,02	,08	
	Üç	226,17	,01	,04	
4. Büroda kullanılan bilgisayar sayısı?	İki	216,36	,01	,06	X^2=13,768
	Üç	219,66	,01	,04	p=,008
	Dört	256,10	,08	,16	
	Beş	229,45	,02	,07	
	Altı+	228,44	,02	,08	
5. Büroda kullanılan yazıcı sayısı?	Bir	222,53	,02	,07	X^2=29,896
	İki	215,71	,01	,07	p=,000
	Üç	264,63	,07	,13	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	231,71	,03	,09	U=24312
	Evet	221,01	,02	,08	p=,064
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	226,87	,02	,07	U=25352
	Evet	226,08	,03	,09	p=,892
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	231,92	,03	,10	U=24208
	Evet	220,57	,01	,05	p=,049
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	232,50	,03	,09	U=23232
	Evet	218,07	,01	,06	p=,014
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	222,54	,02	,08	U=24312
	Evet	229,53	,03	,08	p=,230
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	227,00	,02	,07	U=25320
	Evet	225,93	,02	,09	p=,854
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	234,73	,03	,10	U=23664
	Evet	219,48	,01	,06	p=,008
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	228,44	,02	,08	U=23952
	Evet	223,57	,02	,08	p=,408
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	219,55	,01	,05	U=23848
	Evet	234,09	,04	,11	p=,012
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	228,68	,02	,08	U=25040
	Evet	224,43	,02	,09	p=,461

Çizelge 6.13. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=15,996; p=,003), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (208,50) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin "Beş ve üzeri" (250,88) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
    - Büroda çalışan avukat sayısı "Üç" (218,07) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin "Beş ve üzeri" (250,88) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=13,768; p=,008), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "İki" (216,36) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin "Dört" (256,10) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
    - Büroda kullanılan bilgisayar sayısı "Üç" (219,66) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin "Dört" (256,10) olanlara göre daha düşük olduğu tespit edilmiştir (p=,023).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=29,896; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "İki" (215,71) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin "Üç" (264,63) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda kullanılan yazıcı sayısı "Bir" (222,53) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin "Üç" (264,63) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

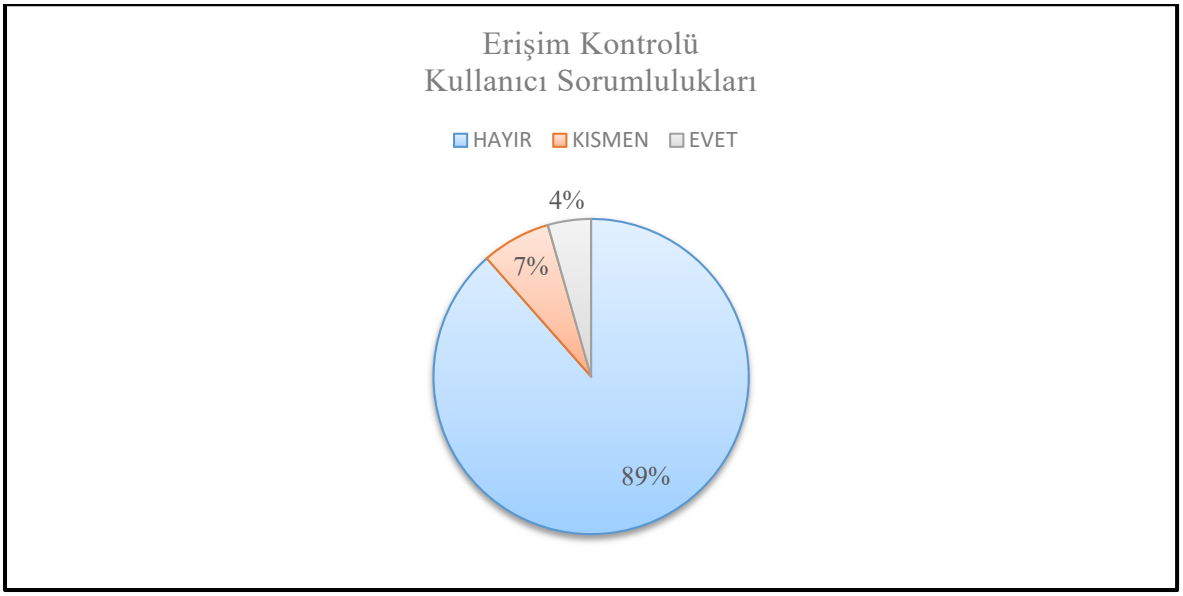
Çizelge 6.13. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Kullanıcı Erişim Yönetimi düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=24208; p=,049), özel bir paket programı olan (220,57) hukuk bürolarının olmayanlara (231,92) göre daha düşük olduğu tespit edilmiştir.

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=23232; p=,014), özel bir web sitesi olan (218,07) hukuk bürolarının olmayanlara (232,50) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23664; p=,008), kablolu bilgisayar ağı kullanan (219,48) hukuk bürolarının kullanmayanlara (234,73) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23848; p=,012), bağlanmasına izin veren (234,09) hukuk bürolarının, vermeyenlere (219,55) göre daha yüksek olduğu tespit edilmiştir.

6.3.12. Erişim kontrolü - Kullanıcı sorumlulukları düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Kullanıcı Sorumlulukları" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 2 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %4' ünün Evet, %7' sinin Kısmen ve %89' ünün Hayır cevabını verdikleri görülmüştür (Şekil 6.12.).



Şekil 6.12. Erişim kontrolü - Kullanıcı sorumlulukları alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.14.' de verilmiştir.

Çizelge 6.14. Erişim kontrolü - Kullanıcı sorumlulukları düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	171,00	,25	,62	X^2=35,679
	İki	236,21	,67	,83	p=,000
	Üç	192,59	,35	,57	
	Dört	231,88	,62	,77	
	Beş+	282,75	1,00	,89	
2. Bürodaki çalışan personel sayısı?	Bir	196,67	,42	,73	X^2=17,328
	İki	254,43	,75	,75	p=,001
	Üç	238,50	,67	,78	
	Dört+	225,05	,64	,90	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	224,98	,62	,86	X^2=18,899
	Bir	219,32	,53	,72	p=,000
	İki	216,02	,52	,74	
	Üç	294,33	1,08	,90	
4. Büroda kullanılan bilgisayar sayısı?	İki	209,05	,52	,83	X^2=9,308
	Üç	244,39	,74	,87	p=,054
	Dört	215,50	,50	,71	
	Beş	211,55	,48	,68	
	Altı+	243,85	,71	,80	
5. Büroda kullanılan yazıcı sayısı?	Bir	224,88	,59	,79	X^2=2,860
	İki	219,11	,52	,67	p=,239
	Üç	248,25	,81	,98	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	226,47	,60	,79	U=25512
	Evet	226,54	,60	,78	p=,995
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	226,40	,60	,79	U=25416
	Evet	226,61	,60	,79	p=,984
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	226,40	,59	,77	U=25464
	Evet	226,61	,61	,81	p=,984
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	243,14	,73	,85	U=20424
	Evet	203,14	,43	,65	p=,000
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	239,89	,67	,77	U=22464
	Evet	216,25	,55	,80	p=,031
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	231,03	,63	,80	U=24352
	Evet	221,37	,57	,77	p=,375
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	231,96	,63	,79	U=24240
	Evet	221,84	,57	,78	p=,353

Çizelge 6.14. (devam) Erişim kontrolü - Kullanıcı sorumlulukları düzeyinin analizi

13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	208,50	,47	,70	U=19584
	Evet	253,70	,80	,87	p=,000
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	224,74	,56	,70	U=25072
	Evet	228,43	,65	,87	p=,735
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	226,61	,62	,83	U=25496
	Evet	226,40	,59	,75	p=,984

Çizelge 6.14. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=35,679; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (171,00) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "İki" (236,21) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
    - Büroda çalışan avukat sayısı "Bir" (171,00) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "Beş ve üzeri" (282,75) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Üç" (192,59) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "İki" (236,21) olanlara göre daha düşük olduğu tespit edilmiştir (p=,028).
    - Büroda çalışan avukat sayısı "Üç" (192,59) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "Beş ve üzeri" (282,75) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=17,328; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Bir" (196,67) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "Üç" (238,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,027).
    - Büroda çalışan personel sayısı "Bir" (196,67) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "İki" (254,43) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

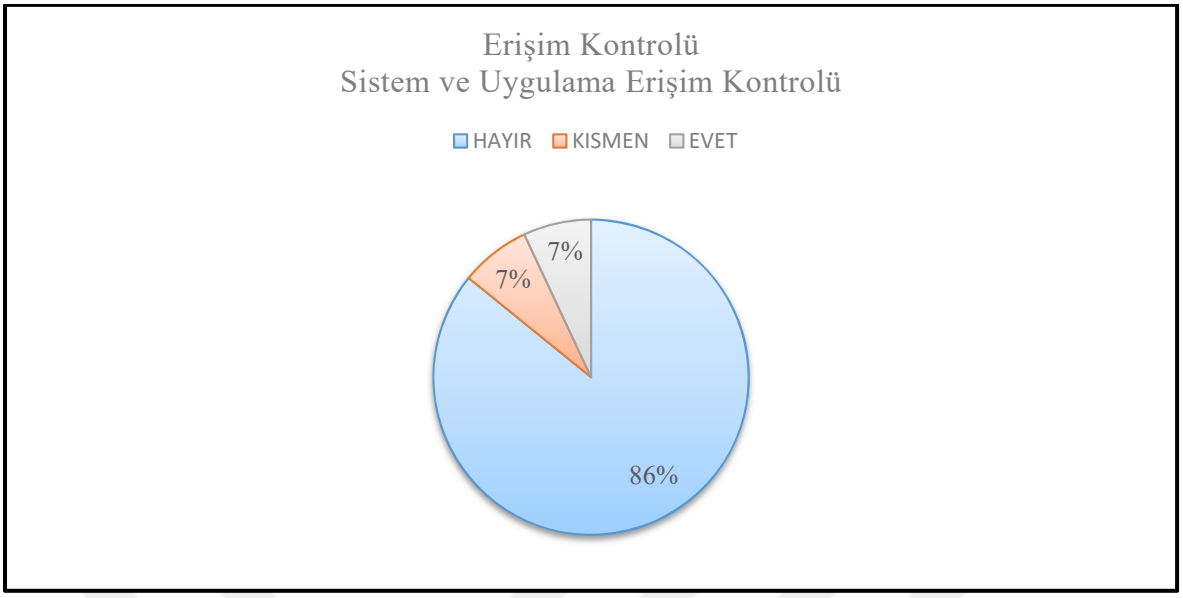
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=18,899; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "İki" (216,02) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "Üç" (294,33) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan yardımcı personel sayısı "Bir" (219,32) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "Üç" (294,33) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
    - Büroda çalışan yardımcı personel sayısı "Sıfır" (224,98) olan hukuk bürolarının Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin "Üç" (294,33) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).

Çizelge 6.14. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Kullanıcı Sorumlulukları düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=20424; p=,000), özel bir web sitesi olan (203,14) hukuk bürolarının olmayanlara (243,14) göre daha düşük olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22464; p=,031), tedarikçisi olan (216,25) hukuk bürolarının, olmayanlara (239,89) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=19584; p=,000), kablosuz bilgisayar ağı kullanan (253,70) hukuk bürolarının kullanmayanlara (208,50) göre daha yüksek olduğu tespit edilmiştir.

6.3.13. Erişim kontrolü - Sistem ve uygulama erişim kontrolü düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 7 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %7' sinin Evet, %7' sinin Kısmen ve %86' sının Hayır cevabını verdikleri görülmüştür (Şekil 6.13.).



Şekil 6.13. Erişim kontrolü - Sistem ve uygulama erişim kontrolü alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.15.' de verilmiştir.

Çizelge 6.15. Erişim kontrolü - Sistem ve uygulama erişim kontrolü düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	171,33	,02	,08	X^2=34,203 p=,000
	İki	239,28	,27	,48	
	Üç	205,28	,16	,38	
	Dört	205,88	,14	,34	
	Beş+	276,00	,31	,51	
2. Bürodaki çalışan personel sayısı?	Bir	195,17	,16	,45	X^2=25,768 P=,000
	İki	254,64	,24	,37	
	Üç	249,31	,32	,55	
	Dört+	213,95	,13	,25	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	219,74	,19	,39	X^2=2,919 p=,404
	Bir	234,50	,24	,47	
	İki	222,53	,19	,40	
	Üç	247,83	,30	,59	
4. Büroda kullanılan bilgisayar sayısı?	İki	203,74	,18	,46	X^2=21,823 p=,000
	Üç	259,87	,31	,54	
	Dört	228,10	,29	,57	
	Beş	198,31	,13	,32	
	Altı+	244,21	,21	,35	

Çizelge 6.15. (devam) Erişim kontrolü - Sistem ve uygulama erişim kontrolü düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	223,06	,21	,42	X^2=,672
	İki	232,44	,19	,38	p=,715
	Üç	228,00	,27	,57	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	226,91	,22	,42	U=25424
	Evet	226,06	,20	,44	p=,933
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	223,77	,18	,39	U=24784
	Evet	229,59	,24	,47	p=,567
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	228,84	,22	,43	U=24936
	Evet	223,94	,20	,43	p=,630
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	232,32	,24	,45	U=23280
	Evet	218,33	,17	,40	p=,174
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	243,60	,27	,47	U=21736
	Evet	213,41	,17	,39	p=,003
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	228,37	,24	,46	U=24992
	Evet	224,39	,18	,40	p=,696
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	223,54	,18	,35	U=24760
	Evet	229,02	,24	,49	p=,590
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,24	,15	,35	U=21416
	Evet	243,52	,30	,52	p=,006
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	225,86	,19	,37	U=25336
	Evet	227,20	,24	,49	p=,894
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	219,37	,18	,39	U=23952
	Evet	233,26	,24	,46	p=,172

Çizelge 6.15. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=34,203; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (171,33) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin "İki" (239,28) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
    - Büroda çalışan avukat sayısı "Bir" (171,33) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin "Beş ve üzeri" (276,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

- Büroda çalışan avukat sayısı “Üç” (205,28) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Beş ve üzeri” (276,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
- Büroda çalışan avukat sayısı “Dört” (205,88) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Beş ve üzeri” (276,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).

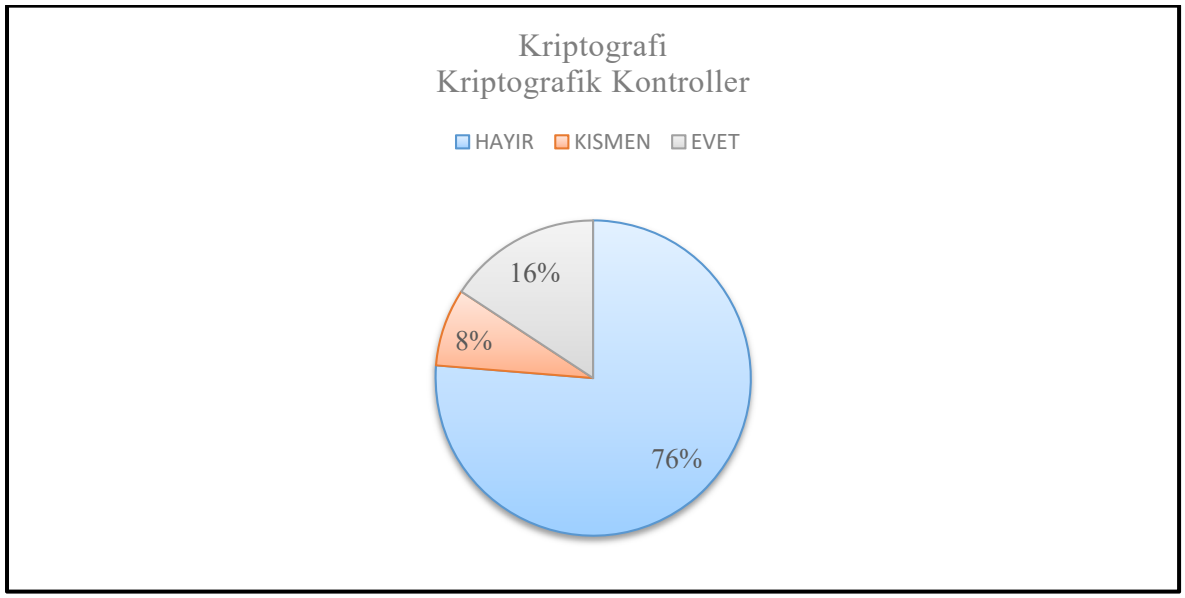
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=25,768; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan personel sayısı “Bir” (195,17) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Üç” (249,31) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “Bir” (195,17) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “İki” (254,64) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “Dört ve üzeri” (213,95) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “İki” (254,64) olanlara göre daha düşük olduğu tespit edilmiştir (p=,049).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=21,823; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Beş” (198,31) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Altı ve üzeri” (244,21) olanlara göre daha düşük olduğu tespit edilmiştir (p=,022).
  - Büroda kullanılan bilgisayar sayısı “Beş” (198,31) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Üç” (259,87) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
  - Büroda kullanılan bilgisayar sayısı “İki” (203,74) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Altı ve üzeri” (244,21) olanlara göre daha düşük olduğu tespit edilmiştir (p=,030).
  - Büroda kullanılan bilgisayar sayısı “İki” (203,74) olan hukuk bürolarının Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin “Üç” (259,87) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).

Çizelge 6.15. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü düzeyinin;

- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=21736; p=,003), tedarikçisi olan (213,41) hukuk bürolarının, olmayanlara (243,60) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21416; p=,006), kablosuz bilgisayar ağı kullanan (243,52) hukuk bürolarının kullanmayanlara (215,24) göre daha yüksek olduğu tespit edilmiştir.

6.3.14. Kriptografi - Kriptografik kontroller düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Kriptografi - Kriptografik Kontroller" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 5 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %16' sının Evet, %8' inin Kısmen ve %76' sının Hayır cevabını verdikleri görülmüştür (Şekil 6.14.).



Şekil 6.14. Kriptografi - Kriptografik kontroller alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Kriptografi - Kriptografik Kontroller düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit

edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.16.' da verilmiştir.

Çizelge 6.16. Kriptografi - Kriptografik kontroller düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	277,67	,60	,55	X^2=31,642
	İki	221,60	,36	,44	p=,000
	Üç	261,89	,55	,55	
	Dört	196,35	,28	,44	
	Beş+	176,75	,21	,46	
2. Bürodaki çalışan personel sayısı?	Bir	233,39	,41	,47	X^2=14,462
	İki	237,93	,43	,49	p=,002
	Üç	240,57	,44	,49	
	Dört+	183,41	,26	,52	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	271,07	,57	,53	X^2=29,109
	Bir	172,50	,19	,41	p=,000
	İki	220,63	,36	,44	
	Üç	255,83	,57	,64	
4. Büroda kullanılan bilgisayar sayısı?	İki	284,91	,62	,50	X^2=59,347
	Üç	258,71	,47	,36	p=,000
	Dört	163,50	,14	,33	
	Beş	188,02	,25	,43	
	Altı+	200,97	,32	,54	
5. Büroda kullanılan yazıcı sayısı?	Bir	222,03	,38	,50	X^2=,841
	İki	233,05	,39	,44	p=,657
	Üç	230,88	,44	,56	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	226,05	,40	,52	U=25416
	Evet	226,97	,39	,45	p=,935
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	235,40	,43	,51	U=23304
	Evet	216,42	,35	,46	p=,092
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	214,33	,36	,51	U=22616
	Evet	239,80	,43	,46	p=,024
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	207,98	,34	,51	U=19928
	Evet	252,50	,47	,45	p=,000
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	207,23	,30	,40	U=21312
	Evet	241,25	,47	,54	p=,003
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	243,20	,47	,53	U=21432
	Evet	207,59	,31	,41	p=,002
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	217,38	,38	,53	U=23480
	Evet	234,27	,41	,45	p=,134
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	216,24	,36	,49	U=21688
	Evet	242,01	,45	,49	p=,025
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	242,91	,43	,45	U=21616
	Evet	208,57	,35	,52	p=,002

Çizelge 6.16. (devam) Kriptografi - Kriptografik kontroller düzeyinin analizi

15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	219,48	,37	,50	U=23976
	Evet	233,16	,41	,47	p=,224

Çizelge 6.16. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Kriptografi - Kriptografik Kontroller düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=31,642; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (176,75) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Üç" (261,89) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (176,75) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Bir" (277,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Dört" (196,35) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Üç" (261,89) olanlara göre daha düşük olduğu tespit edilmiştir (p=,016).
    - Büroda çalışan avukat sayısı "Dört" (196,35) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Bir" (277,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).
    - Büroda çalışan avukat sayısı "İki" (221,60) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Bir" (277,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,036).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=14,462; p=,002), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Dört ve üzeri" (183,41) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Bir" (233,39) olanlara göre daha düşük olduğu tespit edilmiştir (p=,012).
    - Büroda çalışan personel sayısı "Dört ve üzeri" (183,41) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "İki" (237,93) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).

  - Büroda çalışan personel sayısı "Dört ve üzeri" (183,41) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Üç" (240,57) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=29,109; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan yardımcı personel sayısı "Bir" (172,50) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "İki" (220,63) olanlara göre daha düşük olduğu tespit edilmiştir (p=,019).
  - Büroda çalışan yardımcı personel sayısı "Bir" (172,50) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Üç" (255,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
  - Büroda çalışan yardımcı personel sayısı "Bir" (172,50) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Sıfır" (271,07) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan yardımcı personel sayısı "İki" (220,63) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Sıfır" (271,07) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=59,347; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı "Dört" (163,50) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Üç" (258,71) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda kullanılan bilgisayar sayısı "Dört" (163,50) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "İki" (284,91) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda kullanılan bilgisayar sayısı "Beş" (188,02) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "Üç" (258,71) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).
  - Büroda kullanılan bilgisayar sayısı "Beş" (188,02) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin "İki" (284,91) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

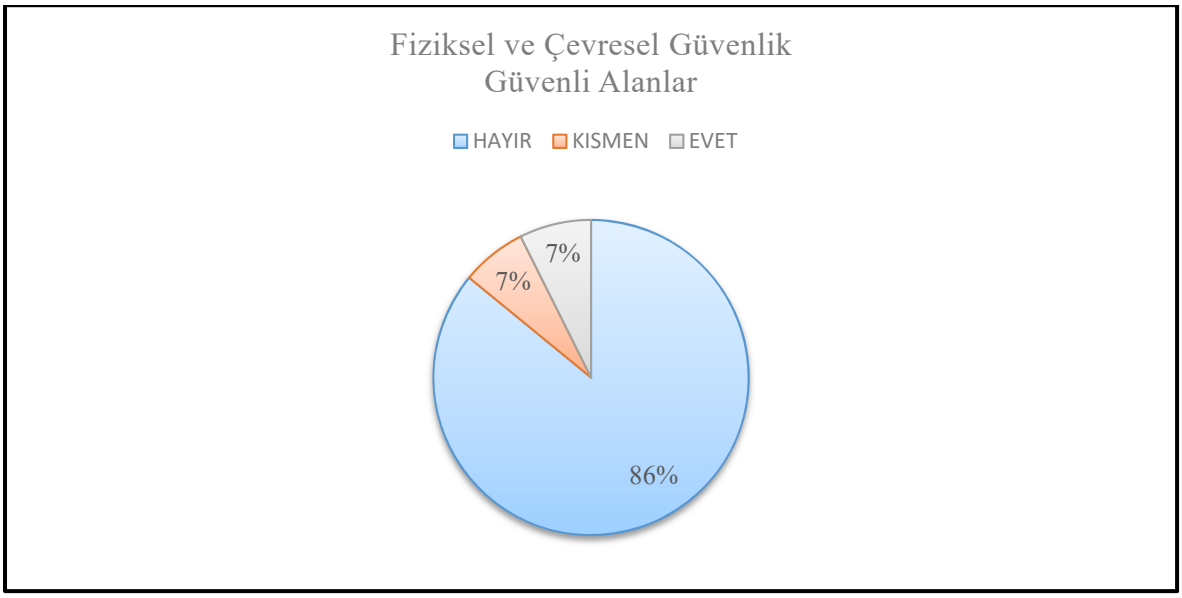
- Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (200,97) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin “Üç” (258,71) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).
- Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (200,97) olan hukuk bürolarının Kriptografi - Kriptografik Kontroller düzeyinin “İki” (284,91) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.16. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Kriptografi - Kriptografik Kontroller düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=22616; p=,024), özel bir paket programı olan (239,80) hukuk bürolarının olmayanlara (214,33) göre daha yüksek olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=19928; p=,000), özel bir web sitesi olan (252,50) hukuk bürolarının olmayanlara (207,98) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=21312; p=,003), tedarikçisi olan (241,25) hukuk bürolarının, olmayanlara (207,23) göre daha yüksek olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=21312; p=,002), danışmanlık alınan tedarikçisi olan (207,59) hukuk bürolarının olmayanlara (243,20) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21688; p=,025), kablosuz bilgisayar ağı kullanan (242,01) hukuk bürolarının kullanmayanlara (216,24) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21616; p=,002), bağlanmasına izin veren (208,57) hukuk bürolarının, vermeyenlere (242,91) göre daha düşük olduğu tespit edilmiştir.

6.3.15. Fiziksel ve çevresel güvenlik - Güvenli alanlar düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 12 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %7' sinin Evet, %7' sinin Kısmen ve %86' sının Hayır cevabını verdikleri görülmüştür (Şekil 6.15.).



Şekil 6.15. Fiziksel ve çevresel güvenlik - Güvenli alanlar alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.17.' de verilmiştir.

Çizelge 6.17. Fiziksel ve çevresel Güvenlik - güvenli alanlar düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	224,67	,21	,44	X^2=2,302
	İki	233,36	,23	,39	p=,608
	Üç	215,11	,20	,46	
	Dört	227,73	,25	,49	
	Beş+	222,25	,17	,31	

Çizelge 6.17. (devam) Fiziksel ve çevresel güvenlik - Güvenli alanlar düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	229,50	,24	,45	X^2=10,364
	İki	245,00	,30	,47	p=,016
	Üç	202,57	,11	,33	
	Dört+	227,41	,19	,32	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	234,88	,25	,46	X^2=,942
	Bir	222,97	,20	,39	p=,815
	İki	223,90	,20	,40	
	Üç	230,50	,22	,40	
4. Büroda kullanılan bilgisayar sayısı?	İki	234,22	,26	,47	X^2=4,277
	Üç	235,76	,28	,50	p=,370
	Dört	211,30	,11	,27	
	Beş	232,40	,23	,40	
	Altı+	215,56	,16	,34	
5. Büroda kullanılan yazıcı sayısı?	Bir	228,84	,22	,39	X^2=7,436
	İki	236,56	,28	,48	p=,024
	Üç	196,38	,08	,23	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	220,05	,18	,37	U=24024
	Evet	233,30	,25	,45	p=,155
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	240,17	,28	,46	U=22160
	Evet	211,03	,14	,32	p=,002
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	228,77	,23	,42	U=24952
	Evet	224,02	,20	,39	p=,610
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	234,92	,24	,41	U=22592
	Evet	214,67	,18	,41	p=,032
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	253,97	,32	,47	U=19704
	Evet	205,47	,14	,34	p=,000
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	222,10	,19	,39	U=24384
	Evet	231,48	,24	,42	p=,315
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	243,54	,27	,43	U=21832
	Evet	211,98	,17	,38	p=,001
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	219,62	,18	,37	U=22608
	Evet	236,90	,26	,46	p=,069
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	243,01	,28	,45	U=21592
	Evet	208,46	,14	,34	p=,000
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	241,15	,28	,46	U=22296
	Evet	212,60	,15	,34	p=,002

Çizelge 6.17. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar düzeyinin;

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=10,364; p=,016), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Üç" (202,57) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar düzeyinin "İki" (245,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=7,436; p=,024), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "Üç" (196,38) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar düzeyinin "İki" (236,56) olanlara göre daha düşük olduğu tespit edilmiştir (p=,023).

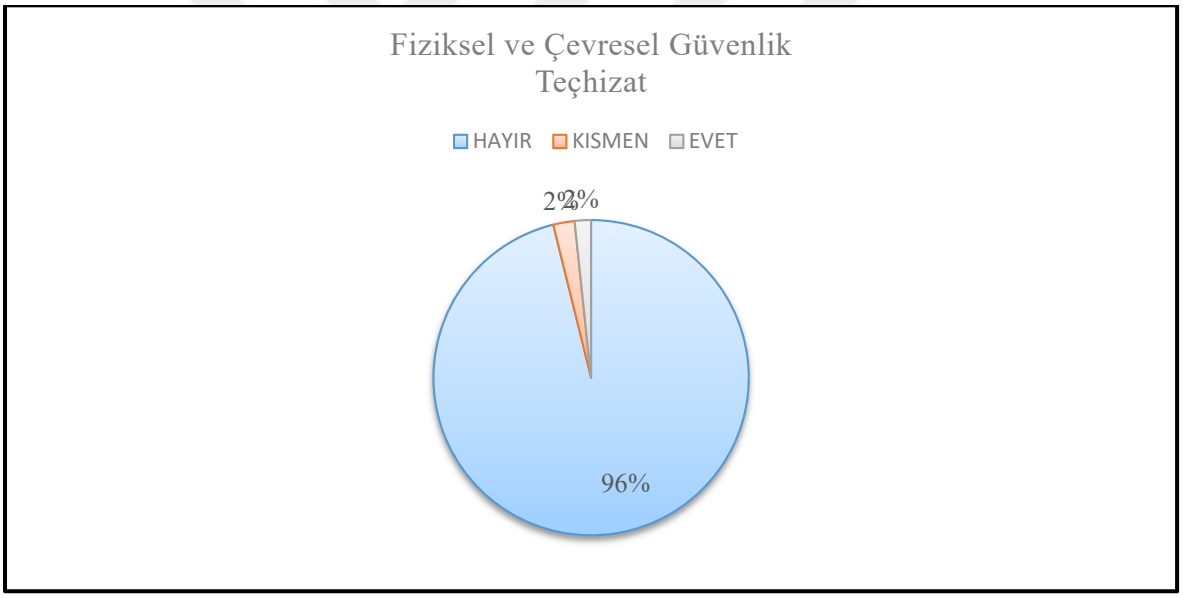
Çizelge 6.17. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22160; p=,002), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (211,03) hukuk bürolarının vermeyenlere (240,17) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=22592; p=,032), özel bir web sitesi olan (214,67) hukuk bürolarının olmayanlara (234,92) göre daha düşük olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=19704; p=,000), tedarikçisi olan (205,47) hukuk bürolarının, olmayanlara (253,97) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21832; p=,001), kablolu bilgisayar ağı kullanan (211,98) hukuk bürolarının kullanmayanlara (243,54) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21592; p=,000), bağlanmasına izin veren (208,46) hukuk bürolarının, vermeyenlere (243,01) göre daha düşük olduğu tespit edilmiştir.

- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22296; p=,002), bağlanmasına izin veren (212,60) hukuk bürolarının, vermeyenlere (241,15) göre daha düşük olduğu tespit edilmiştir.

6.3.16. Fiziksel ve çevresel güvenlik - Teçhizat düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Fiziksel ve Çevresel Güvenlik - Teçhizat" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 30 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %2' sinin Evet, %s' sinin Kısmen ve %96' sının Hayır cevabını verdikleri görülmüştür (Şekil 6.16.).



Şekil 6.16. Fiziksel ve çevresel güvenlik - Teçhizat alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.18.' de verilmiştir.

Çizelge 6.18. Fiziksel ve çevresel güvenlik - Teçhizat düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	239,83	,09	,22	X^2=20,667
	İki	233,11	,08	,26	p=,000
	Üç	238,24	,05	,12	
	Dört	200,50	,00	,00	
	Beş+	200,50	,00	,00	
2. Bürodaki çalışan personel sayısı?	Bir	226,61	,06	,18	X^2=15,712
	İki	224,93	,08	,31	p=,001
	Üç	208,87	,01	,07	
	Dört+	249,95	,07	,15	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	254,69	,15	,38	X^2=16,674
	Bir	228,03	,06	,18	p=,001
	İki	218,34	,03	,11	
	Üç	217,83	,02	,07	
4. Büroda kullanılan bilgisayar sayısı?	İki	248,16	,13	,33	X^2=22,389
	Üç	213,24	,04	,15	p=,000
	Dört	200,50	,00	,00	
	Beş	211,83	,03	,12	
	Altı+	232,15	,04	,11	
5. Büroda kullanılan yazıcı sayısı?	Bir	232,31	,07	,24	X^2=9,961
	İki	227,83	,05	,15	p=,007
	Üç	200,50	,00	,00	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	223,29	,04	,12	U=24776
	Evet	229,88	,08	,25	p=,333
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	221,90	,03	,09	U=24336
	Evet	231,71	,09	,27	p=,150
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	230,77	,05	,14	U=24480
	Evet	221,83	,06	,24	p=,190
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	225,26	,06	,23	U=24488
	Evet	228,24	,04	,13	p=,665
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	220,17	,07	,27	U=23848
	Evet	231,34	,05	,12	p=,104
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	230,47	,07	,24	U=24488
	Evet	222,01	,04	,14	p=,215
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	235,08	,08	,25	U=23592
	Evet	219,19	,04	,13	p=,020
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	227,03	,05	,14	U=24336
	Evet	225,70	,07	,26	p=,848
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	231,75	,08	,26	U=24248
	Evet	220,76	,03	,09	p=,107
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	229,63	,07	,25	U=24832
	Evet	223,53	,04	,12	p=,371

Çizelge 6.18. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=20,667; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Dört" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "İki" (233,11) olanlara göre daha düşük olduğu tespit edilmiştir (p=,039).
    - Büroda çalışan avukat sayısı "Dört" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Üç" (238,24) olanlara göre daha düşük olduğu tespit edilmiştir (p=,026).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "İki" (233,11) olanlara göre daha düşük olduğu tespit edilmiştir (p=,017).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Üç" (238,24) olanlara göre daha düşük olduğu tespit edilmiştir (p=,014).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Bir" (239,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,044).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=15,712; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Üç" (208,87) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Dört ve üzeri" (249,95) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=16,674; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Üç" (217,83) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Sıfır" (254,69) olanlara göre daha düşük olduğu tespit edilmiştir (p=,029).

- Büroda çalışan yardımcı personel sayısı "İki" (218,34) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Sıfır" (254,69) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

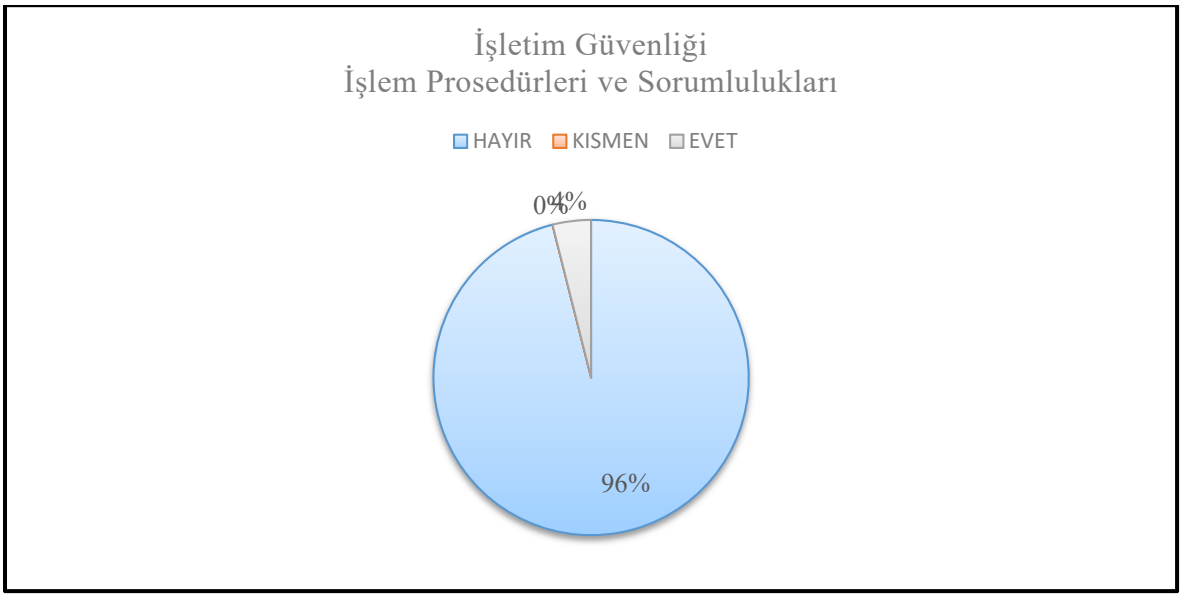
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=22,389; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı "Dört" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "İki" (248,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
  - Büroda kullanılan bilgisayar sayısı "Beş" (211,83) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "İki" (248,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
  - Büroda kullanılan bilgisayar sayısı "Üç" (213,24) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "İki" (248,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,011).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=9,961; p=,007), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan yazıcı sayısı "Üç" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "İki" (277,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,039).
  - Büroda kullanılan yazıcı sayısı "Üç" (200,50) olan hukuk bürolarının Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin "Bir" (232,31) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).

Çizelge 6.18. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Fiziksel ve Çevresel Güvenlik - Teçhizat düzeyinin;

- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23592; p=,020), kablolu bilgisayar ağı kullanan (219,19) hukuk bürolarının kullanmayanlara (235,08) göre daha düşük olduğu tespit edilmiştir.

6.3.17. İşlem güvenliği - İşlem prosedürleri ve sorumlulukları düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 9 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %4' ünün Evet, %0' ının Kısmen ve %96' sının Hayır cevabını verdikleri görülmüştür (Şekil 6.17.).



Şekil 6.17. İşlem güvenliği - İşlem prosedürleri ve sorumlulukları alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.19.' da verilmiştir.

Çizelge 6.19. İşlem güvenliği - İşlem prosedürleri ve sorumlulukları düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	206,50	,00	,00	X^2=20,531
	İki	220,34	,05	,22	p=,000
	Üç	226,15	,08	,26	
	Dört	258,65	,21	,39	
	Beş+	234,75	,11	,30	

Çizelge 6.19. (devam) İşlem güvenliği - İşlem prosedürleri ve sorumlulukları düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	231,61	,10	,28	X^2=4,937
	İki	230,71	,10	,28	p=,176
	Üç	214,87	,03	,17	
	Dört+	227,05	,08	,26	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	217,26	,04	,19	X^2=2,608
	Bir	233,09	,10	,30	p=,456
	İki	228,02	,08	,26	
	Üç	225,33	,07	,26	
4. Büroda kullanılan bilgisayar sayısı?	İki	222,09	,06	,23	X^2=12,475
	Üç	206,50	,00	,00	p=,014
	Dört	229,10	,09	,28	
	Beş	238,79	,13	,32	
	Altı+	233,09	,10	,29	
5. Büroda kullanılan yazıcı sayısı?	Bir	224,16	,07	,24	X^2=1,405
	İki	227,05	,08	,26	p=,495
	Üç	234,75	,11	,30	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	222,09	,06	,23	U=24496
	Evet	231,15	,10	,28	p=,134
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	225,33	,07	,25	U=25160
	Evet	227,82	,08	,26	p=,681
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	233,31	,11	,29	U=23880
	Evet	219,06	,05	,21	p=,018
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	227,05	,08	,26	U=24672
	Evet	225,73	,08	,25	p=,831
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	229,56	,09	,27	U=24488
	Evet	224,16	,07	,24	p=,375
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	232,87	,10	,29	U=23912
	Evet	219,29	,05	,21	p=,025
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	241,27	,14	,32	U=22304
	Evet	213,91	,03	,16	p=,000
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	223,12	,07	,23	U=23560
	Evet	231,61	,10	,28	p=,169
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	225,65	,08	,25	U=25288
	Evet	227,43	,08	,26	p=,769
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	235,26	,11	,30	U=23592
	Evet	218,19	,05	,20	p=,005

Çizelge 6.19. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=20,531; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (206,50) olan hukuk bürolarının İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin "Dört" (258,65) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
    - Büroda çalışan avukat sayısı "İki" (220,34) olan hukuk bürolarının İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin "Dört" (258,65) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
    - Büroda çalışan avukat sayısı "Üç" (226,15) olan hukuk bürolarının İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin "Dört" (258,65) olanlara göre daha düşük olduğu tespit edilmiştir (p=,036).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=12,475; p=,014), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Üç" (206,50) olan hukuk bürolarının İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin "Altı ve üzeri" (233,09) olanlara göre daha düşük olduğu tespit edilmiştir (p=,039).
    - Büroda kullanılan bilgisayar sayısı "Üç" (206,50) olan hukuk bürolarının İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin "Beş" (238,79) olanlara göre daha düşük olduğu tespit edilmiştir (p=,015).

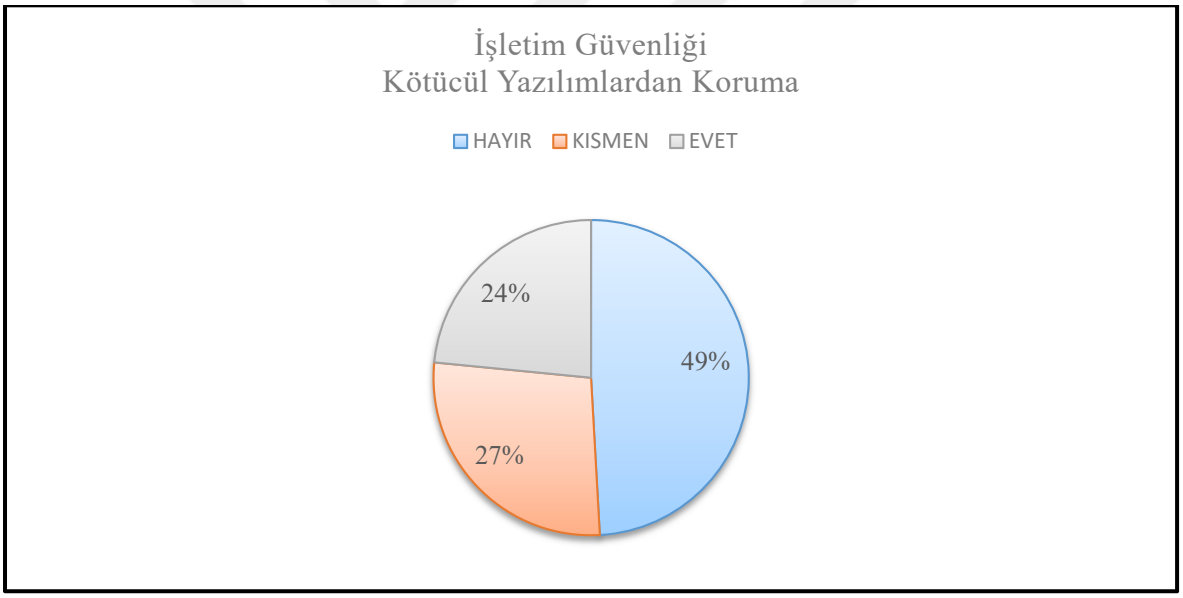
Çizelge 6.19. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - İşlem Prosedürleri ve Sorumlulukları düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=23880; p=,018), özel bir paket programı olan (219,06) hukuk bürolarının olmayanlara (233,31) göre daha düşük olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=23912; p=,025), danışmanlık alınan tedarikçisi olan (219,29) hukuk bürolarının olmayanlara (232,87) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22304; p=,000), kablolu bilgisayar ağı kullanan (213,91) hukuk bürolarının kullanmayanlara (241,27) göre daha düşük olduğu tespit edilmiştir.

- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23592; p=,005), bağlanmasına izin veren (218,19) hukuk bürolarının, vermeyenlere (235,26) göre daha düşük olduğu tespit edilmiştir.

6.3.18. İşlem güvenliği - Kötücül yazılımlardan koruma düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşlem Güvenliği - Kötücül Yazılımlardan Korunma" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 2 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %24' ünün Evet, %27' sinin Kısmen ve %49' unun Hayır cevabını verdikleri görülmüştür (Şekil 6.18.).



Şekil 6.18. İşlem güvenliği - Kötücül yazılımlardan korunma alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - Kötücül Yazılımlardan Koruma düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.20.' de verilmiştir.

Çizelge 6.20. İşlem güvenliği - Kötücül yazılımlardan koruma düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	239,67	,83	,83	X^2=10,968
	İki	235,52	,80	,76	p=,027
	Üç	216,50	,70	,82	
	Dört	247,58	,85	,69	
	Beş+	186,25	,50	,73	
2. Bürodaki çalışan personel sayısı?	Bir	224,28	,72	,74	X^2=1,299
	İki	222,43	,75	,89	p=,729
	Üç	237,91	,81	,79	
	Dört+	221,32	,68	,65	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	244,69	,86	,79	X^2=7,991
	Bir	242,62	,88	,93	p=,046
	İki	223,29	,71	,73	
	Üç	188,67	,50	,67	
4. Büroda kullanılan bilgisayar sayısı?	İki	245,40	,86	,79	X^2=6,709
	Üç	211,76	,68	,89	p=,152
	Dört	205,90	,60	,70	
	Beş	212,40	,62	,59	
	Altı+	233,38	,79	,81	
5. Büroda kullanılan yazıcı sayısı?	Bir	217,53	,67	,69	X^2=10,264
	İki	254,14	,94	,86	p=,006
	Üç	205,38	,63	,81	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	212,74	,66	,74	U=22328
	Evet	241,01	,84	,79	p=,013
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	239,53	,82	,75	U=22312
	Evet	211,75	,66	,78	p=,015
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	221,11	,69	,70	U=24216
	Evet	232,39	,80	,83	p=,322
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	236,35	,80	,77	U=22216
	Evet	212,67	,66	,76	P=,040
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	218,13	,69	,77	U=23448
	Evet	232,91	,78	,77	p=,198
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	216,23	,68	,77	U=22976
	Evet	238,12	,81	,76	p=,055
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	223,08	,71	,72	U=24664
	Evet	229,42	,77	,80	p=,578
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	219,88	,71	,77	U=22680
	Evet	236,50	,80	,76	p=,152
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	239,89	,83	,79	U=22328
	Evet	211,87	,65	,73	p=,014
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	216,50	,67	,72	U=23320
	Evet	235,98	,81	,80	p=,087

Çizelge 6.20. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=10,968; p=,027), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (186,25) olan hukuk bürolarının İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin "İki" (235,52) olanlara göre daha düşük olduğu tespit edilmiştir (p=,046).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=7,991; p=,046), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Üç" (188,67) olan hukuk bürolarının İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin "Bir" (242,62) olanlara göre daha düşük olduğu tespit edilmiştir (p=,018).
    - Büroda çalışan yardımcı personel sayısı "Üç" (188,67) olan hukuk bürolarının İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin "Sıfır" (244,69) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=10,264; p=,006), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "Üç" (205,38) olan hukuk bürolarının İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin "İki" (254,14) olanlara göre daha düşük olduğu tespit edilmiştir (p=,024).
    - Büroda kullanılan yazıcı sayısı "Bir" (217,53) olan hukuk bürolarının İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin "İki" (254,14) olanlara göre daha düşük olduğu tespit edilmiştir (p=,014).

Çizelge 6.20. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Kötücül Yazılımlardan Korunma düzeyinin;

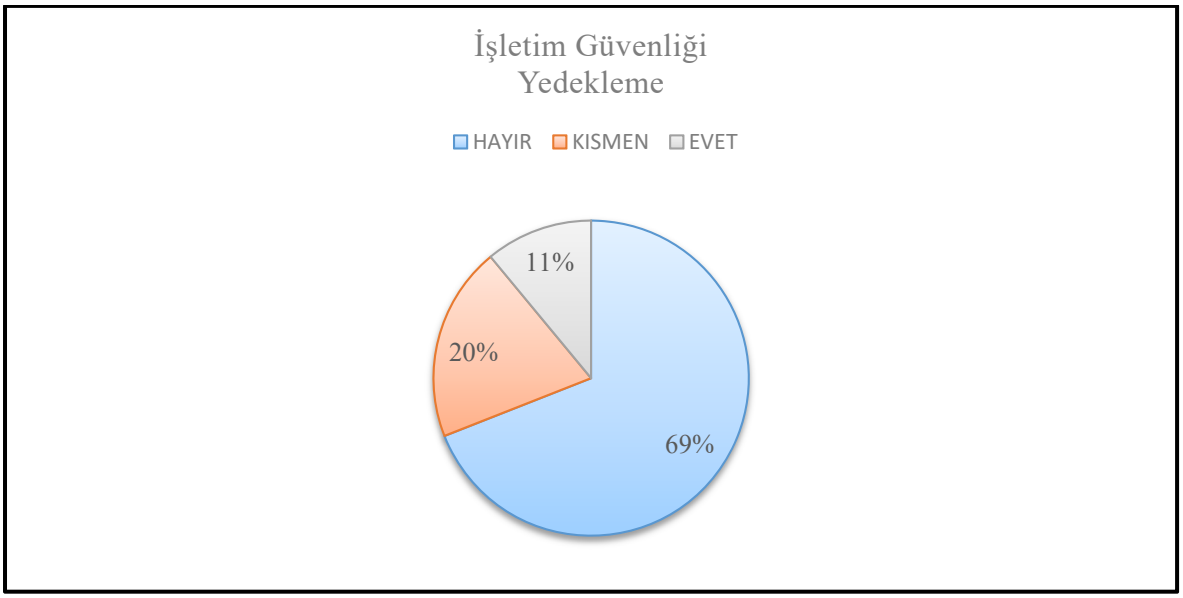
- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22328; p=,013), bilgisayar ağında mobil cihazlar kullanan (241,01)

hukuk bürolarının kullanmayanlara (212,74) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22312; p=,015), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (211,75) hukuk bürolarının vermeyenlere (239,53) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=22216; p=,040), özel bir web sitesi olan (212,67) hukuk bürolarının olmayanlara (236,35) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22328; p=,014), bağlanmasına izin veren (211,87) hukuk bürolarının, vermeyenlere (239,89) göre daha düşük olduğu tespit edilmiştir.

6.3.19. İşlem güvenliği - Yedekleme düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşlem Güvenliği - Yedekleme" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 7 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %11' inin Evet, %20' sinin Kısmen ve %69' unun Hayır cevabını verdikleri görülmüştür (Şekil 6.19.).



Şekil 6.19. İşlem güvenliği - Yedekleme alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - Yedekleme düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.21.' de verilmiştir.

Çizelge 6.21. İşlem güvenliği - Yedekleme düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	222,50	,40	,59	X^2=44,604
	İki	231,15	,44	,56	p=,000
	Üç	196,67	,32	,52	
	Dört	318,35	,84	,63	
	Beş+	183,50	,17	,29	
2. Bürodaki çalışan personel sayısı?	Bir	227,39	,44	,61	X^2=,225
	İki	228,57	,48	,68	p=,974
	Üç	227,54	,35	,39	
	Dört+	221,14	,38	,47	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	240,79	,51	,64	X^2=1,579
	Bir	221,79	,39	,57	p=,664
	İki	224,56	,40	,52	
	Üç	218,33	,39	,60	
4. Büroda kullanılan bilgisayar sayısı?	İki	217,60	,41	,63	X^2=8,450
	Üç	207,66	,32	,45	p=,076
	Dört	226,10	,41	,55	
	Beş	258,40	,58	,61	
	Altı+	225,03	,39	,51	
5. Büroda kullanılan yazıcı sayısı?	Bir	232,94	,45	,58	X^2=10,035
	İki	235,35	,47	,59	p=,007
	Üç	182,50	,19	,29	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	216,12	,37	,52	U=23112
	Evet	237,45	,47	,59	p=,059
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	231,83	,45	,58	U=24160
	Evet	220,46	,38	,52	p=,315
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	222,06	,40	,56	U=24440
	Evet	231,35	,44	,56	p=,411
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	226,74	,43	,58	U=24752
	Evet	226,16	,41	,51	p=,959
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	241,19	,52	,63	U=22208
	Evet	215,25	,34	,47	p=,023
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	195,30	,31	,55	U=17952
	Evet	261,82	,55	,53	p=,000
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	233,46	,48	,63	U=23928
	Evet	220,57	,37	,48	p=,255

Çizelge 6.21. (devam) İşlem güvenliği - Yedekleme düzeyinin analizi

13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	213,85	,36	,52	U=21040
	Evet	245,61	,51	,59	p=,006
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	239,89	,49	,59	U=22328
	Evet	211,87	,34	,50	p=,013
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	232,72	,46	,61	U=24152
	Evet	220,60	,38	,50	p=,284

Çizelge 6.21. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Yedekleme düzeyinin;

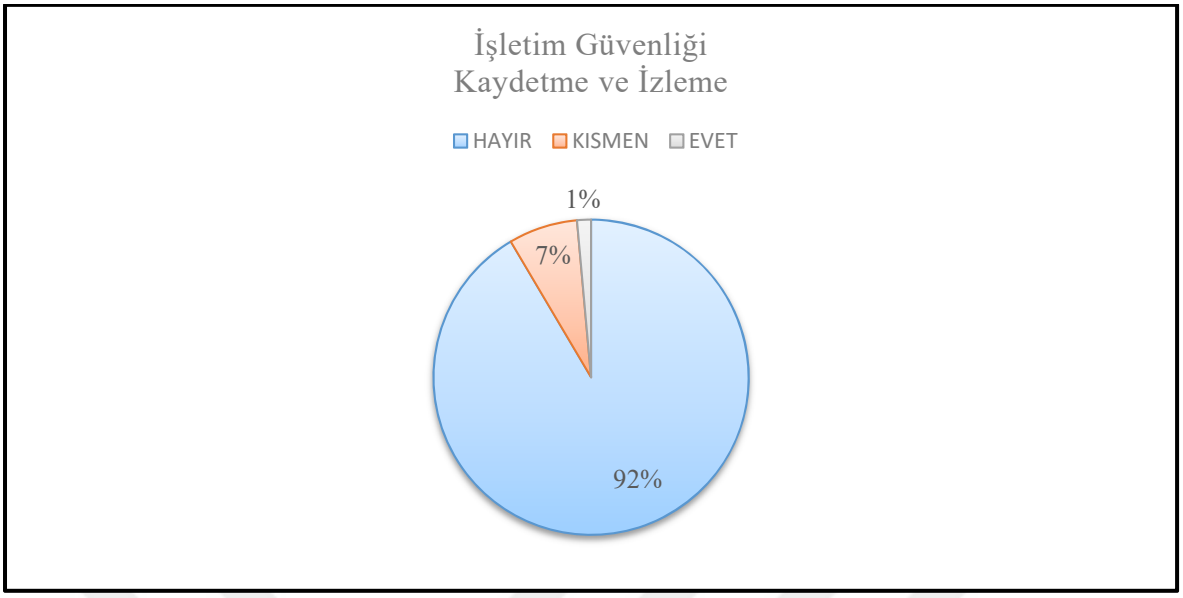
- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=44,604; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (183,50) olan hukuk bürolarının İşlem Güvenliği - Yedekleme düzeyinin "Dört" (318,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Üç" (196,67) olan hukuk bürolarının İşlem Güvenliği - Yedekleme düzeyinin "Dört" (318,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Bir" (222,50) olan hukuk bürolarının İşlem Güvenliği - Yedekleme düzeyinin "Dört" (318,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
    - Büroda çalışan avukat sayısı "İki" (231,15) olan hukuk bürolarının İşlem Güvenliği - Yedekleme düzeyinin "Dört" (318,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=10,035; p=,007), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "Üç" (182,50) olan hukuk bürolarının İşlem Güvenliği - Yedekleme düzeyinin "Bir" (232,94) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).
    - Büroda kullanılan yazıcı sayısı "Üç" (182,50) olan hukuk bürolarının İşlem Güvenliği - Yedekleme düzeyinin "İki" (235,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,012).

Çizelge 6.21. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Yedekleme düzeyinin;

- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22208; p=,023), tedarikçisi olan (215,25) hukuk bürolarının, olmayanlara (241,19) göre daha düşük olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=17952; p=,000), danışmanlık alınan tedarikçisi olan (261,82) hukuk bürolarının olmayanlara (195,30) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21040; p=,006), kablosuz bilgisayar ağı kullanan (245,61) hukuk bürolarının kullanmayanlara (213,85) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22328; p=,013), bağlanmasına izin veren (211,87) hukuk bürolarının, vermeyenlere (239,89) göre daha düşük olduğu tespit edilmiştir.

6.3.20. İşlem güvenliği - Kaydetme ve izleme düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre “İşlem Güvenliği - Kaydetme ve Yedekleme” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 13 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %1’ inin Evet, %7’ sinin Kısmen ve %92’ sinin Hayır cevabını verdikleri görülmüştür (Şekil 6.20.).



Şekil 6.20. İşlem güvenliği - kaydetme ve izleme alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - Kaydetme ve İzleme düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.22.' de verilmiştir.

Çizelge 6.22. İşlem güvenliği - Kaydetme ve izleme düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	206,33	,08	,20	X^2=15,225
	İki	220,17	,09	,17	p=,004
	Üç	224,50	,10	,19	
	Dört	277,42	,20	,24	
	Beş+	222,50	,06	,10	
2. Bürodaki çalışan personel sayısı?	Bir	214,72	,09	,18	X^2=9,523
	İki	225,86	,10	,17	p=,023
	Üç	252,13	,13	,18	
	Dört+	215,14	,09	,18	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	228,98	,11	,19	X^2=4,571
	Bir	211,21	,06	,13	p=,206
	İki	224,88	,10	,18	
	Üç	252,33	,13	,19	
4. Büroda kullanılan bilgisayar sayısı?	İki	210,64	,08	,17	X^2=8,334
	Üç	229,97	,09	,17	p=,080
	Dört	200,30	,04	,08	
	Beş	240,69	,13	,21	
	Altı+	237,03	,12	,19	

Çizelge 6.22. (devam) İşlem güvenliği - Kaydetme ve izleme düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	226,63	,10	,18	X^2=,112
	İki	224,62	,10	,18	p=,946
	Üç	229,88	,10	,17	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	230,26	,11	,19	U=24648
	Evet	222,54	,09	,17	p=,429
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	222,77	,09	,18	U=24544
	Evet	230,73	,11	,18	p=,415
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	223,28	,10	,17	U=24728
	Evet	230,02	,10	,18	p=,490
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	208,86	,07	,15	U=20160
	Evet	251,27	,14	,20	p=,000
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	217,15	,08	,17	U=23256
	Evet	233,66	,11	,19	p=,093
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	215,20	,08	,17	U=22728
	Evet	239,29	,12	,19	p=,014
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	214,81	,08	,17	U=22944
	Evet	236,47	,11	,18	p=,027
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,62	,08	,16	U=21520
	Evet	242,94	,13	,19	p=,006
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	229,11	,11	,19	U=24872
	Evet	223,65	,09	,17	p=,576
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	224,61	,10	,18	U=25104
	Evet	228,29	,10	,18	p=,706

Çizelge 6.22. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Kaydetme ve İzleme düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=15,225; p=,004), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (206,33) olan hukuk bürolarının İşlem Güvenliği - Kaydetme ve İzleme düzeyinin "Dört" (277,42) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
    - Büroda çalışan avukat sayısı "İki" (220,17) olan hukuk bürolarının İşlem Güvenliği - Kaydetme ve İzleme düzeyinin "Dört" (277,42) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (222,50) olan hukuk bürolarının İşlem Güvenliği - Kaydetme ve İzleme düzeyinin "Dört" (277,42) olanlara göre daha düşük olduğu tespit edilmiştir (p=,045).

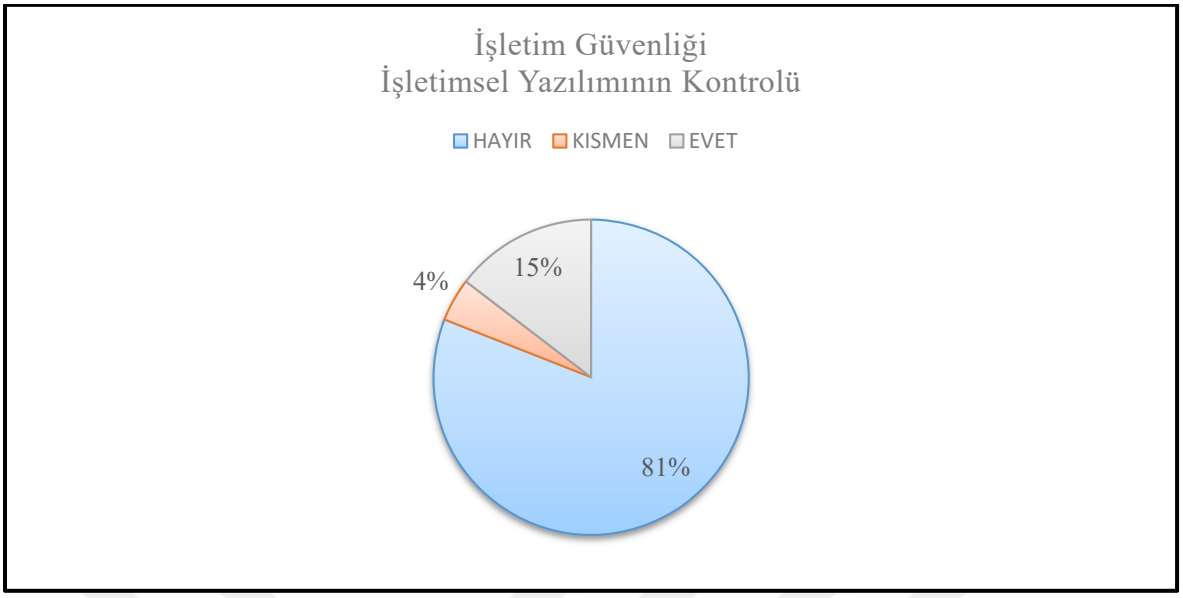
  - Büroda çalışan avukat sayısı “Üç” (224,50) olan hukuk bürolarının İşlem Güvenliği - Kaydetme ve İzleme düzeyinin “Dört” (277,42) olanlara göre daha düşük olduğu tespit edilmiştir (p=,033).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=9,523; p=,023), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan personel sayısı “Bir” (214,72) olan hukuk bürolarının İşlem Güvenliği - Kaydetme ve İzleme düzeyinin “Üç” (252,13) olanlara göre daha düşük olduğu tespit edilmiştir (p=,028).

Çizelge 6.22. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Kaydetme ve İzleme düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=20160; p=,000), özel bir web sitesi olan (251,27) hukuk bürolarının olmayanlara (208,86) göre daha yüksek olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22728; p=,014), danışmanlık alınan tedarikçisi olan (239,29) hukuk bürolarının olmayanlara (215,20) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22944; p=,027), kablolu bilgisayar ağı kullanan (236,47) hukuk bürolarının kullanmayanlara (214,81) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21520; p=,006), kablosuz bilgisayar ağı kullanan (242,94) hukuk bürolarının kullanmayanlara (215,62) göre daha yüksek olduğu tespit edilmiştir.

6.3.21. İşlem güvenliği - İşletimsel yazılımının kontrolü düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre “İşlem Güvenliği - İşletimsel Yazılımının Kontrolü” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 2 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %15’ inin Evet, %4’ ünün Kısmen ve %81’ inin Hayır cevabını verdikleri görülmüştür (Şekil 6.21.).



Şekil 6.21. İşlem güvenliği - İşletimsel yazılımının kontrolü alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.23.' te verilmiştir.

Çizelge 6.23. İşlem güvenliği - İşletimsel yazılımının kontrolü düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	215,50	,25	,62	X^2=11,591 p=,021
	İki	221,72	,33	,72	
	Üç	234,33	,35	,65	
	Dört	262,04	,54	,78	
	Beş+	209,25	,25	,68	
2. Bürodaki çalışan personel sayısı?	Bir	233,33	,36	,68	X^2=19,124 p=,000
	İki	245,36	,50	,84	
	Üç	227,83	,33	,68	
	Dört+	189,68	,09	,43	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	232,50	,38	,74	X^2=4,470 p=,215
	Bir	245,21	,47	,80	
	İki	221,55	,30	,66	
	Üç	215,50	,25	,62	
4. Büroda kullanılan bilgisayar sayısı?	İki	236,22	,45	,83	X^2=7,910 p=,095
	Üç	209,76	,16	,37	
	Dört	203,10	,20	,63	
	Beş	239,64	,38	,67	
	Altı+	226,32	,35	,73	

Çizelge 6.23. (devam) İşlem güvenliği - İşletimsel yazılımının kontrolü düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	227,81	,34	,70	X^2=,533
	İki	227,77	,36	,74	p=,766
	Üç	218,63	,25	,58	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	225,26	,33	,69	U=25232
	Evet	227,81	,35	,70	p=,771
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	230,30	,35	,68	U=24528
	Evet	222,20	,32	,70	p=,356
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	224,47	,32	,68	U=25008
	Evet	228,72	,35	,70	p=,628
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	236,77	,41	,74	U=22104
	Evet	212,07	,23	,60	p=,005
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	235,81	,43	,79	U=23264
	Evet	219,38	,27	,60	p=,063
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	236,80	,43	,79	U=22968
	Evet	214,84	,23	,54	p=,012
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	232,50	,40	,77	U=24128
	Evet	221,39	,28	,61	p=,206
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	216,97	,25	,58	U=21888
	Evet	240,90	,47	,81	p=,008
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	232,81	,39	,74	U=24000
	Evet	219,61	,28	,63	p=,133
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	231,41	,36	,70	U=24440
	Evet	221,84	,31	,68	p=,275

Çizelge 6.23. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=11,591; p=,021), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (209,25) olan hukuk bürolarının İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin "Dört" (262,04) olanlara göre daha düşük olduğu tespit edilmiştir (p=,024).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=19,124; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Dört ve üzeri" (189,68) olan hukuk bürolarının İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin "Üç" (227,83) olanlara göre daha düşük olduğu tespit edilmiştir (p=,026).

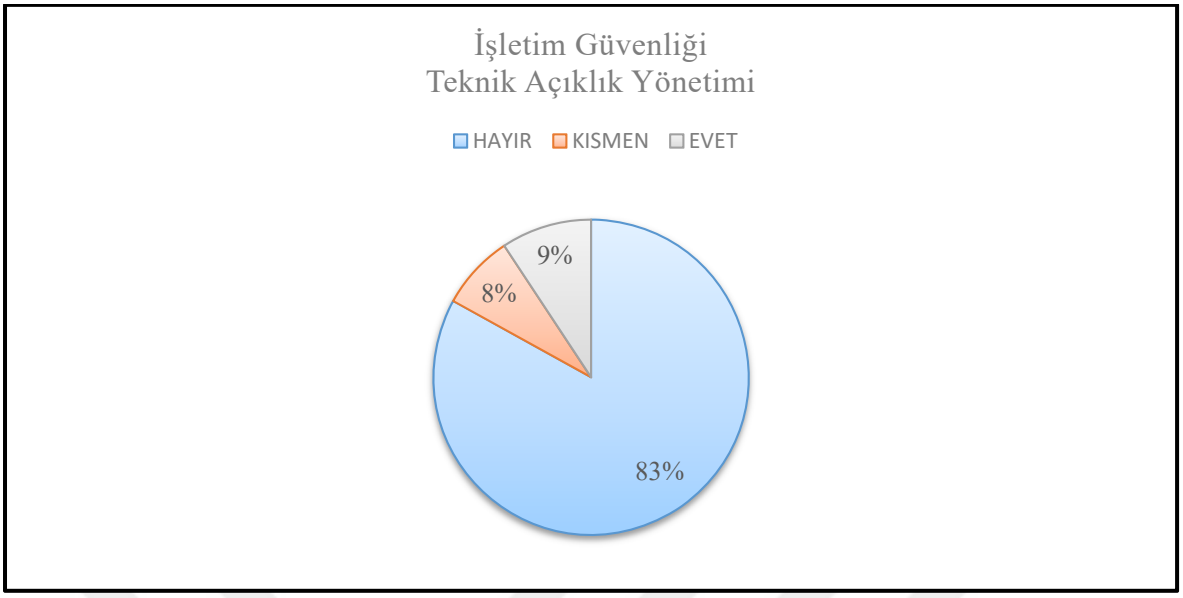
- Büroda çalışan personel sayısı “Dört ve üzeri” (189,68) olan hukuk bürolarının İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin “Bir” (233,33) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
- Büroda çalışan personel sayısı “Dört ve üzeri” (189,68) olan hukuk bürolarının İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin “İki” (245,36) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.23. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - İşletimsel Yazılımının Kontrolü düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=22104; p=,005), özel bir web sitesi olan (212,07) hukuk bürolarının olmayanlara (236,77) göre daha düşük olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22968; p=,012), danışmanlık alınan tedarikçisi olan (214,84) hukuk bürolarının olmayanlara (236,80) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21888; p=,008), kablosuz bilgisayar ağı kullanan (240,90) hukuk bürolarının kullanmayanlara (216,97) göre daha yüksek olduğu tespit edilmiştir.

6.3.22. İşlem güvenliği - Teknik açıklık yönetimi düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre “İşlem Güvenliği - Teknik Açıklık Yönetimi” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 6 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %9’ unun Evet, %8’ inin Kısmen ve %83’ inin Hayır cevabını verdikleri görülmüştür (Şekil 6.22.).



Şekil 6.22. İşlem güvenliği - Teknik açıklık yönetimi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - Teknik Açıklık Yönetimi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.24.' te verilmiştir.

Çizelge 6.24. İşlem güvenliği - Teknik açıklık yönetimi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	240,17	,36	,66	X^2=9,512 p=,050
	İki	227,60	,23	,43	
	Üç	212,50	,22	,50	
	Dört	258,04	,46	,67	
	Beş+	207,38	,19	,42	
2. Bürodaki çalışan personel sayısı?	Bir	240,39	,36	,63	X^2=3,844 p=,279
	İki	220,29	,23	,43	
	Üç	218,28	,22	,48	
	Dört+	221,77	,20	,36	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	236,69	,30	,55	X^2=6,106 p=,107
	Bir	206,15	,20	,46	
	İki	232,47	,27	,48	
	Üç	206,17	,25	,62	
4. Büroda kullanılan bilgisayar sayısı?	İki	237,81	,29	,50	X^2=12,457 p=,014
	Üç	207,55	,16	,37	
	Dört	227,10	,28	,63	
	Beş	252,98	,42	,65	
	Altı+	210,91	,20	,41	

Çizelge 6.24. (devam) İşlem güvenliği - Teknik açıklık yönetimi düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	221,13	,27	,55	X^2=4,219
	İki	241,89	,29	,46	p=,121
	Üç	216,25	,19	,38	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	220,78	,28	,59	U=24192
	Evet	232,54	,24	,40	p=,228
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	228,50	,26	,49	U=24960
	Evet	224,24	,27	,51	p=,663
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	223,31	,26	,53	U=24736
	Evet	229,98	,27	,47	p=,495
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	239,05	,32	,54	U=21504
	Evet	208,88	,18	,42	p=,002
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	254,26	,38	,59	U=19648
	Evet	205,25	,17	,40	p=,000
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	222,77	,26	,52	U=24544
	Evet	230,73	,27	,49	p=,416
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	240,15	,36	,62	U=22536
	Evet	214,86	,18	,35	p=,010
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	226,82	,28	,53	U=24392
	Evet	226,01	,24	,45	p=,935
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	239,18	,32	,56	U=22496
	Evet	212,65	,20	,42	p=,007
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	246,75	,32	,51	U=21064
	Evet	207,29	,20	,49	p=,000

Çizelge 6.24. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Teknik Açıklık Yönetimi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=9,512; p=,050), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (207,38) olan hukuk bürolarının İşlem Güvenliği - Teknik Açıklık Yönetimi düzeyinin "Dört" (258,04) olanlara göre daha düşük olduğu tespit edilmiştir (p=,009).
    - Büroda çalışan avukat sayısı "Üç" (212,50) olan hukuk bürolarının İşlem Güvenliği - Teknik Açıklık Yönetimi düzeyinin "Dört" (258,04) olanlara göre daha düşük olduğu tespit edilmiştir (p=,011).

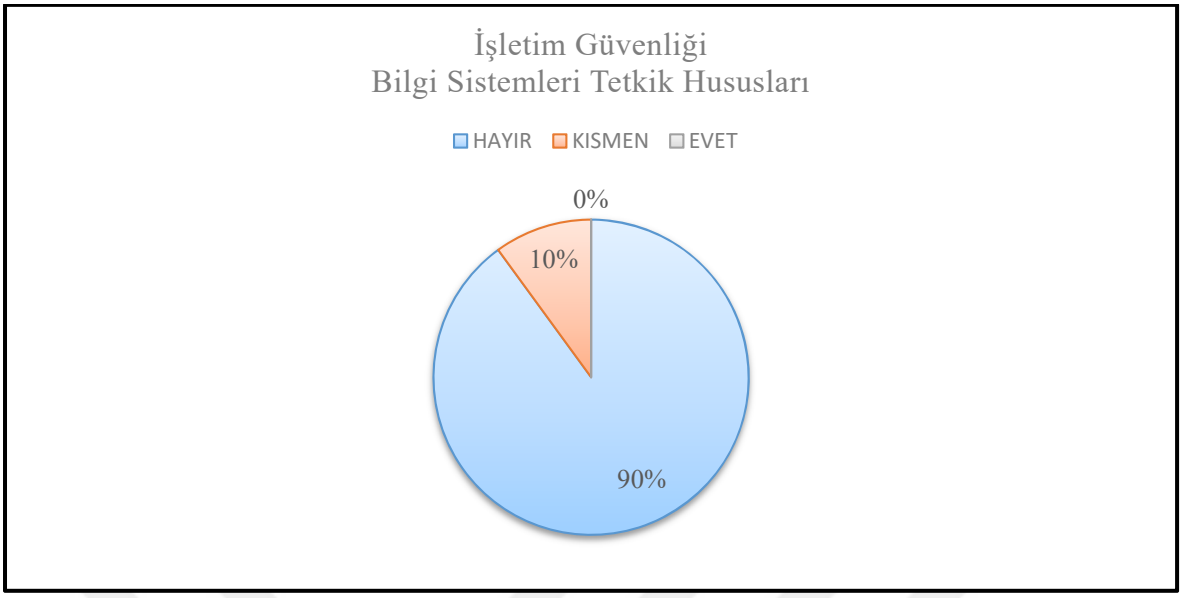
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=12,457; p=,014), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (210,91) olan hukuk bürolarının İşlem Güvenliği - Teknik Açıklık Yönetimi düzeyinin "Beş" (252,98) olanlara göre daha düşük olduğu tespit edilmiştir (p=,035).

Çizelge 6.24. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Teknik Açıklık Yönetimi düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=21504; p=,002), özel bir web sitesi olan (208,88) hukuk bürolarının olmayanlara (239,05) göre daha düşük olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=19648; p=,000), tedarikçisi olan (205,25) hukuk bürolarının, olmayanlara (254,26) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22496; p=,007), bağlanmasına izin veren (212,65) hukuk bürolarının, vermeyenlere (239,18) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21064; p=,000), bağlanmasına izin veren (207,29) hukuk bürolarının, vermeyenlere (246,75) göre daha düşük olduğu tespit edilmiştir.

6.3.23. İşlem güvenliği - Bilgi sistemleri tetkik hususları düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 3 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %0' ının Evet, %10' unun Kısmen ve %90' ının Hayır cevabını verdikleri görülmüştür (Şekil 6.23.).



Şekil 6.23. İşlem güvenliği - Bilgi sistemleri tetkik hususları alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.25.' de verilmiştir.

Çizelge 6.25. İşlem güvenliği - Bilgi sistemleri tetkik hususları düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	250,00	,22	,41	X^2=7,793 p=,099
	İki	216,30	,07	,23	
	Üç	235,63	,10	,23	
	Dört	222,50	,08	,20	
	Beş+	230,25	,10	,26	
2. Bürodaki çalışan personel sayısı?	Bir	226,33	,10	,26	X^2=3,541 p=,315
	İki	219,14	,06	,16	
	Üç	238,94	,14	,30	
	Dört+	220,86	,11	,30	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	233,55	,14	,33	X^2=5,064 p=,167
	Bir	226,74	,08	,19	
	İki	220,02	,07	,21	
	Üç	247,83	,19	,39	
4. Büroda kullanılan bilgisayar sayısı?	İki	228,29	,11	,29	X^2=5,230 p=,265
	Üç	210,39	,04	,11	
	Dört	213,70	,10	,32	
	Beş	231,45	,11	,27	
	Altı+	234,68	,12	,27	

Çizelge 6.25. (devam) İşlem güvenliği - Bilgi sistemleri tetkik hususları düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	234,72	,13	,28	X^2=17,540
	İki	201,11	,02	,08	p=,000
	Üç	246,00	,17	,34	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	223,05	,09	,24	U=24720
	Evet	230,14	,12	,27	p=,376
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	225,50	,09	,23	U=25200
	Evet	227,63	,11	,28	p=,790
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	227,62	,11	,28	U=25224
	Evet	225,28	,09	,23	p=,770
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	233,20	,12	,28	U=23048
	Evet	217,10	,07	,21	p=,047
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	215,40	,06	,19	U=22912
	Evet	235,00	,13	,29	p=,015
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	233,03	,11	,27	U=23872
	Evet	219,10	,09	,25	p=,082
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	219,19	,08	,24	U=23856
	Evet	232,73	,11	,27	p=,092
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	222,18	,09	,25	U=23304
	Evet	233,03	,11	,27	p=,184
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	226,87	,10	,26	U=25400
	Evet	226,09	,10	,26	p=,922
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	225,08	,09	,24	U=25208
	Evet	227,84	,11	,27	p=,730

Çizelge 6.25. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları düzeyinin;

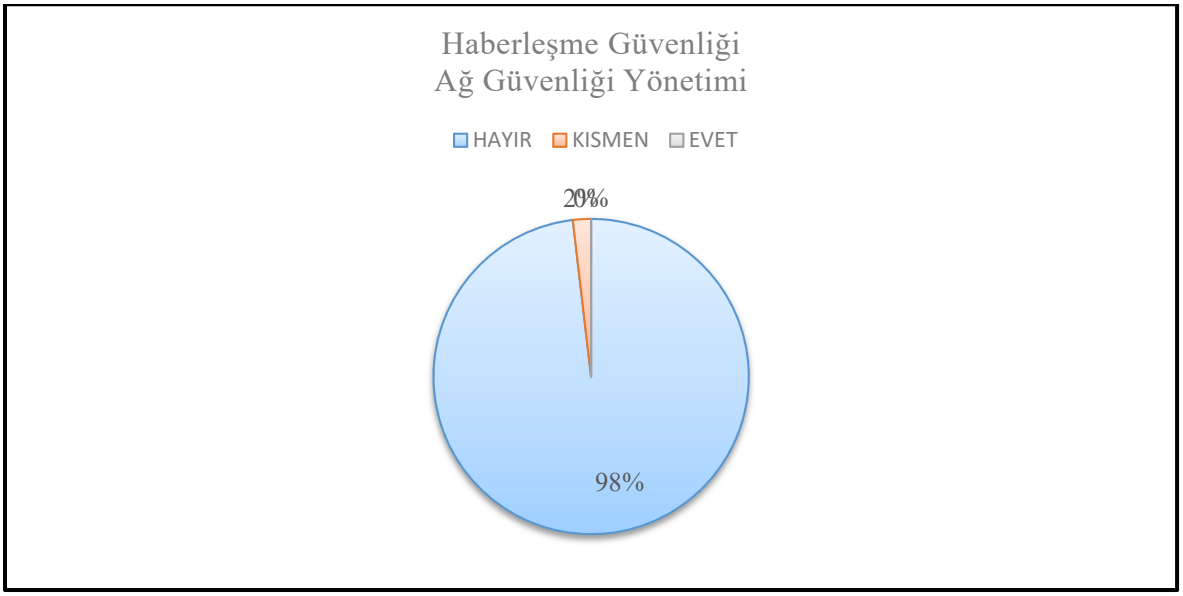
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=17,540; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "İki" (201,11) olan hukuk bürolarının İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları düzeyinin "Bir" (234,72) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
    - Büroda kullanılan yazıcı sayısı "İki" (201,11) olan hukuk bürolarının İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları düzeyinin "Üç" (246,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).

Çizelge 6.25. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İşlem Güvenliği - Bilgi Sistemleri Tetkik Hususları düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=23048; p=,047), özel bir web sitesi olan (217,10) hukuk bürolarının olmayanlara (233,20) göre daha düşük olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22912; p=,015), tedarikçisi olan (235,00) hukuk bürolarının, olmayanlara (215,40) göre daha yüksek olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=23872; p=,082), danışmanlık alınan tedarikçisi olan (219,10) hukuk bürolarının olmayanlara (233,03) göre daha düşük olduğu tespit edilmiştir.

6.3.24. Haberleşme güvenliği - Ağ güvenliği Yönetimi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Haberleşme Güvenliği - Ağ Güvenliği Yönetimi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 10 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %0' ının Evet, %2' sinin Kısmen ve %98' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.24.).



Şekil 6.24. Haberleşme güvenliği - Ağ güvenliği yönetimi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.26.' da verilmiştir.

Çizelge 6.26. Haberleşme güvenliği - Ağ güvenliği yönetimi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	223,67	,02	,06	X^2=19,602
	İki	232,50	,03	,08	p=,001
	Üç	242,93	,03	,06	
	Dört	204,50	,00	,00	
	Beş+	204,50	,00	,00	
2. Bürodaki çalışan personel sayısı?	Bir	217,28	,01	,05	X^2=24,016
	İki	252,29	,04	,08	p=,000
	Üç	212,35	,00	,02	
	Dört+	226,14	,03	,09	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	227,17	,03	,10	X^2=1,929
	Bir	216,97	,01	,02	p=,587
	İki	229,39	,02	,06	
	Üç	223,67	,02	,06	
4. Büroda kullanılan bilgisayar sayısı?	İki	235,60	,02	,06	X^2=21,653
	Üç	251,66	,04	,08	p=,000
	Dört	204,50	,00	,00	
	Beş	214,60	,00	,02	
	Altı+	218,50	,02	,08	
5. Büroda kullanılan yazıcı sayısı?	Bir	225,75	,02	,07	X^2=11,197
	İki	238,62	,03	,07	p=,004
	Üç	204,50	,00	,00	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	227,88	,02	,06	U=25200
	Evet	225,05	,02	,07	p=,654
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	234,53	,02	,07	U=23512
	Evet	217,41	,01	,05	p=,007
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	231,35	,02	,08	U=24344
	Evet	221,20	,01	,05	p=,109
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	221,11	,01	,04	U=23392
	Evet	234,07	,03	,09	p=,043
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	218,46	,01	,05	U=23512
	Evet	232,66	,02	,07	p=,026
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	227,40	,02	,06	U=25224
	Evet	225,48	,02	,06	p=,762
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	230,88	,02	,08	U=24464
	Evet	222,76	,01	,05	p=,200
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	227,79	,02	,07	U=24128
	Evet	224,54	,02	,05	p=,615

Çizelge 6.26. (devam) Haberleşme güvenliği - Ağ güvenliği yönetimi düzeyinin analizi

14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	227,45	,02	,07	U=25264
	Evet	225,46	,02	,05	p=,753
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	220,86	,01	,06	U=24280
	Evet	231,84	,02	,07	p=,082

Çizelge 6.26. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=19,602; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Dört" (204,50) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "Üç" (242,93) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (204,50) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "İki" (232,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,038).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (204,50) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "Üç" (242,93) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=24,016; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Üç" (212,35) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "İki" (252,29) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan personel sayısı "Bir" (217,28) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "İki" (252,29) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan personel sayısı "Dört ve üzeri" (226,14) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "İki" (252,29) olanlara göre daha düşük olduğu tespit edilmiştir (p=,038).

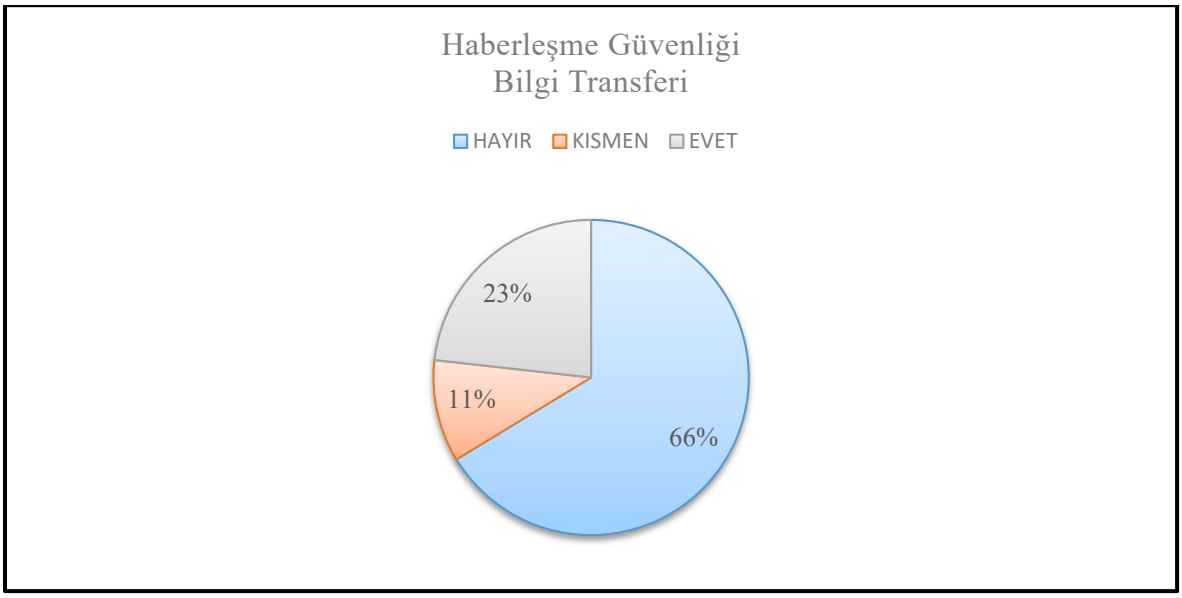
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=21,653; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Dört" (204,50) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "Üç" (251,66) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
    - Büroda kullanılan bilgisayar sayısı "Beş" (214,60) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "Üç" (251,66) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
    - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (218,50) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "Üç" (251,66) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=11,197; p=,004), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "Üç" (204,50) olan hukuk bürolarının Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin "İki" (238,62) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).

Çizelge 6.26. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Haberleşme Güvenliği - Ağ Güvenliği Yönetimi düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23512; p=,007), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (217,41) hukuk bürolarının vermeyenlere (234,53) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=23392; p=,043), özel bir web sitesi olan (234,07) hukuk bürolarının olmayanlara (221,11) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=23512; p=,026), tedarikçisi olan (232,66) hukuk bürolarının, olmayanlara (218,46) göre daha yüksek olduğu tespit edilmiştir.

6.3.25. Haberleşme güvenliği - Bilgi transferi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Haberleşme Güvenliği - Bilgi Transferi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 12 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %23' ünün Evet, %11 inin Kısmen ve %66' sının Hayır cevabını verdikleri görülmüştür (Şekil 6.25.).



Şekil 6.25. Haberleşme güvenliği - Bilgi transferi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Haberleşme Güvenliği - Bilgi Transferi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.27.' de verilmiştir.

Çizelge 6.27. Haberleşme güvenliği - Bilgi transferi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	174,33	,33	,60	X^2=18,802
	İki	250,50	,68	,63	p=,001
	Üç	226,33	,58	,65	
	Dört	200,81	,40	,42	
	Beş+	213,25	,52	,69	

Çizelge 6.27. (devam) Haberleşme güvenliği - Bilgi transferi düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	206,72	,47	,60	X^2=8,085
	İki	235,64	,58	,54	p=,044
	Üç	222,65	,57	,68	
	Dört+	251,95	,70	,69	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	199,17	,44	,59	X^2=11,848
	Bir	222,85	,53	,57	p=,008
	İki	227,13	,57	,62	
	Üç	276,17	,86	,76	
4. Büroda kullanılan bilgisayar sayısı?	İki	212,78	,49	,58	X^2=10,306
	Üç	231,34	,57	,55	p=,036
	Dört	208,30	,53	,78	
	Beş	263,07	,75	,68	
	Altı+	218,26	,53	,63	
5. Büroda kullanılan yazıcı sayısı?	Bir	237,41	,62	,63	X^2=4,828
	İki	209,11	,47	,56	p=,089
	Üç	218,75	,56	,70	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	234,02	,62	,67	U=23776
	Evet	218,57	,52	,57	p=,186
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	230,93	,58	,59	U=24376
	Evet	221,48	,56	,67	p=,419
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	234,06	,61	,65	U=23704
	Evet	218,24	,52	,59	p=,175
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	223,41	,56	,63	U=24000
	Evet	230,84	,59	,61	p=,530
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	239,81	,62	,61	U=22480
	Evet	216,31	,53	,63	p=,046
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	237,37	,63	,67	U=22832
	Evet	214,20	,50	,57	p=,047
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	226,77	,57	,63	U=25320
	Evet	226,27	,57	,62	p=,966
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	207,94	,48	,60	U=19432
	Evet	254,54	,71	,64	p=,000
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	225,35	,56	,62	U=25216
	Evet	227,76	,58	,63	p=,836
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	227,66	,56	,59	U=25264
	Evet	225,40	,58	,65	p=,846

Çizelge 6.27. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Haberleşme Güvenliği - Bilgi Transferi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=18,802; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (174,33) olan hukuk bürolarının Haberleşme Güvenliği - Bilgi Transferi düzeyinin "İki" (250,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=8,085; p=,044), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Bir" (206,72) olan hukuk bürolarının Haberleşme Güvenliği - Bilgi Transferi düzeyinin "Dört ve üzeri" (251,95) olanlara göre daha düşük olduğu tespit edilmiştir (p=,042).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=11,848; p=,008), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Sıfır" (199,17) olan hukuk bürolarının Haberleşme Güvenliği - Bilgi Transferi düzeyinin "Üç" (276,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=10,306; p=,036), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "İki" (212,78) olan hukuk bürolarının Haberleşme Güvenliği - Bilgi Transferi düzeyinin "Beş" (263,07) olanlara göre daha düşük olduğu tespit edilmiştir (p=,046).

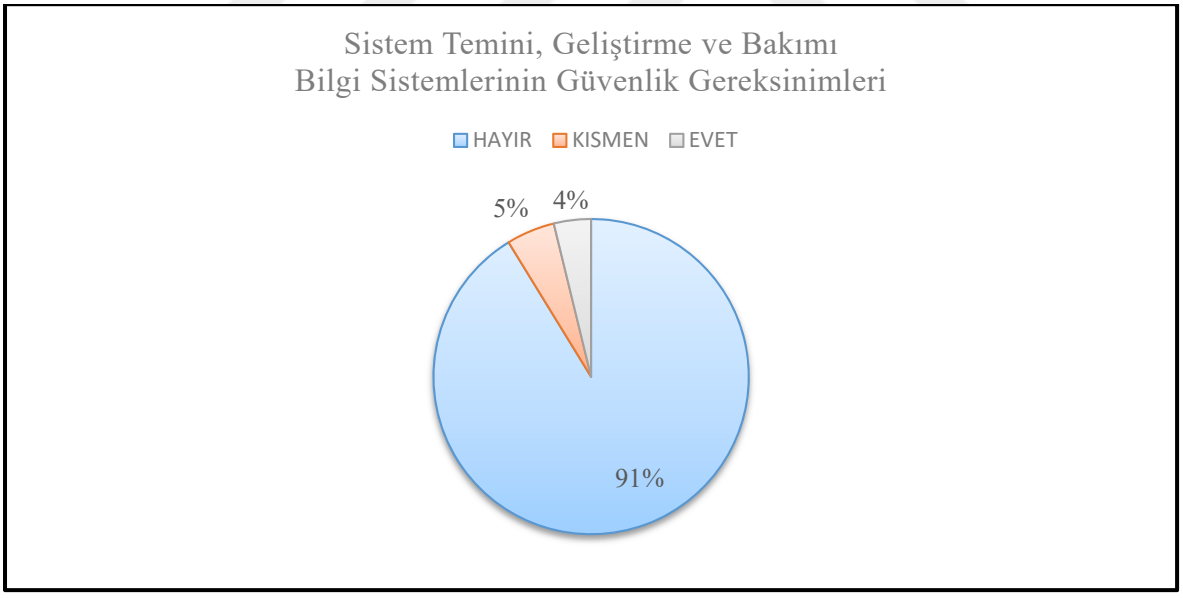
Çizelge 6.27. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Haberleşme Güvenliği - Bilgi Transferi düzeyinin;

- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22480; p=,046), tedarikçisi olan (216,31) hukuk bürolarının, olmayanlara (239,81) göre daha düşük olduğu tespit edilmiştir.

- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22832; p=,047), danışmanlık alınan tedarikçisi olan (214,20) hukuk bürolarının olmayanlara (237,37) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=19432; p=,000), kablosuz bilgisayar ağı kullanan (254,54) hukuk bürolarının kullanmayanlara (207,94) göre daha yüksek olduğu tespit edilmiştir.

6.3.26. Sistem temini, geliştirme ve bakımı - Bilgi sistemlerinin güvenlik gereksinimleri düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 10 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %4' ünün Evet, %5' inin Kısmen ve %91' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.26.).



Şekil 6.26. Sistem temini, geliştirme ve bakımı - Bilgi sistemlerinin güvenlik gereksinimleri alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.28.' de verilmiştir.

Çizelge 6.28. Sistem temini, geliştirme ve bakımı - Bilgi sistemlerinin güvenlik gereksinimleri düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	238,17	,23	,48	X^2=9,245
	İki	223,64	,10	,23	p=,055
	Üç	205,80	,05	,15	
	Dört	238,50	,24	,47	
	Beş+	246,50	,14	,25	
2. Bürodaki çalışan personel sayısı?	Bir	217,61	,12	,33	X^2=3,139
	İki	235,14	,15	,30	p=,371
	Üç	233,54	,11	,21	
	Dört+	221,41	,13	,32	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	221,64	,14	,37	X^2=4,342
	Bir	247,56	,18	,30	p=,227
	İki	221,90	,11	,28	
	Üç	229,33	,08	,18	
4. Büroda kullanılan bilgisayar sayısı?	İki	218,78	,13	,34	X^2=11,054
	Üç	255,45	,14	,24	p=,026
	Dört	201,50	,06	,19	
	Beş	223,45	,13	,32	
	Altı+	226,15	,13	,29	
5. Büroda kullanılan yazıcı sayısı?	Bir	218,13	,11	,28	X^2=5,619
	İki	241,77	,18	,36	p=,060
	Üç	228,50	,07	,16	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	219,98	,10	,27	U=24008
	Evet	233,37	,15	,31	p=,128
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	219,53	,11	,30	U=23768
	Evet	234,39	,14	,29	p=,091
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	217,28	,11	,31	U=23312
	Evet	236,57	,14	,28	p=,028
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	215,53	,08	,21	U=21920
	Evet	241,90	,18	,37	p=,003
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	228,05	,12	,26	U=24784
	Evet	225,31	,13	,32	p=,757
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	229,93	,12	,28	U=24616
	Evet	222,61	,13	,31	p=,406
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	213,46	,10	,27	U=22664
	Evet	237,61	,15	,31	p=,006
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	221,38	,11	,30	U=23088
	Evet	234,23	,14	,29	p=,152
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	232,87	,15	,33	U=23984
	Evet	219,54	,10	,24	p=,129
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	214,97	,09	,24	U=22984
	Evet	237,43	,16	,33	p=,011

Çizelge 6.28. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri düzeyinin;

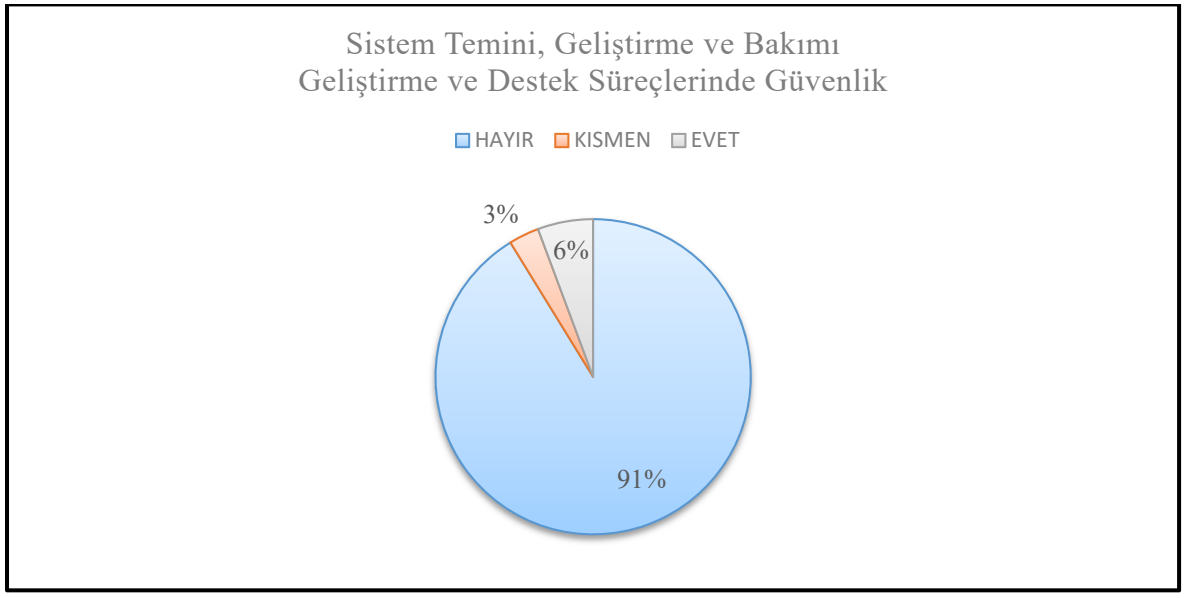
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=11,054; p=,026), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Dört" (201,50) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri düzeyinin "Üç" (255,45) olanlara göre daha düşük olduğu tespit edilmiştir (p=,031).

Çizelge 6.28. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=23312; p=,028), özel bir paket programı olan (236,57) hukuk bürolarının olmayanlara (217,28) göre daha yüksek olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=21920; p=,003), özel bir web sitesi olan (241,90) hukuk bürolarının olmayanlara (215,53) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22664; p=,006), kablolu bilgisayar ağı kullanan (237,61) hukuk bürolarının kullanmayanlara (213,46) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22984; p=,011), bağlanmasına izin veren (237,43) hukuk bürolarının, vermeyenlere (214,97) göre daha yüksek olduğu tespit edilmiştir.

6.3.27. Sistem temini, geliştirme ve bakımı - Geliştirme ve destek süreçlerinde güvenlik düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 31 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %6' sının Evet, %3' ünün Kısmen ve %91' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.27.).



Şekil 6.27. Sistem temini, geliştirme ve bakımı - Geliştirme ve destek süreçlerinde güvenlik alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.29' da verilmiştir.

Çizelge 6.29. Sistem temini, geliştirme ve bakımı - Geliştirme ve destek süreçlerinde güvenlik düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	218,67	,13	,22	X^2=8,591
	İki	244,30	,17	,28	p=,072
	Üç	211,37	,10	,18	
	Dört	206,04	,23	,45	
	Beş+	216,25	,09	,14	
2. Bürodaki çalışan personel sayısı?	Bir	217,89	,12	,23	X^2=2,382
	İki	240,00	,18	,32	p=,497
	Üç	223,98	,13	,21	
	Dört+	226,50	,16	,32	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	219,74	,15	,26	X^2=3,768
	Bir	204,74	,13	,30	p=,288
	İki	233,71	,15	,28	
	Üç	231,33	,13	,20	
4. Büroda kullanılan bilgisayar sayısı?	İki	246,16	,17	,27	X^2=45,605
	Üç	280,50	,22	,28	p=,000
	Dört	153,70	,01	,03	
	Beş	234,21	,16	,27	
	Altı+	196,21	,11	,29	
5. Büroda kullanılan yazıcı sayısı?	Bir	216,47	,14	,27	X^2=6,448
	İki	247,71	,17	,30	p=,040
	Üç	222,88	,12	,19	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	213,43	,14	,27	U=22488
	Evet	240,28	,16	,26	p=,013
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	217,77	,14	,27	U=23344
	Evet	236,39	,15	,26	p=,087
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	227,42	,14	,27	U=25272
	Evet	225,50	,15	,27	p=,860
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	214,41	,13	,27	U=21624
	Evet	243,48	,17	,27	p=,008
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	246,66	,19	,31	U=21136
	Evet	211,06	,11	,22	p=,001
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	229,40	,16	,27	U=24744
	Evet	223,22	,13	,27	p=,570
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	223,65	,17	,32	U=24784
	Evet	228,93	,12	,21	p=,629
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	225,21	,14	,27	U=24128
	Evet	228,46	,16	,27	p=,770
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	234,23	,16	,28	U=23664
	Evet	218,06	,13	,26	p=,137
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	230,06	,15	,28	U=24736
	Evet	223,12	,14	,26	p=,523

Çizelge 6.29. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin;

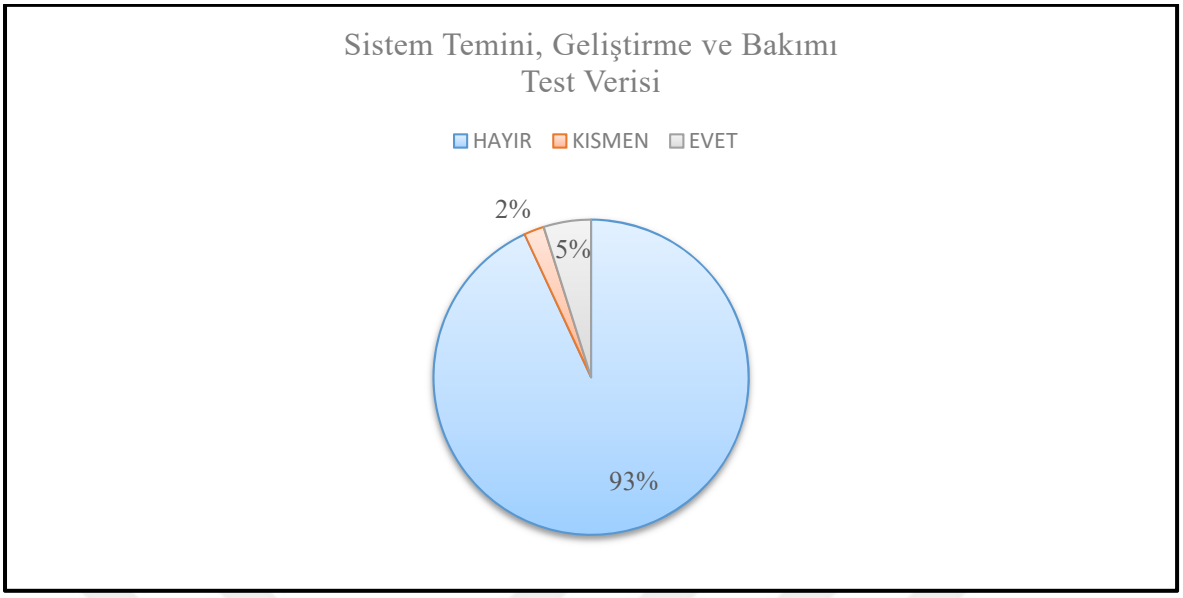
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=45,605; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan bilgisayar sayısı "Dört" (153,70) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin "Beş" (234,21) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
    - Büroda kullanılan bilgisayar sayısı "Dört" (153,70) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin "İki" (246,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda kullanılan bilgisayar sayısı "Dört" (153,70) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin "Üç" (280,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (196,21) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin "İki" (246,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
    - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (196,21) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin "Üç" (280,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=6,448; p=,040), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda kullanılan yazıcı sayısı "Bir" (216,47) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin "İki" (247,71) olanlara göre daha düşük olduğu tespit edilmiştir (p=,035).

Çizelge 6.29. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik düzeyinin;

- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22488; p=,013), bilgisayar ağında mobil cihazlar kullanan (240,28) hukuk bürolarının kullanmayanlara (213,43) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=21624; p=,008), özel bir web sitesi olan (243,48) hukuk bürolarının olmayanlara (214,41) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=21136; p=,001), tedarikçisi olan (211,06) hukuk bürolarının, olmayanlara (246,66) göre daha düşük olduğu tespit edilmiştir.

6.3.28. Sistem temini, geliştirme ve bakımı - Test verisi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Test Verisi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 6 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %5' inin Evet, %2' sinin Kısmen ve %93' ünün Hayır cevabını verdikleri görülmüştür (Şekil 6.28.).



Şekil 6.28. Sistem temini, geliştirme ve bakımı - Test verisi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.30.' da verilmiştir.

Çizelge 6.30. Sistem temini, geliştirme ve bakımı - Test verisi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	198,50	,00	,00	X^2=17,389
	İki	231,32	,15	,42	p=,002
	Üç	246,50	,17	,44	
	Dört	215,88	,08	,28	
	Beş+	212,63	,06	,25	
2. Bürodaki çalışan personel sayısı?	Bir	217,44	,08	,32	X^2=20,966
	İki	239,14	,18	,49	p=,000
	Üç	206,87	,04	,19	
	Dört+	249,32	,20	,40	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	219,45	,07	,24	X^2=7,549
	Bir	224,97	,11	,40	p=,056
	İki	224,02	,12	,38	
	Üç	254,00	,21	,46	
4. Büroda kullanılan bilgisayar sayısı?	İki	244,50	,17	,46	X^2=17,222
	Üç	223,45	,14	,43	p=,002
	Dört	198,50	,00	,00	
	Beş	209,83	,06	,29	
	Altı+	231,38	,13	,34	

Çizelge 6.30. (devam) Sistem temini, geliştirme ve bakımı - Test verisi düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	223,00	,10	,32	X^2=7,082
	İki	240,02	,19	,48	p=,029
	Üç	212,63	,06	,25	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	225,33	,10	,33	U=25248
	Evet	227,74	,14	,40	p=,732
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	224,33	,09	,31	U=24920
	Evet	228,95	,15	,42	p=,512
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	232,43	,13	,35	U=24088
	Evet	220,02	,11	,38	p=,078
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	225,59	,11	,33	U=24576
	Evet	227,78	,13	,41	p=,759
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	227,19	,15	,44	U=24952
	Evet	225,97	,09	,30	p=,863
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	225,00	,12	,37	U=25080
	Evet	228,20	,12	,37	p=,650
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	228,88	,13	,37	U=24880
	Evet	224,47	,11	,37	p=,531
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	231,91	,14	,41	U=23008
	Evet	218,32	,08	,28	p=,058
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	225,75	,13	,39	U=25312
	Evet	227,31	,11	,34	p=,825
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	231,23	,13	,38	U=24480
	Evet	222,02	,10	,36	p=,190

Çizelge 6.30. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=17,389; p=,002), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Bir" (198,50) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin "Üç" (246,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=20,966; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

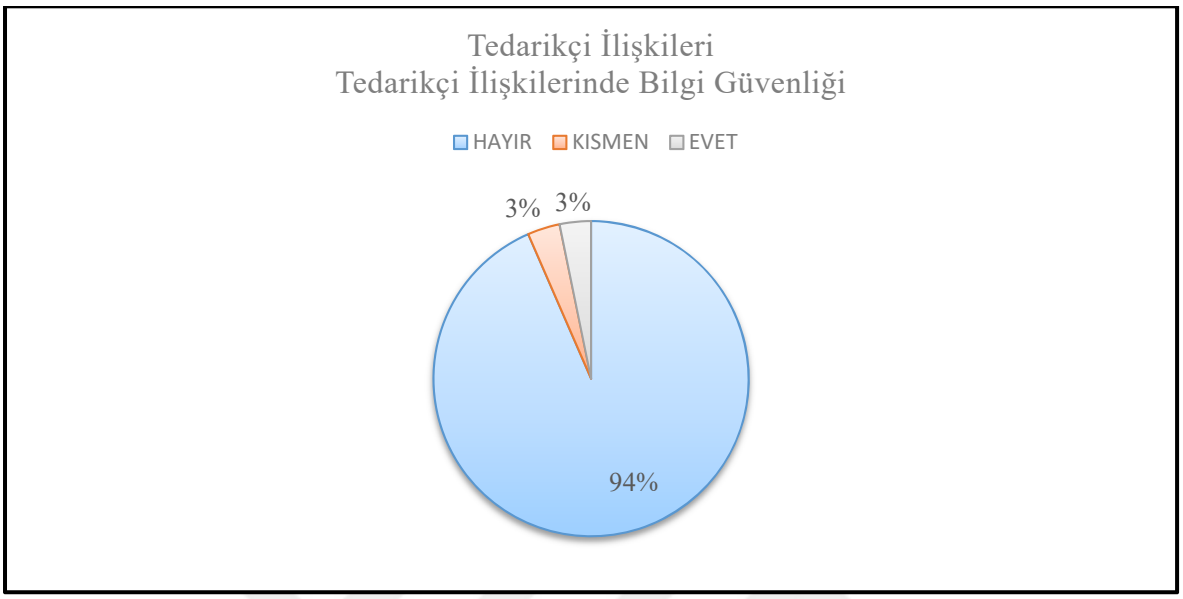
  - Büroda çalışan personel sayısı “Üç” (206,87) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin “İki” (239,14) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).
  - Büroda çalışan personel sayısı “Üç” (206,87) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin “Dört ve üzeri” (249,32) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “Bir” (217,44) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin “Dört ve üzeri” (249,32) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=17,222; p=,002), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Dört” (198,50) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin “İki” (244,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).
  - Büroda kullanılan bilgisayar sayısı “Beş” (209,83) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin “İki” (244,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,012).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=7,082; p=,029), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan yazıcı sayısı “Üç” (212,63) olan hukuk bürolarının Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyinin “İki” (240,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,048).

Çizelge 6.30. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Sistem Temini, Geliştirme ve Bakımı - Test Verisi düzeyin anlamsal bir farklılık olmadığı tespit edilmiştir.

6.3.29. Tedarikçi ilişkileri - Tedarikçi ilişkilerinde bilgi güvenliği düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre “Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 8 soru

yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %3' ünün Evet, %3' ünün Kısmen ve %94' ünün Hayır cevabını verdikleri görülmüştür (Şekil 6.29.).



Şekil 6.29. Tedarikçi ilişkileri - Tedarikçi ilişkilerinde bilgi güvenliği alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.31.' de verilmiştir.

Çizelge 6.31. Tedarikçi ilişkileri - Tedarikçi ilişkilerinde bilgi güvenliği düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	206,50	,00	,00	X^2=8,075 p=,089
	İki	234,13	,13	,35	
	Üç	225,89	,09	,32	
	Dört	225,27	,13	,48	
	Beş+	220,00	,04	,18	
2. Bürodaki çalışan personel sayısı?	Bir	218,50	,04	,17	X^2=32,299 p=,000
	İki	256,36	,28	,56	
	Üç	214,50	,03	,14	
	Dört+	216,32	,03	,15	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	239,74	,18	,46	X^2=29,021 p=,000
	Bir	233,56	,14	,44	
	İki	213,48	,02	,14	
	Üç	261,67	,23	,45	

Çizelge 6.31. (devam) Tedarikçi ilişkileri - Tedarikçi ilişkilerinde bilgi güvenliği düzeyinin analizi

4. Büroda kullanılan bilgisayar sayısı?	İki	230,09	,11	,34	X^2=5,208
	Üç	217,87	,04	,16	p=,267
	Dört	230,30	,14	,45	
	Beş	236,98	,10	,24	
	Altı+	220,68	,09	,38	
5. Büroda kullanılan yazıcı sayısı?	Bir	230,91	,10	,32	X^2=2,781
	İki	221,11	,10	,38	p=,249
	Üç	220,00	,04	,18	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	225,84	,09	,32	U=25368
	Evet	227,19	,10	,33	p=,824
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	224,97	,08	,28	U=25072
	Evet	228,24	,11	,36	p=,590
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	229,55	,11	,36	U=24768
	Evet	223,17	,07	,27	p=,292
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	230,26	,11	,33	U=23824
	Evet	221,22	,08	,31	p=,141
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	243,81	,19	,45	U=21969
	Evet	213,25	,02	,13	p=,000
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	236,13	,12	,34	U=23128
	Evet	215,59	,06	,30	p=,001
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	237,08	,15	,41	U=23176
	Evet	217,48	,05	,22	p=,001
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	219,82	,07	,29	U=22664
	Evet	236,59	,14	,37	p=,007
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	229,92	,12	,38	U=24680
	Evet	222,76	,06	,24	p=,237
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	230,57	,10	,29	U=24624
	Evet	222,64	,09	,35	p=,190

Çizelge 6.31. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin;

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=32,299; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Üç" (214,50) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin "İki" (256,36) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

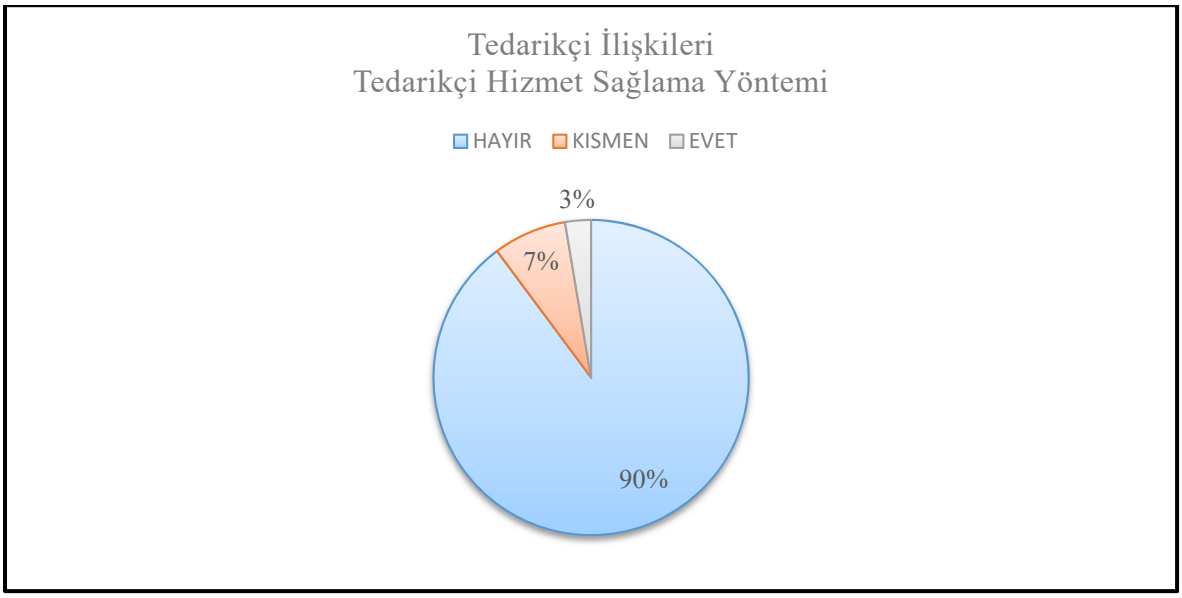
  - Büroda çalışan personel sayısı “Dört ve üzeri” (216,32) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin “Bir” (218,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “Bir” (218,50) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin “İki” (256,36) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=29,021; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan yardımcı personel sayısı “İki” (213,48) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin “Sıfır” (239,74) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).
  - Büroda çalışan yardımcı personel sayısı “İki” (213,48) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin “Üç” (261,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.31. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği düzeyinin;

- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=21696; p=,000), tedarikçisi olan (213,25) hukuk bürolarının, olmayanlara (243,81) göre daha düşük olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=23128; p=,001), danışmanlık alınan tedarikçisi olan (215,59) hukuk bürolarının olmayanlara (236,13) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23176; p=,001), kablolu bilgisayar ağı kullanan (217,48) hukuk bürolarının kullanmayanlara (237,08) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22664; p=,007), kablosuz bilgisayar ağı kullanan (236,59) hukuk bürolarının kullanmayanlara (219,82) göre daha yüksek olduğu tespit edilmiştir.

6.3.30. Tedarikçi ilişkileri - Tedarikçi hizmet sağlama yöntemi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Tedarikçi İlişkileri - Tedarikçi Sağlama Yöntemi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 10 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %3' ünün Evet, %7' sinin Kısmen ve %90' ının Hayır cevabını verdikleri görülmüştür (Şekil 6.30.).



Şekil 6.30. Tedarikçi ilişkileri - Tedarikçi hizmet sağlama yöntemi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.32.' de verilmiştir.

Çizelge 6.32. Tedarikçi ilişkileri - Tedarikçi hizmet sağlama yöntemi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	X̄	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	231,00	,18	,43	X^2=13497
	İki	235,81	,14	,34	p=,009
	Üç	231,37	,18	,48	
	Dört	190,50	,00	,00	
	Beş+	216,88	,06	,22	

Çizelge 6.32. (devam) Tedarikçi ilişkileri - Tedarikçi hizmet sağlama yöntemi düzeyinin analizi

2. Bürodaki çalışan personel sayısı?	Bir	209,50	,07	,26	X^2=9,980
	İki	231,64	,17	,43	p=,019
	Üç	230,80	,12	,33	
	Dört+	242,50	,19	,40	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	224,21	,14	,36	X^2=29,581
	Bir	204,85	,06	,27	p=,000
	İki	221,87	,10	,27	
	Üç	285,50	,38	,63	
4. Büroda kullanılan bilgisayar sayısı?	İki	221,12	,09	,29	X^2=7,064
	Üç	247,34	,16	,32	p=,133
	Dört	235,70	,16	,44	
	Beş	223,36	,12	,32	
	Altı+	218,68	,14	,41	
5. Büroda kullanılan yazıcı sayısı?	Bir	223,13	,13	,34	X^2=1,018
	İki	230,02	,12	,36	p=,601
	Üç	232,75	,15	,40	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	229,33	,14	,37	U=24864
	Evet	223,52	,12	,33	p=,458
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	234,77	,14	,31	U=23456
	Evet	217,14	,12	,39	p=,025
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	236,47	,17	,40	U=23136
	Evet	215,61	,09	,28	p=,008
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	224,83	,12	,34	U=24376
	Evet	228,84	,14	,36	p=,614
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	218,74	,11	,37	U=23568
	Evet	232,44	,14	,33	p=,083
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	228,47	,14	,35	U=24968
	Evet	224,27	,12	,35	p=,593
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	224,27	,10	,26	U=24912
	Evet	228,40	,15	,41	p=,599
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	220,03	,10	,33	U=22720
	Evet	236,28	,17	,38	p=,042
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	221,14	,11	,30	U=24224
	Evet	232,35	,15	,39	p=,153
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	226,97	,12	,35	U=25416
	Evet	226,05	,13	,35	p=,906

Çizelge 6.32. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=13,497; p=,009), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Dört" (190,50) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin "Üç" (231,37) olanlara göre daha düşük olduğu tespit edilmiştir (p=,046).
    - Büroda çalışan avukat sayısı "Dört" (190,50) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin "İki" (235,81) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=9,980; p=,019), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Bir" (209,50) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin "Dört ve üzeri" (242,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,020).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=29,581; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "Bir" (204,85) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin "Üç" (285,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan yardımcı personel sayısı "İki" (221,87) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin "Üç" (285,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan yardımcı personel sayısı "Sıfır" (224,21) olan hukuk bürolarının Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin "Üç" (285,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.32. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi düzeyinin;

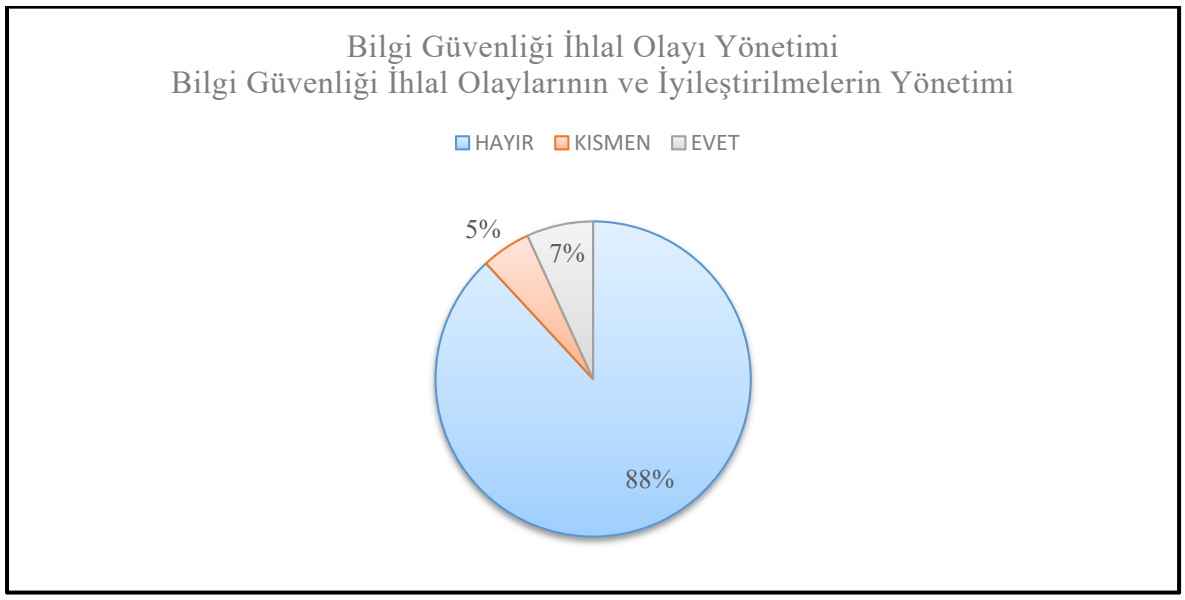
- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=23456; p=,025), çalışanların büro ağında

kişisel mobil cihazlarını kullanmalarına izin veren (217,14) hukuk bürolarının vermeyenlere (234,77) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=23136; p=,008), özel bir paket programı olan (215,61) hukuk bürolarının olmayanlara (236,47) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22720; p=,042), kablosuz bilgisayar ağı kullanan (236,28) hukuk bürolarının kullanmayanlara (220,03) göre daha yüksek olduğu tespit edilmiştir.

6.3.31. Bilgi güvenliği ihlal olayı yönetimi - Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 14 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %7' sinin Evet, %5' inin Kısmen ve %88' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.31.).



Şekil 6.31. Bilgi güvenliği ihlal olayı - Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin

anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.33.' te verilmiştir.

Çizelge 6.33. Bilgi güvenliği ihlal olayı yönetimi - Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	278,50	,29	,28	X^2=48,311
	İki	225,68	,20	,36	p=,000
	Üç	217,02	,14	,22	
	Dört	286,35	,33	,32	
	Beş+	155,00	,02	,07	
2. Bürodaki çalışan personel sayısı?	Bir	241,17	,19	,25	X^2=23,101
	İki	202,36	,12	,20	p=,000
	Üç	259,31	,25	,32	
	Dört+	192,95	,18	,45	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	272,69	,33	,46	X^2=17,588
	Bir	201,68	,15	,30	p=,001
	İki	219,42	,16	,25	
	Üç	218,00	,13	,21	
4. Büroda kullanılan bilgisayar sayısı?	İki	241,53	,19	,25	X^2=11,945
	Üç	247,45	,20	,24	p=,018
	Dört	207,50	,11	,16	
	Beş	235,26	,20	,25	
	Altı+	202,15	,19	,43	
5. Büroda kullanılan yazıcı sayısı?	Bir	223,97	,20	,35	X^2=,347
	İki	228,32	,17	,23	p=,841
	Üç	232,88	,18	,25	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	216,05	,16	,25	U=23096
	Evet	237,52	,22	,36	p=,050
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	235,10	,21	,34	U=23376
	Evet	216,76	,16	,26	p=,094
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	223,21	,18	,33	U=24712
	Evet	230,09	,20	,28	p=,529
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	205,08	,14	,24	U=19160
	Evet	256,59	,26	,37	p=,000
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	222,17	,16	,22	U=24240
	Evet	229,81	,21	,36	p=,488
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	223,77	,17	,25	U=24784
	Evet	229,59	,21	,36	p=,594
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	223,23	,20	,36	U=24969
	Evet	229,29	,18	,26	p=,581
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	220,62	,19	,33	U=22880
	Evet	235,39	,18	,26	p=,186

Çizelge 6.33. (devam) Bilgi güvenliği ihlal olayı yönetimi - Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi düzeyinin analizi

14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	242,74	,24	,36	U=21656
	Evet	208,76	,13	,21	p=,002
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	219,34	,19	,35	U=23944
	Evet	233,29	,18	,26	p=,202

Çizelge 6.33. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=48,311; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (155,00) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin "Üç" (217,02) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (155,00) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin "İki" (225,68) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (155,00) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin "Bir" (278,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (155,00) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin "Dört" (286,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Üç" (217,02) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin "Bir" (278,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,029).

- Büroda çalışan avukat sayısı “Üç” (217,02) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Dört” (286,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
- Büroda çalışan avukat sayısı “İki” (225,68) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Bir” (278,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,047).
- Büroda çalışan avukat sayısı “İki” (225,68) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Dört” (286,35) olanlara göre daha düşük olduğu tespit edilmiştir (p=,008).

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=23,101; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan personel sayısı “Dört ve üzeri” (192,95) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Bir” (241,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,013).
  - Büroda çalışan personel sayısı “Dört ve üzeri” (192,95) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Üç” (259,31) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “İki” (202,36) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Bir” (241,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,048).
  - Büroda çalışan personel sayısı “İki” (202,36) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Üç” (259,31) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).
- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=17.588; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

- Büroda çalışan yardımcı personel sayısı “Bir” (201,68) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Sıfır” (272,69) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
- Büroda çalışan yardımcı personel sayısı “İki” (219,42) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Sıfır” (272,69) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).

- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=11,945; p=,018), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (202,15) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Beş” (235,26) olanlara göre daha düşük olduğu tespit edilmiştir (p=,040).
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (202,15) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “İki” (241,53) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (202,15) olan hukuk bürolarının Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin “Üç” (247,45) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).

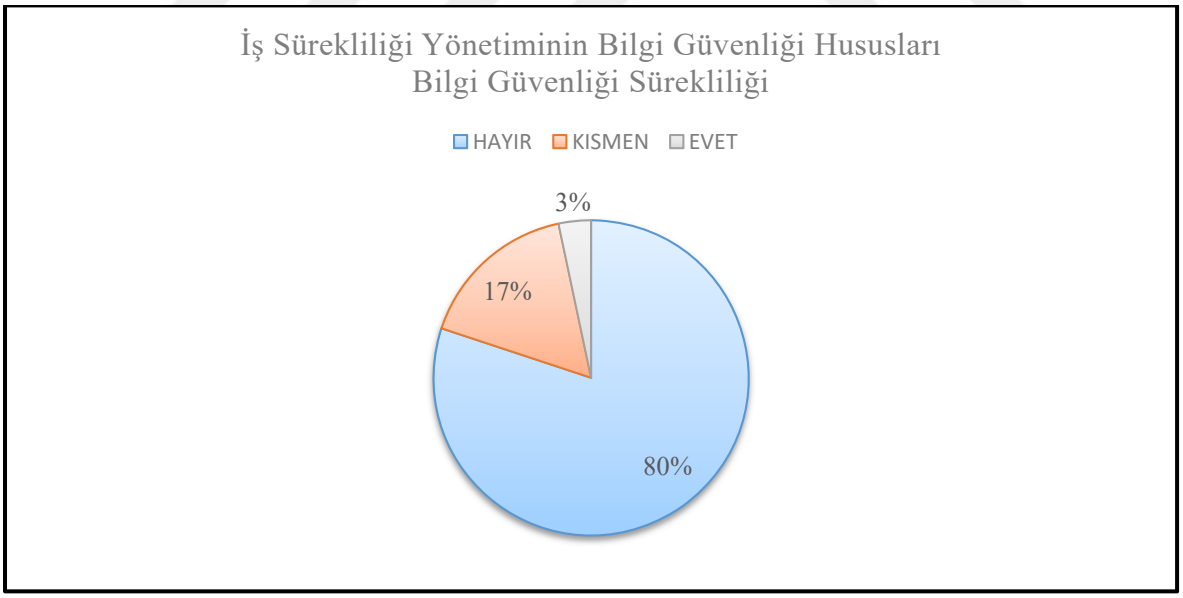
Çizelge 6.33. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Bilgi Güvenliği İhlal Olayı - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyinin;

- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23096; p=,050), bilgisayar ağında mobil cihazlar kullanan (237,52) hukuk bürolarının kullanmayanlara (216,05) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.

- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=19160; p=,000), özel bir web sitesi olan (256,29) hukuk bürolarının olmayanlara (205,08) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21656; p=,002), bağlanmasına izin veren (208,76) hukuk bürolarının, vermeyenlere (242,74) göre daha düşük olduğu tespit edilmiştir.

6.3.32. İş sürekliliği yönetiminin bilgi güvenliği hususları - Bilgi güvenliği sürekliliği düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?" problemi ile ilgili olarak anket katılımcılarına 8 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %3' ünün Evet, %17' sinin Kısmen ve %80' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.32.).



Şekil 6.32. İş sürekliliği yönetiminin bilgi güvenliği hususları - Bilgi güvenliği sürekliliği alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin anlamlı bir

şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.34.' te verilmiştir.

Çizelge 6.34. İş sürekliliğinin bilgi güvenliği hususları - Bilgi güvenliği sürekliliği düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	245,00	,31	,49	X^2=19,911
	İki	236,87	,28	,50	p=,001
	Üç	233,37	,24	,40	
	Dört	220,81	,23	,44	
	Beş+	175,63	,02	,09	
2. Bürodaki çalışan personel sayısı?	Bir	248,17	,32	,51	X^2=13,147
	İki	213,29	,18	,37	p=,004
	Üç	230,57	,25	,49	
	Dört+	202,86	,13	,30	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	233,74	,27	,46	X^2=13,812
	Bir	203,68	,14	,34	p=,003
	İki	237,71	,27	,47	
	Üç	187,33	,09	,32	
4. Büroda kullanılan bilgisayar sayısı?	İki	258,16	,36	,53	X^2=23,998
	Üç	246,39	,28	,40	p=,000
	Dört	210,70	,24	,63	
	Beş	209,26	,17	,38	
	Altı+	203,68	,14	,33	
5. Büroda kullanılan yazıcı sayısı?	Bir	220,50	,24	,49	X^2=19,110
	İki	255,41	,30	,39	p=,000
	Üç	190,88	,09	,26	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	225,16	,25	,49	U=25208
	Evet	227,92	,21	,38	p=,775
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	236,87	,28	,49	U=22952
	Evet	214,76	,18	,36	p=,022
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	226,30	,23	,44	U=25440
	Evet	226,72	,23	,44	p=,965
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	226,80	,23	,44	U=24736
	Evet	226,07	,23	,44	p=,941
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	229,15	,24	,45	U=24568
	Evet	224,47	,22	,43	p=,630
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	222,47	,23	,45	U=24472
	Evet	231,07	,24	,43	p=,373
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	233,54	,25	,45	U=23912
	Evet	220,50	,21	,43	p=,178
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,26	,17	,33	U=21424
	Evet	243,48	,33	,55	p=,004

Çizelge 6.34. (devam) İş sürekliliğinin bilgi güvenliği hususları - Bilgi güvenliği sürekliliği düzeyinin analizi

14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	244,91	,31	,50	U=21144
	Evet	206,39	,15	,35	p=,000
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	219,37	,18	,34	U=23952
	Evet	233,26	,28	,51	p=,150

Çizelge 6.34. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=19,911; p=,001), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (175,63) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "Üç" (233,37) olanlara göre daha düşük olduğu tespit edilmiştir (p=,005).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (175,63) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "İki" (236,87) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (175,63) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "Bir" (245,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=13,147; p=,004), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Dört ve üzeri" (202,86) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "Bir" (248,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).

- Büroda çalışan personel sayısı "İki" (213,29) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "Bir" (248,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,041).

- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=13,812; p=,003), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan yardımcı personel sayısı "Üç" (187,33) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "İki" (237,71) olanlara göre daha düşük olduğu tespit edilmiştir (p=,011).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=23,998; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (203,68) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "Üç" (246,39) olanlara göre daha düşük olduğu tespit edilmiştir (p=,036).
  - Büroda kullanılan bilgisayar sayısı "Altı ve üzeri" (203,68) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "İki" (258,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda kullanılan bilgisayar sayısı "Beş" (209,26) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "İki" (258,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,009).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=19,110; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan yazıcı sayısı "Üç" (190,88) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin "İki" (255,41) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

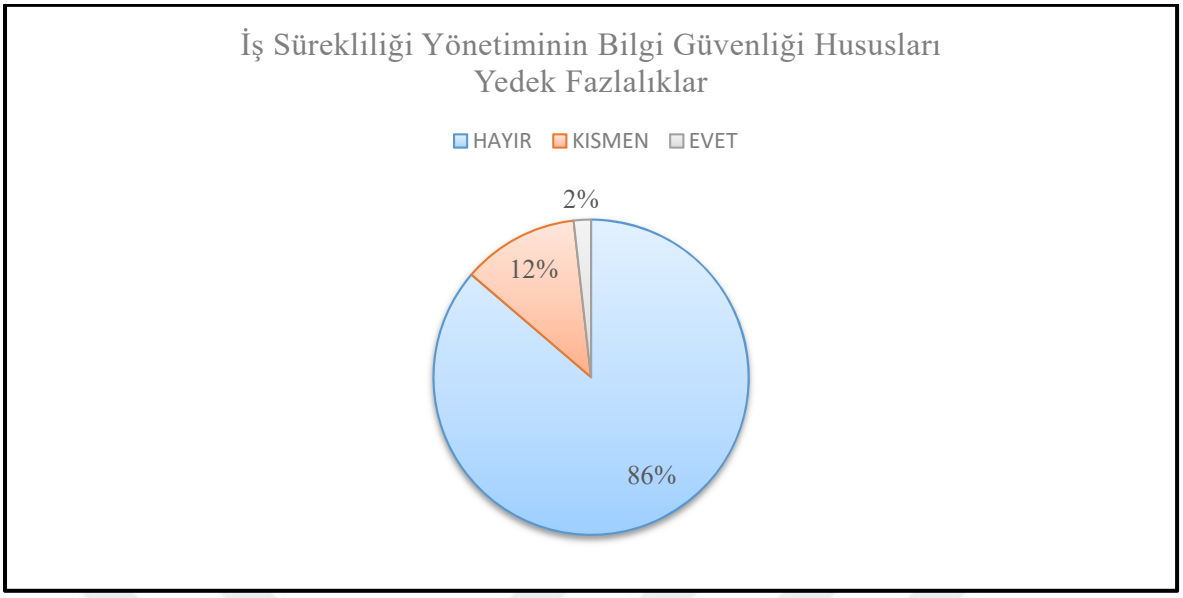
- Büroda kullanılan yazıcı sayısı “Bir” (220,50) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin “İki” (255,41) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).

Çizelge 6.34. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22952; p=,022), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (214,76) hukuk bürolarının vermeyenlere (236,87) göre anlamsal olarak daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21424; p=,004), kablosuz bilgisayar ağı kullanan (243,48) hukuk bürolarının kullanmayanlara (215,26) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21144; p=,000), bağlanmasına izin veren (206,39) hukuk bürolarının, vermeyenlere (244,91) göre daha düşük olduğu tespit edilmiştir.

6.3.33. İş sürekliliği yönetiminin bilgi güvenliği hususları - Yedek fazlalıklar düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre “İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 4 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %2’ sinin Evet, %12’ sinin Kısmen ve %86’ sının Hayır cevabını verdikleri görülmüştür (Şekil 6.33.).



Şekil 6.33. İş sürekliliği yönetiminin bilgi güvenliği hususları - Yedek fazlalıklar alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.35.' de verilmiştir.

Çizelge 6.35. İş sürekliliği yönetiminin bilgi güvenliği hususları - Yedek fazlalıklar düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	247,00	,27	,52	X^2=12,465 p=,014
	İki	228,54	,15	,33	
	Üç	238,85	,21	,44	
	Dört	206,65	,08	,28	
	Beş+	203,25	,06	,25	
2. Bürodaki çalışan personel sayısı?	Bir	247,17	,26	,48	X^2=23,733 p=,000
	İki	210,14	,07	,21	
	Üç	238,13	,19	,38	
	Dört+	199,23	,05	,21	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	231,17	,18	,41	X^2=6,449 p=,092
	Bir	202,38	,06	,24	
	İki	230,82	,16	,35	
	Üç	229,83	,21	,50	

Çizelge 6.35. (devam) İş sürekliliği yönetiminin bilgi güvenliği hususları - Yedek fazlalıklar düzeyinin analizi

4. Büroda kullanılan bilgisayar sayısı?	İki	249,88	,25	,44	X^2=38,258
	Üç	257,45	,25	,41	p=,000
	Dört	212,10	,10	,32	
	Beş	223,36	,17	,43	
	Altı+	195,44	,03	,17	
5. Büroda kullanılan yazıcı sayısı?	Bir	231,44	,18	,40	X^2=2,047
	İki	221,05	,11	,29	p=,359
	Üç	218,00	,13	,34	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	216,88	,12	,35	U=23288
	Evet	236,65	,19	,38	p=,013
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	226,37	,16	,39	U=25408
	Evet	226,65	,15	,34	p=,972
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	231,01	,18	,40	U=24424
	Evet	221,57	,13	,32	p=,239
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	219,86	,14	,36	U=23064
	Evet	235,82	,18	,37	p=,049
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	234,13	,18	,39	U=23592
	Evet	220,66	,14	,35	p=,095
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	230,60	,18	,40	U=24456
	Evet	221,86	,13	,32	p=,275
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	226,69	,15	,36	U=25336
	Evet	226,34	,16	,37	p=,965
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,74	,12	,33	U=21552
	Evet	242,77	,21	,41	p=,001
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	233,48	,17	,35	U=23840
	Evet	218,87	,14	,38	p=,068
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	228,61	,15	,36	U=25056
	Evet	224,50	,16	,37	p=,608

Çizelge 6.35. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=12,465; p=,014), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan avukat sayısı "Beş ve üzeri" (203,25) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin "İki" (228,54) olanlara göre daha düşük olduğu tespit edilmiştir (p=,039).

- Büroda çalışan avukat sayısı “Beş ve üzeri” (203,25) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Üç” (238,85) olanlara göre daha düşük olduğu tespit edilmiştir (p=,010).
- Büroda çalışan avukat sayısı “Beş ve üzeri” (203,25) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Bir” (247,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,007).
- Büroda çalışan avukat sayısı “Dört” (206,65) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Üç” (238,85) olanlara göre daha düşük olduğu tespit edilmiştir (p=,029).
- Büroda çalışan avukat sayısı “Dört” (206,65) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Bir” (247,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,018).

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=23,733; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan personel sayısı “Dört ve üzeri” (199,23) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Üç” (238,13) olanlara göre daha düşük olduğu tespit edilmiştir (p=,009).
  - Büroda çalışan personel sayısı “Dört ve üzeri” (199,23) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Bir” (247,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “İki” (210,14) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Bir” (247,17) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=38,258; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (195,44) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “İki” (249,88) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

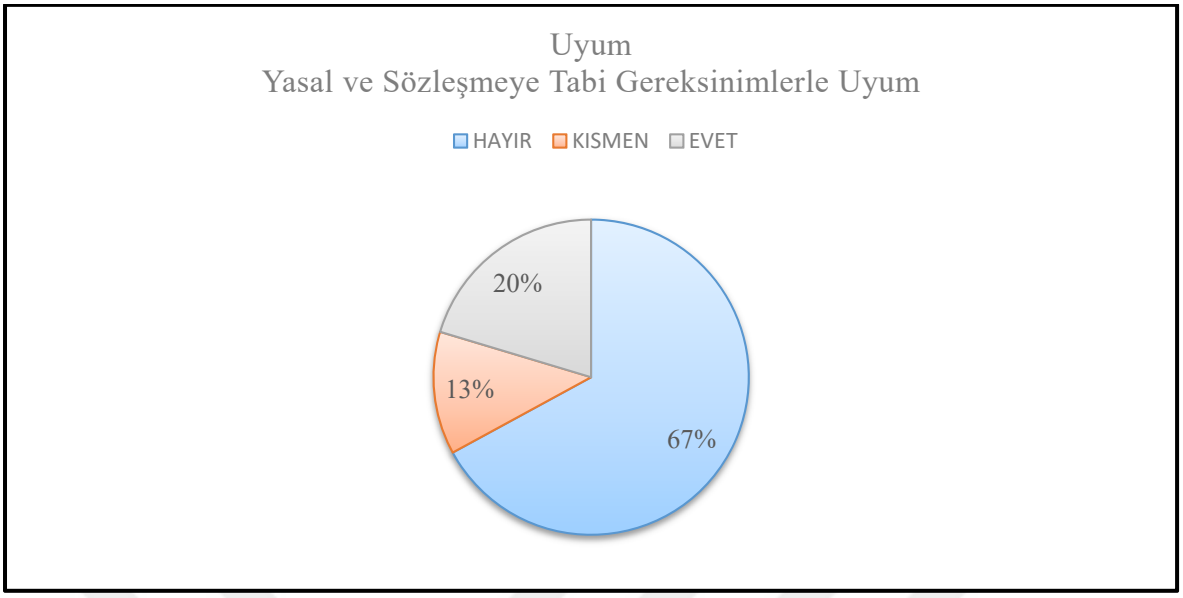
- Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (195,44) olan hukuk bürolarının İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin “Üç” (257,45) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).

Çizelge 6.35. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar düzeyinin;

- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=23288; p=,013), bilgisayar ağında mobil cihazlar kullanan (236,65) hukuk bürolarının kullanmayanlara (216,88) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre anlamsal farklılaştığı (U=23064; p=,049), özel bir web sitesi olan (235,82) hukuk bürolarının olmayanlara (219,86) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21552; p=,001), kablosuz bilgisayar ağı kullanan (242,77) hukuk bürolarının kullanmayanlara (215,74) göre daha yüksek olduğu tespit edilmiştir.

6.3.34. Uyum - Yasal ve sözleşmeye tabi gereksinimlerle uyum düzeyinin analizi

Katılımcılara “Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ göre “Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum” düzeyi anlamlı bir şekilde farklılaşmakta mıdır?” problemi ile ilgili olarak anket katılımcılarına 9 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %20’ sinin Evet, %13’ ünün Kısmen ve %67’ sinin Hayır cevabını verdikleri görülmüştür (Şekil 6.34.).



Şekil 6.34. Uyum - Yasal ve sözleşmeye tabi gereksinimlerle uyum alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.36.' da verilmiştir.

Çizelge 6.36. Uyum - Yasal ve sözleşmeye tabi gereksinimlerle uyum düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		SO	$\bar{X}$	SS	Test İstatistikleri
1. Bürodaki çalışan avukat sayısı?	Bir	230,83	,56	,63	X^2=2,213 p=,697
	İki	230,50	,58	,61	
	Üç	210,07	,45	,55	
	Dört	236,50	,64	,78	
	Beş+	226,50	,53	,58	
2. Bürodaki çalışan personel sayısı?	Bir	197,50	,43	,57	X^2=18,627 p=,000
	İki	251,00	,64	,55	
	Üç	252,94	,67	,60	
	Dört+	210,32	,51	,72	
3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	254,31	,67	,58	X^2=25,681 p=,000
	Bir	235,79	,60	,66	
	İki	202,91	,46	,60	
	Üç	288,50	,80	,58	
4. Büroda kullanılan bilgisayar sayısı?	İki	229,67	,55	,56	X^2=1,338 p=,855
	Üç	218,92	,47	,43	
	Dört	220,90	,53	,63	
	Beş	218,69	,57	,74	
	Altı+	234,50	,59	,66	

Çizelge 6.36. (devam) Uyum - Yasal ve sözleşmeye tabi gereksinimlerle uyum düzeyinin analizi

5. Büroda kullanılan yazıcı sayısı?	Bir	229,69	,57	,64	X^2=8,458 p=,015
	İki	204,80	,44	,53	
	Üç	258,50	,69	,62	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	226,16	,55	,61	U=25440
	Evet	226,86	,55	,60	p=,952
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	229,00	,57	,62	U=24840
	Evet	223,67	,54	,60	p=,649
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	213,62	,48	,55	U=22448
	Evet	240,57	,63	,66	p=,021
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	217,53	,54	,66	U=22448
	Evet	239,10	,57	,52	p=,069
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	223,85	,53	,53	U=24568
	Evet	228,53	,57	,66	p=,691
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	247,03	,63	,58	U=20512
	Evet	203,25	,47	,62	p=,000
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	218,54	,50	,56	U=23720
	Evet	233,29	,60	,65	p=,208
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	215,12	,51	,62	U=21384
	Evet	243,70	,62	,58	p=,017
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	230,84	,58	,62	U=24464
	Evet	221,76	,52	,60	p=,437
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	221,55	,55	,62	U=24432
	Evet	231,19	,56	,60	p=,409

Çizelge 6.36. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin;

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=18,627; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan personel sayısı "Bir" (197,50) olan hukuk bürolarının Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin "İki" (251,00) olanlara göre daha düşük olduğu tespit edilmiştir (p=,004).
    - Büroda çalışan personel sayısı "Bir" (197,50) olan hukuk bürolarının Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin "Üç" (252,94) olanlara göre daha düşük olduğu tespit edilmiştir (p=,003).

- Büroda çalışan yardımcı personel sayısına göre anlamlı farklılaştığı (X^2=25,681; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "İki" (202,91) olan hukuk bürolarının Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin "Sıfır" (254,31) olanlara göre daha düşük olduğu tespit edilmiştir (p=,006).
    - Büroda çalışan yardımcı personel sayısı "İki" (202,91) olan hukuk bürolarının Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin "Üç" (288,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=8,458; p=,015), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
    - Büroda çalışan yardımcı personel sayısı "İki" (204,80) olan hukuk bürolarının Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin "Üç" (258,50) olanlara göre daha düşük olduğu tespit edilmiştir (p=,014).

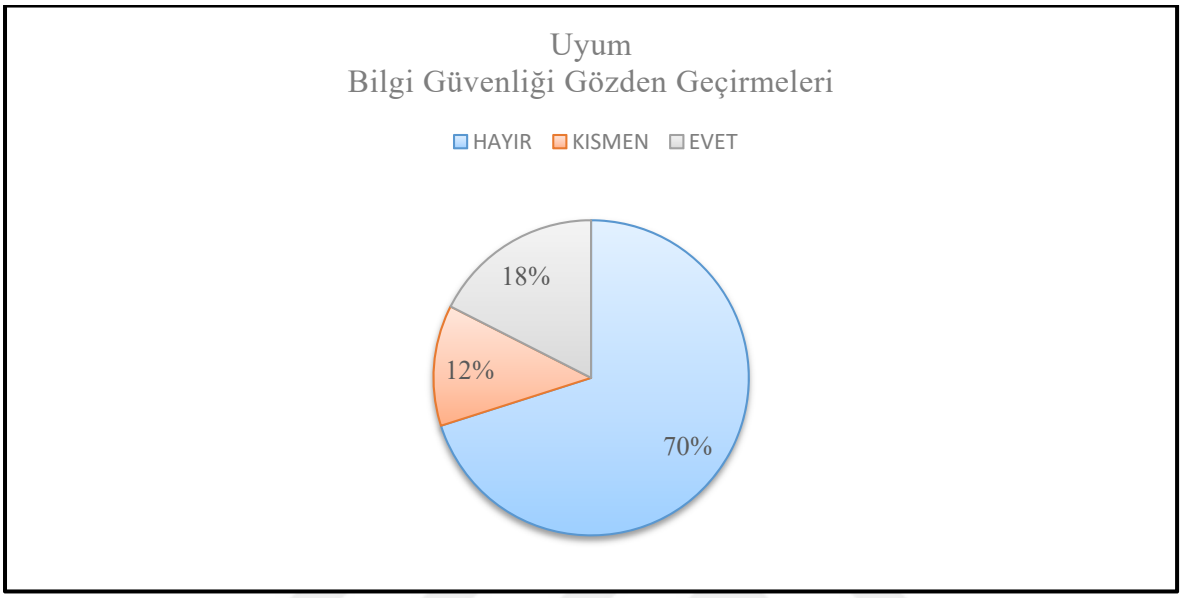
Çizelge 6.36. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum düzeyinin;

- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre anlamsal farklılaştığı (U=22448; p=,021), özel bir paket programı olan (240,57) hukuk bürolarının olmayanlara (213,62) göre daha yüksek olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=20512; p=,000), danışmanlık alınan tedarikçisi olan (203,25) hukuk bürolarının olmayanlara (247,03) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=21384; p=,017), kablosuz bilgisayar ağı kullanan (243,70) hukuk bürolarının kullanmayanlara (215,12) göre daha yüksek olduğu tespit edilmiştir.

6.3.35. Uyum - Bilgi güvenliği gözden geçirmeleri düzeyinin analizi

Katılımcılara "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Uyum - Bilgi Güvenliği Gözden Geçirmeleri" düzeyi anlamlı bir şekilde farklılaşmakta mıdır?"

problemi ile ilgili olarak anket katılımcılarına 5 soru yönlendirilmiştir. Bu sorulara 452 anket katılımcısının %18' inin Evet, %12' sinin Kısmen ve %70' inin Hayır cevabını verdikleri görülmüştür (Şekil 6.35.).



Şekil 6.35. Uyum - Bilgi güvenliği gözden geçirmeleri alt amacına verdikleri cevapların dağılımı

Hukuk Bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin anlamlı bir şekilde farklılaşıp farklılaşmadığını tespit edebilmek amacıyla Kruskal Wallis ve Mann Whitney U testleri uygulanmış sonuçlar Çizelge 6.37.' de verilmiştir.

Çizelge 6.37. Uyum - Bilgi güvenliği gözden geçirmeleri düzeyinin analizi

İnsan Kaynakları, BTE ve BTİ Özellikleri		**SO**	**X̄**	**SS**	**Test İstatistikleri**
1. Bürodaki çalışan avukat sayısı?	Bir	240,33	,60	,80	X^2=10,128 p=,038
	İki	236,38	,55	,70	
	Üç	234,67	,50	,68	
	Dört	197,12	,25	,46	
	Beş+	198,00	,30	,59	
2. Bürodaki çalışan personel sayısı?	Bir	219,39	,46	,70	X^2=25,299 p=,000
	İki	215,79	,39	,59	
	Üç	272,13	,71	,72	
	Dört+	195,77	,32	,61	

Çizelge 6.37. (devam) Uyum - Bilgi güvenliği gözden geçirmeleri düzeyinin analizi

3. Bürodaki çalışan yardımcı personel sayısı?	Sıfır	230,40	,52	,74	X^2=2,878
	Bir	208,15	,39	,66	p=,411
	İki	227,01	,48	,66	
	Üç	243,00	,48	,66	
4. Büroda kullanılan bilgisayar sayısı?	İki	244,16	,59	,72	X^2=22,044
	Üç	266,92	,67	,69	p=,000
	Dört	204,90	,36	,63	
	Beş	220,60	,45	,70	
	Altı+	198,85	,31	,60	
5. Büroda kullanılan yazıcı sayısı?	Bir	212,91	,40	,65	X^2=8,926
	İki	240,20	,55	,68	p=,012
	Üç	252,63	,60	,74	
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	Hayır	230,74	,48	,65	U=24536
	Evet	222,03	,47	,69	p=,416
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin veriliyor mu?	Hayır	208,13	,36	,58	U=21032
	Evet	247,29	,61	,74	p=,000
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	Hayır	217,55	,43	,66	U=23376
	Evet	236,28	,52	,68	p=,081
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	Hayır	219,53	,45	,70	U=22976
	Evet	236,29	,50	,64	p=,123
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi var mı?	Hayır	228,58	,49	,68	U=24680
	Evet	224,91	,47	,67	p=,734
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	Hayır	238,20	,53	,68	U=22632
	Evet	213,25	,41	,66	p=,020
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	Hayır	214,15	,40	,64	U=22808
	Evet	237,02	,53	,69	p=,033
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	Hayır	222,06	,46	,68	U=23272
	Evet	233,21	,50	,66	p=,308
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	238,40	,55	,70	U=22680
	Evet	213,50	,39	,63	p=,020
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	Hayır	221,95	,44	,65	U=24520
	Evet	230,81	,51	,69	p=,409

Çizelge 6.37. incelendiğinde, Kruskal Wallis testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin;

- Büroda çalışan avukat sayısına göre anlamlı farklılaştığı (X^2=10,128; p=,038), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

- Büroda çalışan avukat sayısı “Dört” (197,12) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “İki” (236,38) olanlara göre daha düşük olduğu tespit edilmiştir (p=,027).
- Büroda çalışan avukat sayısı “Beş ve üzeri” (198,00) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “Üç” (234,67) olanlara göre daha düşük olduğu tespit edilmiştir (p=,048).
- Büroda çalışan avukat sayısı “Beş ve üzeri” (198,00) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “İki” (236,38) olanlara göre daha düşük olduğu tespit edilmiştir (p=,019).

- Büroda çalışan personel sayısına göre anlamsal farklılaştığı (X^2=25,299; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda çalışan personel sayısı “Dört ve üzeri” (195,77) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “Üç” (272,13) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
  - Büroda çalışan personel sayısı “İki” (215,79) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “Üç” (272,13) olanlara göre daha düşük olduğu tespit edilmiştir (p=,001).
  - Büroda çalışan personel sayısı “Bir” (219,39) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “Üç” (272,13) olanlara göre daha düşük olduğu tespit edilmiştir (p=,002).
- Büroda kullanılan bilgisayar sayısına göre anlamsal farklılaştığı (X^2=22,044; p=,000), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (198,85) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “İki” (244,16) olanlara göre daha düşük olduğu tespit edilmiştir (p=,016).
  - Büroda kullanılan bilgisayar sayısı “Altı ve üzeri” (198,85) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “Üç” (266,92) olanlara göre daha düşük olduğu tespit edilmiştir (p=,000).
- Büroda kullanılan yazıcı sayısına göre anlamsal farklılaştığı (X^2=8,926; p=,012), bu farklılaşmanın hangi alt gruplar arasında olduğunu tespit edebilmek için yapılan Dunn çoklu karşılaştırma testi sonucunda;

- Büroda kullanılan yazıcı sayısı “Bir” (212,91) olan hukuk bürolarının Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin “Üç” (252,63) olanlara göre daha düşük olduğu tespit edilmiştir (p=,038).

Çizelge 6.37. incelendiğinde, Mann Whitney U testlerinde, test istatistikleri kısmındaki değerler incelendiğinde Uyum - Bilgi Güvenliği Gözden Geçirmeleri düzeyinin;

- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre anlamsal farklılaştığı (U=21032; p=,000), çalışanların büro ağında kişisel mobil cihazlarını kullanmalarına izin veren (247,29) hukuk bürolarının vermeyenlere (208,13) göre anlamsal olarak daha yüksek olduğu tespit edilmiştir.
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre anlamsal farklılaştığı (U=22632; p=,020), danışmanlık alınan tedarikçisi olan (213,25) hukuk bürolarının olmayanlara (238,20) göre daha düşük olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre anlamsal farklılaştığı (U=22808; p=,033), kablolu bilgisayar ağı kullanan (237,02) hukuk bürolarının kullanmayanlara (214,15) göre daha yüksek olduğu tespit edilmiştir.
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre anlamsal farklılaştığı (U=22680; p=,020), bağlanmasına izin veren (213,50) hukuk bürolarının, vermeyenlere (238,40) göre daha düşük olduğu tespit edilmiştir.

6.4. Hukuk Bürolarının ISO/IEC 27001 BGYS Amaçlarının Regresyon Analizi ve Formüle Edilmesi

Çok Değişkenli Regresyon Analizi ile bir BGYS Puanı hesaplamaktaki amaç, öz değerlendirme anketini herhangi bir zamanda yanıtlayan hukuk büroları için de ISO/IEC 27001 BGYS’ ne uyum seviyelerini diğer hukuk büroları ile kıyaslanabilir bir puan hesaplayabilmektir.

Analiz sonrasında, verilerin formüle edilebilir olduğu formülün anketin tamamını kapsayabileceği ve bir sabite ihtiyaç olmadığı (R Square=1,000) görülmüştür.

Çizelge 6.38. ISO/IEC 27001 BGYS amaçlar regresyon analizi sonuçları

Amaçlar	Beta Katsayısı	B Katsayısı	p
Bilgi Güvenliği Politikaları	,138	,071	,000
Bilgi Güvenliği Organizasyonu	,088	,071	,000
İnsan Kaynakları Güvenliği	,186	,071	,000
Varlık Yönetimi	,238	,071	,000
Erişim Kontrolü	,169	,071	,000
Kriptografi	,278	,071	,000
Fiziksel ve Çevresel Güvenlik	,140	,071	,000
İşlem Güvenliği	,140	,071	,000
Haberleşme Güvenliği	,178	,071	,000
Sistem Temini, Geliştirme ve Bakımı	,106	,071	,000
Tedarikçi İlişkileri	,136	,071	,000
Bilgi Güvenliği İhlal Olayı Yönetimi	,174	,071	,000
İş Sürekliliğinin Bilgi Güvenliği Hususları	,211	,071	,000
Uyum	,288	,071	,000

Katılımcılar açısından Çizelge 6.38' de görüleceği üzere ISO/IEC 27001 BGYS amaçlarından en önem verileninin Uyum (,288) ve en az önem verilenin ise Bilgi Güvenliği Organizasyonu (,088) olduğu görülmüştür.

Regresyon analizi amaç seviyesinde formüle edildiğinde;

BGYS Puanı = 0,071 * Bilgi Güvenliği Politikaları Puanı + 0,071 * Bilgi Güvenliği Organizasyonu Puanı + 0,071 * İnsan Kaynakları Güvenliği Puanı + 0,071 * Varlık Yönetimi Puanı + ,071 * Erişim Kontrolü Puanı + ,071 * Kriptografi Puanı + ,071 * Fiziksel ve Çevresel Güvenlik Puanı + ,071 * İşlem Güvenliği Puanı + ,071 * Haberleşme Güvenliği Puanı + ,071 * Sistem Temini, Geliştirme ve Bakımı Puanı + ,071 * Tedarikçi İlişkileri Puanı + ,071 * Bilgi Güvenliği İhlal Olayı Yönetimi Puanı + ,071 * İş Sürekliliğinin Bilgi Güvenliği Hususları Puanı + ,071 * Uyum Puanı

Daha kısa hali ile;

BGYS Puanı = 0,071 * (Bilgi Güvenliği Politikaları Puanı + Bilgi Güvenliği Organizasyonu Puanı + İnsan Kaynakları Güvenliği Puanı + Varlık Yönetimi Puanı + Erişim Kontrolü Puanı + Kriptografi Puanı + Fiziksel ve Çevresel Güvenlik Puanı + İşlem Güvenliği Puanı +

Haberleşme Güvenliği Puanı + Sistem Temini, Geliştirme ve Bakımı Puanı + Tedarikçi İlişkileri Puanı + Bilgi Güvenliği İhlal Olayı Yönetimi Puanı + İş Sürekliliğinin Bilgi Güvenliği Hususları Puanı + Uyum Puanı)

olarak yazılabildiği görülmüştür.

Anketin yanıtları Evet yanıtları 2, Kısmen yanıtları 1 ve Hayır yanıtları 0 olarak kodlanmıştır. Kodlama puanları üzerinden BGYS puanlarına erişim her amaç, katılımcı ve anket maddesi puanları ile hesaplama detayları aşağıdaki şekildedir.

m: Amaç sıra numarası (1-14)
n: Madde sıra numarası (1-n)
o: Katılımcı sıra numarası (1-452)
EP: Madde evet puanı
KP: Madde kısmen puanı
HP: Madde hayır puanı
MCP: Madde Cevap Puanı
MCP=EP veya KP veya HP
$MCP_{m.o.n}$=$EP_{m.o.n}$ veya $KP_{m.o.n}$ veya $HP_{m.o.n}$
$KAP_{m.o}$: Bir amaç için bir katılımcının puanı
KAP_{m}: Bir amaç için tüm katılımcıların puanı
KAP_{o}: Tüm amaçlar için bir katılımcıların puanı
KAP: Tüm amaçlar tüm katılımcıların anket puanı
BGYSP: Bilgi güvenliği yönetim sistemi puanı
BGYSP100: 0-100 aralığında bilgi güvenliği yönetim sistemi puanı
BGYSP100 = KAP * 0,071 * 50

Herhangi bir amaç için ayrı ayrı puan hesaplamaları yapılacak olursa;

$KAP_{1.o}$: Bilgi Güvenliği Politikaları (Amaç Madde Sayısı:8)

$$KAP_{1.O} = \sum_{MCP_n=1}^{8} MCP_n \tag{6.1}$$

Eşitlik 6.1.' de görüldüğü gibi BGYS bilgi güvenliği politikaları amaç puanı hesaplanabilmektedir.

$KAP_{2.o}$: Bilgi Güvenliği Organizasyonu Puanı (Amaç Madde Sayısı:12)

$$KAP_{2.O} = \sum_{MCP_n=1}^{12} MCP_n \quad (6.2)$$

Eş.6.2.' de görüldüğü gibi BGYS bilgi güvenliği organizasyonu amaç puanı hesaplanabilmektedir.

$KAP_{3.o}$: İnsan Kaynakları Güvenliği Puanı (Amaç Madde Sayısı:15)

$$KAP_{3.O} = \sum_{MCP_n=1}^{15} MCP_n \quad (6.3)$$

Eş.6.3.' de görüldüğü gibi BGYS insan kaynakları güvenliği amaç puanı hesaplanabilmektedir.

$KAP_{4.o}$: Varlık Yönetimi Puanı (Amaç Madde Sayısı:18)

$$KAP_{4.O} = \sum_{MCP_n=1}^{18} MCP_n \quad (6.4)$$

Eş.6.4.' de görüldüğü gibi BGYS varlık yönetimi amaç puanı hesaplanabilmektedir.

$KAP_{5.o}$: Erişim Kontrolü Puanı (Amaç Madde Sayısı:25)

$$KAP_{5.O} = \sum_{MCP_n=1}^{25} MCP_n \quad (6.5)$$

Eş.6.5.' de görüldüğü gibi BGYS erişim kontrolü amaç puanı hesaplanabilmektedir.

$KAP_{6.o}$: Kriptografi Puanı (Amaç Madde Sayısı:5)

$$KAP_{6.O} = \sum_{MCP_n=1}^{5} MCP_n \quad (6.6)$$

Eş.6.6.' da görüldüğü gibi BGYS kriptografi amaç puanı hesaplanabilmektedir.

$KAP_{7.o}$: Fiziksel ve Çevresel Güvenlik Puanı (Amaç Madde Sayısı:42)

$$KAP_{7.O} = \sum_{MCP_n=1}^{42} MCP_n \quad (6.7)$$

Eş.6.7.' de görüldüğü gibi BGYS fiziksel ve çevresel güvenlik amaç puanı hesaplanabilmektedir.

$KAP_{8.o}$: İşlem Güvenliği Puanı (Amaç Madde Sayısı:42)

$$KAP_{8.O} = \sum_{MCP_n=1}^{42} MCP_n \quad (6.8)$$

Eş.6.8.' de görüldüğü gibi BGYS işlem güvenliği amaç puanı hesaplanabilmektedir.

$KAP_{9.o}$: Haberleşme Güvenliği Puanı (Amaç Madde Sayısı:22)

$$KAP_{9.O} = \sum_{MCP_n=1}^{22} MCP_n \quad (6.9)$$

Eş.6.9.' da görüldüğü gibi BGYS haberleşme güvenliği amaç puanı hesaplanabilmektedir.

$KAP_{10.o}$: Sistem Temini, Geliştirme ve Bakımı Puanı (Amaç Madde Sayısı:47)

$$KAP_{10.O} = \sum_{MCP_n=1}^{47} MCP_n \quad (6.10)$$

Eş.6.10.' da görüldüğü gibi BGYS sistem temini, geliştirme ve bakımı amaç puanı hesaplanabilmektedir.

$KAP_{11.o}$: Tedarikçi İlişkileri Puanı (Amaç Madde Sayısı:18)

$$KAP_{11.O} = \sum_{MCP_n=1}^{18} MCP_n \quad (6.11)$$

Eş.6.11.' de görüldüğü gibi BGYS tedarikçi ilişkileri amaç puanı hesaplanabilmektedir.

$KAP_{12.o}$: Bilgi Güvenliği İhlal Olayı Yönetimi Puanı (Amaç Madde Sayısı:14)

$$KAP_{12.O} = \sum_{MCP_n=1}^{14} MCP_n \quad (6.12)$$

Eş.6.12.' de görüldüğü gibi BGYS bilgi güvenliği ihlal olayı yönetimi amaç puanı hesaplanabilmektedir.

$KAP_{13.o}$: İş Sürekliliğinin Bilgi Güvenliği Hususları Puanı (Amaç Madde Sayısı:12)

$$KAP_{13.O} = \sum_{MCP_n=1}^{12} MCP_n \quad (6.13)$$

Eş.6.13.' de görüldüğü gibi BGYS iş sürekliliğinin bilgi güvenliği hususları amaç puanı hesaplanabilmektedir.

$KAP_{14.o}$: Uyum Puanı (Amaç Madde Sayısı:14)

$$KAP_{14.O} = \sum_{MCP_n=1}^{14} MCP_n \quad (6.14)$$

Eş.6.14.' de görüldüğü gibi BGYS uyum amaç puanı hesaplanabilmektedir.

Kısaca;

$KAP_o = MCP_{1.o} + MCP_{2.o} + MCP_{3.o} + \ldots + MCP_{mo}$

olacaktır. Yani herhangi bir amaç için herhangi bir katılımcının puanını aşağıdaki şekilde formüle edilebilecektir.

$$KAP_{m.O} = \frac{\sum_{MCP_n=1}^{n} MCP_n}{n} \quad (6.15)$$

Eş.6.15.' de görüldüğü gibi herhangi bir katılımcının herhangi bir BGYS amacından alabileceği puanı hesaplanabilmektedir.

Bu durumda bir katılımcının tüm amaçlardan alacağı puanı aşağıdaki formülle hesaplayabiliriz.

$$KAP_O = \frac{\sum_{KAP_{mo}=1}^{14} KAP_{mo}}{m} \quad (6.16)$$

Eş.6.16.' da görüldüğü gibi herhangi bir katılımcının bütün BGYS amaçlarından alabileceği puanı hesaplanabilmektedir.

Tüm katılımcıların belirli bir amaçtan alacağı puanı aşağıdaki formülle hesaplayabiliriz.

$$KAP_m = \frac{\sum_{KAP_{mo}=1}^{452} KAP_{mo}}{o} \quad (6.17)$$

Eş.6.17.' de görüldüğü gibi bütün katılımcıların herhangi bir BGYS amacından alabileceği puanı hesaplanabilmektedir.

Tüm katılımcıların tüm amaçlardan alacağı puanı aşağıdaki formülle hesaplayabiliriz.

$$KAP = \frac{\sum_{KAP_m=1}^{14} KAP_m}{m} \quad (6.18)$$

Eş.6.18.' de görüldüğü gibi bütün katılımcıların bütün BGYS amaçlarından alabileceği puanı hesaplanabilmektedir.

Regresyon analizi sonucu amaçlara ait katsayıların eşit olması nedeni ile bu formül uygulanabilir olmakla birlikte, regresyon katsayılarını kullanarak aynı formülü aşağıdaki şekilde yazmak da mümkündür.

$$BGYSP = 0{,}071\ x \sum_{KAP_m=1}^{14} KAP_m \quad (6.19)$$

Eş.6.19.' da görüldüğü gibi regresyon analizi sonucunda elde edilen katsayılar ile bütün katılımcıların bütün BGYS amaçlarından alabileceği puanı hesaplanabilmektedir.

Bu noktada elde edilen puan anket madde cevaplarında kullanılan 0-2 aralığında olacaktır. Puan aralığı 0-100 aralığına indirgenecek olursa kullanılması gereken formül aşağıdaki şekilde olacaktır.

$$BGYSP100 = 0{,}071\ x\ 50\ x \sum_{KAP_m=1}^{14} KAP_m \qquad (6.20)$$

Eş.6.20.' de görüldüğü gibi regresyon analizi sonucunda elde edilen katsayılar ile bütün katılımcıların bütün BGYS amaçlarından alabileceği 0-100 aralığına indirgenmiş puanı hesaplanabilmektedir.

Çizelge 6.39.' da 452 katılımcı için hesaplanan Genel BGYS Puanları görülmektedir.

Çizelge 6.39. Katılımcıların tamamına ait ISO/IEC amaç BGYS puanları

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	**m**	**n**	**o**	**KAP_m**	**BGYSP**	**BGYSP100**
Bilgi Güvenliği Politikaları	1	1-8	1-452	0,105088	0,007461	0,373
Bilgi Güvenliği Organizasyonu	2	1-12	1-452	0,065634	0,004660	0,233
İnsan Kaynakları Güvenliği	3	1-15	1-452	0,134513	0,009550	0,478
Varlık Yönetimi	4	1-18	1-452	0,331858	0,023562	1,178
Erişim Kontrolü	5	1-25	1-452	0,099469	0,007062	0,353
Kriptografi	6	1-5	1-452	0,394690	0,028023	1,401
Fiziksel ve Çevresel Güvenlik	7	1-42	1-452	0,100927	0,007166	0,358
İşletim Güvenliği	8	1-42	1-452	0,213654	0,015169	0,758
Haberleşme Güvenliği	9	1-22	1-452	0,318986	0,022648	1,132
Sistem Temini, Geliştirme ve Bakımı	10	1-47	1-452	0,139145	0,009879	0,494
Tedarikçi İlişkileri	11	1-18	1-452	0,114553	0,008133	0,407
Bilgi Güvenliği İhlal Olayı Yönetimi	12	1-14	1-452	0,187105	0,013284	0,664
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	13	1-12	1-452	0,206490	0,014661	0,733
Uyum	14	1-14	1-452	0,512010	0,036353	1,818
TOPLAM					0,207613	10,381

Herhangi bir katılımcının, katılımcıların tamamı ile kıyaslanması hukuk bürosunun tek başına hesaplanacak BGYS Puanı ile yapılabilecektir.

Örneğin 30 sıra numaralı katılımcı ile anketi yanıtlayan tüm katılımcılar arasında bir kıyaslama yapılmak istenirse, katılımcıların tamamı ve 30 sıra numaralı katılımcı için hesaplanan BGYS Puanları kullanılabilecektir.

Çizelge 6.40. 30 Sıra numaralı katılımcıya ait ISO/IEC 27001 amaç BGYS puanları

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	**m**	**n**	**o**	**$KAP_{m.30}$**	**$BGYSP_{30}$**	**$BGYSP100_{30}$**
Bilgi Güvenliği Politikaları	1	1-8	30	0,000000	0,000000	0,000
Bilgi Güvenliği Organizasyonu	2	1-12	30	0,000000	0,000000	0,000
İnsan Kaynakları Güvenliği	3	1-15	30	0,000000	0,000000	0,000
Varlık Yönetimi	4	1-18	30	0,500000	0,035500	1,775
Erişim Kontrolü	5	1-25	30	0,000000	0,000000	0,000
Kriptografi	6	1-5	30	0,000000	0,000000	0,000
Fiziksel ve Çevresel Güvenlik	7	1-42	30	0,000000	0,000000	0,000
İşletim Güvenliği	8	1-42	30	0,309524	0,021976	1,099
Haberleşme Güvenliği	9	1-22	30	0,318182	0,022591	1,130
Sistem Temini, Geliştirme ve Bakımı	10	1-47	30	0,000000	0,000000	0,000
Tedarikçi İlişkileri	11	1-18	30	0,000000	0,000000	0,000
Bilgi Güvenliği İhlal Olayı Yönetimi	12	1-14	30	0,428571	0,030429	1,521
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	13	1-12	30	0,000000	0,000000	0,000
Uyum	14	1-14	30	1,785714	0,126786	6,339
TOPLAM					0,237281	11,864

Çizelge 6.39. ve Çizelge 6.40. birlikte incelendiğinde, 452 katılımcının BGYS Puanı (10,381) ile 30 sıra numarasındaki katılımcının BGYS Puanı (11.864) karşılaştırıldığında, 30 sıra numaralı katılımcının BGYS puanının daha yüksek olduğu görülmüştür.

Çizelge 6.39. ve Çizelge 6.40. birlikte incelendiğinde, 30 sıra numaralı katılımcının her ne kadar BGYS Puanı, tüm katılımcıların puanından yüksek olsa da, 14 alt amacın dokuzundan hiç puan alamadığı, puan aldığı alt amaçlardan ise Haberleşme Güvenliği amacında, tüm katılımcılara kıyasla daha düşük puana sahip olduğu görülmüştür.

Benzer şekilde 452 katılımcı arasında herhangi iki katılımcının kıyaslanması bu hukuk bürolarının ayrı ayrı hesaplanacak BGYS Puanı ile yapılabilecektir.

Örneğin 30 sıra numaralı katılımcı ile 50 sıra numaralı katılımcı arasında bir kıyaslama yapılmak istenirse, 30 sıra numaralı katılımcı için hesaplanan BGYS puanı ile 50 sıra numaralı katılımcı için hesaplanan BGYS Puanları kullanılabilecektir.

Çizelge 6.41. 50 Sıra numaralı katılımcıya ait ISO/IEC 27001 amaç BGYS puanları

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	**m**	**n**	**o**	**$KAP_{m.50}$**	**$BGYSP_{50}$**	**$BGYSP100_{50}$**
Bilgi Güvenliği Politikaları	1	1-8	50	0,000000	0,000000	0,000
Bilgi Güvenliği Organizasyonu	2	1-12	50	0,000000	0,000000	0,000
İnsan Kaynakları Güvenliği	3	1-15	50	0,000000	0,000000	0,000
Varlık Yönetimi	4	1-18	50	0,055556	0,003944	0,197
Erişim Kontrolü	5	1-25	50	0,240000	0,017040	0,852
Kriptografi	6	1-5	50	0,800000	0,056800	2,840
Fiziksel ve Çevresel Güvenlik	7	1-42	50	0,309524	0,021976	1,099
İşletim Güvenliği	8	1-42	50	0,809524	0,057476	2,874
Haberleşme Güvenliği	9	1-22	50	0,363636	0,025818	1,291
Sistem Temini, Geliştirme ve Bakımı	10	1-47	50	0,553191	0,039277	1,964

Çizelge 6.41. (devam) 50 Sıra numaralı katılımcıya ait ISO/IEC 27001 amaç BGYS puanları

Tedarikçi İlişkileri	11	1-18	50	0,777778	0,055222	2,761
Bilgi Güvenliği İhlal Olayı Yönetimi	12	1-14	50	0,000000	0,000000	0,000
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	13	1-12	50	0,000000	0,000000	0,000
Uyum	14	1-14	50	1,642857	0,116643	5,832
TOPLAM					0,394197	19,710

Çizelge 6.40. ve Çizelge 6.41. birlikte incelendiğinde, 30 sıra numaralı katılımcının BGYS Puanı (11,864) ile 50 sıra numaralı katılımcının BGYS Puanı (19,710) karşılaştırıldığında, 50 sıra numaralı katılımcının BGYS Puanının daha yüksek olduğu, Kriptografi, Fiziksel ve Çevresel Güvenlik ile Sistem Temini, Geliştirme ve Bakımı amaçlarında 30 sıra numaralı katılımcıya kıyasla daha yüksek puanlara sahip olduğu görülmüştür.

7. SONUÇ VE ÖNERİLER

Bu bölümde, anket katılımcılarının regresyon analizi sonucu elde edilen BGYSP100 puanları her bir ISO/IEC 27001 BGYS amacı için değerlendirilmiş, her bir araştırma problemi açısından bu puanlar değerlendirilmiş, güçlendirici ve tamamlayıcı iki farklı model ortaya koyulmuştur. Son olarak bu model, anket katılımcısı herhangi bir hukuk bürosu açısından test edilmiştir.

7.1. Katılımcıların BGYSP100 Puanlarının Değerlendirilmesi

Çizelge 7.1.' de görüleceği üzere katılımcıların BGYSP puanları 0,233 ile 1,818 arasındadır. BGYSP' lerin toplamı ile elde edilen BGYSP100 puanının ise 10,381 olduğu hesaplanmıştır.

BGYSP puanları 0-2 aralığında değerlendirilmesi gereken puanlar olmakla birlikte, 1,818 puanla en yüksek amaç değerinin "Uyum" amacına ait olduğu görülmüştür. Bu amacın alt amaçları olan "Yasal ve sözleşmeye tabi gereksinimlerle uyum" ve "Bilgi güvenliği gözden geçirmeleri" ile birlikte değerlendirildiğinde, hukuk bürolarının, yasal mevzuat uyumlulukları ve veri gizliliği sorumluluklarından dolayı bu amaca ait puanlarının, diğer amaçlardan çok daha yüksek olduğu değerlendirilmiştir.

En düşük BGYSP olan 0,233 puanının "Bilgi Güvenliği Organizasyonu" amacına ait olduğu görülmüştür. Bu amacın alt amaçları olan "İç organizasyon" ve "Mobil cihazlarla uzaktan çalışma" ile birlikte değerlendirildiğinde, hukuk bürolarından belirli bir yönetim hiyerarşisinin olmaması, büroda çalışan avukatların birbirine denk olması, elektronik imza kullanımı nedeni ile büro faaliyetlerinin büro içinden veya herhangi bir yerden, büro ağına bağlanma gereksinimi olmadan yapılabiliyor olması nedenlerinden dolayı bu amaca ait puanlarının, diğer amaçlardan çok daha düşük olduğu değerlendirilmiştir.

Ancak, 0-100 aralığına indirgenmiş BGYSP100 puanının 10,381' de kalması, hukuk bürolarının, ISO/IEC 27001 BGYS açısından oldukça yetersiz olduğunu göstermektedir.

Çizelge 7.1. Katılımcıların tamamına ait ISO/IEC amaç BGYS puanları

ISO/IEC 27001 Kontrol Amaçları ve Alt Amaçları	M	n	o	KAP_m	BGYSP	BGYSP100
Bilgi Güvenliği Politikaları	1	1-8	1-452	0,105088	0,007461	0,373
Bilgi Güvenliği Organizasyonu	2	1-12	1-452	0,065634	0,004660	0,233
İnsan Kaynakları Güvenliği	3	1-15	1-452	0,134513	0,009550	0,478
Varlık Yönetimi	4	1-18	1-452	0,331858	0,023562	1,178
Erişim Kontrolü	5	1-25	1-452	0,099469	0,007062	0,353
Kriptografi	6	1-5	1-452	0,394690	0,028023	1,401
Fiziksel ve Çevresel Güvenlik	7	1-42	1-452	0,100927	0,007166	0,358
İşletim Güvenliği	8	1-42	1-452	0,213654	0,015169	0,758
Haberleşme Güvenliği	9	1-22	1-452	0,318986	0,022648	1,132
Sistem Temini, Geliştirme ve Bakımı	10	1-47	1-452	0,139145	0,009879	0,494
Tedarikçi İlişkileri	11	1-18	1-452	0,114553	0,008133	0,407
Bilgi Güvenliği İhlal Olayı Yönetimi	12	1-14	1-452	0,187105	0,013284	0,664
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	13	1-12	1-452	0,206490	0,014661	0,733
Uyum	14	1-14	1-452	0,512010	0,036353	1,818
ORTALAMA						**0,741**
TOPLAM					0,207613	**10,381**

7.2. Araştırma Problemlerinin Değerlendirilmesi

Araştırma Problemi 1 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Politikaları - Bilgi Güvenliği İçin Yönetimin Yönlendirmesi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi güvenliği için, iş gereksinimleri ve ilgili yasalar ve düzenlemelere göre yönetimin yönlendirmesi ve desteğini sağlanmasını öngören bu alt amaç ile büroda çalışan personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, anlaşmalı teknik destek alınan tedarikçilerin varlığı ve bürodaki kablolu bilgisayar ağlarına misafirlerin bağlantı yapmasına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Bilgi Güvenliği Politikaları amacına bağlı tek alt amaç Bilgi Güvenliği İçin Yönetimin Yönlendirmesi düzeyidir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Bilgi Güvenliği Politikaları amacının puanı 0,373 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 2 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Organizasyonu - İş Organizasyon" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Kuruluş içerisinde bilgi güvenliği operasyonu ve uygulamasının başlatılması ve kontrol edilmesi amacıyla bir yönetim çerçevesi kurulmasını öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, kablolu ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 3 "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği Organizasyonu - Mobil Cihazlar ve Uzaktan Çalışma" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Uzaktan çalışma ve mobil cihazların güvenliğini sağlamayı öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, özel bir paket program kullanılıp kullanılmaması, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Bilgi Güvenliği Organizasyonu amacına bağlı iki alt amaç İş Organizasyon ve Mobil Cihazlar ve Uzaktan Çalışma düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Bilgi Güvenliği Organizasyonu amacının puanı 0,233 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 4 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - İstihdam Öncesi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Çalışanlar ve yüklenicilerin kendi sorumluluklarını anlamalarını ve düşünüldükleri roller için uygun olmalarını temin etmeyi öngören bu alt amaç ile büroda çalışan personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile yazıcı sayısı, ağda mobil cihazlar kullanılıp kullanılmaması, özel bir paket program kullanılıp kullanılmaması, web sitesinin varlığı, misafirlerin kablosuz ağa bağlanmalarına izin verilip verilmemesinin arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 5 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - Çalışma Esnasında" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Çalışanların ve yüklenicilerin bilgi güvenliği sorumluluklarının farkında olmalarını ve yerine getirmelerini temin etmeyi öngören bu alt amaç ile büroda çalışan yardımcı personel sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, özel bir paket program kullanılıp kullanılmaması, kablolu ve kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 6 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İnsan Kaynakları Güvenliği - İstihdamın Sonlandırılması ve Değiştirilmesi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

İstihdamın sonlandırılması ve değiştirilmesi prosesinin bir parçası olarak kuruluşun çıkarlarını korumayı öngören bu alt amaç ile büroda çalışan avukat ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile yazıcı

sayısı, misafirlerin kablosuz ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de İnsan Kaynakları Güvenliği amacına bağlı üç alt amaç İstihdam Öncesi, Çalışma Esnasında ve İstihdamın Sonlandırılması ve Değiştirilmesi düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, İnsan Kaynakları Güvenliği amacının puanı 0,478 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 7 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Varlıkların Sorumluluğu" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Kuruluşun varlıklarını tespit etmek ve uygun koruma sorumluluklarını tanımlamayı öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 8 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Bilgi Sınıflandırması" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilginin kurum için önemi derecesinde uygun seviyede korunmasını temin etmeyi öngören bu alt amaç ile büroda çalışan personel sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile ağda kişisel mobil cihazlara izin verilip verilmemesi, özel bir paket program kullanılıp kullanılmaması, anlaşmalı teknik destek alınan tedarikçilerin varlığı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 9 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Varlık Yönetimi - Ortam İşleme" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Ortamda depolanan bilginin yetkisiz ifşası, değiştirilmesi, kaldırılması ve yok edilmesini engellemeyi öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile ağda

kişisel mobil cihazlara izin verilip verilmemesi, web sitesinin varlığı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Varlık Yönetimi amacına bağlı üç alt amaç Varlıkların Sorumluluğu, Bilgi Sınıflandırması ve Ortam İşleme düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Varlık Yönetimi amacının puanı 1,178 olup, amaçlara ait ortalama puan olan 0,741' den yüksek olması nedeni ile yeterli olduğu değerlendirilmiştir.

Araştırma Problemi 10 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Erişim Kontrolünün İş Gereklilikleri" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi ve bilgi işleme olanaklarına erişimi kısıtlamayı öngören bu alt amaç ile büroda çalışan avukat ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, ağda kişisel mobil cihazlara izin verilip verilmemesi, kablolu ve kablosuz ağ kullanımı, misafirlerin kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 11 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Kullanıcı Erişim Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Yetkili kullanıcı erişimini temin etmek ve sistem ve hizmetlere yetkisiz erişimi engellemeyi öngören bu alt amaç ile büroda çalışan avukat sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, özel bir paket program kullanılıp kullanılmaması, web sitesinin varlığı, kablolu ağ kullanımı, misafirlerin kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 12 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Kullanıcı Sorumlulukları" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Kullanıcıları kendi kimlik doğrulama bilgilerinin korunması konusunda sorumlu tutmayı öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile web sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 13 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Erişim Kontrolü - Sistem ve Uygulama Erişim Kontrolü" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Sistem ve uygulamalara yetkisiz erişimi engellemeyi öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Erişim Kontrolü amacına bağlı dört alt amaç Erişim Kontrolünün İş Gereklilikleri, Kullanıcı Erişim Yönetimi, Kullanıcı Sorumlulukları ve Sistem ve Uygulama Erişim Kontrolü düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Erişim Kontrolü amacının puanı 0,353 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 14 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Kriptografi - Kriptografik Kontroller" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilginin gizliliği, aslına uygunluğu ve/veya bütünlüğü 'nün korunması için kriptografi' nin doğru ve etkin kullanımın temin etmeyi öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, özel bir paket program kullanılıp kullanılmaması, web sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablosuz ağ kullanımı, misafirlerin

kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Kriptografi amacına bağlı tek alt amaç Kriptografik Kontroller düzeyidir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Kriptografi amacının puanı 1,401 olup, amaçlara ait ortalama puan olan 0,741' den yüksek olması nedeni ile yeterli olduğu değerlendirilmiştir.

Araştırma Problemi 15 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Fiziksel ve Çevresel Güvenlik - Güvenli Alanlar" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Yetkisiz fiziksel erişimi, kuruluşun bilgi ve bilgi işleme olanaklarına hasar verilmesi ve müdahale edilmesini engellemeyi öngören bu alt amaç ile büroda çalışan personel sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile yazıcı sayısı, ağda kişisel mobil cihazlara izin verilip verilmemesi, web sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, kablolu ağ kullanımı, misafirlerin kablolu ve kablosuz ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 16 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Fiziksel ve Çevresel Güvenlik - Teçhizat" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Varlıkların kaybedilmesi, hasar görmesi, çalınması veya ele geçirilmesini ve kuruluşun faaliyetlerinin kesintiye uğramasını engellemeyi öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, kablolu ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Fiziksel ve Çevresel Güvenlik amacına bağlı iki alt amaç Güvenli Alanlar ve Sistem ve Teçhizat düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Fiziksel ve Çevresel Güvenlik

amacının puanı 0,358 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 17 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - İşlem Prosedürleri ve Sorumlulukları" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır

Bilgi işleme olanaklarının doğru ve güvenli işletimlerini temin etmeyi öngören bu alt amaç ile büroda çalışan avukat sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, özel bir paket program kullanılıp kullanılmaması, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablolu ağ kullanımı, misafirlerin kablosuz ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 18 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Kötücül Yazılımlardan Koruma" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi ve bilgi işleme olanaklarının kötücül yazılımlardan korunmasını temin etmeyi öngören bu alt amaç ile büroda çalışan avukat ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile yazıcı sayısı, ağda mobil cihazlar kullanılıp kullanılmaması, ağda kişisel mobil cihazlara izin verilip verilmemesi, web sitesinin varlığı, misafirlerin kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 19 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Yedekleme" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Veri kaybına karşı koruma sağlamayı öngören bu alt amaç ile büroda çalışan avukat sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile yazıcı sayısı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablosuz ağ kullanımı, misafirlerin kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 20 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Kaydetme ve İzleme" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Olayları kaydetme ve kanıt üretmeyi öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile web sitesinin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablolu ve kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 21 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - İşletimsel Yazılımın Kontrolü" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

İşletimsel sistemlerin bütünlüğünü temin etmeyi öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile web sitesinin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 22 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Teknik Açıklık Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır

Teknik açıklıkların kullanılmasını engellemeyi öngören bu alt amaç ile büroda çalışan avukat sayısı arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, web sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, misafirlerin kablolu ve kablosuz ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 23 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İşletim Güvenliği - Bilgi Sistemleri Tetkik Hususları" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Tetkik faaliyetlerinin işletimsel sistemler üzerindeki etkilerini asgariye indirmeyi öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olmadığı görülmüştür. Ayrıca, bu alt amaç ile yazıcı sayısı, web

sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de İşletim Güvenliği amacına bağlı yedi alt amaç İşlem Prosedürleri ve Sorumlulukları, Kötücül Yazılımlardan Koruma, Yedekleme, Kaydetme ve İzleme, İşletimsel Yazılımın Kontrolü, Teknik Açıklık Yönetimi ve Bilgi Sistemleri Tetkik Hususları düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, İşletim Güvenliği amacının puanı 0,758 olup, amaçlara ait ortalama puan olan 0,741' den yüksek olması nedeni ile yeterli olduğu değerlendirilmiştir.

Araştırma Problemi 24 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Haberleşme Güvenliği - Ağ Güvenliği Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Ağdaki bilgi ve destekleyici bilgi işleme olanaklarının korunmasını sağlamayı öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, ağda kişisel mobil cihazlara izin verilip verilmemesi, web sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 25 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Haberleşme Güvenliği - Bilgi Transferi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bir kuruluş içerisinde ve herhangi bir dış varlık arasında transfer edilen bilginin güvenliğini sağlamayı öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, anlaşmalı teknik destek alınan tedarikçilerin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Haberleşme Güvenliği amacına bağlı iki alt amaç Ağ Güvenliği Yönetimi ve Bilgi Transferi düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının

BGYSP100 puanı olan 10,381 içerisinde, Haberleşme Güvenliği amacının puanı 1,132 olup, amaçlara ait ortalama puan olan 0,741' den yüksek olması nedeni ile yeterli olduğu değerlendirilmiştir.

Araştırma Problemi 26 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Bilgi Sistemlerinin Güvenlik Gereksinimleri" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dahili bir parçası olmasını sağlamayı öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olmadığı görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, özel bir paket program kullanılıp kullanılmaması, web sitesinin varlığı, kablolu ağ kullanımı, misafirlerin kablosuz ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 27 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Geliştirme ve Destek Süreçlerinde Güvenlik" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi güvenliğinin bilgi sistemleri geliştirme yaşam döngüsü içerisinde tasarlanıyor ve uygulanıyor olmasını sağlamayı öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olmadığı görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, ağda mobil cihazlar kullanılıp kullanılmaması, web sitesinin varlığı, anlaşmalı teknik destek alınan tedarikçilerin varlığı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 28 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Sistem Temini, Geliştirme ve Bakımı - Test Verisi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Test için kullanılan verinin korunmasını sağlamayı öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Sistem Temini, Geliştirme ve Bakımı amacına bağlı üç alt amaç Bilgi Sistemlerinin Güvenlik Gereksinimleri, Geliştirme ve Destek Süreçlerinde Güvenlik ve Test Verisi düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Sistem Temini, Geliştirme ve Bakımı amacının puanı 0,494 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 29 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Tedarikçi İlişkileri - Tedarikçi İlişkilerinde Bilgi Güvenliği" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Kuruluşa ait tedarikçiler tarafından erişilen varlıkların korunmasını sağlamayı öngören bu alt amaç ile büroda çalışan personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile anlaşmalı teknik destek alınan tedarikçilerin varlığı, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablolu ve kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 30 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Tedarikçi İlişkileri - Tedarikçi Hizmet Sağlama Yöntemi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Tedarikçi anlaşmalarıyla uyumlu olarak kararlaştırılan seviyede bir bilgi güvenliğini ve hizmet sunumunu sürdürmeyi öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile ağda kişisel mobil cihazlara izin verilip verilmemesi, özel bir paket program kullanılıp kullanılmaması, kablolu ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Tedarikçi İlişkileri amacına bağlı iki alt amaç Tedarikçi İlişkilerinde Bilgi Güvenliği ve Tedarikçi Hizmet Sağlama Yöntemi düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Tedarikçi İlişkileri amacının puanı 0,407 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 31 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Bilgi Güvenliği İhlal Olayı Yönetimi - Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi güvenliği ihlal olaylarının yönetimine, güvenlik olayları ve açıklıklar üzerindeki bağlantısını da içeren, tutarlı ve etkili yaklaşımın uygulanmasını sağlamayı öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, ağda mobil cihazlar kullanılıp kullanılmaması, web sitesinin varlığı, misafirlerin kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Bilgi Güvenliği İhlal Olayı Yönetimi amacına bağlı tek alt amaç Bilgi Güvenliği İhlal Olaylarının ve İyileştirilmelerin Yönetimi düzeyidir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Bilgi Güvenliği İhlal Olayı Yönetimi amacının puanı 0,664 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 32 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Bilgi Güvenliği Sürekliliği" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi güvenliği sürekliliği, kuruluşun iş sürekliliği yönetim sistemlerinin içerisine dahil edilmesini öngören bu alt amaç ile büroda çalışan avukat, personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, ağda kişisel mobil cihazlara izin verilip verilmemesi, kablosuz ağ kullanımı, misafirlerin kablosuz ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 33 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Yedek Fazlalıklar" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Bilgi işleme olanaklarının erişilebilirliğini temin etmeyi öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, ağda mobil cihazlar kullanılıp kullanılmaması, kablosuz ağ kullanımı arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları amacına bağlı iki alt amaç Bilgi Güvenliği Sürekliliği ve Yedek Fazlalıklar düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, İş Sürekliliği Yönetiminin Bilgi Güvenliği amacının puanı 0,733 olup, amaçlara ait ortalama puan olan 0,741' den düşük olması nedeni ile yetersiz olduğu değerlendirilmiştir.

Araştırma Problemi 34 açısından "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Uyum - Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır.

Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemeyi öngören bu alt amaç ile büroda çalışan personel ve yardımcı personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, özel bir paket program kullanılıp kullanılmaması, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablosuz ağ kullanımı, arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

Araştırma Problemi 35 "Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre "Uyum - Bilgi Güvenliği Gözden Geçirmeleri" düzeyleri anlamlı farklılaşmakta mıdır?" sorusuna yanıt aranmıştır

Bilgi güvenliğinin kurumsal politika ve prosedürler uyarınca gerçekleştirilmesini ve yürütülmesini sağlamayı öngören bu alt amaç ile büroda çalışan avukat ve personel sayıları arasında anlamsal farklılıklar olduğu görülmüştür. Ayrıca, bu alt amaç ile bilgisayar sayısı, yazıcı sayısı, ağda kişisel mobil cihazlara izin verilip verilmemesi, güvenlik konusunda danışmanlık alınan tedarikçilerin varlığı, kablolu ağ kullanımı, misafirlerin kablolu ağa bağlanmalarına izin verilip verilmemesi arasında da anlamsal farklılıklara sahip olduğu görülmüştür.

ISO/IEC 27001 BGYS' de Uyum amacına bağlı iki alt amaç Yasal ve Sözleşmeye Tabi Gereksinimlerle Uyum ve Bilgi Güvenliği Gözden Geçirmeleri düzeyleridir. Çizelge 7.1' de görüleceği üzere hukuk bürolarının BGYSP100 puanı olan 10,381 içerisinde, Uyum amacının puanı 1,818 olup, amaçlara ait ortalama puan olan 0,741' den yüksek olması nedeni ile yeterli olduğu değerlendirilmiştir.

Hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre, anlamsal farklılık gösteren ISO/IEC 27001 BGYS alt amaç sayıları incelendiğinde;

- Bürodaki çalışan avukat sayısı' na göre, 25 alt amacın,
- Bürodaki çalışan personel sayısı' na göre, 24 alt amacın,
- Bürodaki çalışan yardımcı personel sayısına göre, 18 alt amacın,
- Büroda kullanılan bilgisayar sayısına göre, 21 alt amacın,
- Büroda kullanılan yazıcı sayısına göre, 17 alt amacın,
- Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıp kullanılmamasına göre, 5 alt amacın,
- Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verilip verilmemesine göre, 9 alt amacın,
- Büro ve avukatlık hizmetleri için kullanılan özel bir paket program olup olmamasına göre, 10 alt amacın,
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmamasına göre, 16 alt amacın,
- Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetlerin alındığı anlaşmalı bir tedarikçi olup olmamasına göre, 14 alt amacın,
- Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi olup olmamasına göre, 10 alt amacın,
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmamasına göre, 16 alt amacın,
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmamasına göre, 16 alt amacın,
- Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre, 12 alt amacın,
- Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin verilip verilmemesine göre, 6 alt amacın,

anlamsal farklılık gösterdiği görülmüştür.

7.3. Hukuk Büroları İçin ISO/IEC 27001 BGYS Uyumlu BGYS Modeli

Araştırma Problemi 36 "ISO/IEC 27001 içerisinde yer alan 14 Amaç düzeyinde hukuk büroları için optimal bir BGYS modeli ortaya koyulabilir mi?" sorusuna yanıt aranmıştır.

Hukuk bürolarının, ISO/IEC 27001 BGYS amaçlarından aldıkları BGYSP100 puanlarının kendi içerisinde ortalamaları ile karşılaştırılmaları sonucunda yeterli ve yetersiz oldukları amaçların aşağıdakiler oldukları tespit edilmiştir.

Yeterli olunan amaçlar

- Varlık Yönetimi
- Kriptografi
- İşletim Güvenliği
- Haberleşme Güvenliği
- Uyum

Yetersiz olunan amaçlar

- Bilgi Güvenliği Politikaları
- Bilgi Güvenliği Organizasyonu
- İnsan Kaynakları Güvenliği
- Erişim Kontrolü
- Fiziksel ve Çevresel Güvenlik
- Sistem Temini, Geliştirme ve Bakımı
- Tedarikçi İlişkileri
- Bilgi Güvenliği İhlal Olayı Yönetimi
- İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları

Diğer taraftan, alt amaç seviyesinde incelenen hukuk bürolarının İnsan Kaynakları, BTE ve BTİ özelliklerine göre de, ISO/IEC 27001 BGYS alt amaç sayılarının da değişken olduğu görülmekle birlikte, toplamda 35 alt amacın kriter olarak en az 15' i ile anlamsal bir ilişkinin

varlığı aranacak olursa, İnsan Kaynakları, BTE ve BTİ özelliklerine ilişkin olarak aşağıdaki özelliklerin öncelikli olarak dikkate alınması gerektiği görülecektir.

- Bürodaki çalışan avukat sayısı
- Bürodaki çalışan personel sayısı
- Bürodaki çalışan yardımcı personel sayısı
- Büroda kullanılan bilgisayar sayısı
- Büroda kullanılan yazıcı sayısı
- Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmaması
- Büroda kablolu bilgisayar ağı kullanılıp kullanılmaması
- Büroda kablosuz bilgisayar ağı kullanılıp kullanılmaması

Hukuk bürolarının ISO/IEC 27001 BGYS amaçlarına göre hesaplanan BGYSP100 puanlarının 0-100 aralığı için 10,381 gibi oldukça düşük bir seviyede kalmış olmasından dolayı, yeterliliklerinin artırılması için iki farklı bakış açısı geliştirilmiştir.

Birincisi, hukuk bürolarının, BGYSP puanı ortalamasına göre yeterli oldukları amaçlardan aldıkları BGYSP puanlarının artırılmasının amaçlanmasıdır.

İkincisi ise hukuk bürolarının, BGYSP puanı ortalamasına göre yetersiz oldukları amaçlardan aldıkları BGYSP puanlarının artırılmasıdır.

7.3.1. Güçlendirici model ve öneriler

Bu modelde, BGYSP puanları, ortalama BGYSP puanlarından düşük olan amaçların, amaçlarla anlamsal farklılık gösteren İnsan Kaynakları, BTE ve BTİ özelliklerine öncelik verilerek yükseltilmesi öngörülmüştür.

Bu amaçlar, Varlık Yönetimi, Kriptografi, İşletim Güvenliği, Haberleşme Güvenliği ve Uyum amaçları ile 15 ve üzeri amaçla anlamsal farklılığa sahip İnsan Kaynakları, BTE ve BTİ özellikleri arasındaki ilişki incelenmiş ve amaca ait alt amaç sayıları açısından değerlendirilmiştir.

Çizelge 7.2. 15 ve üzeri alt amaç ile anlamsal farklılığa sahip insan kaynakları, BTE ve BTİ özellikleri ile ortalama BGYSP puanına göre yeterli olunan ISO/IEC amaç ve alt amaç sayılarının incelenmesi

	Bürodaki çalışan avukat sayısı	Bürodaki çalışan personel sayısı	Bürodaki çalışan yardımcı personel sayısı	Büroda kullanılan bilgisayar sayısı	Büroda kullanılan yazıcı sayısı	Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmaması	Büroda kablolu bilgisayar ağı kullanılıp kullanılmaması	Büroda kablosuz bilgisayar ağı kullanılıp kullanılmaması
Varlık Yönetimi	2/3	3/3	2/3	1/3	-/3	1/3	-/3	1/3
Kriptografi	1/1	1/1	1/1	1/1	-/1	1/1	-/1	1/1
İşletim Güvenliği	4/5	2/5	-/5	1/5	2/5	4/5	1/5	3/5
Haberleşme Güvenliği	2/2	2/2	1/2	2/2	1/2	1/2	-/2	1/2
Uyum	1/2	2/2	1/2	1/2	2/2	-/2	1/2	1/2

Güçlendirici modelde, hukuk büroları için, Çizelge 7.2. incelendiğinde;

- Varlık Yönetimi amacı için öncelikli olarak büroda kullanılan yazıcı sayısı ve kablolu ağ kullanımı, ikincil öncelikli olarak büro web sitesi ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Kriptografi amacı için öncelikli olarak, büroda kullanılan yazıcı sayısı ve kablolu ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- İşletim Güvenliği amacı için büroda çalışan yardımcı personel sayısı, ikincil öncelikli olarak, büroda kullanılan yazıcı sayısı ve kablolu ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Haberleşme Güvenliği amacı için öncelikli olarak, büroda kablolu ağ kullanımı, ikincil öncelikli olarak büroda çalışan yardımcı personel sayısı, büroda kullanılan

yazıcı sayısı, büro web sitesi ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.

- Uyum amacı için öncelikli olarak, büro web sitesi, ikincil öncelikli olarak büroda çalışan avukat sayısı, yardımcı personel sayısı, kablolu ağ kullanımı ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.

7.3.2. Tamamlayıcı model ve öneriler

Bu modelde, BGYSP puanları, ortalama BGYSP puanlarından düşük olan amaçların, amaçlarla anlamsal farklılık gösteren İnsan Kaynakları, BTE ve BTİ özelliklerine öncelik verilerek yükseltilmesi öngörülmüştür.

Çizelge 7.3. 15 ve üzeri alt amaç ile anlamsal farklılığa sahip insan kaynakları, BTE ve BTİ özellikleri ile ortalama BGYSP puanına göre yetersiz olunan ISO/IEC amaç ve alt amaç sayılarının incelenmesi

	Bürodaki çalışan avukat sayısı	Bürodaki çalışan personel sayısı	Bürodaki çalışan yardımcı personel sayısı	Büroda kullanılan bilgisayar sayısı	Büroda kullanılan yazıcı sayısı	Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi olup olmaması	Büroda kablolu bilgisayar ağı kullanılıp kullanılmaması	Büroda kablosuz bilgisayar ağı kullanılıp kullanılmaması
Bilgi Güvenliği Politikaları	-/1	1/1	1/1	1/1	-/1	-/1	-/1	-/1
Bilgi Güvenliği Organizasyonu	2/2	2/2	1/2	2/2	2/2	-/2	1/2	1/2
İnsan Kaynakları Güvenliği	1/3	1/3	3/3	1/3	3/3	1/3	-/3	1/3
Erişim Kontrolü	4/4	2/4	2/4	3/4	1/4	2/4	2/4	3/4
Fiziksel ve Çevresel Güvenlik	1/2	2/2	1/2	1/2	2/2	1/2	2/2	-/2
Sistem Temini, Geliştirme ve Bakımı	1/3	1/3	-/3	3/3	2/3	2/3	1/3	-/3

Çizelge 7.3. (devam) 15 ve üzeri alt amaç ile anlamsal farklılığa sahip insan kaynakları, BTE ve BTİ özellikleri ile ortalama BGYSP puanına göre yetersiz olunan ISO/IEC amaç ve alt amaç sayılarının incelenmesi

Tedarikçi İlişkileri	1/2	2/2	2/2	-/2	-/2	-/2	1/2	2/2
Bilgi Güvenliği İhlal Olayı Yönetimi	1/1	1/1	1/1	1/1	-/1	1/1	-/1	-/1
İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	2/2	2/2	1/2	2/2	1/2	1/2	-/2	2/2

Tamamlayıcı modelde, hukuk büroları için, Çizelge 7.3. incelendiğinde;

- Bilgi Güvenliği Politikaları amacı için öncelikli olarak büroda çalışan avukat sayısı, yazıcı sayısı, kablolu ağ kullanımı, büro web sitesi, kablolu ağ kullanımı ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Bilgi Güvenliği Organizasyonu amacı için öncelikli olarak, büro web sitesi, ikincil öncelikli olarak büroda çalışan yardımcı personel sayısı, kablolu ağ kullanımı ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- İnsan Kaynakları Güvenliği amacı için öncelikli olarak, büroda kablolu ağ kullanımı, ikincil öncelikli olarak büroda çalışan personel sayısı, büroda kullanılan bilgisayar sayısı, büro web sitesi ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Erişim Kontrolü amacı için öncelikli olarak, büroda kullanılan yazıcı sayısı, ikincil öncelikli olarak büroda çalışan personel sayısı, yardımcı personel sayısı, büro web sitesi ve kablolu ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Fiziksel ve Çevresel Güvenlik amacı için öncelikli olarak, büroda kablosuz ağ kullanımı, ikincil öncelikli olarak, büroda çalışan avukat sayısı, yardımcı personel sayısı, kullanılan yazıcı sayısı ve büro web sitesi konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Sistem Temini, Geliştirme ve Bakımı amacı için öncelikli olarak, büroda çalışan yardımcı personel sayısı ve kablosuz ağ kullanımı, ikincil öncelikli olarak, büroda çalışan avukat sayısı, personel sayısı ve kablosuz ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.

- Tedarikçi ilişkileri amacı için öncelikli olarak, büroda kullanılan bilgisayar sayısı, yazıcı sayısı ve büro web sitesi, ikincil öncelikli olarak büroda çalışan avukat sayısı ve kablolu ağ kullanımı konularında BG' ne yönelik çalışma yapılması önerilmektedir.
- Bilgi Güvenliği İhlal Olayı Yönetimi amacı için öncelikli olarak, büroda kullanılan yazıcı sayısı, kablolu ağ kullanımı ve kablosuz ağ kullanımı BG' ne yönelik çalışma yapılması önerilmektedir.
- İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları amacı için öncelikli olarak, büroda kablolu ağ kullanımı, ikincil öncelikli olarak büroda çalışan yardımcı personel sayısı, kullanılan yazıcı sayısı ve büro web sitesi konularında BG' ne yönelik çalışma yapılması önerilmektedir.

KAYNAKLAR

1. Lopeaz, I.I.B., Caraguay, A.L.V., Vidal, J.V, Monge, M.A.S. ve Villalba, L.J.G. (2017). Towards Incidence Management in 5G Based on Situational Awareness, Future Internet, 9(1).
2. Semma, A. ve Motii, M. (2017). Towards a New Approach to Pooling COBIT 5 and ITIL V3 with ISO IEC 27002 for Better Use of ITG in the Morrocan Parliament, IJCSI International Journal of Computer Science Issues, 14(3), 49-58.
3. Song, K.. (2017, Ekim). Exploring the Factors Influencing the Adoption of ISMS Standards or Frameworks, Master's Degree Thesis, University of Dublin, Management of Information Systems, Dublin.
4. Dashti, S., Giorgini, P. ve Paja, E. (2017). Information Security Risk Management, IFIP International Federation for Information Processing, 18-33.
5. Khan, M.A. (2017). Efficacy of OCTAVE Risk Assessment Methodology in Information Systems Organizations, International Journal of Computer Applications Technology and Research, 6(6), 242-244.
6. Eloff, J.H.P., Labuschange, L. ve Badenhorst, K.P. (1993). A Comparative Framework for Risk Analysis Methods, Computer & Security, 12(1), 597-603.
7. Yazar, Z. (2002). A Qualitative Risk Analysis and Management Tool-CRAMM, SANS Institute.
8. Hong, K.S., Chi, Y.P., Chao, L.R. ve Tang, J.H. (2003). An Integrated System Theory of Information Security Management, Information Management & Computer Security, 11(5), 243-248.
9. Gautam, B. (2017, Haziran). Improving Information Technology (IT) Risk Analysis with Resource, Master's Degree Thesis, St. Cloud State University, Information Assurance, Minnesota, USA.
10. Mwambe, O.O. ve Echizen, I. (2017). Security Modeling Tool for Information Systems Security Oriented Malicious Activity Diagrams Meta Model Validation, MIS Review, 22(1-2), 57-91.
11. MUKAMA, J. (2016, Ocak). Risk Analysis as a Security Metric for Industrial Control Systems, Master's Degree Thesis, Chalmers University of Technology Department of Computer Science and Engineering, Gothenburg, Sweden.
12. Große, C. (2016). Towards an Integrated Framework for Quality and Information Security Management in Small Companies, Master's Degree Thesis, Luleå University of Technology Department of Computer Science, Electrical and Space Engineering, Luleå, Sweden.
13. Shojaie, B., Federrath, H. ve Saberi, I. (2016). The Effects of National Culture on the Implementation of ISM Standards based on the ISO 27001, Atiner Conference Paper Series No: COM2016-1986.
14. Ilvonen, A., Jussila, J.J. ve Kärkkäinen, H. (2016). Towards a Business-Driven Process Model for Knowledge Security Risk Management Making Sense of Knowledge Risks, International Journal of Knowledge Management, 11(4), 1-18.

15. Ali, F.A.B.H. ve Jali, M.Z. (2017). Human-Technology Centric In Cyber Security Maintenance for Digital Transformation ERA, 1st International Conference on Big Data and Cloud Computing (ICoBiC).
16. Almuhammadi, S. ve Alsaleh, M. (2017). Information Security Maturity Model for NIST Cyber Security Framework, Computer Science & Information Technology (CS & IT), 51-62.
17. Giulio, C.D., Kamhoua, C., Campbell, R.H., Sprabery, R., Kwiat, K. ve Bashir, M.N. (2017). IT Security and Privacy Standards in Comparison, 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 1090-1099.
18. Kovačević, S.M. (2018, Haziran). Smart Homes from a Risk Management Perspective, Master's Degree Thesis, University of Stavanger, Faculty of Science and Technology, Stavanger, Norway.
19. Wendy, Guwan, W. (2019). Measuring ınformation Security and Cyber Security on Private Cloud Computing, Journal of Theoretical and Applied Information Technology, 96(1), 156-168.
20. Ateş, V. (2016). Bilişim Teknolojileri Risk Yönetimi ve Yöntemleri Üzerine Bir Değerlendirme, 3th Yönetim Bilişim Sistemleri Konferansı, 1-14.
21. Mataracıoğlu, T. ve Özkan, S., (2011), Govering Information Security in Conjunction with COBIT and ISO 27001, International Journal of Network Security & Its Applications (IJNSA), 3(1).
22. Mataracıoğlu, T. ve Yıldırım, S.O. (2014). Obstructions of Turkish Public Organizations Getting ISO/IEC 27001 Certified, International Journal of Managing Value and Supply Chains (IJMVSC), 5(2).
23. Vahidnia, S., Tanrıöver, Ö.Ö. ve Askerzade, I.N. (2016). An Evaluation Study of General Software Project Risk Based on Software Practitioners Experiences, International Journal of Computer Science & Information Technology (IJCSIT), 8(6).
24. Eray, I.E. ve Pejas, J. (2017). A Graph-Based Risk Assessment and Prediction in IT Systems, Przegląd Elektrotechniczny, 91-95.
25. Stergiopoulos, G., Kouktzoglou, V., Theochridou, M. ve Gritzalis, D. (2017). A Process-Based Dependency Risk Analysis Methodology for Critical Infrastructures, Int. J. Critical Infrastructures.
26. Correia, A., Gonçalves, A. ve Teodoro M.F. (2017). A Model-Driven Approach to Information Security Compliance, AIP Conference Proceedings.
27. Lechner, N.H. (2017). An Overview of Cybersecurity Regulations and Standards for Medical Devices Software, Proceeding of the 28th Central European Conference on Information and Intelligent Systems, 237-249.
28. Olifer, D., Goranin, N., Kaceniauskas, A. ve Cenys, A. (2017). Controls-Based Approach for Evaluation of Information Security Standards Implementation Costs, Technological and Economic Development of Economy, 23(1), 196-219.
29. Moratta, A., Martinelli, F., Nanni, S. ve Orlando, A. (2017). Cyber-Insurance Survey, Computer Science Review.
30. Ghazouani, M., Medromi, H. ve MOUSSAID, L. (2017). Design and Implementation of a Comprehensive Information Security Risk Management Tool based on Multi-agents Systems, International Journal of Applied Information Systems (IJAIS), 12(7).

31. Granadillo, G.G., Dubus, S., Motzek, A., Alvarez, E., Merialdo, M., Papillon, S., Debar, H. ve Alfaro, J.G. (2017). Dynamic Risk Management Response System to Handle Cyber Threats, Computers and System Sciences.

32. Kurnianto, A., Isnanto, R. ve Widodo, A.P. (2018). Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs, E3S Web of Conferences (ICENIS).

33. Singh, U.K. ve Joshi, C. (2018). Comparative Study of Information Security Risk Assessment Frameworks, International Journal of Computer Application, 8(2), 82-89.

34. ETH Zürich. (2018, Ekim). National Cybersecurity and Cyberdefense Policy Snapshots, Center for Security Studies (CSS), Haldeneggsteig 4, Zürich, Switzerland.

35. Romero, S.M.R. ve Heredero, C.D.P. (2018). Data Protection by Design Organizational Integration, Harvard Deusto Business Research, 7(2), 60-71.

36. European Union Agency for Network and Information Security (ENISA). (2018, Kasım). Guidelines on Assessing DSP and OES Compliance to the NISD Security Requirements, Vassilika Vouton, 700 13, Heraklion, Greece.

37. European Union (EU). (2018, Şubat). Business, Technical and Organizational Evaluation, European Union.

38. European Union (EU). (2018). European Cybersecurity Centres of Expertise Map: Definition and Taxonomy, Publications Office of the European Union, Luxembourg.

39. Eugen, P. ve Petrut, D. (2018). Exploring the New Era of Cybersecurity Governance, Ovidius University Annals, Economic Sciences Series, 18(1), 358-363.

40. Singh, U.K. ve Joshi, C. (2018). Information Security Risk Management Framework for University Computing Enviroment, International Journal of Network Security, 19(5).

41. Yalçın, N. ve Kılıç, B., (2018), Information Security Risk Management and Risk Assessment Methodology and Tools, International Conference on Cyber Security and Computer Science (ICONCS'18).

42. National Institute of Standards and Technology (NIST). (2018, Kasım). 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, U.S. Department of Commerce, Gaithersburg, USA.

43. Schluga, O., Bauer, E., Bicaku, A., Maksuti, S., Tauber, M. ve Wöhrer, A. (2018). Operations Security Evaluation of IaaS-Cloud Backend for Industry 4.0, In Proceedings of the 8th International Conference on Cloud Computing and Services Science (CLOSER 2018), 392-399.

44. Hashim, N.A., Abidin, Z.Z., Zakaria, N.A. ve Ahmad, R. (2018). Risk Assessment Method for Insider Threats in Cyber Security A Review Security-A Review, (IJACSA) International Journal of Advanced Computer Science and Applications, 9(11), 126-130.

45. Almeida, L.M.S.T.D. (2018). Decision Support for Selecting Information Security Controls, Unıversıdade de Lisboa, Faculdade de Ciências, Departamento de Informática, Liboa, Portugal.

46. Hurttila, S. (2018). From Information Security to Cyber Security Management-ISO 27001 and 27032 Approach, Master's Degree Thesis, Tallinn University of Technology, School of Information Technology, Tallinn, Estonia.

47. Carnegie Mellon Universıty. (2018, Temmuz). Threat Modeling-A Summary of Available Methods, 4500 Fifth Avenue, Pittsburgh, USA.

48. Mamers, T. (2018, Ocak). The Art and Science of Information Security Investments For Small Enterprise, Master's Degree Thesis, Tallinn university of Technology, School of Information Technology, Tallinn, Estonia.

49. Internet: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), Biz Kimiz, URL: https://bilgem.tubitak.gov.tr/tr/kurumsal/biz-kimiz, Son Erişim Tarihi: 15.04.2019.

50. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi, Kocaeli.

51. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2015). DDOS (Servis Dışı Bırakma Saldırıları) İle Mücadele Kılavuzu, Kocaeli.

52. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2015). Ağ Mimarisi Güvenliği Kılavuzu, Kocaeli.

53. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2015). Web Sunucu (IIS 7.0 ve IIS 7.5) Güvenliği Kılavuzu, Kocaeli.

54. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2015). Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Kılavuzu, Kocaeli.

55. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2015). Erişim Kontrol Politikası Oluşturma Kılavuzu, Kocaeli.

56. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TUBİTAK) Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM). (2015). Sosyal Mühendislik: Zaafiyetler ve Korunma Yöntemleri Kılavuzu, Kocaeli.

57. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2015). ISO/IEC 27000, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Genel Bakış ve Sözlük, Ankara.

58. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27001, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler, Ankara.

59. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27002, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri, Ankara.

61. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2014). ISO/IEC 27005, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Risk Yönetimi, Ankara.

62. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2015). ISO/IEC 27006, Bilgi Teknolojisi - Güvenlik

Teknikleri - Bilgi Güvenliği Yönetim Sistemlerinin Tetkik ve Belgelendirmesini Yapan Kuruluşlar İçin Şartlar, Ankara.

63. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27007, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Kılavuz, Ankara.
64. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2015). ISO/IEC 27008, Bilgi Teknolojisi - Güvenlik Teknikleri - Denetçiler İçin Bilgi Güvenliği Kontrolleri Kılavuzu, Ankara.
65. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2011). ISO/IEC 27011, Bilgi Teknolojisi - Güvenlik Teknikleri - Telekomünikasyon Kuruluşları İçin ISO/IEC 27002 Standardını Temel Alan Bilgi Güvenliği Yönetimi Kılavuzu, Ankara.
66. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2015). ISO/IEC 27013, Bilgi Teknolojisi - Güvenlik Teknikleri - ISO/IEC 27001 ve ISO/IEC 20000-1 Standartlarının Tümleşik Uygulaması Hakkında Kılavuz, Ankara.
67. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2015). ISO/IEC 27014, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetişimi, Ankara.
68. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2014). ISO/IEC 27015, Bilgi Teknolojisi - Güvenlik Teknikleri - Finansal Hizmetler İçin Bilgi Güvenliği Kılavuzu, Ankara.
69. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27017, Bilgi Teknolojisi - Bilgi Teknolojisi - Güvenlik Teknikleri - Bulut Hizmetlerinde ISO/IEC 27002 Standardına Dayalı Bilgi Güvenliği Kontrolleri İçin Uygulama Kuralları, Ankara.
70. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27003, Bilgi Teknolojisi - Güvenlik teknikleri - Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu, Ankara.
71. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2014). ISO/IEC 27031, Bilgi Teknolojisi - Güvenlik Teknolojileri - Bilgi ve İletişim Teknolojileri İçin İş Sürekliliği Yönergeleri, Ankara.
72. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27033-1, Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 1: Genel Bakış ve Kavramlar, Ankara.
73. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27033-2, Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 2: Ağ Güvenliğinin Tasarımı ve Uygulanması İçin Tavsiyeler, Ankara.
74. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27033-3, Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 3: Referans Ağ Oluşturma Senaryoları - Tehditler, Tasarım Teknikleri ve Kontrol Konuları, Ankara.
75. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27033-4, Bilgi Teknolojisi - Güvenlik

Teknikleri - Ağ Güvenliği - Bölüm 4: Güvenlik Ağ Geçitleri Kullanılarak Ağlar Arasında Güvenli İletişim, Ankara.

76. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27033-5, Bilgi Teknolojisi - Güvenlik Teknikleri - Ağ Güvenliği - Bölüm 5: Sanal Özel Ağlar (VPNs) Kullanılarak Ağlar Arasında Çapraz Güvenli İletişim, Ankara.
77. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 27035, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği İhlal Olayı Yönetimi, Ankara.
78. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27036-1, Bilgi Teknolojisi - Güvenlik Teknikleri - Tedarikçi İlişkileri İçin Bilgi Güvenliği - Bölüm 1: Genel Bakış ve Kavramlar, Ankara.
79. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27036-2, Bilgi Teknolojisi - Güvenlik Teknikleri - Tedarikçi İlişkileri İçin Bilgi Güvenliği - Bölüm 2: Gereksinimler, Ankara.
80. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27036-3, Bilgi Teknolojisi - Güvenlik Teknikleri - Tedarikçi İlişkileri İçin Bilgi Güvenliği - Bölüm 3: Bilgi ve İletişim Teknolojisi Tedarik Zinciri Güvenliği İçin Tavsiyeler, Ankara.
81. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27039, Bilgi Teknolojisi - Güvenlik Teknikleri - Saldırı Tespit Sistemlerinin Seçimi, Kurulumu ve İşletimi (IDPS), Ankara.
82. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2016). ISO/IEC 27040, Bilgi Teknolojisi - Güvenlik Teknikleri - Depolama Güvenliği, Ankara.
83. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2010). ISO/IEC 15408-1, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Teknolojisi (BT) Güvenliği İçin Değerlendirme Kriterleri - Bölüm 1: Giriş ve Genel Model, Ankara.
84. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2009). ISO/IEC 15408-2, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Teknolojisi (BT) Güvenliği İçin Değerlendirme Kriterleri - Bölüm 2: Güvenlik Fonksiyonel Bileşenleri, Ankara.
85. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 15408-3, Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Teknolojisi (BT) Güvenliği İçin Değerlendirme Kriterleri - Bölüm 3: Güvenlik Garanti Bileşenleri, Ankara.
86. International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). (2013). ISO/IEC 20000-1, Bilgi Teknolojisi - Hizmet Yönetimi - Bölüm 1: Özellikler, Ankara.
87. IT Governance. (2016). ISO 27001 Global Report 2016, London, United Kingdom.
88. HM Goverment. (2015). 2015 Information Security Breaches Survey, London, United Kingdom.

89. PWC. (2016). Turnaround and Transformation in Cybersecurity, London, United Kingdom.

90. Ernst&Young. (2011). Into the Cloud, Out of the Fog: Ernst & Young' s 2011 Global Information Security Survey, London, United Kingdom.

91. Paja, E., Dalpiaz, F. ve Giorgini, P. (2015). Modelling and Reasoning About Security Requirements in Socio-Technical Systems, 24th International Conference on Advanced Information Systems Engineering (CAiSE), 855(1).

92. Nikolic, B. ve Ruzic-Dimitrijevic. L. (2009). Risk Assessment of Information Technology Systems, Informing Science and Information Technology 6(55), 595-615.

93. National Institute of Standards and Technology (NIST). (2012). NIST Special Publication 800-30: Guide for Conducting Risk Assessments, Gaithersburg, USA.

94. Mellado, D., Fern'andez-Madina, E. ve Piattini, M. (2006). Applying a Security Requirements Engineering Process, ESORICS'06 Proceedings of the 11th European conference on Research in Computer Security.

95. Sun, L., Srivastava, R. ve Mock, T. (2006). An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions, Journal of Management Information Systems, 22(4), 109-142.

96. National Institute of Standards and Technology (NIST). (2012). NIST-SP800 Series Special Publications on Computer Security, Gaithersburg, USA.

97. Forum of Incident Response and Security Teams (FIRST). (2015). Common Vulnerability Scoring System v3.0: Specification Document, North Carolina, USA.

98. İspanya Ministry of Finance and Public Administration. (2014). MAGERIT - Version 3.0. Methodology for Information Systems Risk Analysis and Management, Book I - The Method, Madrid, İspanya.

99. Parvizi, R., Oghbaei, F. ve Khayami, S.R. (2013). Using COBIT and ITIL Frameworks to Establish the Alignment of Business and IT Organizations as One of the Critical Success Factors in ERP Implementation, In Proceedings of the 5th IEEE Conference on Information and Knowledge Technology (IKT), 274-278.

100. Jourdan, Z., Rainer, K., Marshall, E., ve Ford, N. (2010) An Investigation of Organizational Information Security Risk Analysis, Journal of Service Science. 3(1), 33-42.

101. Rabai, L.B.A., Jouini, M., Aissa, A.B., ve Milli, A. (2012). A Cyber Security Model in Cloud Computing Environments, Journal of King Saud University, Computer and Information Sciences, 1(1), 63-75.

102. Eloff, M.M., ve Solms, S.H.V. (2000). Information Security Management: An Approach to Combine Process Certification and Product Evaluation, Computers & Security, 19(3), 698-709.

103. Joshi, C., ve Singh, U. K. (2017). Information Security Risks Management Framework - A Step Towards Mitigating Security Risks in University Network, Journal of Information Security and Applications, 35(1), 128-137.

104. Thierauf, R. J. (2001). Effective Business Intelligence Systems, Greenwood Publishing Group.

105. Szulanski, G. (2000). The Process of Knowledge Transfer: A Diachronic Analysis of Stickiness, Organizational Behavior and Human Decision Processes, 82(1), 9-27.

106. Alavi, M., ve Leidner, D.E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. Management Information Systems Quarterly, 25(1), 107-136.

107. Ahmad, A., Bosua, R., ve Scheepers, R. (2014). Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective, Computers & Security, 42(1), 27-39.

108. Grant, R.M. (1996). Toward a Knowledge-Based Theory of the Firm, Strategic Management Journal, 17(2), 109-122.

109. Von Krogh, G. (2009). Individualist and Collectivist Perspectives on Knowledge in Organizations: Implications for Information Systems Research, The Journal of Strategic Information Systems, 18(3), 119-129.

110. Guarro, S.B. (1987). Principles and Procedures of the ALRAM Approach to Information System Risk Analysis and Management, Computers&Security, 6(1), 493-504.

111. Hendre, A. ve Joski, K.P. (2015). A Semantic Approach to Cloud Security and Compliance, Proceedings of the 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015, 1081-1084.

112. European Parliament & Council of the European Union. (2016). Directive 95/46/EC (General Data Protection Regulation), 119(59), 1-88.

113. European Parliament. (2014). General Data Protection Regulation, (COM(2012)0011-C7-0025/2012-2012/0011(COD)).

114. Landwehr, C.E. (1981). Formal Models for Computer Security, ACM Computer Survey, 13(1), 247-278.

115. Nazareth, D.L. ve Choi, J. (2012). Information Security Management: A System Dynamics Approach, Eighteenth Americas Conference on Information Systems (AMCIS- 2012).

116. Trcek, D. (2008). Using System Dynamics for Managing Risks in Information Systems, WSEAS Trans. Inf. Sci. Appl. 2(1), 175-180.

117. Kouns, J. ve Minoli, D. (2010). Information Technology Risk Management In Enterprise Environments, New Jersey: A John Wiley & Sons Inc. Yayınları.

118. Rot, A. (2008). IT Risk Assessment: Quantitative and Qualitative Approach, The World Congress on Engineering and Computer Science.

119. Yazar, Z. (2002). A Qualitative Risk Analysis and Management Tool-CRAMM, SANS InfoSec Reading Room White Paper, 11(1), 12-32.

120. Internet: European Union Agency for Network and Information Security (ENISA), MIGRA, URL: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rmra-methods/m_migra.html, Son Erişim Tarihi: 20.02.2019.

121. Hemery, H., Akmouche, W. ve Tatout, F. (2007). Utilisation de la Methodologie EBIOS en securite globale, REE. Revue de l'électricité et de l'électronique, 10(1), 29-125.

122. Beckers, K., Cote, I., Fabbender, S., Heisel, M. ve Hofbauer, S. (2013). A Pattern-Based Method for Establishing a Cloud-Specific Information Security Management System,

Establishing Information Security Management Systems or Cloud Considering Security, Privacy, and Legal Compliance, Requirements Engineering for Security, Privacy & Services in Cloud Environments. 18(4), Springer, 343-395.

123. Murugesan, S., ve Bojanova, I. (2016). Encyclopedia of Cloud Computing, John Wiley & Sons, Ltd.
124. Creese, S., Goldsmith, M., ve Hopkins, P. (2013). Inadequacies of Current Risk Controls for the Cloud, Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010, 659-666.
125. Gleeson, N., ve Walden, I. (2014). 'It's a Jungle Out There'?: Cloud Computing, Standards and The Law, European Journal of Law and Technology, 5(2), 1-22.
126. Rasheed, H. (2014). Data and Infrastructure Security Auditing in Cloud Computing Environments, In International Journal of Information Management, 34(1), 364-368.
127. Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005, Jurnal Informasi, 7(2), 48-57.
128. Islami, D.C., IH, K.B. ve Candiwan, C. (2016). Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia, INKOM Journal, 10(1), 19-26.
129. Abawajy J. (2014). User Preference of Cyber Security Awareness Delivery Methods, Behav Inf Technol 2014, 33(1), 236-47.
130. Sohrabi, Safa N., Von Solms R. ve Furnell, S. (2016). Information Security Policy Compliance Model in Organizations, Comput Secur 2016, 56(1), 1-13.
131. Shojaie, B., Federrath, H. ve Saberi, I. (2014). Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A, In Availability, Reliability and Security (ARES), 2014 Ninth International Conference, 259-264.
132. Fomin, V.V., Vries, H. ve Barlette, Y. (2008). ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption, EUROMOT 2008.
133. International Organization for Standardization (ISO). (2018, Ağustos). The ISO Survey of Management System Standard Certifications - 2017 - Explanartory Note,
134. International Organization for Standardization (ISO). (2018, Ağustos). The ISO Survey of Management System Standard Certifications - ISO IEC 27001 Data Per Country and Sector 2006 to 2017.
135. Internet: Türkiye Barolar Birliği (TBB), 31.12.2018 İtibariyle Baroların Avukat Sayıları, URL: https://www.barobirlik.org.tr/Haberler/avukat-sayilari-31122018-80448, Son Erişim Tarihi: 05.06.2019.
136. Türkiye Büyük Millet Meclisi (TBMM). (2019, Temmuz). On Birinci Kalkınma Planı (2019-2023), Türkiye Büyük Millet Meclisi Genel Kurulunun 18.07.2019 tarihli 105' inci Birleşimi.
137. Cumhurbaşkanlığı. (2019, Temmuz). 2019/12 Sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi.
138. Internet: Siber Güvenlik Kurulu, Bilgi ve İletişim Teknolojileri Kurumu, Siber Güvenlik Kurulu, URL: https://www.btk.gov.tr/siber-guvenlik-kurulu, Son Erişim Tarihi: 04.07.2019.

EKLER

EK-1. Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİLERİ STANDARDI ÇERÇEVESİNDE

AVUKATLIK BÜROLARININ DEĞERLENDİRİLMESİ

Sayın Yetkili;

Bu anket Uluslararası ISO 27001 Bilgi Güvenliği Yönetim Sistemleri Standardı çerçevesinde büronuzun bu standart içerisinde yer alan 14 ana başlık altındaki 35 kategori ve 113 kontrol çerçevesinde kapsamlı bir şekilde öz değerlendirmesini ortaya koymayı amaçlamaktadır.

Anket aracılığı ile sağlayacağınız bilgiler, yalnızca istatistiksel analiz ve değerlendirmelerde kullanılacak olup, hiç bir şekilde üçüncü şahıslarla paylaşılmayacak, talep edilmesi durumunda büronuza özel olarak raporlanacaktır.

İstatistiksel analiz ve değerlendirmeler, standart gereksinimleri ile örtüştürülerek ülkemize özgü ideal bir avukatlık bürosunun ihtiyacı olan Bilgi Güvenliği Yönetim Sistemi yapısı ortaya koyulmaya çalışılacaktır.

Katılımızdan dolayı teşekkür eder, saygılarımı sunarım.

Berker KILIÇ
Gazi Üniversitesi, Bilişim Enstitüsü
Adli Bilişim Anabilim Dalı
Yüksek Lisans Öğrencisi
(Bilişim Teknolojileri Öğretmeni)

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

BÖLÜM-1: AVUKATLIK BÜROSU TEMEL BİLGİLERİ

Lütfen büronuz için aşağıdaki anket maddelerini yanıtlayınız.

1. Bürodaki çalışan avukat sayısı? _____

2. Bürodaki çalışan personel sayısı? _____

3. Bürodaki çalışanyardımcı personel sayısı? _____

4. Büroda kullanılan bilgisayar sayısı? _____

5. Büroda kullanılan yazıcı sayısı sayısı? _____

	EVET	HAYIR
6. Büroda bilgisayar ağına bağlı mobil cihazlar kullanılıyor mu?	[ ]	[ ]
7. Büro çalışanlarının büro ağında kişisel mobil cihazlarını kullanmalarına izin verliyor mu?	[ ]	[ ]
8. Büro ve avukatlık hizmetleri için kullanılan özel bir paket program var mı?	[ ]	[ ]
9. Büro ve avukatlık hizmetleri için kullanılan özel bir web sitesi var mı?	[ ]	[ ]
10. Büroda kullanılan bilişim teknolojileri ekipmanı için teknik destek, bakım, onarım ve benzeri hizmetler alınan anlaşmalı bir tedarikçi var mı?	[ ]	[ ]
11. Büro bilişim güvenliği konusunda danışmanlık alınan bir tedarikçi var mı?	[ ]	[ ]
12. Büroda kablolu bilgisayar ağı kullanılıyor mu?	[ ]	[ ]
13. Büroda kablosuz bilgisayar ağı kullanılıyor mu?	[ ]	[ ]
14. Büroda kablolu bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	[ ]	[ ]
15. Büroda kablosuz bilgisayar ağlarına misafir bilgisayar, laptop, cep telefonu bağlanmasına izin veriliyor mu?	[ ]	[ ]

BÖLÜM-2: BİLGİ GÜVENLİĞİ POLİTİKALARI

1. Büro yönetimi tarafından bilgi güvenliği konusunda yasal düzenlemelerle uyumlu, paydaşlara yönelik yazılı bir yönlendirme/bilgilendirme yapıldı mı?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

	EVET	HAYIR	KISMEN
1. Bilgi güvenliği politika dokümanı hazırlandı mı?	[ ]	[ ]	[ ]
2. Bilgi güvenliği politika dokümanı yönetim tarafından onaylandı mı?	[ ]	[ ]	[ ]
3. Bilgi güvenliği politika dokümanı yayınlandı mı?	[ ]	[ ]	[ ]
4. Bilgi güvenliği yönetim politika dokümanı çalışanlara bildirildi mi?	[ ]	[ ]	[ ]
5. Bilgi güvenliği yönetim politika dokümanı paydaşlara bildirildi mi?	[ ]	[ ]	[ ]
6. Bilgi güvenliği yönetim politika dokümanı belirli aralıklarla uygunluğu ve doğruluğu açısından gözden geçiriliyor mu?	[ ]	[ ]	[ ]
7. Bilgi güvenliği yönetim politika dokümanı önemli değişiklikler ortaya çıktığında uygunluğu ve doğruluğu açısından gözden geçiriliyor mu?	[ ]	[ ]	[ ]
8. Bilgi güvenliği yönetim politika dokümanının etkinliği belirli aralıklarla veya önemli değişiklikler ortaya çıktığında değerlendiriliyor mu?	[ ]	[ ]	[ ]

BÖLÜM-3: BİLGİ GÜVENLİĞİ ORGANİZASYONU

1. Büro hizmetlerinin yerine getirilmesinde, bilgi güvenliği sorumluları belirlenerek bilgi güvenliği kapsamında, ilgili kamu kurumları ve STK' lar gibi taraflarla bilgi alışverişinde bulunuldu mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
1. Büro içerisinde bilgi güvenliği sorumlulukları tanımlandı mı?	[ ]	[ ]	[ ]
2. Büro içerisinde bilgi güvenliği sorumlulukları kişilere tahsis edildi mi?	[ ]	[ ]	[ ]
3. Büro içerisinde bilgi güvenliği rollerinin tahsisinde görevler ve sorumluluklar arasındaki çelişkiler giderildi mi?	[ ]	[ ]	[ ]
4. Büro içerisinde bilgi güvenliği ile ilgili yetkilendirilmemiş görevler temizlendi veya gereksiz yetkilendirmeler giderildi mi?	[ ]	[ ]	[ ]
5. Büro hizmetlerinin bilgi güvenliği kapsamında değerlendirilmesinde üst kurum ve kuruluşlarla iletişim kuruldu mu?	[ ]	[ ]	[ ]
6. Büro hizmetlerinin bilgi güvenliği kapsamında değerlendirilmesinde özel ilgi grupları veya derneklerle iletişim kuruldu mu?	[ ]	[ ]	[ ]
7. Büro hizmetlerinin bilgi güvenliği kapsamında değerlendirilmesinde profesyonel yardım alındı mı?	[ ]	[ ]	[ ]
8. Büro hizmetleri sunulurken, hizmetin türüne bakılmaksızın bilgi güvenliğine dikkat ediliyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

2. Büro çalışanlarının, mevcut ağ sistemine kişisel bilgisayarı, mobil cihazları gibi araç gereçlerle bağlanmasında, büro dışından uzaktan erişim ile mevcut ağ sistemine bağlanmasında belirlenmiş kurallar/standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
9. Büro çalışanlarına yönelik olarak, kendi mobil cihazlarını büro ağ sistemine bağlanması nedeniyle ortaya çıkabilecek risklere karşı alınan güvenlik tedbirleri mevcut mu?	[ ]	[ ]	[ ]
10. Büro çalışanlarına yönelik olarak, büro dışından büro ağ sistemine bağlanarak erişebildiği bilgiyi korumak amacı ile alınan tedbirler mevcut mu?	[ ]	[ ]	[ ]
11. Büro çalışanlarına yönelik olarak, büro dışından büro ağ sistemine bağlanarak işleyebildiği bilgiyi korumak amacı ile alınan tedbirler mevcut mu?	[ ]	[ ]	[ ]
12. Büro çalışanlarına yönelik olarak, büro dışından büro ağına bağlanarak depolayabildiği bilgiyi korumak amacı ile alınan tedbirler mevcut mu?	[ ]	[ ]	[ ]

BÖLÜM-4: İNSAN KAYNAKLARI GÜVENLİĞİ

1. İşe alınan büro çalışanları ve ürün/hizmet alınan yükleniciler hakkında, çalışma öncesinde geçmiş doğrulaması yapılarak, bilgi güvenliği açısından sorumlulukları kendisine açıklanıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Büro çalışanlarının işe alımında yapacakları işe göre ilgili yasa ve düzenlemeler göz önünde bulundurularak geçmiş doğrulama kontrolleri yapılıyor mu?	[ ]	[ ]	[ ]
2. Büro çalışanları ile yapılan sözleşmelerde, kişilere bilgi güvenliği sorumlulukları bildiriliyor mu?	[ ]	[ ]	[ ]
3. Büronun mal ve hizmet aldığı kişi ve kurumlara, bilgi güvenliği sorumlulukları bildiriliyor mu?	[ ]	[ ]	[ ]

2. Çalışanlar ve ürün/hizmet alınan yükleniciler, çalışma süreci içerisinde kendi fonksiyonları ile ilgili büronun bilgi güvenliği politikaları ve bu politikalara uymamaları durumunda karşı karşıya kalabilecekleri sorumluluklar hakkında yazılı olarak bilgilendiriliyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
4. Büro çalışanları, büro hizmetlerinin yerine getirilmesinde bilgi güvenliği prosedürlerine uymamaları durumunda karşılaşacakları sorumluluklar hakkında yazılı olarak bilgilendiriliyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

5. Büronun mal ve hizmet aldığı kişi ve kurumlar, büronun bilgi güvenliği prosedürlerine uymamaları durumunda karşılaşacakları sorumluluklar hakkında yazılı olarak bilgilendiriliyor mu?	[ ]	[ ]	[ ]
6. Büro çalışanlarına, büronun bilgi güvenliği prosedürleri ile ilgili bir iç eğitim verildi mi?	[ ]	[ ]	[ ]
7. Büro çalışanlarının, bilgi güvenliği konusunda bir dış eğitim alması sağlandı mı?	[ ]	[ ]	[ ]
8. Büronun mal ve hizmet aldığı kişi ve kurumlara, büronun bilgi güvenliği prosedürleri ile ilgili bir eğitim verildi mi?	[ ]	[ ]	[ ]
9. Büronun mal ve hizmet aldığı kiş ve kurumlardan, bilgi güvenliği konusunda bir eğitim alması istendi mi?	[ ]	[ ]	[ ]
10. Büro çalışanlarının ve büronun mal ve hizmet aldığı kişi ve kurumların bilgi güvenliği konusundaki eğitimlerini düzenli olarak güncelleştirmeleri takip ediliyor mu?	[ ]	[ ]	[ ]
11. Büronun mal ve hizmet satın aldığı kişi ve kurumlardan bilgi güvenliği konusunda yeterliliklerini ispatlamaları isteniyor mu?	[ ]	[ ]	[ ]
12. Büro çalışanlarına yönelik büronun bilgi güvenliği prosedürlerini ihlal etmeleri durumunda uygulanacak büro çalışanına bildirilmiş bir yaptırım mevcut mu?	[ ]	[ ]	[ ]
13. Büronun mal ve hizmet satın aldığı kişi ve kurumlara yönelik büronun bilgi güvenliği prosedürlerini ihlal etmeleri durumunda uygulanacak kendilerine bildirilmiş bir yaptırım mevcut mu?	[ ]	[ ]	[ ]

3. Çalışanların işten çıkarılması veya ürün/hizmet alınan yüklenicilerle çalışmanın sonlandırılması durumunda, sonrasında ortaya çıkabilecek olası bilgi güvenliği zaafiyetlerine karşı tedbirler alınıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
14. Büro çalışanlarına işten ayrılmaları veya görevlerinin değişmesi durumunda bilgi güvenliği sorumluluklarının devam ettiğine ilişkin bilgilendirme yapılıyor mu?	[ ]	[ ]	[ ]
15. Büronun mal ve hizmet aldığı kişi ve kurumlara, büro ile çalışmalarının sonlandırılması veya değişmesi durumunda bilgi güvenliğine ilişkin sorumluluklarının devam ettiğine ilişkin bilgilendirme yapılıyor mu?	[ ]	[ ]	[ ]

BÖLÜM-5: VARLIK YÖNETİMİ

1. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanına ait durum ve sahiplikleri de kapsayan bir envanter çalışması yapıldı mı?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının tamamı kayıt altında tutuluyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

2. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının tamamına sahiplik belirlenmiş mi?	[ ]	[ ]	[ ]
3. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının tamamının kullanımına dair belirlenmiş kurallar var mı?	[ ]	[ ]	[ ]
4. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının tamamının kullanımına dair belirlenmiş kurallar uygulanıyor mu?	[ ]	[ ]	[ ]
5. Büro çalışanlarının işten ayrılmaları durumunda, büro tarafından kendilerine sağlanan bilgi işlem ekipmanlarını ne şekilde iade edeceklerine ilişkin belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
6. Büronun mal ve hizmet satın aldığı kişi ve kurumların, büro tarafından sağlanan bilgi işlem ekipmanlarını ne şekilde iade edeceklerine ilişkin belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]

2. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilginin sınıflandırılması, etiketlenmesi ve korunmasına ilişkin yöntemler/standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
7. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi yasal şartlara göre sınıflandırılıyor mu?	[ ]	[ ]	[ ]
8. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi değerine göre sınıflandırılıyor mu?	[ ]	[ ]	[ ]
9. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi kritikliğine göre sınıflandırılıyor mu?	[ ]	[ ]	[ ]
10. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi yetkisiz ifşa edilebilirliğine göre sınıflandırılıyor mu?	[ ]	[ ]	[ ]
11. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital değiştirilmeye karşı hassasiyetine göre sınıflandırılıyor mu?	[ ]	[ ]	[ ]
12. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilginin sınıflandırılmasına ilişkin kullanılan belirli bir prosedür mevcut mu?	[ ]	[ ]	[ ]
13. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilginin kullanımına ilişkin sınıflandırma düzeni ile örtüşen bir etiketleme sistemi mevcut mu?	[ ]	[ ]	[ ]

3. Büro hizmetlerinin yerine getirilmesinde, depolanmış dijital bilgiyi koruma, bilgiye erişim, bilgiyi güncelleme, bilgiyi silme, bilgiyi yok etme işlemlerine ilişkin standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

	EVET	HAYIR	KISMEN
14. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi depolama birimlerine kaydedilirken bilgi sınıflandırma prosedürlerine uyuluyor mu?	[ ]	[ ]	[ ]
15. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilginin geçmişte depolanmış olduğu birimler güvenli bir şekilde yok ediliyor mu?	[ ]	[ ]	[ ]
16. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi depolama birimlerine kaydedilirken yetkisiz erişime karşı tedbir alınıyor mu?	[ ]	[ ]	[ ]
17. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi depolama birimlerine kaydedilirken kötüye kullanıma karşı tedbir alınıyor mu?	[ ]	[ ]	[ ]
18. Büro hizmetlerinin yerine getirilmesinde ihtiyaç duyulan veya büro hizmetlerinin gerçekleştirilmesi esnasında üretilen dijital bilgi depolama birimlerine kaydedilirken bozulmaya karşı tedbir alınıyor mu?	[ ]	[ ]	[ ]

BÖLÜM-6: ERİŞİM KONTROLÜ

1. Büro hizmetlerini yerine getiren ağ kullanıcılarının yaptıkları iş çerçevesinde ağ hizmetlerine erişimlerini düzenleyici kurallar/standartlar mevcut mudur?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
1. Büro hizmetlerini yerine getiren ağ kullanıcıları için iş ve bilgi güvenliği temelinde hazırlanmış yazılı bir erişim kontrol politikası mevcut mu?	[ ]	[ ]	[ ]
2. Büro hizmetlerini yerine getiren ağ kullanıcılarının yönetimi için tanımlanmış yetkiler doğrultusunda kullanıcı erişim politikaları uygulanıyor mu?	[ ]	[ ]	[ ]
3. Büro hizmetlerini yerine getiren ağ kullanıcıları için gerekli durumlarda verilen ayrıcalıklı yetkilerin tahsis edilmesi, kısıtlanması ve kontrolü gerçekleştiriliyor mu?	[ ]	[ ]	[ ]

2. Büro hizmetlerini yerine getiren ağ kullanıcılarının, ağ kaynakları üzerindeki haklarının belirlenmesi ve hak atamalarının yapılması konularında yazılı standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
4. Büro hizmetlerini yerine getiren kullanıcılar için erişim haklarının verilmesinde belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
5. Büro hizmetlerini yerine getiren kullanıcılar için yeni kullanıcı hesabı açmada belirlenmiş kurallar var mı?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

6. Büro hizmetlerini yerine getirmede kullanıcılar için kullanıcı hesaplarını silmede belirlenmiş bir kurallar var mı?	[ ]	[ ]	[ ]
7. Büro hizmetlerini yerine getirmede sistemler ve hizmetlere erişim hakları verilirken uyulacak kullanıcı erişim kuralları mevcut mu?	[ ]	[ ]	[ ]
8. Büro hizmetlerini yerine getiren kullanıcılara verilen erişim haklarının tahsisi ve kısıtlanması düzenli olarak kontrol ediliyor mu?	[ ]	[ ]	[ ]
9. Büro hizmetlerini yerine getiren kullanıcılara tahsis edilen kimlik doğrulama bilgilerinin tesliminde uyulan kurallar mevcut mu?	[ ]	[ ]	[ ]
10. Büro hizmetlerini yerine getiren kullanıcılara tahsis edilen kimlik doğrulama bilgileri farklı sistem ve hizmetler için birbirinden farklı mı?	[ ]	[ ]	[ ]
11. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına erişim hakları düzenli aralıklarla gözden geçiriliyor mu?	[ ]	[ ]	[ ]
12. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına erişim hakları düzenli aralıklarla veya gereksinimler doğrultusunda güncelleniyor mu?	[ ]	[ ]	[ ]
13. Büro hizmetlerini yerine getiren çalışanların ve mal/hizmet alınan dış tarafların sahip olduğu bilgi işleme olanaklarına erişim yetkileri sözleşmeleri/anlaşmaları sona erdiğinde kaldırılıyor mu?	[ ]	[ ]	[ ]
14. Büro hizmetlerini yerine getiren çalışanların ve mal/hizmet alınan dış tarafların sahip olduğu bilgi işleme olanaklarına erişim yetkileri sözleşmeleri/anlaşmaları sona erdiğinde değişikliğe uygun olarak yeniden düzenleniyor mu?	[ ]	[ ]	[ ]
15. Büro hizmetlerini yerine getiren çalışanların ve mal/hizmet alınan dış tarafların sahip olduğu bilgi işleme olanaklarına erişim yetkileri sözleşmeleri/anlaşmaları değiştiğinde kaldırılıyor mu?	[ ]	[ ]	[ ]
16. Büro hizmetlerini yerine getiren çalışanların ve mal/hizmet alınan dış tarafların sahip olduğu bilgi işleme olanaklarına erişim yetkileri sözleşmeleri/anlaşmaları değiştiğinde, değişikliğe uygun olarak yeniden düzenleniyor mu?	[ ]	[ ]	[ ]

3. Büro hizmetlerini yerine getiren kullanıcılar, sahip oldukları erişim ve kullanım kimliklerini korumaları konusunda bilgilendirildi mi?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
17. Büro hizmetlerini yerine getiren çalışanların, bilgi işleme olanaklarına erişmede kullandıkları gizli kimlik doğrulama bilgilerini kullanmalarında uymaları gereken kurallar mevcut mu?	[ ]	[ ]	[ ]
18. Büro hizmetlerini yerine getiren çalışanların, bilgi işleme olanaklarına kullanımda kullandıkları gizli kimlik doğrulama bilgilerini kullanmalarında uymaları gereken kurallar mevcut mu?	[ ]	[ ]	[ ]

4. Büro çalışanları tarafından kullanılan sistem açılış, bağlantı ve uygulama şifreleri kullanıcının ihtiyacı olan yetkilerle orantılı olarak seviyelendirildi mi?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

	EVET	HAYIR	KISMEN
19. Büro hizmetlerinde kullanılan bilgi işleme olanaklarının kullanımı, erişim kontrol kuralları ile kısıtlanıyor mu?	[ ]	[ ]	[ ]
20. Büro hizmetlerinde kullanılan bilgi işleme olanaklarına erişim esnasında, şart koşulan durumlarda güvenli oturum açma kontrolleri mevcut mu?	[ ]	[ ]	[ ]
21. Büro hizmetlerinde kullanılan bilgi işleme olanaklarına erişmede kullanılan parola yönetim sistemi güvenilir parolalar kullanmayı zorunlu hale getiriyor mu?	[ ]	[ ]	[ ]
22. Büro hizmetlerinde kullanılan bilgi işleme olanaklarına erişimde kullanılan parola yönetim sistemi kullanıcılara güvenilir parolalar sağlayabiliyor mu?	[ ]	[ ]	[ ]
23. Büro hizmetlerinde kullanılan sistem ve uygulamaların kontrollerini geçeriz kılma kabiliyetine sahip destek programları kullanılıyor mu?	[ ]	[ ]	[ ]
24. Büro hizmetlerinde kullanılan sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip destek programları düzenli olarak kontrol ediliyor mu?	[ ]	[ ]	[ ]
25. Büro hizmetlerinde kullanılan sistem ve uygulamaların yönetici ayarlarına erişim diğer kullanıcılardan kısıtlanıyor mu?	[ ]	[ ]	[ ]

BÖLÜM-7: KRİPTOGRAFİ

1. Büro hizmetlerinin yerine getirilmesinde kullanılan ve bu hizmetler sonrasında üretilen bilginin gizliliği, bilginin aslına uygunluğu ve bilginin bütünlüğünü sağlama amacı ile şifreleme işlemlerinden faydalanılıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
1. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin korunması için şifreleme kuralları mevcut mu?	[ ]	[ ]	[ ]
2. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin korunması için şifreleme kuralları kullanılıyor mu?	[ ]	[ ]	[ ]
3. Büro hizmetlerinin şifrelenmesinde kullanılan kriptografik anahtarların kullanımına ilişkin kurallar mevcut mu?	[ ]	[ ]	[ ]
4. Büro hizmetlerinin şifrelenmesinde kullanılan kriptografik anahtarların korunmasına ilişkin kurallar mevcut mu?	[ ]	[ ]	[ ]
5. Büro hizmetlerinin şifrelenmesinde kullanılan kriptografik anahtarların yaşam sürelerine ilişkin kurallar mevcut mu?	[ ]	[ ]	[ ]

BÖLÜM-8: FİZİKSEL VE ÇEVRESEL GÜVENLİK

1. Büro ortamında fiziksel ve elektronik sistemler (kamera ve alarm sistemleri gibi) ile yetkisiz erişimlere karşı koruma tedbirleri mevcut mudur?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

	EVET	HAYIR	KISMEN
1. Büro ortamında hassas ve kritik bilgilerin bulunduğu ortamlar genel kullanıma açık alanlardan ayrılmış mı?	[ ]	[ ]	[ ]
2. Büro ortamında hassas ve kritik bilgilerin bulunduğu ortamlara genel kullanıma açık alanlardan geçişte kullanılan güvenlik kontrolleri belirlenmiş mi?	[ ]	[ ]	[ ]
3. Büro ortamında hassas ve kritik bilgilerin bulunduğu ortamlara genel kullanıma açık alanlardan geçişte kullanılan güvenlik kontrolleri uygulanıyor mu?	[ ]	[ ]	[ ]
4. Büro ortamının ve çevresinin fiziksel güvenliğini sağlamak için bir güvenlik tasarımı yapıldı mı?	[ ]	[ ]	[ ]
5. Büro ortamının ve çevresinin fiziksel güvenliğini sağlamak için bir güvenlik uygulaması mevcut mu?	[ ]	[ ]	[ ]
6. Büro ortamının ve çevresinin fiziksel olarak doğal afetlere karşı güvenliğini sağlamak için tedbirler tasarlandı mı?	[ ]	[ ]	[ ]
7. Büro ortamının ve çevresinin fiziksel olarak doğal afetlere karşı güvenliğini sağlamak için tedbirler mevcut mu?	[ ]	[ ]	[ ]
8. Büro ortamının ve çevresinin kötü niyetli saldırılara karşı güvenliğini sağlamak için tedbirler tasarlandı mı?	[ ]	[ ]	[ ]
9. Büro ortamının ve çevresinin kötü niyetli saldırılara karşı güvenliğini sağlamak için tedbirler mevcut mu?	[ ]	[ ]	[ ]
10. Büro ortamında genel kullanıma açık olmayan alanlarda çalışanlar için tanımlanmış iş süreçleri mevcut mu?	[ ]	[ ]	[ ]
11. Büro ortamında genel kullanıma açık olmayan alanlarda çalışanlar için tanımlanmış iş süreçlerine uyuluyor mu?	[ ]	[ ]	[ ]
12. Yetkisiz kişilerin büroda bulunabildiği sekreterlik, bekleme alanları benzeri alanlarda güvenlik zaafiyetlerine karşı kontrol ediliyor mu?	[ ]	[ ]	[ ]

2. Büro hizmetlerinde kullanılan bilişim teknolojileri varlıklarının kaybedilmesi, hasar görmesi, çalınması veya ele geçirilmesi gibi durumlara karşı, büro hizmetlerinin sürekliliğini sağlamaya yönelik tedbirler mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
13. Büro hizmetlerinde kullanılan bilişim teknolojileri araçları çevresel tehditlerden kaynaklanan riskleri azaltacak şekilde konumlandırıldı mı?	[ ]	[ ]	[ ]
14. Büro hizmetlerinde kullanılan bilişim teknolojileri araçları yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde konumlandırıldı mı?	[ ]	[ ]	[ ]
15. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici altyapı sebepli enerji kesintilerine karşı tedbirler alındı mı?	[ ]	[ ]	[ ]
16. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici ağ alt yapısı sebepli Internet bağlantı kesintilerine karşı tedbirler alındı mı?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

17. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici ağ alt yapısında dinlemeye karşı tedbirler alındı mı?	[ ]	[ ]	[ ]
18. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici ağ alt yapısında yetkisiz bağlantıya karşı tedbirler alındı mı?	[ ]	[ ]	[ ]
19. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici ağ alt yapısında hasara oluşumuna karşı tedbirler alındı mı?	[ ]	[ ]	[ ]
20. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarının bakımı düzenli olarak yapılıyor mu?	[ ]	[ ]	[ ]
21. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarının sürekli kullanılabilirliği sağlanıyor mu?	[ ]	[ ]	[ ]
22. Büro hizmetlerinde kullanılan bilişim teknolojileri araçları bileşenlerinin bir arada çalışması sağlanıyor mu?	[ ]	[ ]	[ ]
23. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarının büro dışına çıkarılmasında belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
24. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarının büro dışına çıkarılmasında belirlenmiş kurallara uyuluyor mu?	[ ]	[ ]	[ ]
25. Büro hizmetlerinde kullanılan veya büro hizmetleri sonucunda üretilen bilginin büro dışına çıkarılmasında belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
26. Büro hizmetlerinde kullanılan veya büro hizmetleri sonucunda üretilen bilginin büro dışına çıkarılmasında belirlenmiş kurallara uyuluyor mu?	[ ]	[ ]	[ ]
27. Büro hizmetlerinde kullanılan yazılımların büro dışına çıkarılmasında belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
28. Büro hizmetlerinde kullanılan yazılımların büro dışına çıkarılmasında belirlenmiş kurallara uyuluyor mu?	[ ]	[ ]	[ ]
29. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarının büro dışında da kullanılması durumunda uyulması gereken kurallar mevcut mu?	[ ]	[ ]	[ ]
30. Büro hizmetlerinde kullanılan bilişim teknolojileri araçlarının büro dışında da kullanılması durumunda uyulması gereken kurallara uyuluyor mu?	[ ]	[ ]	[ ]
31. Büro hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının yok edilecek olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
32. Büro hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının yok edilecek olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallara uyuluyor mu?	[ ]	[ ]	[ ]
33. Büro hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının bir başkası tarafından tekrar kullanılacak olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
34. Büro hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının bir başkası tarafından tekrar kullanılacak olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallara uyuluyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

35. Büro hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının büroda tekrar kullanılacak olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
36. Büro hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının büroda tekrar kullanılacak olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallara uyuluyor mu?	[ ]	[ ]	[ ]
37. Büro hizmetlerinde artık ihtiyaç duyulmayan ve sahipliği olmayan bilişim teknolojileri ekipmanının korunması için alınmış tedbirler mevcut mu?	[ ]	[ ]	[ ]
38. Büro hizmetlerinde artık ihtiyaç duyulmayan ve sahipliği olmayan bilişim teknolojileri ekipmanının korunması için alınmış tedbirler uygulanıyor mu?	[ ]	[ ]	[ ]
39. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanının yetkilisi gözetimi dışındayken korunması için alınmış tedbirler mevcut mu?	[ ]	[ ]	[ ]
40. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanının yetkilisi gözetimi dışındayken korunması için alınmış tedbirler uygulanıyor mu?	[ ]	[ ]	[ ]
41. Büro hizmetlerinde kağıt ve taşınabilir depolama ortamlarının düzenli olmasını sağlamak üzere temiz masa politikası uygulanıyor mu?	[ ]	[ ]	[ ]
42. Büro hizmetlerinde kullanılan veri işleme olanaklarının düzenli olmasını sağlamak üzere temiz ekran politikası uygulanıyor mu?	[ ]	[ ]	[ ]

BÖLÜM-9: İŞLEM GÜVENLİĞİ

1. Büro hizmetlerinin doğru ve güvenli şekilde gerçekleştirilmesine yönelik ilgili iş süreçleri ve bilgi işleme olanakları hakkında çalışanlara yazılı bilgilendirme yapıldı mı?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Büro hizmetlerinde bilişim sistemleri ekipmanları aracılığı ile yerine getirilen işlemler yazılı hale getirildi mi?	[ ]	[ ]	[ ]
2. Büro hizmetlerinde bilişim sistemleri ekipmanları aracılığı ile yerine getirilen işlemler yazılı olarak tüm kullanıcılara temin edildi mi?	[ ]	[ ]	[ ]
3. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında bilgi güvenliğini etkileyen yeni kurulum işlemleri kontrol ediliyor mu?	[ ]	[ ]	[ ]
4. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında bilgi güvenliğini etkileyen işletim değişiklikleri kontrol ediliyor mu?	[ ]	[ ]	[ ]
5. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında bilgi güvenliğini etkileyen yeni olanaklar kontrol ediliyor mu?	[ ]	[ ]	[ ]
6. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında bilgi güvenliğini etkileyen sistem değişiklikleri kontrol ediliyor mu?	[ ]	[ ]	[ ]
7. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında kaynak kullanımı kontrol ediliyor ve gelecekteki gereksinimler için tahminler oluşturuluyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

8. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında kaynak kullanımı gerekli performansı sağlamak üzere ayarlanıyor ve gelecekteki gereksinimler için tahminler oluşturuluyor mu?	[ ]	[ ]	[ ]
9. Büro hizmetlerinde veri girişi, veri işleme, depolama, yedekleme, arşivleme yetkisiz erişim veya bilişim sistemleri ekipmanlarındaki değişiklik risklerinin azaltılması için birbirinden ayrıldı mı?	[ ]	[ ]	[ ]

2. Büro hizmetlerinde kullanılan bilişim teknolojileri varlıklarını kötücül yazılımlara karşı koruma amacıyla tedbirler alınıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
10. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarını kötücül yazılımlardan korunması için tedbirler alınıyor mu?	[ ]	[ ]	[ ]
11. Büro ağına bağlanan kişisel kullanıcıların kötücül yazılımlardan korunması için tedbirler alınıyor mu?	[ ]	[ ]	[ ]

3. Büro hizmetlerinde kullanılan ve üretilen dijital bilgi düzenli olarak yedekleniyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
12. Büro hizmetlerinde kullanılan veya büro hizmetleri esnasında üretilen bilginin yedeklemesi yapılıyor mu?	[ ]	[ ]	[ ]
13. Büro hizmetlerinde kullanılan veya büro hizmetleri esnasında üretlen bilginin yedekleri harici bir bilişim sistemi ekipmanı üzerinde mi yapılıyor?	[ ]	[ ]	[ ]
14. Büro hizmetlerinde kullanılan veya büro hizmetleri esnasında üretilen bilginin yedekleri düzenli olarak test ediliyor mu?	[ ]	[ ]	[ ]
15. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarının düzenli olarak sistem yedekleri (imajları) alınıyor mu?	[ ]	[ ]	[ ]
16. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarının düzenli olarak sistem yedekleri (imajları) harici bir bilişim sistemi ekipmanı üzerinde mi yapılıyor?	[ ]	[ ]	[ ]
17. Büro hizmetlerinde kullanılan bilişim sistemleri ekipmanlarının yedekleri düzenli olarak test ediliyor mu?	[ ]	[ ]	[ ]
18. Yedekleme işlemleri için çalışanlara duyurulmuş yedekleme kuralları mevcut mu?	[ ]	[ ]	[ ]

4. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri varlıklarında gerçekleştirilen işlemler, olay/zaman parametreleri ile kayıt altına alınıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

	EVET	HAYIR	KISMEN
19. Büro hizmetlerinin yerine getirilmesi esnasında bilişim sistemleri ekipmanları üzerindeki kullanıcı işlemleri olay aktiviteleri kaydediliyor ve düzenli olarak gözden geçiriliyor mu?	[ ]	[ ]	[ ]
20. Büro hizmetlerinin yerine getirilmesi esnasında bilişim sistemleri ekipmanları üzerindeki kural dışı kullanıcı aktiviteleri kaydediliyor ve düzenli olarak gözden geçiriliyor mu?	[ ]	[ ]	[ ]
21. Büro hizmetlerinin yerine getirilmesi esnasında bilişim sistemleri ekipmanları üzerinde ortaya çıkan hatalara ilişkin aktiviteler kaydediliyor ve düzenli olarak gözden geçiriliyor mu?	[ ]	[ ]	[ ]
22. Büro hizmetlerinin yerine getirilmesi esnasında bilişim sistemleri ekipmanları üzerindeki bilgi güvenliği aktiviteleri kaydediliyor ve düzenli olarak gözden geçiriliyor mu?	[ ]	[ ]	[ ]
23. Büro hizmetlerinin yerine getirilmesi esnasında bilişim sistemleri üzerinde olay kaydetme olanakları yetkisiz erişime karşı korunuyor mu?	[ ]	[ ]	[ ]
24. Büro hizmetlerinin yerine getirilmesi esnasında bilişim sistemleri üzerinde olay kayıtları yetkisiz erişime karşı korunuyor mu?	[ ]	[ ]	[ ]
25. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının sistem yöneticilerinin işlemleri kayıt altına alınıyor mu?	[ ]	[ ]	[ ]
26. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının sistem operatörleri işlemleri kayıt altına alınıyor mu?	[ ]	[ ]	[ ]
27. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının sistem yöneticilerinin işlemlerine ait kayıtlar korunuyor mu?	[ ]	[ ]	[ ]
28. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının sistem operatörleri işlemlerine ait kayıtlar korunuyor mu?	[ ]	[ ]	[ ]
29. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının sistem yöneticilerinin işlemlerine ait kayıtlar düzenli olarak inceleniyor mu?	[ ]	[ ]	[ ]
30. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının sistem operatörleri işlemlerine ait kayıtlar düzenli olarak inceleniyor mu?	[ ]	[ ]	[ ]
31. Bir hizmetlerinde kullanılan bilişim teknolojileri kipmanlarının saatleri tek bir referans zaman kaynağına ayarlanarak senktonize ediliyor mu?	[ ]	[ ]	[ ]

5. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları ve ağ alt yapısınına yapılacak yazılımsal eklemeler (yazılım güncellemeleri ve yamaları gibi) için bir kurulum kontrolü standardı mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
32. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarına yazılım kurulumunun kontrolü için geliştirilmiş kurallar mevcut mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

33. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarına yazılım kurulumu kontrolü için geliştirilmiş kurallar uygulanıyor mu?	[ ]	[ ]	[ ]

6. Büro hizmetlerinde kullanılan bilişim teknolojileri varlıklarında olası teknik zaafiyetlere karşı tespit ve tedbir alma kapsamında uygulanan standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
34. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarının geçmişte ortaya çıkmış teknik açıklıkları biliniyor mu?	[ ]	[ ]	[ ]
35. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarının yeni ortaya çıkan teknik açıklıkları çok kısa süre içerisinde öğrenilebiliyor mu?	[ ]	[ ]	[ ]
36. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarının teknik açıklıkları nedeniyle ne tür zaafiyetlerin ortaya çıkabileceği biliniyor mu?	[ ]	[ ]	[ ]
37. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarının teknik açıklıklarına karşı tedbirler alınıyor mu?	[ ]	[ ]	[ ]
38. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarına kullanıcıları tarafından yazılım kurulumuna dair oluşturulmuş kurallar mevcut mu?	[ ]	[ ]	[ ]
39. Büro hizmetlerinin yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarına kullanıcıları tarafından yazılım kurulumuna dair oluşturulmuş kurallara uyuluyor mu?	[ ]	[ ]	[ ]

7. Büro hizmetlerinde kullanılan bilişim teknolojileri varlıkları üzerinde yapılan bilişim güvenliğine yönelik çalışmalar, hizmetlerin yavaşlamasına veya aksamasına sebep olacak nitelikte mi?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
40. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları üzerinde zorunlu olarak gerçekleştirilen donanımsal tetkik işlemlerinin büro hizmetlerinde asgari kesintiye neden olacak çekilde planlanması yapılıyor mu?	[ ]	[ ]	[ ]
41. Büro hizmetlerinde kullanılan ağ alt yapısı üzerinde zorunlu olarak gerçekleştirilen tetkik işlemlerinin büro hizmetlerinde asgari kesintiye neden olacak çekilde planlanması yapılıyor mu?	[ ]	[ ]	[ ]
42. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları üzerinde zorunlu olarak gerçekleştirilen yazılımsal tetkik işlemlerinin büro hizmetlerinde asgari kesintiye neden olacak çekilde planlanması yapılıyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

BÖLÜM-10: HABERLEŞME GÜVENLİĞİ

1. Büro hizmetlerinde kullanılan ağ alt yapısında olası teknik zaafiyetlere karşı tespit ve tedbir alma kapsamında uygulanan standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Büro hizmetlerinde kullanılan veya büro hizmetleri sonrasında ortaya çıkan veriyi korumak amacı ile birden fazla alt ağ kurulumu yapıldı mı?	[ ]	[ ]	[ ]
2. Büro hizmetlerinde kullanılan veya büro hizmetleri sonrasında ortaya çıkan veriyi korumak amacı ile ağda olası teknik zaafiyetlere karşı bir tespit çalışması yapıldı mı?	[ ]	[ ]	[ ]
3. Büro hizmetlerinde kullanılan veya büro hizmetleri sonrasında ortaya çıkan veriyi korumak amacı uygulanan standartlar mevcut mu?	[ ]	[ ]	[ ]
4. Büro hizmetlerinde kullanılan ağ alt yapısının güvenliğinin tesisi amacı ile çeşitli ağ güvenlik mekanizmaları kullanılıyor mu?	[ ]	[ ]	[ ]
5. Büro hizmetlerinde kullanılan ağ alt yapısının güvenliğinin tesisi amacı ile hizmetler saviyelendiriliyor mu?	[ ]	[ ]	[ ]
6. Büro hizmetlerinde kullanılan ağ alt yapısının güvenliğinin tesisi amacı ile belirlenmiş yetkin bir ağ sorumlusu var mı?	[ ]	[ ]	[ ]
7. Büro hizmetlerinde kullanılan ağ alt yapısının güvenliğinin tesisi amacı ile yetkin bir kişi/kurumdan hizmet alımı gerçekleştiriliyor mu?	[ ]	[ ]	[ ]
8. Büro hizmetlerinde kullanılan ağ alt yapısı güvenlik amaçlı olarak alt ağlara ayrılmış mı?	[ ]	[ ]	[ ]
9. Büro hizmetlerinde kullanılan ağ alt yapısı güvenlik amaçlı olarak alt ağlara ayrılırken kullanıcı gereksinimleri göz önünde bulunduruldu mu?	[ ]	[ ]	[ ]
10. Büro hizmetlerinde kullanılan ağ alt yapısı güvenlik amaçlı olarak alt ağlara ayrılırken kullanıcıların ihtiyaç duydukları kaynaklar göz önünde bulunduruldu mu?	[ ]	[ ]	[ ]

2. Büro hizmetleri kapsamında dijital bilginin büro dışına elektronik yollarla yapılan transferlerinde, bilginin güvenliğini sağlamak için tedbirler alınıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
11. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin büro dışına çeşitli yollarla transferinde uyulması gereken güvenlik kuralları mevcut mu?	[ ]	[ ]	[ ]
12. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin büro dışına çeşitli yollarla transferinde uyulması gereken güvenlik kuralları uygulanıyor mu?	[ ]	[ ]	[ ]
13. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin büro dışına çeşitli yollarla transferinde uyulması gereken güvenlik kontrolleri mevcut mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

14. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin büro dışına çeşitli yollarla transferinde uyulması gereken güvenlik kontrolleri uygulanıyor mu?	[ ]	[ ]	[ ]
15. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin büro dışına çeşitli yollarla transferinde güvenli transferi sağlama amaçlı tedbirler alınıyor mu?	[ ]	[ ]	[ ]
16. Büro hizmetlerinde kullanılan veya büro hizmetleri neticesinde üretilen bilginin büro dışına çeşitli yollarla transferinde, transfer sonrası bilgi doğrulama yapılıyor mu?	[ ]	[ ]	[ ]
17. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları aracılığı ile gerçekleşen elektronik mesajlaşma kayıtlarını korumak amaçlı tedbirler alınıyor mu?	[ ]	[ ]	[ ]
18. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları aracılığı ile gerçekleşen elektronik mesajlaşma kayıtlarını korumak amaçlı yedekleniyor mu?	[ ]	[ ]	[ ]
19. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları aracılığı ile gerçekleşen elektronik mesajlaşma kayıtlarını korumak amaçlı şifreleniyor mu?	[ ]	[ ]	[ ]
20. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları aracılığı ile gerçekleşen elektronik mesajlaşma kayıtlarını korumak amaçlı elektronik imza kullanılıyor mu?	[ ]	[ ]	[ ]
21. Büro hizmetlerinde çalışanlar, büro hizmetlerinde kullanılan veya büro hizmetleri sonrasında ortaya çıkarılan bilgileri ifşa etmemeleri konusunda yazılı bir sözleşme ile bağlayıcı hale getiriliyor mu?	[ ]	[ ]	[ ]
22. Büro hizmetlerinde mal/hizmet alınan firmalar, büro hizmetlerinde kullanılan veya büro hizmetleri sonrasında ortaya çıkarılan bilgileri ifşa etmemeleri konusunda yazılı bir sözleşme ile bağlayıcı hale getiriliyor mu?	[ ]	[ ]	[ ]

BÖLÜM-11: SİSTEM TEMİNİ, GELİŞTİRME VE BAKIMI

1. Büro hizmetleri içerisinde kullanıcıların aldatılarak veya teknik zaafiyetlerin kullanılması ile ortaya çıkabilecek saldırılara karşı bilgi güvenliği tedbirleri alınıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Büro hizmetlerinin bilgi güvenliği gereksinimlerinin belirlenmesine dair bir çalışma yapıldı mı?	[ ]	[ ]	[ ]
2. Büro hizmetlerinin yeni bilgi sistemleri gereksinimlerinin belirlenmesine dair bir çalışma yapıldı mı?	[ ]	[ ]	[ ]
3. Büro hizmetlerinin var olan bilgi sistemlerinin iyileştirilmesine dair bir çalışma yapıldı mı?	[ ]	[ ]	[ ]
4. Büro hizmetlerinde kullanılan veya büro hizmetlerin sonrasında üretilen bilginin halka açık ağlar üzerinden geçmesi sonrasında bilgiyi hileli faaliyetlerden korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

5. Büro hizmetlerinde kullanılan veya büro hizmetlerin sonrasında üretilen bilginin halka açık ağlar üzerinden geçmesi sonrasında bilgiyi yetkisiz ifşaya karşı korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]
6. Büro hizmetlerinde kullanılan veya büro hizmetlerin sonrasında üretilen bilginin halka açık ağlar üzerinden geçmesi sonrasında bilgiyi değiştirilmeye karşı korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]
7. Büro hizmetlerinde kullanılan veya büro hizmetleri sonasında üretilen bilgiyi, ağ üzerinde transfer edilirken yanlış yönlendirmeye karşı korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]
8. Büro hizmetlerinde kullanılan veya büro hizmetleri sonasında üretilen bilgiyi, ağ üzerinde transfer edilirken yetkisiz değiştirmeye karşı korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]
9. Büro hizmetlerinde kullanılan veya büro hizmetleri sonasında üretilen bilgiyi, ağ üzerinde transfer edilirken yetkisiz kopyalamaya karşı korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]
10. Büro hizmetlerinde kullanılan veya büro hizmetleri sonasında üretilen bilgiyi, ağ üzerinde transfer edilirken yeniden oluşturmaya karşı korumak için tedbirler alınıyor mu?	[ ]	[ ]	[ ]

2. Büro hizmetlerinin gerçekleştirilmesi süreçleri içerisinde entegre bir bilgi güvenliği yaşam döngüsü belirlenmiş ve uygulanıyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
11. Büro hizmetlerinin gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü çalışanları kapsıyor mu?	[ ]	[ ]	[ ]
12. Büro hizmetlerinin gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü bilişim teknolojileri ekipmanını kapsıyor mu?	[ ]	[ ]	[ ]
13. Büro hizmetlerinin gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü ağ alt yapısını kapsıyor mu?	[ ]	[ ]	[ ]
14. Büro hizmetlerinin gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü kullanılan yazılımları kapsıyor mu?	[ ]	[ ]	[ ]
15. Büro hizmetlerinin gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü mal/hizmet satın alınan firmaları kapsıyor mu?	[ ]	[ ]	[ ]
16. Büro hizmetlerinde kullanılan bilişim sistemlerinde yapılan değişiklikler için belirlenmiş kurallar mevcut mu?	[ ]	[ ]	[ ]
17. Büro hizmetlerinde kullanılan bilişim sistemlerinde yapılan değişiklikler için belirlenmiş kurallar uygulanıyor mu?	[ ]	[ ]	[ ]
18. Büro hizmetlerinde kullanılan bilişim sistemlerinde yapılan değişiklikler kayıt altına alınıyor mu?	[ ]	[ ]	[ ]
19. Büro hizmetlerinde kullanılan işletim sistemi platformu değişiklikleri sonrasında kritik uygulamalar test edilerek uyumluluk güvencesi sağlanıyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

20. Büro hizmetlerinde kullanılan işletim sistemi platformu güncellemeleri sonrasında kritik uygulamalar test edilerek uyumluluk güvencesi sağlanıyor mu?	[ ]	[ ]	[ ]
21. Büro hizmetlerinin yerine getirilmesinde kullanılan kritik uygulamaların seçiminde teknik zaafiyetler göz önünde bulunduruluyor mu?	[ ]	[ ]	[ ]
22. Büro hizmetlerinin yerine getirilmesinde kullanılan kritik uygulamaların ilk kurulum sonrasında mevcut bilişim sistemleri ile uyumluluğu test edildi mi?	[ ]	[ ]	[ ]
23. Büro hizmetlerinin yerine getirilmesinde kullanılan kritik uygulamaların güncellemeler sonrasında mevcut bilişim sistemleri ile uyumluluğu test edildi mi?	[ ]	[ ]	[ ]
24. Büro hizmetlerinin yerine getirilmesinde kullanılan kritik uygulamaların tekrar kurulum sonrasında mevcut bilişim sistemleri ile uyumluluğu test edildi mi?	[ ]	[ ]	[ ]
25. Büro hizmetlerinin gerçekleştirilmesinde belirlenmiş sistem güvenliği prensipleri mevcut mu?	[ ]	[ ]	[ ]
26. Büro hizmetlerinin gerçekleştirilmesinde belirlenmiş sistem güvenliği prensipleri yazılı halde mi?	[ ]	[ ]	[ ]
27. Büro hizmetlerinin gerçekleştirilmesinde belirlenmiş sistem güvenliği prensipleri uygulanıyor mu?	[ ]	[ ]	[ ]
28. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal değişikliklerin mevcut bilişim sistemleri ekipmanları ile uyumluluğunun test edilebilme imkanı mevcut mu?	[ ]	[ ]	[ ]
29. Büro hizmetlerinin gerçekleştirilmesinde, yazılımsal değişikliklerin mevcut bilişim sistemleri ekipmanları ile uyumluluğunun test edilebilme imkanı mevcut mu?	[ ]	[ ]	[ ]
30. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal değişiklikleri sağlayan dış kaynakların yetkinliği denetleniyor mu?	[ ]	[ ]	[ ]
31. Büro hizmetlerinin gerçekleştirilmesinde, yazılımsal değişiklikleri sağlayan dış kaynakların yetkinliği denetleniyor mu?	[ ]	[ ]	[ ]
32. Büro hizmetlerinin gerçekleştirilmesinde, bakım/onarım hizmeti sağlayan dış kaynakların yetkinliği denetleniyor mu?	[ ]	[ ]	[ ]
33. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal değişiklikleri sağlayan dış kaynaklardan yetkinliğini ispatlaması talep ediliyor mu?	[ ]	[ ]	[ ]
34. Büro hizmetlerinin gerçekleştirilmesinde, yazılımsal değişiklikleri sağlayan dış kaynaklardan yetkinliğini ispatlaması talep ediliyor mu?	[ ]	[ ]	[ ]
35. Büro hizmetlerinin gerçekleştirilmesinde, bakım/onarım hizmeti sağlayan dış kaynaklardan yetkinliğini ispatlaması talep ediliyor mu?	[ ]	[ ]	[ ]
36. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal değişiklikleri sonrasında sistem güvenliği test ediliyor mu?	[ ]	[ ]	[ ]
37. Büro hizmetlerinin gerçekleştirilmesinde, yazılımsal değişiklikleri sonrasında sistem güvenliği test ediliyor mu?	[ ]	[ ]	[ ]
38. Büro hizmetlerinin gerçekleştirilmesinde, bakım/onarım hizmeti sonrasında sistem güvenliği test ediliyor mu?	[ ]	[ ]	[ ]
39. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal değişiklikleri sonrasında belirlenmiş bir kabul prosedürü uygulanıyor mu?	[ ]	[ ]	[ ]
40. Büro hizmetlerinin gerçekleştirilmesinde, yazılımsal değişiklikleri sonrasında belirlenmiş bir kabul prosedürü uygulanıyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

41. Büro hizmetlerinin gerçekleştirilmesinde, bakım/onarım hizmeti sonrasında belirlenmiş bir kabul prosedürü uygulanıyor mu?	[ ]	[ ]	[ ]

3. Büro hizmetleri iş süreçleri içerisinde, bilgi güvenliği zaafiyetlerinin tespitine yönelik test/tatbikat çalışması yapıldı mı?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
42. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal değişiklikleri sonrasında sistem güvenliği testleri için belirlenmiş test süreçleri mevcut mu?	[ ]	[ ]	[ ]
43. Büro hizmetlerinin gerçekleştirilmesinde, yazılımsal değişiklikleri sonrasında sistem güvenliği testleri için belirlenmiş test süreçleri mevcut mu?	[ ]	[ ]	[ ]
44. Büro hizmetlerinin gerçekleştirilmesinde, bakım/onarım hizmeti sonrasında sistem güvenliği testleri için belirlenmiş test süreçleri mevcut mu?	[ ]	[ ]	[ ]
45. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal/yazılımsal değişiklikler ve bakım/onarım hizmeti sonrasında sistem güvenliği testlerinde kullanılan test verisi seçimi yapılmış mı?	[ ]	[ ]	[ ]
46. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal/yazılımsal değişiklikler ve bakım/onarım hizmeti sonrasında sistem güvenliği testlerinde kullanılan test verisi korunuyor mu?	[ ]	[ ]	[ ]
47. Büro hizmetlerinin gerçekleştirilmesinde, donanımsal/yazılımsal değişiklikler ve bakım/onarım hizmeti sonrasında sistem güvenliği testlerinde kullanılan test verisi düzenli olarak kontrol ediliyor mu?	[ ]	[ ]	[ ]

BÖLÜM-12: TEDARİKÇİ İLİŞKİLERİ

1. Ürün/hizmet satın alınan tedarikçilere karşı kritik verileri korumak için belirlenmiş bir standart mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına erişiminde kararlaştırılmış kısıtlamalar/kurallar mevcut mu?	[ ]	[ ]	[ ]
2. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına erişiminde kararlaştırılmış kısıtlamalar/kurallar yazılı hale getirildi mi?	[ ]	[ ]	[ ]
3. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına üzerinde kayıtlı bilgilere erişiminde üzerinde anlaşılmış kısıtlamalar/kurallar mevcut mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

4. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına üzerinde kayıtlı bilgileri işletiminde üzerinde anlaşılmış kısıtlamalar/kurallar mevcut mu?	[ ]	[ ]	[ ]
5. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına üzerinde kayıtlı bilgileri depolamasında anlaşılmış kısıtlamalar/kurallar mevcut mu?	[ ]	[ ]	[ ]
6. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılmak üzere yeni bilişim teknolojileri alt yapı bileşenleri temininde üzerinde anlaşılmış kısıtlamalar/kurallar mevcut mu?	[ ]	[ ]	[ ]
7. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılmak üzere yeni bilişim teknolojileri alt yapı bileşenleri temininde tedarik zincirinden kaynaklı zaafiyetlere karşı üzerinde anlaşılmış kısıtlamalar/kurallar mevcut mu?	[ ]	[ ]	[ ]
8. Ürün/hizmet satın alınan tedarikçilerin büro hizmetlerinde kullanılmak üzere yeni bilişim teknolojileri alt yapı bileşenleri temininde tedarik zincirinden kaynaklı ne tür zaafiyetler ortaya çıkabileceği yazılı hale getirildi mi?	[ ]	[ ]	[ ]

2. Ürün/hizmet satın alınan tedarikçilerle büro arasında bilgi güvenliği ve hizmet kalitesi konularını kapsayan yazılı bir sözleşme var mı?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
9. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar kayıt altına alınıyor mu?	[ ]	[ ]	[ ]
10. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar gözden geçiriliyor mu?	[ ]	[ ]	[ ]
11. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar gerekli durumlarda güncelleniyor mu?	[ ]	[ ]	[ ]
12. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar kapsamında hizmet kalitesinin sağlanması adına alınan önlemler var mı?	[ ]	[ ]	[ ]
13. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar kapsamında tedarikçinin iş süreçleri yetkinliği izleniyor/ölçülüyor mu?	[ ]	[ ]	[ ]
14. Ürün/hizmet satın alınan tedarikçilerden büro hizmetlerinin gerçekleştirilmesinde bilgi güvenliği risklerinin azaltılmasına yönelik öneriler talep ediliyor mu?	[ ]	[ ]	[ ]
15. Ürün/hizmet satın alınan tedarikçilerden büro hizmetlerinin gerçekleştirilmesinde bilgi güvenliği risklerinin azaltılmasına yönelik önerilerde bulunuluyor mu?	[ ]	[ ]	[ ]
16. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar kapsamında tedarikçinin personel yetkinliği izleniyor/ölçülüyor mu?	[ ]	[ ]	[ ]
17. Ürün/hizmet satın alınan tedarikçiler tarafından büro hizmetlerinin gerçekleştirilmesinde kullanılan bilişim teknolojileri ekipmanlarında/yazılımlarında gerçekleşen değişiklik ve güncellemelerle ilgili ortaya çıkabilecek bilgi güvenliği riskleri açıklanıyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

18. Ürün/hizmet satın alınan tedarikçiler tarafından büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanları/yazılımları kapsamında ortaya çıkan güncel zaafiyetler bildiriliyor mu?	[ ]	[ ]	[ ]

BÖLÜM-13: BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

1. Bilgi güvenliği ihlali olaylarını tespit ve en aza indirgeme amaçlı, tedbir, tespit, kanıt toplama, iyileştirme, raporlama işlemlerini kapsayan prosedürler/standartlar mevcut mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Büro çalışmaları kapsamında ortaya çıkan bir bilgi güvenliği ihlali durumunda büroda konuyla ilgilenecek bir sorumlu belirlendi mi?	[ ]	[ ]	[ ]
2. Büro çalışmaları kapsamında ortaya çıkan bir bilgi güvenliği ihlali durumunda büroda konuyla ilgilenecek sorumlunun izleyeceği süreçler belirlendi mi?	[ ]	[ ]	[ ]
3. Büro çalışmaları kapsamında ortaya çıkan bir bilgi güvenliği ihlali durumunda büroda konuyla ilgilenecek sorumlunun durumu ne şekilde raporlayacağı belirlendi mi?	[ ]	[ ]	[ ]
4. Büro çalışanlarından, sistemler veya hizmetlerde gözlenen/şüphelenilen bir bilgi güvenliği zaafiyeti olması durumunda bunu bildirmeleri istendi mi?	[ ]	[ ]	[ ]
5. Ürün/hizmet satın alınan tedarikçilerden, sistemler veya hizmetlerde gözlenen/şüphelenilen bir bilgi güvenliği zaafiyeti olması durumunda bunu bildirmeleri istendi mi?	[ ]	[ ]	[ ]
6. Büro çalışanları veya ürün/hizmet satın alınan tedarikçiler tarafından bildirilen bilgi güvenliği zaafiyetlerinin bir bilgi güvenliği ihlali olup olmadığına karar verebilmek için belirlenmiş kurallar var mı?	[ ]	[ ]	[ ]
7. Bilgi güvenliği ihlali gerçekleşmesi durumunda uygulanacak yazılı bir planlama mevcut mu?	[ ]	[ ]	[ ]
8. Bilgi güvenliği ihlali gerçekleşmesi durumunda uygulanacak yazılı planlama uygulanıyor mu?	[ ]	[ ]	[ ]
9. Bilgi güvenliği ihlali gerçekleşmesi durumunda, ihlale ilişkin detaylı teknik inceleme yapılıyor mu?	[ ]	[ ]	[ ]
10. Bilgi güvenliği ihlali gerçekleşmesi durumunda, teknik inceleme sonrası gerekli tedbirler alınıyor mu?	[ ]	[ ]	[ ]
11. Bilgi güvenliği ihlali gerçekleşmesi durumunda, teknik incelemeye temel olacak bilgiler sistemlerden toplanması ile ilgili belirlenmiş süreçler mevcut mu?	[ ]	[ ]	[ ]
12. Bilgi güvenliği ihlali gerçekleşmesi durumunda, teknik incelemeye temel olacak bilgiler sistemlerden toplanması ile ilgili belirlenmiş süreçler uygulanıyor mu?	[ ]	[ ]	[ ]
13. Bilgi güvenliği ihlali gerçekleşmesi durumunda, teknik incelemeye temel olacak bilgilerin korunması ile ilgili belirlenmiş süreçler mevcut mu?	[ ]	[ ]	[ ]
14. Bilgi güvenliği ihlali gerçekleşmesi durumunda, teknik incelemeye temel olacak bilgilerin korunması ile ilgili belirlenmiş süreçler uygulanıyor mu?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

BÖLÜM-14: İŞ SÜREKLİLİĞİNİN BİLGİ GÜVENLİĞİ HUSUSLARI

1. Bilgi güvenliği sürekliliğini sağlamak üzere, bilgi güvenliği büro hizmetlerinin olağan iş süreçlerinden birisi haline getirildi mi?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
1. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliğini ve bilgi güvenliği sürekliliğini sağlamaya yönelik alınan tedbirler mevcut mu?	[ ]	[ ]	[ ]
2. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliği yönetimini ve bilgi güvenliği yönetiminin sürekliliğini sağlamaya yönelik alınan tedbirler mevcut mu?	[ ]	[ ]	[ ]
3. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliğini ve bilgi güvenliği sürekliliğini sağlamaya yönelik alınan tedbirler yazılı halde mi?	[ ]	[ ]	[ ]
4. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliğini ve bilgi güvenliği sürekliliğini sağlamaya yönelik alınan tedbirler uygulanıyor mu?	[ ]	[ ]	[ ]
5. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliği yönetimini ve bilgi güvenliği yönetiminin sürekliliğini sağlamaya yönelik alınan tedbirler yazılı halde mi?	[ ]	[ ]	[ ]
6. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliği yönetimini ve bilgi güvenliği yönetiminin sürekliliğini sağlamaya yönelik alınan tedbirler uygulanıyor mu?	[ ]	[ ]	[ ]
7. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliğini sağlamaya yönelik alınan tedbirlerin etkinliğinden emin olmak için belirli aralıklarla doğruluğu sınanıyor mu?	[ ]	[ ]	[ ]
8. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliği yönetimini sağlamaya yönelik alınan tedbirlerin etkinliğinden emin olmak için belirli aralıklarla doğruluğu sınanıyor mu?	[ ]	[ ]	[ ]

2. Büro hizmetlerinde kullanılan bilişim teknolojileri varlıklarının büro hizmetlerinin gerçekleştirilmesinde yeterliliği ve verimliliği konularında yazılı bir çalışma yapıldı mı?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	**HAYIR**	**KISMEN**
9. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanının yeterliliği ve verimliliği konusunda çalışma yapıldı mı?	[ ]	[ ]	[ ]
10. Büro hizmetlerinde kullanılan bilişim teknolojileri ekipmanının yeterliliği ve verimliliği konusunda çalışma yazılı rapor haline getirildi mi?	[ ]	[ ]	[ ]
11. Büro hizmetlerinde kullanılan yazılımların yeterliliği ve verimliliği konusunda çalışma yapıldı mı?	[ ]	[ ]	[ ]
12. Büro hizmetlerinde kullanılan yazılımların yeterliliği ve verimliliği konusunda çalışma yazılı rapor haline getirildi mi?	[ ]	[ ]	[ ]

EK-1. (devam) Hukuk büroları için ISO/IEC 27001 BGYS öz değerlendirme anketi

BÖLÜM-15: UYUM

1. Büro hizmetlerinin gerçekleştirilmesinde, bilişim güvenliği konusunda yasal zorunluluklara uyuluyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
1. Büro hizmetlerinin gerçekleştirilmesinde kullanılan bilişim teknolojileri ekipmanı ile ilgili tanımlanmış yasal mevzuata uyuluyor mu?	[ ]	[ ]	[ ]
2. Büro hizmetlerin gerçekleştirilmesinde kullanılan bilişim teknolojileri ekipmanı ile ilgili tanımlanmış yasal mezvuat ilgili kısımları açısından yazılı halde tutuluyor mu?	[ ]	[ ]	[ ]
3. Büro hizmetlerin gerçekleştirilmesinde kullanılan bilişim teknolojileri ekipmanı ile ilgili tanımlanmış yasal mezvuat ilgili kısımları açısından yazılı halde güncelleniyor mu?	[ ]	[ ]	[ ]
4. Büro hizmetlerinde kullanılan fikir mülkiyet hakları veya patent hakları başkasına ait olup ücret karşılığı kullanmanın mümkün olduğu yazılımlar ile ilgili belirlenmiş prosedürler mevcut mu?	[ ]	[ ]	[ ]
5. Büro hizmetlerinde kullanılan fikir mülkiyeti veya patent hakları başkasına ait olup ücret karşılığı kullanmanın mümkün olduğu yazılımlar izinsiz olarak kullanılıyor mu?	[ ]	[ ]	[ ]
6. Büro hizmetleri esnasında üretilen bilgiler kaybedilmeye karşı uygun şekilde yasa veya sözleşmelerden doğan şartlar kullanılarak korunuyor mu?	[ ]	[ ]	[ ]
7. Büro hizmetleri esnasında üretilen bilgiler yetkisiz yayımlamaya karşı uygun şekilde yasa veya sözleşmelerden doğan şartlar kullanılarak korunuyor mu?	[ ]	[ ]	[ ]
8. Büro hizmetleri esnasında üretilen bilgiler kişisel tespite olanak verecek kalıntılardan arındırılıyor mu?	[ ]	[ ]	[ ]
9. Büro hizmetleri esnasında üretilen bilgiler şifrelenmesi ilgili yasal mevzuata uygun mu?	[ ]	[ ]	[ ]

2. Büronun bilgi güvenliği standartlarına uyumu konusunda iyileştirilmesi düşünülüyor mu?

Cevabınız EVET ise takip eden maddeleri yanıtlayınız, HAYIR ise lütfen bu bölümde işaretleme yapmayınız.

	EVET	HAYIR	KISMEN
10. Büro bilgi güvenliği sistemleri belirli aralıklarla bağımsız şekilde inceleniyor/denetleniyor mu?	[ ]	[ ]	[ ]
11. Büro yönetimi, kendi sorumlulukları kapsamında bilgi işleme prosedürlerini düzenli bir şekilde gözden geçiriyor mu?	[ ]	[ ]	[ ]
12. Büro yönetimi, kendi sorumlulukları kapsamında uygun güvenlik politikalarını düzenli bir şekilde gözden geçiriyor mu?	[ ]	[ ]	[ ]
13. Büro yönetimi, kendi sorumlulukları kapsamında uygun güvenlik standartlarını düzenli bir şekilde gözden geçiriyor mu?	[ ]	[ ]	[ ]
14. Büro bilgi güvenliği sisteminin bilgi güvenliği standartları ile uyumluluğu düzenli şekilde gözden geçiriliyor mu?	[ ]	[ ]	[ ]

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: KILIÇ, Berker
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 19/10/1980 Ankara
Medeni hali	: Evli
Telefon	: 05069302199
e-posta	: berker.kilic@gmail.com
Web	: www.adlibilisimci.com

Eğitim Derecesi	Okul/Program	Mezuniyet yılı
Yüksek lisans	Gazi Üniversitesi/Bilişim Enstitüsü/Adli Bilişim ABD	2019
Ön Lisans	Anadolu Üniversitesi/Adalet	2015
Ön Lisans	Anadolu Üniversitesi/Marka İletişimi	2010
Lisans	Gazi Üniversitesi/Bilgisayar Eğitimi	2006
Lise	Çankırı Anadolu Meslek Lisesi/Bilgisayar Donanım	1999

İş Deneyimi

2017-devam ediyor	Samsun Bölge Bilirkişi Kuruluna bağlı Resmi Bilirkişi ve Adli Bilişim Uzmanı
2015-devam ediyor	Samsun/Canik Mesleki ve Teknik Anadolu Lisesi
2013-2015	Samsun/Terme Mesleki ve Teknik Anadolu Lisesi
2010-2013	Samsun/İlkadım Halk Eğitimi Merkezi
2009-2010	Şanlıurfa/Merkez Kız Teknik ve Meslek Lisesi
2008-2009	Şanlıurfa/Merkez Teknik ve Endüstri Meslek Lisesi
2006-2008	Ankara/Mamak Abidinpaşa Anadolu Tek.Lis., Tek.Lis. ve End.Mes.Lisesi

Yabancı Dili

İngilizce

Yayınlar

1. Kılıç, B. (2006). MEB, Yeni Öğretim Programı Kazanımlarının Tekrar Kullanılabilir Öğrenme Nesneleri (TEKÖN) İle Modellenmesi, VII. Fen Bilimleri ve Matematik Eğitimi Kongresi, Bildiriler Kitabı.
2. Kılıç, B. (2006). Öğretim Görevlisi Yetersizliğine Karşı Intranet ve Medya Teknolojilerini Kullanılarak Paralel Sınıflar Oluşturmak, VII. Fen Bilimleri ve Matematik Eğitimi Kongresi, Bildiriler Kitabı.

3. Kılıç, B. (2006). BENÖĞRETKİN: Ulusal Uzaktan Eğitim Altyapısı, XI. Türkiye' de Internet Konferansı, Bildiriler Kitabı.
4. Kılıç, B. (2007). Internet Bilgi Kaynaklarının İlköğretim Öğrencilerine Uygunluğu ve Bir İçerik Geliştirme Önerisi, I. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu, Bildiriler Kitabı.
5. Kılıç, B. (2007). Matematik Dersi Araştırmaları. Türkiye: Asli Yayınevi.
6. Kılıç, B. ve Çelik, R. (2007). Türkçe Dersi Araştırmaları. Türkiye: Asli Yayınevi.
7. Kılıç, B. ve Söğüt, O. (2007). Fen ve Teknoloji Dersi Araştırmaları. Türkiye: Asli Yayınevi.
8. Kılıç, B. ve Kılıç, E. (2007). Sosyal Bilgiler Dersi Dersi Araştırmaları. Türkiye: Asli Yayınevi.
9. Kılıç, B. ve Çatalkaya, M. (2007). Din Kültürü ve Ahlak Bilgisi Dersi Araştırmaları. Türkiye: Asli Yayınevi.
10. Kılıç, B. (2009). Bilim ve Teknolojinin Gelişiminde Öğretmenlerin Rolünün Etkinleştirilmesi İçin Milli Eğitim Bakanlığı Bünyesinde Akademik Yükselme Modelinin Uygulanması, II. Uluslararası Türkiye Eğitim Araştırmaları Kongresi, Bildiriler Kitabı.
11. Yalçın, N. ve Kılıç, B. (2015). Mesleki Eğitim, Bilişim Teknolojileri Alanı Öğretim Programlarının Güncelliği Üzerine Bir Araştırma, IV. Dünya Eğitim Öğretim Çalışmaları Konferansı, Bildiriler Kitabı.
12. Yalçın, N. ve Kılıç, B. (2016). A Model Suggestion For STEM Activity Design Within The Scope Of The Curriculum, Participatory Educational Research (PER) Special Issue 2016-III, 95-107.
14. Yalçın, N. ve Kılıç, B. (2017). The Evalaution of the EBA Portal in Terms of Learning Objects, New Trends and Issues Proceedings on Humanities and Social Sciences. 7(1), 92-99.
15. Yalçın, N. ve Kılıç, B. (2018). Information Security Risk Management and Risk Assessment Methodology and Tools, International Conference on Cyber Security and Computer Science (ICONCS'18), Bildiriler Kitabı, 73-78.
16. Yalçın, N. ve Kılıç, B. (2019). ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 Standartlarına Göre Sayısal Kanıtlar, 4. Uluslararası Mühendislik ve Doğa Bilimlerinde Yenilikçi Yaklaşımlar Sempozyumu (ISAS'19), 4(6), 444-449.

Hobiler

Araştırma yapmak, Kitap okumak, Küçük çaplı tamirat işleri yapmak.

GAZİLİ OLMAK AYRICALIKTIR...